IBM QRadar User Behavior Analytics (UBA)
Version 3.2.0

Benutzerhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 213 gelesen werden.

Produktinformation

Dieses Dokument bezieht sich auf IBM QRadar Security Intelligence Platform V7.2.8 und nachfolgende Releases, bis es durch eine aktualisierte Version dieses Dokuments ersetzt wird.

Inhaltsverzeichnis

1 User Behavior Analytics for QRadar

Mit der App 'User Behavior Analytics for QRadar' (Benutzerverhaltensanalyse für QRadar) können Sie die Risikoprofile Ihrer Netzwerkbenutzer erfassen und auf Alarme der App hin sofort mit geeigneten Maßnahmen auf bedrohliches Verhalten reagieren.

Bei der App 'Behavior Analytics for QRadar (UBA)' handelt es sich um ein Tool zur Ermittlung von Bedrohungen durch eigene Benutzer in Ihrem Unternehmen. Es basiert auf dem Framework der App und verwendet vorhandene Daten in Ihrem QRadar-System, um neue Erkenntnisse zu Benutzern und Risiken zu generieren. UBA fügt QRadar zwei wichtige Funktionen hinzu: Die Erstellung von Risikoprofilen und einheitliche Benutzeridentitäten.

Die Erstellung von Risikoprofilen wird durch das Zuordnen von Risiken zu verschiedenen Sicherheitsanwendungsfällen vorgenommen. Dazu gehören beispielsweise einfache Regeln und die Prüfung von schädlichen Websites oder erweiterte statusabhängige Analysen, die Machine Learning verwenden. Das Risiko wird je nach Schweregrad und Zuverlässigkeit des erkannten Vorfalls entsprechend zugeordnet. UBA verwendet vorhandene Ereignis- und Datenflussdaten in Ihrem QRadar-System, um diese Erkenntnisse und Risikoprofile von Benutzern zu generieren. UBA verwendet drei Datenverkehrstypen: 1. Datenverkehr beim Zugriff, bei der Authentifizierung und bei Kontoänderungen. 2. Benutzerverhalten im Netz, bei Einheiten wie Proxys, Firewalls, IPS, VPNs. 3. Endpunkt- und Anwendungsprotokolle wie beispielsweise von Windows oder Linux sowie SAAS-Anwendungen. Durch alle drei Datenverkehrstypen wird UBA verbessert und es werden weitere Anwendungsfälle in Bezug auf das Risiko für ein Profil aktiviert.

Die Vereinheitlichung von Benutzeridentitäten wird durch die Kombination unterschiedlicher Konten für einen Benutzer in QRadar hergestellt. Durch den Import von Daten aus einem Active Directory, aus LDAP oder einer CSV-Datei kann UBA lernen, welche Konten zu einer Benutzeridentität gehören. Dadurch können Risiken und der Datenverkehr mit den unterschiedlichen Benutzernamen in QRadar für UBA kombiniert werden.

Bei Machine Learning (ML) handelt es sich um ein Add-on-Tool, mit dem die UBA-App erweitert wird. Damit werden umfangreichere und detailliertere Anwendungsfälle ermöglicht, die das Erstellen von Profilen und Clustern für eine Zeitreihe ausführen. Das Tool wird in der UBA-App auf der Seite mit den Machine Learning-Einstellungen installiert. Mit ML werden der vorhandenen UBA-App weitere Darstellungsmöglichkeiten hinzugefügt, in denen erlerntes Verhalten (Modelle), aktuelles Verhalten und Benachrichtigungen angezeigt werden. Machine Learning nutzt Protokolldaten in QRadar über einen Zeitraum von bis zu vier Wochen, um die Vorhersagemodelle und Referenzen für das normale Verhalten eines Benutzers zu erstellen.

Weitere Informationen zur Verwendung der App 'Reference Data Import - LDAP' finden Sie unter 8, „App 'Reference Data Import - LDAP'", auf Seite 165.

Weitere Informationen zur Verwendung der App 'Machine Learning Analytics' finden Sie unter 9, „App 'Machine Learning Analytics'", auf Seite 177.

Achtung: Vor der Installation der QRadar-App UBA müssen Sie IBM® QRadar V7.2.8 oder höher installieren.

Zugehörige Konzepte:

7, „Regeln und Möglichkeiten zur Optimierung für die UBA-App", auf Seite 49
Die IBM QRadar-App "User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

„App "User Behavior Analytics" konfigurieren" auf Seite 23
Vor Verwendung der IBM QRadar-App "User Behavior Analytics" (UBA) müssen die Anwendungseinstel-

lungen der UBA-App konfiguriert werden.

8, „App 'Reference Data Import - LDAP'", auf Seite 165
Mit der App 'Reference Data Import - LDAP' (Referenzdatenimport - LDAP) können Sie kontextbezogene Identitätsinformationen aus mehreren LDAP-Quellen in Ihrer QRadar-Konsole zusammenstellen.

9, „App 'Machine Learning Analytics'", auf Seite 177
Die ML-App (Machine Learning Analytics) erweitert durch Hinzufügen von Anwendungsfällen für 'Machine Learning Analytics' das Leistungsspektrum des QRadar-Systems sowie der QRadar-App 'User Behavior Analytics' (UBA). Mit den Anwendungsfällen für 'Machine Learning Analytics' erhalten Sie zusätzliche Einblicke in das Benutzerverhalten mit Vorhersagemodellierung. Mithilfe der ML-App erlernt Ihr System das erwartete Verhalten der Benutzer in Ihrem Netz.

Zugehörige Tasks:

„App 'User Behavior Analytics' installieren" auf Seite 17
Sie können das Archiv, das die App enthält, mit dem IBM QRadar-Tool für das Erweiterungsmanagement direkt in die QRadar-Konsole hochladen und dort installieren.

„App 'User Behavior Analytics' aktualisieren" auf Seite 21
Zur Aktualisierung Ihrer App verwenden Sie das IBM QRadar-Tool für das Erweiterungsmanagement.

Neuerungen in der App 'User Behavior Analytics'

In diesem Abschnitt erhalten Sie eine Übersicht über die neuen Funktionen in den einzelnen Releases der App 'User Behavior Analytics' (UBA).

Neuerungen in V3.2.0

- Ermittlung von Benutzern mit ruhenden Konten im Dashboard und auf den Seiten mit dem Benutzerprofil. Weitere Informationen finden Sie im Abschnitt „Ruhende Konten" auf Seite 41.
- Erstellung von Beobachtungslisten zu Servicekonten auf Basis einer fehlenden Benutzereigenschaft. Weitere Informationen finden Sie im Abschnitt „Beobachtungslisten erstellen" auf Seite 37.
- Verbesserung der LDAP-App, damit die in UBA verwendeten LDAP-Attribute ausgewählt werden können. Hinweis: Beim Konfigurieren von LDAP müssen Sie im Abschnitt 'Attribute Mapping' (Attributzuordnung) jetzt einen äußeren Schlüssel auswählen. Weitere Informationen finden Sie im Abschnitt „App "Import von Referenzdaten - LDAP" konfigurieren" auf Seite 23.
- Es wurde die Funktion zum Importieren von Benutzerinformationen aus einer CSV-Datei hinzugefügt. Weitere Informationen finden Sie im Abschnitt „Benutzerdaten aus einer CSV-Datei importieren" auf Seite 166.
- Zusätzlicher Anwendungsfall 'UBA : User Access from Multiple Hosts'. Weitere Informationen finden Sie im Abschnitt „UBA : User Access from Multiple Hosts" auf Seite 61.
- Zusätzlicher Anwendungsfall 'UBA : Possible Directory Services Enumeration'. Weitere Informationen finden Sie im Abschnitt „UBA : Possible Directory Services Enumeration" auf Seite 98.
- Zusätzlicher Anwendungsfall 'UBA : Possible SMB Session Enumeration on a Domain Controller'. Weitere Informationen finden Sie im Abschnitt „UBA : Possible SMB Session Enumeration on a Domain Controller" auf Seite 98.
- Zusätzlicher Anwendungsfall 'UBA : Suspicious Access Followed by Data Exfiltration'. Weitere Informationen finden Sie im Abschnitt „UBA : Suspicious Access Followed by Data Exfiltration" auf Seite 114.
- Zusätzlicher Anwendungsfall 'UBA : Dormant Account Use Attempted'. Weitere Informationen finden Sie im Abschnitt „UBA : Dormant Account Use Attempted" auf Seite 77.

Neuerungen in V3.1.0

- Die können jetzt die Metriken in der Zeitleiste des Benutzers und die Daten anzeigen, aus denen sich die Metriken zusammensetzen.
- Der App wurde die Funktion zum Festlegen eines dynamischen Risikoschwellenwerts hinzugefügt.

- Der Seite 'Rules and Tuning' wurden zwei neue Kategorien für Anwendungsfälle hinzugefügt: 'Cloud' und 'Domain Controller'. Weitere Informationen finden Sie im Abschnitt 7, „Regeln und Möglichkeiten zur Optimierung für die UBA-App", auf Seite 49.
- Zusätzlicher Anwendungsfall 'UBA : Non-Standard User Accessing AWS Resources'. Weitere Informationen finden Sie im Abschnitt „UBA : Non-Standard User Accessing AWS Resources" auf Seite 94.
- Zusätzlicher Anwendungsfall 'UBA : AWS Console Accessed by Unauthorized User'. Weitere Informationen finden Sie im Abschnitt „UBA : AWS Console Accessed by Unauthorized User" auf Seite 93.
- Zusätzlicher Anwendungsfall 'UBA : Replication Request from a Non-Domain Controller'. Weitere Informationen finden Sie im Abschnitt „UBA : Replication Request from a Non-Domain Controller" auf Seite 100.
- Zusätzlicher Anwendungsfall 'UBA : Kerberos Account Enumeration Detected'. Weitere Informationen finden Sie im Abschnitt „UBA : Kerberos Account Enumeration Detected" auf Seite 95.
- Zusätzlicher Anwendungsfall 'UBA : Possible TGT PAC Forgery'. Weitere Informationen finden Sie im Abschnitt „UBA : Possible TGT PAC Forgery" auf Seite 100.
- Zusätzlicher Anwendungsfall 'UBA : DPAPI Backup Master Key Recovery Attempted'. Weitere Informationen finden Sie im Abschnitt „UBA : DPAPI Backup Master Key Recovery Attempted" auf Seite 94.
- Zusätzlicher Anwendungsfall 'UBA : DoS Attack by Account Deletion'. Weitere Informationen finden Sie im Abschnitt „UBA : DoS Attack by Account Deletion" auf Seite 72.
- Zusätzlicher Anwendungsfall 'UBA : Multiple Blocked File Transfers Followed by a File Transfer'. Weitere Informationen finden Sie im Abschnitt „UBA : Multiple Blocked File Transfers Followed by a File Transfer" auf Seite 112.

Neuerungen in V3.0.1

- Es wurde ein Anwendungsfall hinzugefügt, um die DNS-Tunnelungserkennung durch die App 'IBM QRadar DNS Analyzer' zu unterstützen. Weitere Informationen finden Sie im Abschnitt „UBA : Potential Access to Tunneling Domain" auf Seite 134.
- Es wurde ein Problem behoben, das die Möglichkeit zum Einpflegen von Benutzern aus einer Referenztabelle verhindern könnte.

Neuerungen in V3.0.0

- Sie können jetzt Beobachtungslisten so erstellen und verwalten, dass Sie benutzerdefinierte Benutzergruppen überwachen können. Weitere Informationen finden Sie im Abschnitt „Beobachtungslisten erstellen" auf Seite 37.
- Sie können jetzt auf der Seite 'Rules and Tuning' (Regeln und Optimierung) UBA-Anwendungsfälle anzeigen, filtern und optimieren. Weitere Informationen finden Sie im Abschnitt 7, „Regeln und Möglichkeiten zur Optimierung für die UBA-App", auf Seite 49.
- Sie können jetzt gefährliche Ereignisse und Metriken in der Benutzeraktivitätszeitleiste nach Aktivitätssitzungen anzeigen. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard und Benutzerdetails" auf Seite 9.
- Es wurde eine Machine Learning-Analyse hinzugefügt, die abnormales Datenvolumen an externe Domänen erkennt. Weitere Informationen finden Sie im Abschnitt „Analyse *Abnormal Volume of Data to External Domains* konfigurieren" auf Seite 188.
- Zusätzlicher Anwendungsfall 'UBA : Large Outbound Transfer by High Risk User'. Weitere Informationen finden Sie im Abschnitt „UBA : Large Outbound Transfer by High Risk User" auf Seite 112.
- Zusätzlicher Anwendungsfall 'UBA : Honeytoken Activity'. Weitere Informationen finden Sie im Abschnitt „UBA : Honeytoken Activity" auf Seite 129.
- Zusätzlicher Anwendungsfall 'UBA : Bruteforce Authentication Attempts'. Weitere Informationen finden Sie im Abschnitt „UBA : Bruteforce Authentication Attempts" auf Seite 49.
- Zusätzlicher Anwendungsfall 'UBA : User Account Created and Deleted in a Short Period of Time'. Weitere Informationen finden Sie im Abschnitt „UBA : User Account Created and Deleted in a Short Period of Time" auf Seite 76.

- Zusätzlicher Anwendungsfall 'UBA : High Risk User Access to Critical Asset'. Weitere Informationen finden Sie im Abschnitt „UBA : High Risk User Access to Critical Asset” auf Seite 52.
- Zusätzlicher Anwendungsfall 'UBA : Anomalous Account Created From New Location'. Weitere Informationen finden Sie im Abschnitt „UBA : Anomalous Account Created From New Location” auf Seite 116.
- Zusätzlicher Anwendungsfall 'UBA : Anomalous Cloud Account Created From New Location'. Weitere Informationen finden Sie im Abschnitt „UBA : Anomalous Cloud Account Created From New Location” auf Seite 120.

Neuerungen in V2.8.0

- Mit dem Feld **Advanced Search Filter** (Filter für erweiterte Suche) kann beim Konfigurieren der Einstellungen für die Machine Learning-Analyse nach AQL-Abfragen gefiltert werden. Weitere Informationen finden Sie im Abschnitt „Einstellungen für Machine Learning Analytics konfigurieren” auf Seite 180.
- Sie können jetzt Dashboard-Statistikdaten für Benutzer, die aus Ereignissen erkannt und aus einem Verzeichnis importiert wurden, anzeigen. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard und Benutzerdetails” auf Seite 9.
- Sie können jetzt Benutzer angeben, die mit Machine Learning überwacht werden sollen. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard und Benutzerdetails” auf Seite 9.
- Sie können jetzt konfigurieren, ob Grafiken für jede Machine Learning-Analyse angezeigt werden sollen. Weitere Informationen finden Sie im Abschnitt „Einstellungen für Machine Learning Analytics konfigurieren” auf Seite 180.
- Sie können jetzt konfigurieren, ob UBA-Inhaltspakete (QRadar-Regeln, angepasste Eigenschaften und Referenzdaten für Anwendungsfälle) installiert oder aktualisiert werden sollen. Weitere Informationen finden Sie im Abschnitt „Einstellungen für die Inhaltspakete konfigurieren” auf Seite 29.
- Es wurde eine Machine Learning-Analyse hinzugefügt, die Sie zum Erkennen von abnormalen abgehenden Übertragungsversuchen aktivieren können. Weitere Informationen finden Sie im Abschnitt „Analyse *Abnormal Outbound Transfer Attempts* (Abnormale abgehende Übertragungsversuche) konfigurieren” auf Seite 182.
- Es wurden Machine Learning-Speicherkonfigurationen hinzugefügt, damit bei der Ausführung von UBA mit Machine Learning auf einem App-Knoten mehrere Benutzer unterstützt werden.
- Es gibt ein zusätzliches Referenzset zur Ermittlung von Benutzern mit einem hohen Risiko. Weitere Informationen finden Sie im Abschnitt „Referenzsets” auf Seite 47.
- Zusätzliche Anwendungsfälle für die folgenden Kategorien zur Navigation auf Websites: 'Business/ Service', 'LifeStyle' und 'Uncategorized'. Weitere Informationen finden Sie im Abschnitt „Navigationsverhalten” auf Seite 86.
- Zusätzlicher Anwendungsfall 'UBA : Network Share Accessed'. Weitere Informationen finden Sie im Abschnitt „UBA : Network Share Accessed” auf Seite 150.
- Zusätzlicher Anwendungsfall 'UBA : Non-Admin Access to Domain Controller'. Weitere Informationen finden Sie im Abschnitt „UBA : Non-Admin Access to Domain Controller” auf Seite 96.
- Zusätzlicher Anwendungsfall 'UBA : User Access from Prohibited Location'. Weitere Informationen finden Sie im Abschnitt „UBA : User Access from Prohibited Location” auf Seite 122.
- Zusätzlicher Anwendungsfall 'UBA : User Access from Restricted Location'. Weitere Informationen finden Sie im Abschnitt „UBA : Restricted Program Usage” auf Seite 108.
- Zusätzlicher Anwendungsfall 'UBA : Multiple Kerberos Authentication Failures from Same User'. Weitere Informationen finden Sie im Abschnitt „UBA : Multiple Kerberos Authentication Failures from Same User” auf Seite 95.
- Zusätzlicher Anwendungsfall 'UBA : TGT Ticket Used by Multiple Hosts'. Weitere Informationen finden Sie im Abschnitt „UBA : TGT Ticket Used by Multiple Hosts” auf Seite 101.

Neuerungen in V2.7.0

Achtung: Bei einem Upgrade auf V2.7.0 müssen Sie gemäß den Anweisungen im technischen Hinweis http://www.ibm.com/support/docview.wss?uid=swg22005489 vorgehen.

V2.7.0 der App 'User Behavior Analytics' enthält folgende neuen Funktionen:

- Sie können Benutzer jetzt in der App 'QRadar Advisor with Watson' untersuchen. Hinweis: QRadar Advisor with Watson V1.13.0 muss installiert sein. Weitere Informationen finden Sie im Abschnitt „Benutzer in QRadar Advisor with Watson untersuchen" auf Seite 14.
- Sie können jetzt einen General Data Protection Regulation-(GDPR-)Konformitätsbericht für einen Benutzer erstellen und die Überwachung eines Benutzers stoppen.
- Sie können jetzt den Untersuchungsstatus eines Benutzers markieren und im Dashboard **User Analytics** (Benutzeranalyse) alle Benutzer anzeigen, für die eine Untersuchung durchgeführt wird.
- Sie können jetzt konfigurieren, ob Länder- und Regionsflaggen für IP-Adressen angezeigt werden sollen.
- Es werden jetzt Domänenzugriffsereignisse unterstützt, die von der App 'IBM QRadar DNS Analyzer' generiert werden. Weitere Informationen finden Sie im Abschnitt „QRadar DNS Analyzer" auf Seite 132.
- Es wurden 19 neue Anwendungsfälle für ungewöhnliches Scannen hinzugefügt. Weitere Informationen finden Sie im Abschnitt „Ausspähung" auf Seite 140.
- Es wurden 3 neue Anwendungsfälle für verdächtige Anwendung hinzugefügt. Weitere Informationen finden Sie im Abschnitt „Endpunkt" auf Seite 102.
- Es wurden 10 neue Anwendungsfälle für gefährliches Browsing hinzugefügt. Weitere Informationen finden Sie im Abschnitt „Navigationsverhalten" auf Seite 86.
- Es wurden 13 neue Anwendungsfälle für Systemüberwachung (Sysmon) hinzugefügt. Weitere Informationen finden Sie im Abschnitt „Systemüberwachung (Sysmon)" auf Seite 149.

Neuerungen in V2.6.0

Achtung: Bei einem Upgrade auf V2.6.0 müssen Sie gemäß den Anweisungen im technischen Hinweis http://www.ibm.com/support/docview.wss?uid=swg22005489 vorgehen.

V2.6.0 der App 'User Behavior Analytics' enthält die folgenden neuen Funktionen:

- Die App 'Machine Learning Analytics (ML)' wurde erweitert, damit Anomalien auf Grundlage von definieren Peergruppen in LDAP und im Active Directory analysiert werden können.
- Die Analyse 'Peer Group' (Peergruppe) für die ML-App wurde in 'Learned Peer Group' (Erlernte Peergruppe) umbenannt.
- Zusätzlicher Anwendungsfall: UBA : Process Executed Outside Gold Disk Whitelist (Windows / Linux)
- Zusätzlicher Anwendungsfall: UBA : Ransomware Behavior Detected
- Zusätzlicher Anwendungsfall: UBA : Netcat Process Detection (Windows / Linux)
- Zusätzlicher Anwendungsfall: UBA : Multiple VPN Accounts Failed Login from Single IP
- Zusätzlicher Anwendungsfall: UBA : Volume Shadow Copy Created
- Zusätzlicher Anwendungsfall: UBA : Detect Insecure Or Non-Standard Protocol
- Zusätzlicher Anwendungsfall: UBA : Malware Activity - Registry Modified In Bulk
- Zusätzlicher Anwendungsfall: UBA : Internet Settings Modified
- Zusätzlicher Anwendungsfall: UBA : Multiple VPN Accounts Logged In from Single IP
- Zusätzlicher Anwendungsfall: UBA : Suspicious PowerShell Activity (Asset)
- Zusätzlicher Anwendungsfall: UBA : Suspicious PowerShell Activity
- Zusätzlicher Anwendungsfall: UBA : Suspicious Command shell Activity
- Zusätzlicher Anwendungsfall: UBA : Malicious Process Detected

Neuerungen in V2.5.0

Achtung: Bei einem Upgrade auf V2.5.0 müssen Sie gemäß den Anweisungen im technischen Hinweis http://www.ibm.com/support/docview.wss?uid=swg22005489 vorgehen.

V2.5.0 der App 'User Behavior Analytics' enthält folgende Verbesserungen:

- Der App wurde die Funktion zur schnellen Überprüfung des Risikoverhaltens eines Benutzers mithilfe der integrierten kontextbezogenen Ereignisanzeige hinzugefügt. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard und Benutzerdetails" auf Seite 9.
- Der App wurde eine Hilfs- und Unterstützungsseite hinzugefügt, auf der Links zur Dokumentation, zu Lernprogrammen und Unterstützungsinformationen sowie Verwaltungsfunktionen bereitgestellt werden. Weitere Informationen finden Sie im Abschnitt „Seite mit Hilfe und Unterstützung für UBA" auf Seite 207.
- Die Genauigkeit und Skalierbarkeit für Machine Learning wurde erhöht und die Nachrichtenübermittlung im Abschnitt 'Status of Machine Learning Models' (Status der Machine Learning-Modelle) im Dashboard wurde verbessert. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard mit Machine Learning Analytics" auf Seite 196.
- Zusätzlicher Anwendungsfall 'UBA: User Running New Process'. Weitere Informationen finden Sie im Abschnitt „UBA : User Running New Process" auf Seite 109.
- Zusätzlicher Anwendungsfall 'UBA: User Installing Suspicious Application'. Weitere Informationen finden Sie im Abschnitt „UBA : User Installing Suspicious Application" auf Seite 108.
- Zusätzlicher Anwendungsfall 'UBA : Unix/Linux System Accessed With Service or Machine Account'. Weitere Informationen finden Sie im Abschnitt „UBA: Unix/Linux System Accessed With Service or Machine Account" auf Seite 58.
- Zusätzlicher Anwendungsfall 'UBA: User Access to Internal Server From Jump Server'. Weitere Informationen finden Sie im Abschnitt „UBA: User Access to Internal Server From Jump Server" auf Seite 63.
- Zusätzlicher Anwendungsfall 'UBA: Executive Only Asset Accessed by Non-Executive User'. Weitere Informationen finden Sie im Abschnitt „UBA : Executive Only Asset Accessed by Non-Executive User" auf Seite 51.

Neuerungen in V2.4.0

Achtung: Bei einem Upgrade auf V2.4.0 müssen Sie gemäß den Anweisungen im technischen Hinweis http://www.ibm.com/support/docview.wss?uid=swg22005489 vorgehen.

V2.4.0 der App 'User Behavior Analytics' enthält folgende Verbesserungen:

- Anzeige des LDAP-Abrufstatus in LDAP-App
- Import von bis zu 400.000 Benutzern durch die LDAP-App. Lesen Sie den Abschnitt Bekannte Probleme, bevor Sie die Konfiguration ändern.
- Optimierte und vereinfachte Integration und Zuordnung von LDAP/AD-Daten.
- Möglichkeit zur Zuordnung einer unbegrenzten Zahl von Aliasnamen zu einer Primärbenutzer-ID
- Zusätzliche Speicherkonfigurationseinstellungen in den Machine Learning-Einstellungen, um bei der Ausführung von Machine Learning auf einem App-Knoten mehrere Benutzer zu unterstützen
- Zusätzliche Feedbackumfrage.
- Zusätzlicher Anwendungsfall 'UBA: Windows access with Service or Machine Account'. Weitere Informationen finden Sie im Abschnitt „UBA : Windows Access with Service or Machine Account" auf Seite 69.
- Zusätzlicher Anwendungsfall 'UBA: D/DoS Attack Detected'. Weitere Informationen finden Sie im Abschnitt „UBA : D/DoS Attack Detected" auf Seite 128.
- Zusätzlicher Anwendungsfall 'UBA: Detect Persistent SSH session'. Weitere Informationen finden Sie im Abschnitt „UBA : Detect Persistent SSH session" auf Seite 102.

- Zusätzlicher Anwendungsfall 'UBA: Abnormal data volume to external domain'. Weitere Informationen finden Sie im Abschnitt „UBA : Abnormal data volume to external domain (ADE-Regel)" auf Seite 110.
- Zusätzlicher Anwendungsfall 'UBA: Abnormal Outbound Attempts'. Weitere Informationen finden Sie im Abschnitt „UBA : Abnormal Outbound Transfer Attempts (ADE-Regel)" auf Seite 111.

Bekannte Probleme

Die App 'User Behavior Analytics' enthält Informationen, die für Upgrades und bekannte Probleme erforderlich sind.

Anmerkung: Das Aktivieren von ADE-Regeln kann die Leistung der UBA-App und Ihres QRadar-Systems beeinträchtigen.

Bekannte Probleme bei V3.2.0

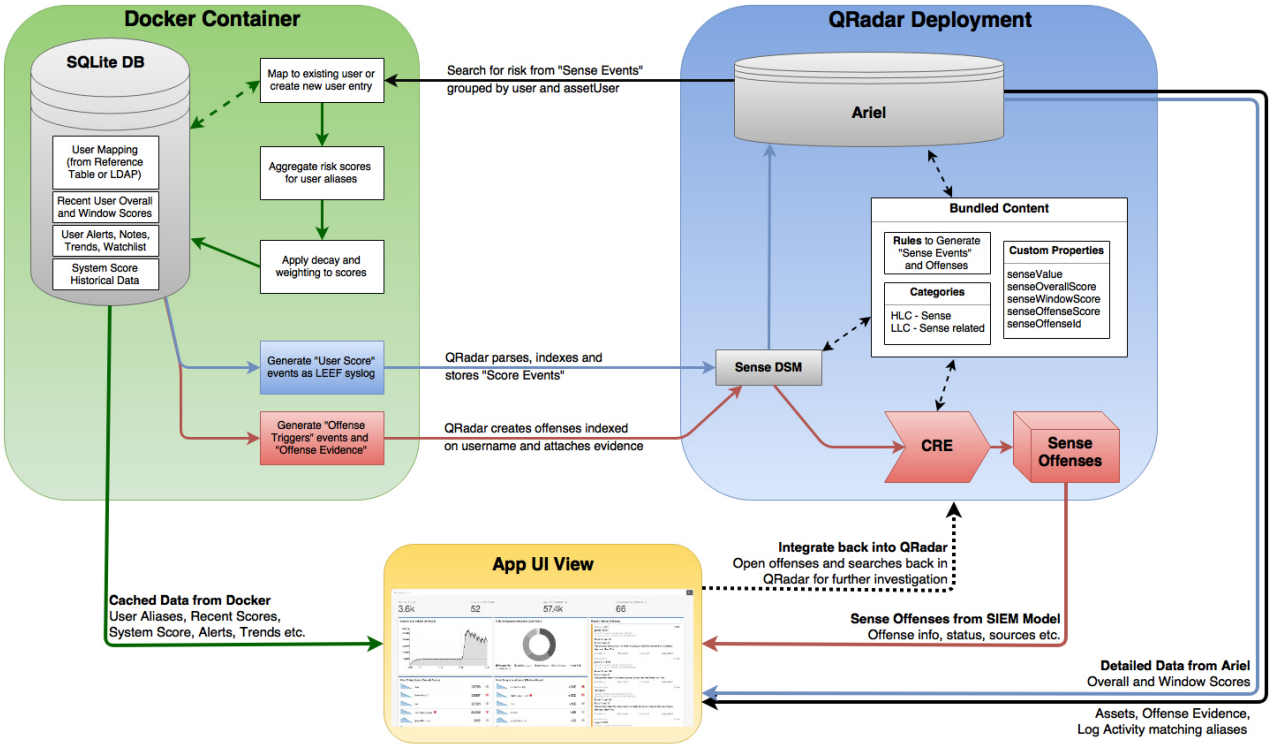
In der App 'User Behavior Analytics' gibt es folgende bekannte Probleme:

- Benutzerverbindungen aus einer Referenztabelle ergeben unvollständige Benutzerinformationen in den UBA-Benutzerdatensätzen, wenn Sie QRadar 7.2.8 Patch 13, QRadar 7.2.8 Patch 13 IF1, QRadar 7.3.1 Patch 3 oder QRadar 7.3.1 Patch 4 verwenden. Das Problem wird in V7.3.1 Patch 4 IF1 behoben. Weitere Informationen siehe APAR IJ06032.
- Wenn Sie bei einem Upgrade der UBA-App einen Ausnahmebedingungsfehler von QRadar Notification erhalten, der besagt, dass ein Regelsatz nicht geladen werden konnte, können Sie den Fehler ignorieren und fortfahren. Falls der Fehler bestehen bleibt, wenden Sie sich an die IBM Kundenunterstützung.
- Da es bekannte Probleme mit QRadar V7.2.8 Patch 12 und QRadar V7.3.1 Patch 3 gibt, sollten Sie ein Upgrade auf QRadar V7.2.8 Patch 13 und QRadar V7.3.1 Patch 4 durchführen.
- Nach dem Upgrade von UBA auf V3.2.0 kann es bis zu einem Tag dauern, bis die Grafik 'Machine Learning Activity Distribution' auf der Seite 'User Details' (Benutzerdetails) angezeigt wird.
- Beim Anzeigen einer Seite mit einem Benutzerprofil wird die Schaltfläche **Add to Whitelist** (Zu Whitelist hinzufügen) möglicherweise nicht angezeigt. In diesem Fall können Sie die Seite aktualisieren, um das Problem zu beheben.
- Der Import von über 100.000 Benutzern in LDAP für UBA kann Ihr QRadar-System und Ihre UBA-App-Installation erheblich beeinträchtigen. Dieses Problem wird aufgrund eines bekannten Problems in APAR IV98655 verursacht. Der Import von über 200.000 Benutzern wird nur bei der Verwendung von QRadar 7.3.0 oder höher auf einer Konsole mit 128 GB empfohlen.
- In seltenen Fällen kann es bei QRadar V7.2.8 und V7.3.0 zu Problemen mit einem neu erstellten SEC-Token kommen - das SEC-Token scheint zunächst fehlerfrei zu sein, wird aber später ungültig. Sie haben folgende Möglichkeiten, dieses Problem zu beheben:
  - Starten Sie den Apache Tomcat-Service über eine Befehlszeile der QRadar-Konsole erneut.
  - Implementieren Sie auf der Registerkarte 'Verwaltung' in QRadar eine beliebige Aktion.
- Wenn in der Grafik 'Systembewertung' ein Datumsbereich von mehr als einem Tag und mit dem aktuellen Tag als Enddatum ausgewählt wird, werden die ersten 8 Datenpunkte als '0s' angezeigt.
- In manchen Teilen der Benutzerschnittstelle werden bei Verwendung von QRadar V7.2.8 und bei einigen Ländereinstellungen englischsprachige Zeichenfolgen oder beschädigter Text angezeigt.

Prozessübersicht

Die App 'User Behavior Analytics' (Benutzerverhaltensanalyse) arbeitet mit Ihrem QRadar-System zusammen, um Daten über Benutzer in Ihrem Netz zu erfassen.

Funktionsweise von UBA



1. Protokolle senden Daten an QRadar.
2. UBA-spezifische Regeln suchen nach bestimmten Ereignissen (abhängig davon, welche UBA-Regeln aktiviert sind) und lösen ein neues Prüfereignis aus, das von der UBA-App gelesen wird.
3. Die UBA-Regeln erfordern, dass die Ereignisse einen Benutzernamen haben, sowie weitere Tests. (Prüfen Sie die Regeln, um zu sehen, wonach sie suchen.)
4. UBA extrahiert den *senseValue* (Prüfwert) und Benutzernamen aus dem Prüfereignis und erhöht dann den Wert für *risk score* (Risikobewertung) des Benutzers um den Betrag von *senseValue*.
5. Wenn der Wert für *risk score* für einen Benutzer den Schwellwert überschreitet, den Sie auf der Seite 'UBA Settings' (UBA-Einstellungen) festgelegt haben, sendet UBA ein Ereignis, das die Regel 'UBA : Create Offense' (UBA: Angriff erstellen) auslöst, und es wird ein Angriff für diesen Benutzer erstellt.

Risikobewertung

Bei einer Risikobewertung handelt es sich um die Summe aller Risikoereignisse, die von UBA-Regeln erkannt wurden. Je höher die Risikobewertung ist, desto wahrscheinlicher stellt ein interner Benutzer ein Sicherheitsrisiko dar und rechtfertigt eine weitere Überprüfung der Netzaktivität des Benutzers. Falls kein neues Ereignis eintritt, wird die Risikobewertung mit der Zeit verringert. Der Betrag der Verringerung wird mit dem Wert in **Decay risk by this factor per hour** (Risiko um diesen Faktor pro Stunde vermindern) auf der Seite mit den UBA-Einstellungen gesteuert.

Mithilfe von Prüfwerten Benutzerrisikobewertungen erstellen

Jeder Regel und Analyse ist ein Wert zugeordnet, der den Schweregrad des gefundenen Problems angibt. Immer wenn Aktionen eines Benutzers eine Regel auslösen, wird dieser Wert zu seiner Risikobewertung hinzugefügt. Je öfter der Benutzer gegen eine Regel "verstößt", desto höher die Bewertung.

Regeln und Prüfereignisse

Werden Regeln ausgelöst, generieren sie Prüfereignisse, die zur Bestimmung der Risikobewertung des Benutzers verwendet werden.

Sie können bestehende Regeln in QRadar aktualisieren, um Prüfereignisse zu erzeugen. Weitere Informationen finden Sie im Abschnitt „Neue oder bestehende QRadar-Inhalte mit der UBA-App integrieren" auf Seite 46.

Machine Learning Analytics und Prüfereignisse

Sie können die App 'Machine Learning Analytics' installieren und eine Analyse auf Basis maschinellen Lernens aktivieren, um anomales Benutzerverhalten zu erkennen. Wird die Analyse ausgelöst, generiert sie Prüfereignisse, die ebenfalls die Risikobewertung eines Benutzers erhöhen.

Videos und Lernprogramme

Weitere Informationen zu den IBM QRadar-Apps 'User Behavior Analytics' (UBA), 'Reference Data Import - LDAP' und 'Machine Learning Analytics' (ML).

IBM Security Learning Academy

Registrieren Sie sich auf der Website IBM Security Learning Academy für Kurse zu 'User Behavior Analytics' (UBA).

Tipp: Für die Registrierung und die Anzeige der Videos ist ein Konto mit einer IBM ID erforderlich.

Schulungsvideos in YouTube

Demo der App 'User Behavior Analytics' mit Machine Learning V2.0.0.0: https://www.youtube.com/watch?v=RgF1RztR1yg

Demo der Konfiguration der App 'Reference Data Import - LDAP': https://www.youtube.com/watch?v=ER-wYxS6wFk

Allgemeine Übersicht über die App 'User Behavior Analytics':

- https://www.youtube.com/watch?v=bf_DODl8Ehs
- https://www.youtube.com/watch?v=ARVsuQaSF9E

UBA-Dashboard und Benutzerdetails

Die IBM QRadar-App 'User Behavior Analytics' (UBA) gibt Ihnen einen Überblick über die Risikodaten der Benutzer in Ihrem Netz.

Dashboard

Klicken Sie nach der Installation und Konfiguration der UBA-App auf die Registerkarte **User Analytics** (Benutzeranalyse), um das Dashboard zu öffnen.

Anmerkung: Die UBA-App kann bis zu 400.000 Benutzer überwachen.

Im Feld **Search for User** (Benutzer suchen) können Sie anhand von Name, E-Mail-Adresse oder Benutzername nach Benutzern suchen. Noch während Sie die ersten Buchstaben eines Namens eingeben, werden die besten fünf Treffer angezeigt.

Das Dashboard wird automatisch jede Minute aktualisiert und enthält folgende Risikodaten:

Monitored Users (Überwachte Benutzer)	Zeigt die Gesamtzahl der Benutzer an, die von der UBA-App aktiv überwacht werden.
High Risk Users (Benutzer mit hohem Risiko)	Zeigt die Anzahl der Benutzer an, die aktuell die Risikobewertung überschreiten. Der Wert zum Ermitteln der Risikobewertung wird in den UBA-Einstellungen unter 'Risk threshold to trigger offenses' (Risikoschwelle für das Auslösen von Angriffen) festgelegt.
Users Discovered from Events (Über Ereignisse erkannte Benutzer)	Zeigt die Anzahl der Benutzer an, die aus Ereignissen erkannt wurden (ohne importierte Benutzer).
Users Imported from Directory (Aus Verzeichnis importierte Benutzer)	Zeigt die Anzahl der Benutzer an, die aus Referenztabellen importiert wurden.
Active Analytics (Aktive Analyse)	• UBA-Regeln: Zeigt den Status der Regelinhalte an. Ein grüner Status gibt an, dass die Regeln installiert und aktiv sind. Grau bedeutet, dass die Regeln inaktiviert sind. Gelb bedeutet, dass die Installation in Bearbeitung ist. • Datenflussregeln: Zeigt den Status der QNI-Regeln an. Ein grüner Status gibt an, dass die QNI-Regeln installiert und aktiv sind. Grau bedeutet, dass die QNI-Regeln nicht installiert sind. • Verhaltensanomalie: Ein grüner Status gibt an, dass ADE-Regeln installiert und aktiv sind. Grau bedeutet, dass ADE-Regeln nicht installiert sind. • Machine Learning Analytics: Ein grüner Status zeigt an, dass die App 'Machine Learning Analytics' installiert ist. Grau bedeutet, dass die App 'Machine Learning Analytics' nicht installiert ist.
Monitored Users (Überwachte Benutzer)	Zeigt die 10 Benutzer mit dem höchsten Risiko an. Die erste Spalte enthält den Anzeigenamen sowie die Jobbezeichnung und die Stadt, falls verfügbar. • Aktuelles Risiko: Zeigt das kumulierte Risiko für den betreffenden Benutzer für die letzten 5 Minuten an. • Risikobewertung: Zeigt eine Grafik an, die den Trend der Gesamtrisikobewertung des Benutzers für die letzte Stunde und die aktuelle Risikobewertung darstellt. Die Farbe der Grafik gibt den allgemeinen Risikograd an. • Beobachtungslistensymbol: Fügen Sie den Benutzer zu einer Beobachtungsliste hinzu oder erstellen Sie eine Beobachtungsliste. Die Zahl gibt an, in wie viele Beobachtungslisten der Benutzer eingetragen ist. • Alle überwachten Benutzer können auf der Seite **Search** (Suche) angezeigt werden.
Letzte Angriffe	Die neuesten Sense-Angriffe nach Benutzern.
[User] Watchlist ([Benutzer] Beobachtungsliste)	Beobachtungslisten, die Sie erstellt haben. Sie können beliebig viele Beobachtungslisten erstellen und sie im Dashboard anzeigen. Alle überwachten Benutzer können in der benutzerdefinierten Beobachtungsliste, die Sie auf der Seite **Search** (Suche) erstellt haben, angezeigt werden. **Tipp:** Wenn Sie einen Benutzer zu einer Beobachtungsliste hinzufügen möchten, klicken Sie auf das Symbol **Beobachtungsliste**  . Die Zahl gibt an, in wie viele Beobachtungslisten der Benutzer eingetragen ist.
Systembewertung	Kumulierte Gesamtrisikobewertung für alle Benutzer über einen bestimmten Zeitraum. Klicken Sie auf das Kalendersymbol, um einen Zeitraum über mehrere Tage einzugeben. Maximal kann ein Zeitraum von 30 Tagen innerhalb des letzten Jahres ausgewählt werden.
Aufschlüsselung nach Risikokategorie	Überblick über die Risikokategorien innerhalb der letzten Stunde. Klicken Sie auf die Grafik, um Unterkategorien anzuzeigen, und klicken Sie dann, um eine Ereignisanzeige aufzurufen.

Benutzer mit inaktiven Konten	Beobachtungsliste mit Benutzern, die als Benutzer mit inaktiven Konten markiert sind. Die Liste der Benutzer mit inaktiven Konten wird automatisch generiert. Verfügbar in V3.2.0 und höher.
Active Investigations (Aktive Untersuchungen)	Benutzer, die aktuell einer Untersuchung unterliegen. Aktivieren Sie das Kontrollkästchen **My investigations** (Eigene Untersuchungen), um nur die von Ihnen gestarteten Untersuchungen anzuzeigen. Verfügbar in V2.7.0 und höher.
Status of Machine Learning Models (Status der Machine Learning-Modelle)	Der Status von 'Machine Learning Analytics' wird angezeigt, wenn die Machine Learning-App installiert ist. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard mit Machine Learning Analytics" auf Seite 196.

Seite mit den Benutzerdetails

Die Details eines Benutzers können Sie überall in der App anzeigen, indem Sie auf dessen Benutzernamen klicken.

Im Fenster *Event Viewer* (Ereignisanzeige) finden Sie weitere Informationen zu den Aktivitäten von Benutzern. In der Ereignisanzeige werden Details zu einer ausgewählten Aktivität oder einem Zeitpunkt angezeigt. Wenn Sie auf ein Ereignis im Fenster *Event Viewer* klicken, werden weitere Details wie Syslog-Ereignisse und Nutzdaten angezeigt. Das Fenster mit der Ereignisanzeige ist für alle Ring- und Kurvendiagramme sowie für Aktivitäten im Zeitraster für gefährliche Aktivitäten (Risky Activity Timeline) auf der Seite **Benutzerangaben** verfügbar.

Die Seite **Benutzerdetails** enthält folgende Benutzerinformationen:

- Es werden der Name und die Aliasnamen des ausgewählten Benutzers und mögliche weitere Details aus den aus LDAP importierten Attributen angezeigt.
- In V3.2.0 und höher können Sie den Status (ruhend, aktiv, nie verwendet) aller Konten anzeigen, die dem Benutzer zugeordnet sind.
- Wenn Sie QRadar Advisor with Watson V1.13.0 oder höher installiert haben, können Sie nach Informationen über den Benutzer suchen. Sie müssen über QRadar-Administratorberechtigungen verfügen. Klicken Sie auf das Symbol **Search Watson** (Watson durchsuchen). (Verfügbar in V2.7.0 oder höher.)
- Um eine Untersuchung zu einem Benutzer einzuleiten, klicken Sie auf das Symbol **Start Investigation**  (Untersuchung starten). Klicken Sie nach Abschluss der Untersuchung auf das Symbol **End Investigation** (Untersuchung beenden). (Verfügbar in V2.7.0 oder höher.)
- Wenn Sie den Benutzer zu einer Beobachtungsliste hinzufügen oder eine Beobachtungsliste erstellen möchten, klicken Sie auf das Symbol **Beobachtungsliste**  .

Die Liste **Advanced Actions** (Erweiterte Aktionen) enthält folgende Aktionen:

Benutzerdefinierten Alert hinzufügen	Sie können einen benutzerdefinierten Alert einstellen, der abhängig vom Benutzernamen angezeigt wird. Klicken Sie dazu auf **Benutzerdefinierten Alert hinzufügen**, geben Sie die Alertnachricht ein und und klicken Sie auf **Festlegen**. Zum Entfernen des benutzerdefinierten Alerts für den ausgewählten Benutzer klicken Sie auf **Benutzerdefinierten Alert entfernen**.
Zur Whitelist hinzufügen	Sie müssen über QRadar-Administratorberechtigungen verfügen. Sie können den ausgewählten Benutzer zur Whitelist hinzufügen, sodass der Benutzer keine Risikobewertungen und Angriffe generiert. Um den ausgewählten Benutzer aus der Whitelist zu entfernen, klicken Sie auf **In Whiteliste**. Eine vollständige Liste der Benutzer, die der Whitelist hinzugefügt wurden, finden Sie im Abschnitt „Whitelist für vertrauenswürdige Benutzer anzeigen" auf Seite 39.

Generate GDPR compliant report for user (GDPR-konformen Bericht für Benutzer erstellen)	Sie können einen General Data Protection Regulation-(GDPR-)Konformitätsbericht für den Benutzer erstellen. **Wichtig:** Erstellen Sie den Bericht, bevor Sie auf **Delete and stop tracking user** (Überwachung von Benutzer löschen und stoppen) klicken.
Delete and stop tracking user (Überwachung von Benutzer löschen und stoppen)	Sie müssen über QRadar-Administratorberechtigungen verfügen. Sie können auf **Delete and stop tracking user** klicken, um Konformität mit General Data Protection Regulation (GDPR) herzustellen. Wählen Sie **Yes** (Ja) aus, um die Überwachung des Benutzers permanent zu löschen und zu stoppen. Wenn der Benutzer wieder überwacht werden soll, löschen Sie die Aliasnamen des Benutzers aus dem Referenzset **UBA : Users Not Tracked** (Nicht überwachte Benutzer). Laden Sie zum Anzeigen aller Aliasnamen des Benutzers den GDPR-Bericht herunter, bevor Sie den Benutzer löschen.
Always track with Machine Learning (Immer mit Machine Learning überwachen)	Sie müssen über QRadar-Administratorberechtigungen verfügen. Sie können auf **Always track with Machine Learning** klicken, um den Benutzer dem Referenzset *UBA: ML Always Tracked Watchlist* hinzuzufügen. Durch das Hinzufügen des Benutzer wird die höchste Wahrscheinlichkeit bereitgestellt, dass der Benutzer in ein Machine Learning-Modell integriert wird. Weitere Informationen zu Referenzsets in UBA finden Sie unter „Referenzsets” auf Seite 47. Wenn Sie den ausgewählten Benutzer aus dem Referenzset entfernen möchten, klicken Sie auf **Tracked with Machine Learning** (Mit Machine Learning überwacht). **Anmerkung:** Verfügbar in V2.8.0 oder höher und nur, wenn Machine Learning installiert ist und Sie über QRadar-Administratorberechtigungen verfügen.

Es können folgende Informationen über den ausgewählten Benutzer angezeigt werden:

Risikoscore - gesamt	Die gesamte Risikobewertung zeigt die Risikotrends für den Benutzer an.
Zeitraster	Die Zeitrastergrafik zeigt gefährliche Ereignisse und Benutzerereignisse an. Gefährliche Ereignisse sind Ereignisse, die zur Risikobewertung beitragen. Benutzerereignisse sind Ereignisse, die nicht als gefährlich eingestuft werden. Die Y-Achse stellt die Ereignisanzahl und die X-Achse die Zeit dar. Sie können auf eine beliebige Aktivität im Zeitraster klicken, um das Fenster mit der Ereignisanzeige zu öffnen, in dem die unterstützten Protokollereignisse aufgeführt werden, die der Aktivität eines Benutzers zugeordnet sind. Klicken Sie auf ein Ereignis, um weitere Details wie Syslog-Ereignisse und Nutzdaten anzuzeigen. • In Version 2.8.0 oder früher können Sie im Abschnitt mit dem Zeitraster für gefährliche Aktivitäten eine Liste der Aktivitäten eines Benutzers anzeigen, indem Sie auf **Group by Activity** (Nach Aktivität gruppieren) oder **Group by Hour** (Nach Stunde gruppieren) klicken, und anschließend nach einer beliebigen Spalte in der Zeitleiste filtern und durchsuchen. • In Version 3.0.0 und höher wird die Zeitrasteraktivität nach Sitzungen und Tagen gruppiert. Sitzungen werden im Abschnitt 'Application Settings' (Anwendungseinstellungen) auf der Seite **UBA Settings** (UBA-Einstellungen) definiert. Die Farben stellen den allgemeinen Risikograd einer Sitzung dar. Klicken Sie auf das Kalendersymbol, um den Zeitraum anzugeben (1 - 14 Tage). • In 3.1.0 und höher können Sie die für das Zeitraster angezeigten metrischen Einstellungen anpassen, indem Sie auf das Symbol **Metric Settings** (Metrische Einstellungen) klicken. Sie können die Kategorien, die Sie anzeigen möchten, hinzufügen und entfernen. Die Daten im Abschnitt mit den Beispielmetriken in der Anzeige **Metric Settings** (Metrikeinstellungen) stellen keine tatsächlichen Werte dar. **Anmerkung:** In “Risky Events” (Gefährliche Ereignisse) und “Use cases” (Anwendungsfälle) werden die gleichen Daten angezeigt. Dabei gibt “Risky Events” die Gesamtzahl der Ereignisse für die angegebenen Anwendungsfälle an. In “URL Categories” (URL-Kategorien) und “URLs” werden die gleichen Daten angezeigt. Dabei gibt “URLs” die Gesamtzahl der Ereignisse für die angegebenen “URL Categories” an. In “Event IDs” (Ereignis-ID) und “Events” (Ereignisse werden die gleichen Daten angezeigt. Dabei gibt “Events” die Gesamtzahl der Ereignisse für die angegebenen Ereignis-IDs an.

Letzte Angriffe	Zeigt alle Benutzertypangriffe an, bei denen der Benutzername mit einem der Aliasnamen des ausgewählten Benutzers übereinstimmte. Es werden die letzten fünf Angriffe angezeigt. Klicken Sie auf einen Angriff, um die Registerkarte **Angriffe** in QRadar zu öffnen.
Aufschlüsselung nach Risikokategorie	Zeigt die Risikokategorien für den ausgewählten Benutzer während der letzten Stunde an.
Notizen hinzufügen	Klicken Sie auf das Symbol **Hinzufügen** + , um Notizen für den ausgewählten Benutzer hinzuzufügen. Die Notizen werden nach einer Aufbewahrungsdauer von 30 Tagen automatisch gelöscht. **Tipp:** Wenn eine Notiz dauerhaft gespeichert werden soll, markieren Sie ihn mit dem Flaggensymbol als wichtig.

Die folgenden Grafiken werden auf der Seite **User Details** (Benutzerdetails) angezeigt, wenn die Machine Learning-App installiert und die angegebene Analyse aktiviert ist. Weitere Informationen finden Sie im Abschnitt „UBA-Dashboard mit Machine Learning Analytics” auf Seite 196.

Total Activity (Gesamtaktivität)	Zeigt die tatsächliche und erlernte Aktivitätsauslastung der Benutzer über den ganzen Tag an, gruppiert nach Stunde.
User Activity by Category (Benutzeraktivität nach Kategorie)	Zeigt die tatsächlichen und erwarteten Verhaltensmuster der Benutzeraktivität nach High-Level-Kategorie an.
Risk Posture (Risikoneigung)	Zeigt an, ob die Risikobewertung für einen Benutzer vom erwarteten Risikobewertungsmuster abweicht.
Abnormal Outbound Transfer Attempts (Abnormale abgehende Übertragungsversuche)	Zeigt die Nutzung des ausgehenden Datenverkehrs für jeden Benutzer und gibt bei abnormalem Verhalten eine Warnung aus. Beachten Sie, dass die Grafik für diese Analyse standardmäßig nicht aktiviert ist. Die Analyse 'Abnormal Outbound Transfer Attempts' wird nur im Dashboard angezeigt, wenn die Machine Learning-App installiert, die Analyse aktiviert und die Option **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) in den Einstellungen für Machine Learning ausgewählt ist. Verfügbar in V2.8.0 oder höher.
Abnormal Volume of Data to External Domains (Abnormales Datenvolumen bei externen Domänen)	Zeigt die Datennutzung bei externen Domänen für jeden Benutzer an und gibt bei abnormalem Verhalten eine Warnung aus. Die Analyse 'Abnormal Volume of Data to External Domains' wird nur im Dashboard angezeigt, wenn die Machine Learning-App installiert, die Analyse aktiviert und die Option **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) in den Einstellungen für Machine Learning ausgewählt ist. Verfügbar in V3.0.0 oder höher.
Activity Distribution (Aktivitätsverteilung)	Zeigt dynamische Verhaltenscluster für alle Benutzer an, die von Machine Learning überwacht werden. Verfügbar in V2.2.0 oder höher.
Learned Peer Group (Erlernte Peergruppe)	Zeigt an, wie stark der Benutzer von der abgeleiteten Peergruppe abwich, der er als zugehörig betrachtet wurde. Verfügbar in V2.2.0 oder höher.
Defined Peer Group (Definierte Peergruppe)	Zeigt an, wie stark die Ereignisaktivität eines Benutzers von der Aktivität der zugehörigen definierten Peergruppe abweicht. Verfügbar in V2.6.0 oder höher.

Klicken Sie auf **Dashboard**, um zum Hauptdashboard zurückzukehren.

Zugehörige Konzepte:

„UBA-Dashboard mit Machine Learning Analytics” auf Seite 196
Die IBM QRadar-App "User Behavior Analytics" (UBA) mit Machine Learning Analytics umfasst den Status von Machine Learning Analytics sowie weitere Details für den ausgewählten Benutzer.

„Ruhende Konten” auf Seite 41
Sie können Benutzer in Ihrem System anzeigen, deren Konten ruhend oder aktiv sind oder nie verwendet wurden.

Zugehörige Tasks:

„Beobachtungslisten erstellen" auf Seite 37
Sie können einen Benutzer zu einer neuen oder vorhandenen Beobachtungsliste hinzufügen.

„Whitelist für vertrauenswürdige Benutzer anzeigen" auf Seite 39
Sie können die Liste der vertrauenswürdigen Benutzer anzeigen, die in der Referenzsetverwaltungsliste in der Whitelist aufgeführt sind.

„Protokollquellen zur Gruppe vertrauenswürdiger Protokollquellen hinzufügen" auf Seite 41
Wenn bestimmte Protokollquellen nicht von der UBA-App überwacht und gemeldet werden sollen, können Sie diese zur **UBA : Trusted Log Source Group** (UBA: Gruppe vertrauenswürdiger Protokollquellen) hinzufügen. Protokollquellen, die zur Gruppe hinzugefügt wurden, werden nicht mehr von der UBA-App überwacht.

„App 'Machine Learning Analytics' installieren" auf Seite 178
Installieren Sie nach der Installation der UBA-App die App 'Machine Learning Analytics' über Extension Manager.

„Benutzer in QRadar Advisor with Watson untersuchen"
Sie können Benutzer in der App 'User Behavior Analytics' (UBA) auswählen, um sie zur Untersuchung an QRadar Advisor with Watson zu senden.

Benutzer in QRadar Advisor with Watson untersuchen

Sie können Benutzer in der App 'User Behavior Analytics' (UBA) auswählen, um sie zur Untersuchung an QRadar Advisor with Watson zu senden.

Vorbereitende Schritte

- Die App 'User Behavior Analytics' (UBA) Version 2.7.0 oder höher muss installiert und mit Benutzerdaten konfiguriert sein.
- Sie müssen über Administratorberechtigungen verfügen.
- QRadar Advisor with Watson Version 1.13.0 oder höher muss installiert sein.

Weitere Informationen finden Sie im Abschnitt https://developer.ibm.com/qradar/advisor.

Informationen zu diesem Vorgang

Anmerkung: Diese Funktion ist nur in User Behavior Analytics V2.7.0 und höher und QRadar Advisor with Watson V1.13.0 und höher verfügbar.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **User Analytics** (Benutzeranalyse), um das UBA-**Dashboard** zu öffnen.
2. Wählen Sie einen Benutzer aus oder suchen Sie nach einem Benutzer, um die Seite **Benutzerdetails** zu öffnen.
3. Klicken Sie auf das Symbol **Search Watson** (Watson durchsuchen). Wenn das Symbol aufhört, sich zu drehen, können Sie die Ergebnisse in der App 'QRadar Advisor with Watson' überprüfen.
4. Wählen Sie auf der Registerkarte **Watson** auf der Seite **Incident Overview** (Vorfallsübersicht) die Benutzeruntersuchung aus. Benutzeruntersuchungen sind durch das Symbol **Investigation initiated from UBA** (Untersuchung eingeleitet von UBA)  gekennzeichnet.

Voraussetzungen für die Installation der App 'User Behavior Analytics'

Stellen Sie vor der Installation der App 'User Behavior Analytics' (UBA) sicher, dass die Voraussetzungen erfüllt sind.

- Stellen Sie sicher, dass IBM Security QRadar V7.2.8 oder höher installiert ist.
  Um das beste Ergebnis zu erzielen, aktualisieren Sie Ihr QRadar-System auf die folgenden Versionen:
  - QRadar 7.2.8 Patch 13 (7.2.8.20180529210357) oder höher
  - QRadar 7.3.1 Patch 6 (7.3.1.20180912181210) oder höher
- Installieren Sie die Content-Packs aus IBM App Exchange
- Fügen Sie das IBM Sense-DSM für die UBA-App hinzu.

Inhaltsabhängigkeiten

Es wurden mehrere Regeln erstellt, um Ereignisse von anderen Apps an UBA zu senden. Für diese Regeln müssen die Inhalte für die anderen Apps installiert werden, damit diese ordnungsgemäß funktionieren.

Weitere Informationen zu UBA-Inhalten und erforderlichen Apps finden Sie in der folgenden Tabelle.

UBA-Inhalt	**Erforderliche Apps**
„QRadar DNS Analyzer" auf Seite 132	IBM QRadar DNS Analyzer
UBA QRadar Network Insights	QRadar Network Insights Content v7.2.8 QRadar Network Insights Content for V7.3.0+
Ausspähung	IBM Security Reconnaissance Content
Systemüberwachung (Sysmon)	IBM QRadar Content for Sysmon

Anmerkung: Wenn Sie diese Regeln bearbeiten, funktionieren Sie möglicherweise nicht wie erwartet.

IBM Sense-DSM manuell installieren

Die App 'User Behavior Analytics' (UBA) fügt mithilfe des IBM Sense-DSM Risikobewertungen und Verstöße zu QRadar hinzu. Dieses DSM können Sie mittels der automatischen Aktualisierung installieren oder Sie können es in QRadar hochladen und manuell installieren.

Anmerkung: Falls Ihr System allerdings vom Internet getrennt ist, müssen Sie das DSM-RPM vermutlich manuell installieren.

Einschränkung: Die Deinstallation eines DSM wird in QRadar nicht unterstützt.

1. Laden Sie die DSM-RPM-Datei von der IBM Support-Website herunter:
   - Für QRadar V7.2.8: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
   - Für QRadar V7.3.1 und höher: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`
2. Kopieren Sie die RPM-Datei auf Ihre QRadar-Konsole.
3. Melden Sie sich mit SSH als Rootbenutzer beim QRadar-Host an.
4. Wechseln Sie in das Verzeichnis, in das Sie die Datei heruntergeladen haben.
5. Geben Sie den folgenden Befehl ein:
   `rpm -Uvh <RPM-Dateiname>`
6. Klicken Sie in den Einstellungen für **Verwaltung** auf **Änderungen implementieren**.
7. Klicken Sie in den Einstellungen für **Verwaltung** auf **Erweitert** > **Web-Services erneut starten**.

Unterstützte Browser für die UBA-App

Um die Funktionen in IBM Security QRadar-Produkten uneingeschränkt nutzen zu können, müssen Sie einen unterstützten Web-Browser verwenden.

In der folgenden Tabelle werden die unterstützten Versionen von Web-Browsern aufgelistet.

Web-Browser	Unterstützte Versionen
Mozilla Firefox	45.2 Extended Support Release
Google Chrome	Neueste

Anmerkung: Für eine optimale Erfahrung mit UBA sollten Sie Folgendes tun:

- Inaktivieren Sie den Popup-Blocker für den Browser.
- Konfigurieren Sie den Browser, um Ausnahmen für Popups, die von der IP-Adresse der QRadar-Konsole kommen, zuzulassen.

Für die UBA-App relevante Protokollquellentypen

Die App "User Behavior Analytics" (UBA) und die ML-App können Ereignisse von bestimmten Protokollquellen akzeptieren und analysieren.

Im Allgemeinen sind Protokollquellen für die UBA-App und die ML-App erforderlich, mit denen ein Benutzername bereitgestellt wird. Wenn für UBA kein Benutzername vorhanden ist, aktivieren Sie das Kontrollkästchen **Search assets for username, when username is not available for event or flow data** (Assets nach Benutzername durchsuchen, wenn für Ereignis- oder Flussdaten kein Benutzername verfügbar ist) in den UBA-Einstellungen, damit UBA den Benutzer in der Asset-Tabelle suchen kann. Wenn kein Benutzer ermittelt werden kann, fährt UBA nicht mit der Verarbeitung des Prozesses fort.

Weitere Details zu spezifischen Anwendungsfällen und den entsprechenden Protokollquellentypen finden Sie im Abschnitt 7, „Regeln und Möglichkeiten zur Optimierung für die UBA-App”, auf Seite 49.

Zugehörige Tasks:

„UBA-Einstellungen konfigurieren” auf Seite 28
Die IBM QRadar-App "User Behavior Analytics" (UBA) muss zunächst konfiguriert werden, damit sie Daten anzeigt.

2 Installation und Deinstallation

App 'User Behavior Analytics' installieren

Sie können das Archiv, das die App enthält, mit dem IBM QRadar-Tool für das Erweiterungsmanagement direkt in die QRadar-Konsole hochladen und dort installieren.

Vorbereitende Schritte

Führen Sie die im Abschnitt „Voraussetzungen für die Installation der App 'User Behavior Analytics'" auf Seite 15 beschriebenen Schritte aus.

Wichtig: Stellen Sie vor der Installation der App sicher, dass IBM QRadar die Mindestanforderungen an den Speicherbedarf (RAM) erfüllt. Für die UBA-App ist 1 GB freier Speicherplatz aus dem Anwendungspool des Hauptspeichers erforderlich. Die Installation der UBA-App schlägt fehl, wenn im Anwendungspool nicht ausreichend freier Speicher zur Verfügung steht.

Informationen zu diesem Vorgang

Die Installation wurde ab V2.8.0 geändert. UBA-spezifische Inhaltspakete mit Regeln zum Auslösen von Verstößen werden jetzt als separate Erweiterungen installiert. Inhaltspakete werden standardmäßig installiert. Wenn Sie Ihre eigenen angepassten Regeln zum Auslösen von Verstößen in UBA erstellen möchten, können Sie die Einstellung **Install and upgrade content packages** (Inhaltspakete installieren und aktualisieren) beim Konfigurieren der UBA-Einstellungen ändern.

Achtung: Nach Installation der App sind folgende Schritte erforderlich:

- Aktivieren Sie Indizes.
- Implementieren Sie die vollständige Konfiguration.
- Löschen Sie den Browser-Cache und aktualisieren Sie das Browserfenster.
- Richten Sie Berechtigungen für die Benutzer ein, die Zugriffsrechte für die Anzeige der Registerkarte **User Analytics** (Benutzeranalyse) benötigen. Die folgenden Berechtigungen müssen jeder Benutzerrolle zugewiesen werden, die Zugriff auf die App benötigt:
  - Benutzeranalyse
  - Angriffe
  - Protokollaktivität

Installieren Sie die App nach dem Download von IBM Security App Exchange mithilfe des Tools für das Erweiterungsmanagement von IBM QRadar in der QRadar-Konsole.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü () und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf **Systemkonfiguration** > **Erweiterungsmanagement**.
3. Klicken Sie im Fenster **Erweiterungsmanagement** auf **Hinzufügen** und wählen Sie das Archiv mit der UBA-App aus, die in die Konsole geladen werden soll.
4. Wählen Sie das Kontrollkästchen **Sofort installieren** aus und klicken Sie auf **Hinzufügen**.
5. Wählen Sie an der Eingabeaufforderung **Überschreiben** aus.

Wichtig: Eventuell müssen Sie einige Minuten warten, bis die App aktiv wird. Nach der Installation der UBA-App werden die Inhaltspakete im Hintergrund installiert. Die Inhalte sind in QRadar möglicherweise nicht direkt nach der Installation der App sichtbar.

6. Klicken Sie in der Einstellungen für **Verwaltung** auf **Systemkonfiguration** > **Indexverwaltung** und aktivieren Sie die folgenden Indizes:
   - High Level Category
   - Low Level Category
   - Username
   - senseValue
7. Klicken Sie in den Einstellungen für **Verwaltung** auf **Erweitert** > **Gesamte Konfiguration implementieren**.

   Anmerkung: Nach Abschluss der UBA-Installation und -Konfiguration sind folgende Inhaltspakete installiert:
   - User Behavior Analytics Access and Authentication Content
   - User Behavior Analytics Accounts and Privileges Content
   - User Behavior Analytics Browsing Behavior Content
   - User Behavior Analytics DNS Analyzer Content
   - User Behavior Analytics Endpoint Content
   - User Behavior Analytics Exfiltration Content
   - User Behavior Analytics Geography Content
   - User Behavior Analytics Network Traffic and Attacks Content
   - User Behavior Analytics QRadar Network Insights Content
   - User Behavior Analytics Reconnaissance Content
   - User Behavior Analytics Sysmon Content
   - User Behavior Analytics Threat Intelligence Content

Nächste Schritte

- Bevor Sie die App nach der Installation verwenden, müssen Sie den Browser-Cache löschen und das Browserfenster aktualisieren.
- Verwalten Sie die Berechtigungen für die Benutzerrollen für die UBA-App.

Zugehörige Tasks:

„Indizes zur Leistungssteigerung aktivieren” auf Seite 45
Um die Leistung der IBM QRadar-App 'User Behavior Analytics' (UBA) zu verbessern, können Sie in IBM QRadar Indizes aktivieren.

„Berechtigungen für die QRadar-App UBA verwalten” auf Seite 37
Administratoren konfigurieren und verwalten Benutzerkonten mithilfe der Funktion "Benutzerrollenverwaltung" in IBM QRadar. Als Administrator müssen Sie die Berechtigungen "Benutzeranalyse", "Angriffe" und "Protokollaktivität" für jede Benutzerrolle aktivieren, die zur Verwendung der QRadar-App UBA berechtigt ist.

UBA-App deinstallieren

Sie können die Anwendung mithilfe des IBM QRadar-Tools für das Erweiterungsmanagement aus der QRadar-Konsole entfernen.

Vorbereitende Schritte

Wenn die ML-App (Machine Learning Analytics) installiert ist, muss diese App zunächst über die Seite 'Machine Learning Settings' (ML-Einstellungen) deinstalliert werden, bevor eine Deinstallation der UBA-

App über das Fenster 'Extension Management' (Erweiterungsmanagement) vorgenommen wird. Wenn Sie die ML-App nicht vor der Deinstallation von UBA entfernen, müssen Sie sie aus der interaktiven API-Dokumentationsschnittstelle entfernen.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü () und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf **Extension Management** (Erweiterungsmanagement).
3. Wählen Sie auf der Registerkarte **INSTALLIERT** des Fensters **Extension Management** (Erweiterungsmanagement) die App 'User Behaviour Analytics' (Analyse des Benutzerverhaltens) aus und klicken Sie auf **Deinstallieren**.

   Die App wird bei der Deinstallation aus dem System entfernt. Soll sie erneut installiert werden, müssen Sie sie erneut hinzufügen.
4. Ab Version 2.8.0 werden bei der Konfiguration der UBA-App die folgenden Inhaltspakete installiert. Sie müssen jedes Inhaltspaket deinstallieren, damit die App vollständig entfernt wird.
   - User Behavior Analytics Access and Authentication Content
   - User Behavior Analytics Accounts and Privileges Content
   - User Behavior Analytics Browsing Behavior Content
   - User Behavior Analytics DNS Analyzer Content
   - User Behavior Analytics Endpoint Content
   - User Behavior Analytics Exfiltration Content
   - User Behavior Analytics Geography Content
   - User Behavior Analytics Network Traffic and Attacks Content
   - User Behavior Analytics QRadar Network Insights Content
   - User Behavior Analytics Reconnaissance Content
   - User Behavior Analytics Sysmon Content
   - User Behavior Analytics Threat Intelligence Content

3 Upgrade

App 'User Behavior Analytics' aktualisieren

Zur Aktualisierung Ihrer App verwenden Sie das IBM QRadar-Tool für das Erweiterungsmanagement.

Vorbereitende Schritte

Wichtig: Der Speicherbedarf hat sich ab V2.8.0 erhöht. Stellen Sie vor der Aktualisierung der App sicher, dass IBM QRadar die Mindestanforderungen an den Speicherbedarf (RAM) erfüllt. Für die UBA-App ist 1 GB freier Speicherplatz aus dem Anwendungspool des Hauptspeichers erforderlich. Die Aktualisierung der UBA-App schlägt fehl, wenn im Anwendungspool nicht ausreichend freier Speicher zur Verfügung steht.

Um das beste Ergebnis zu erzielen, aktualisieren Sie Ihr QRadar-System auf die folgenden Versionen:

- QRadar 7.2.8 Patch 13 (7.2.8.20180529210357) oder höher
- QRadar 7.3.0 Patch 7 (7.3.0.20171205025101) oder höher
- QRadar 7.3.1 Patch 6 (7.3.1.20180912181210) oder höher

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü () und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf **Extension Management** (Erweiterungsmanagement).
3. Klicken Sie im Fenster **Extension Management** (Erweiterungsmanagement) auf **Hinzufügen** und wählen Sie das Archiv mit der UBA-App aus, die in die Konsole geladen werden soll.
4. Wählen Sie an der Eingabeaufforderung **Überschreiben** aus. Ihre vorhandenen UBA-Appdaten bleiben beim Überschreiben intakt.

   Wichtig: Eventuell müssen Sie einige Minuten warten, bis die App aktiv wird. Nach der Aktualisierung der UBA-App werden die Inhaltspakete im Hintergrund aktualisiert. Die Inhalte sind in QRadar möglicherweise nicht direkt nach der Aktualisierung der App sichtbar.

   Anmerkung: Nach Abschluss der UBA-Aktualisierung und -Konfiguration sind folgende Inhaltspakete aktualisiert:
   - User Behavior Analytics Access and Authentication Content
   - User Behavior Analytics Accounts and Privileges Content
   - User Behavior Analytics Browsing Behavior Content
   - User Behavior Analytics DNS Analyzer Content
   - User Behavior Analytics Endpoint Content
   - User Behavior Analytics Exfiltration Content
   - User Behavior Analytics Geography Content
   - User Behavior Analytics Network Traffic and Attacks Content
   - User Behavior Analytics QRadar Network Insights Content
   - User Behavior Analytics Reconnaissance Content
   - User Behavior Analytics Sysmon Content

- User Behavior Analytics Threat Intelligence Content

Nächste Schritte

Bevor Sie die App nach der Aktualisierung verwenden, müssen Sie den Browser-Cache löschen und das Browser-Fenster aktualisieren.

4 Konfiguration

App "User Behavior Analytics" konfigurieren

Vor Verwendung der IBM QRadar-App "User Behavior Analytics" (UBA) müssen die Anwendungseinstellungen der UBA-App konfiguriert werden.

Bei der Installation der UBA-App wird auch die IBM QRadar-App 'Import von Referenzdaten - LDAP' installiert. Wenn Sie Ihre Benutzerdaten mit der LDAP-App importieren möchten, müssen Sie diese App vor der Einrichtung der UBA-App konfigurieren. Die von der UBA-App verwendeten Daten stammen aus einer LDAP-Abfrage. Die LDAP-Abfrage ruft die Liste der Benutzer ab, mit der die UBA-App gefüllt wird.

Für die UBA-App und die LDAP-App sind jeweils separate Berechtigungstoken erforderlich. Sie können die Berechtigungstoken bei der Konfiguration der jeweiligen App erstellen.

Die Erstkonfiguration umfasst die folgenden Vorgänge:

- Konfigurieren der App "Reference Data Import LDAP" (wenn Sie diese App verwenden wollen)
- Konfigurieren der UBA-Einstellungen für die UBA-App

App "Import von Referenzdaten - LDAP" konfigurieren

Bei der Installation der IBM® QRadar®-App 'User Behavior Analytics' (UBA) wird auch die App 'Import von Referenzdaten - LDAP' installiert. Mit dieser App können Sie Benutzerdaten von einem LDAP/AD-Server oder aus einer CSV-Datei in eine QRadar-Referenztabelle importieren. Die Referenztabelle wird anschließend von der UBA-App genutzt oder für QRadar-Suchvorgänge oder -Regeln verwendet.

Vorbereitende Schritte

Achtung: Falls die eigenständige App "Import von Referenzdaten - LDAP" bereits auf dem System installiert ist, wird sie bei der Installation der UBA-App ersetzt. Ihre Konfigurationen werden in diesem Fall der aktualisierten Version der App "Import von Referenzdaten - LDAP" hinzugefügt.

Informationen zu diesem Vorgang

Anmerkung: Notieren Sie sich den Namen der Referenztabelle und, falls Sie für die Attribute benutzerdefinierte Aliasnamen eingeben, auch diese Namen. Bei der Einrichtung der UBA-App müssen Sie die in der App "Import von Referenzdaten - LDAP" erstellte Referenztabelle auswählen.

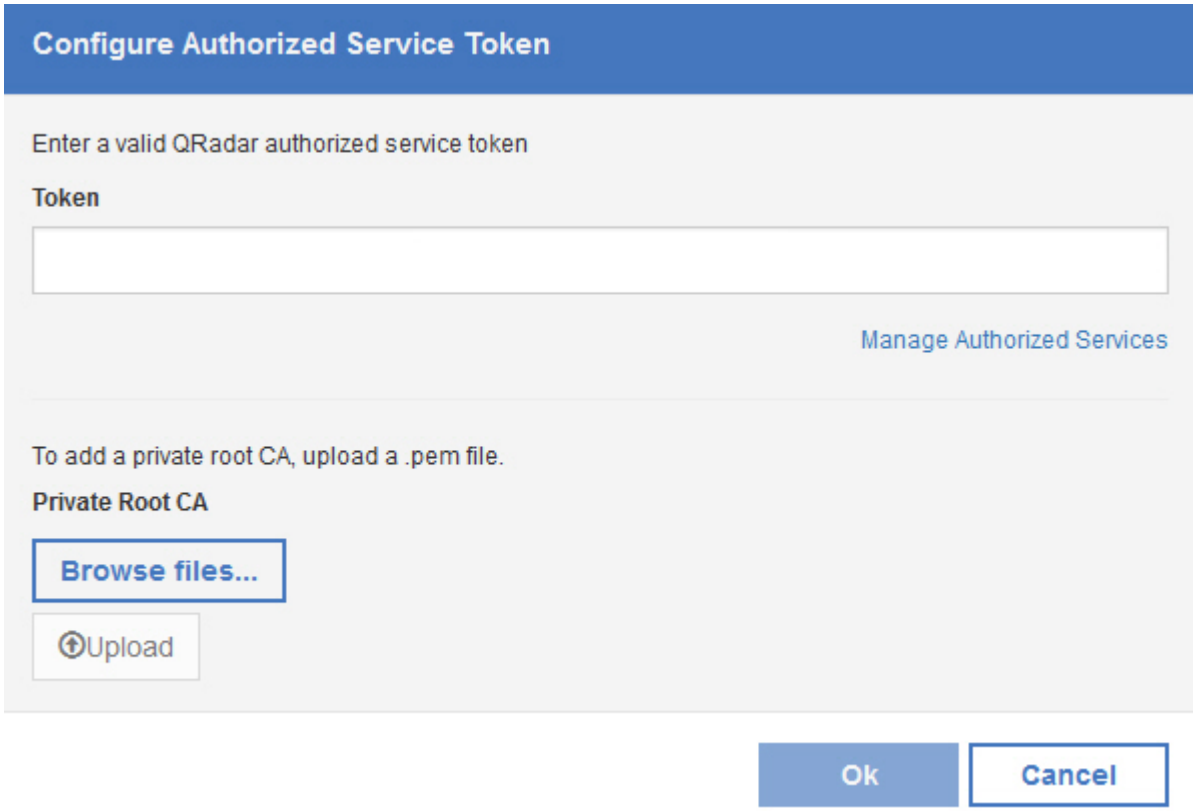
Weitere Informationen zur App "Import von Referenzdaten - LDAP" finden Sie im IBM Knowledge Center unter http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.apps.doc/c_Qapps_LDAP_intro.html.

Vorgehensweise

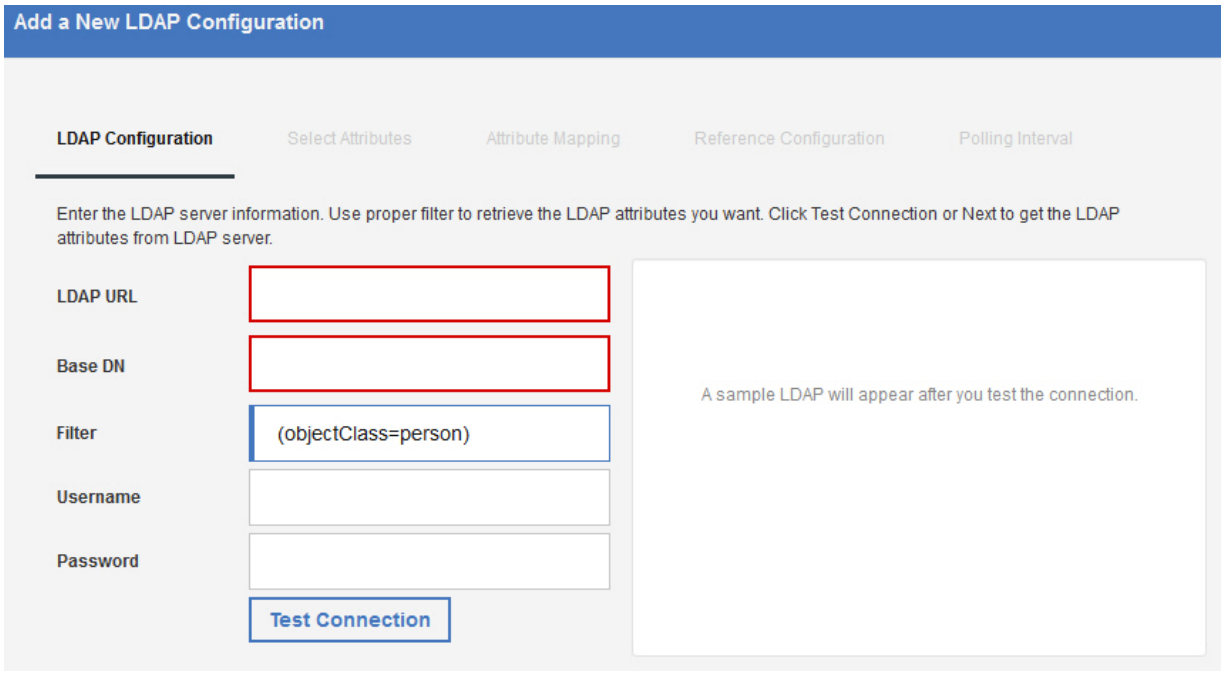
1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Reference Data Import - LDAP** (Import von Referenzdaten - LDAP.
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **UBA Settings** (Plug-ins > Benutzeranalyse > UBA-Einstellungen).

- Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **Reference Data Import - LDAP** > **Reference Data Import - LDAP** (Apps > Import von Referenzdaten - LDAP).

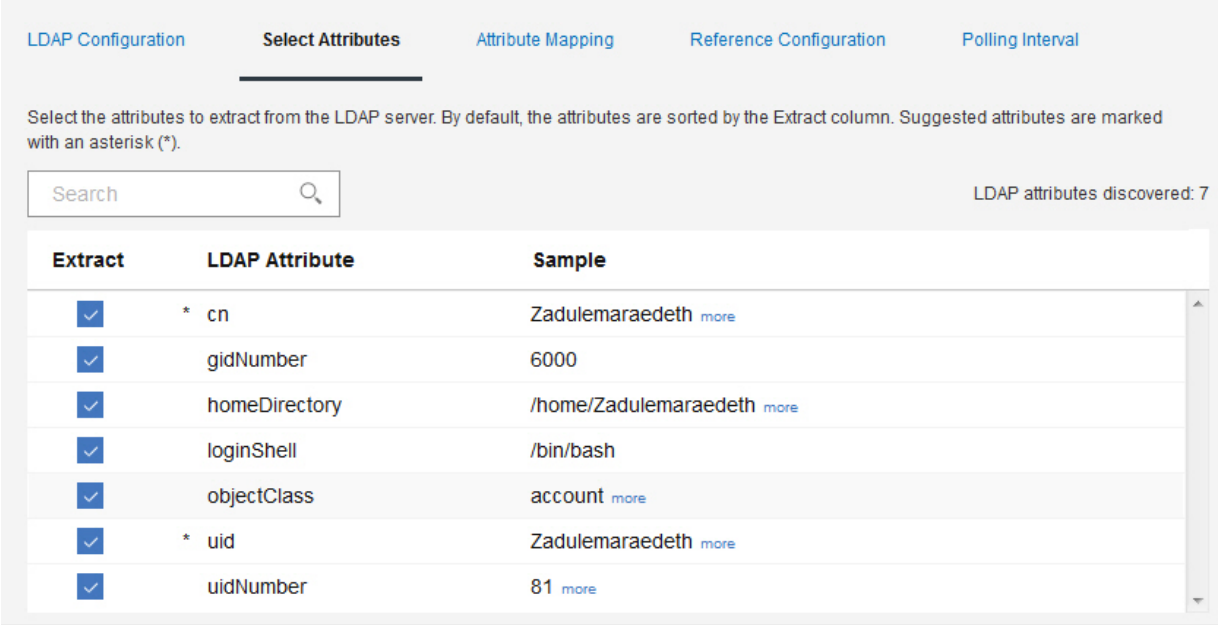
3. Klicken Sie auf **Configure** (Konfigurieren), um ein autorisiertes Service-Token für LDAP zu erstellen. Das Feld **Configure Authorized Service Token** (Autorisiertes Service-Token konfigurieren) wird geöffnet.
   a. Klicken Sie auf den Link **Autorisierte Services verwalten** und klicken Sie anschließend auf **Autorisierten Service hinzufügen**.
   b. Geben Sie im Feld **Servicename** den Namen `LDAP` ein. Dies ist der Benutzer, für den API-Anforderungen aus der LDAP-App ausgeführt werden.
   c. Wählen Sie in der Liste **Benutzerrolle** die Rolle **Verwaltung** aus.
   d. Wählen Sie in der Liste **Sicherheitsprofil** das Sicherheitsprofil aus, das dem autorisierten Service zugewiesen werden soll. Über das Sicherheitsprofil werden die Netze und die Protokollquellen vorgegeben, auf die dieser Service in der QRadar-Benutzerschnittstelle zugreifen kann.
   e. Geben Sie in der Liste **Ablaufdatum** das Datum an, an dem der Service ablaufen soll, bzw. wählen Sie ein Datum aus. Ist kein Ablaufdatum erforderlich, wählen Sie **Kein Ablaufdatum** aus.
   f. Klicken Sie auf **Service erstellen**.
   g. Klicken Sie auf die Zeile mit dem von Ihnen erstellten LDAP-Service, wählen Sie im Feld **Ausgewähltes Token** der Menüleiste die Tokenzeichenfolge aus und kopieren Sie sie.
   h. Fügen Sie die Tokenzeichenfolge für den autorisierten Service im Feld **Configure Authorized Service Token** (Autorisiertes Service-Token konfigurieren) in das Feld **Token** ein.
4. Optional: Wenn Sie eine private Stammzertifizierungsstelle hinzufügen möchten, klicken Sie auf **Browse files** (Dateien durchsuchen), öffnen eine unterstützte Datei, klicken auf **Open** (Öffnen)und anschließend auf **Upload** (Hochladen). Folgender Dateityp wird unterstützt: `.pem`.
5. Klicken Sie auf **OK**.



6. Klicken Sie im Hauptfenster der App **Reference Data Import (LDAP)** (Import von Referenzdaten (LDAP)) auf **Add Import** (Import hinzufügen). Das Dialogfenster **Neue LDAP-Konfiguration hinzufügen** wird geöffnet.
7. Geben Sie auf der Registerkarte **LDAP-Konfiguration** Verbindungsinformationen für den LDAP-Server ein. Das Feld **Filter** wird automatisch mit Attributen aus Ihrem Active Directory gefüllt.
   a. Geben Sie im Feld **LDAP-URL** eine URL ein, die mit `ldap://` oder `ldaps://` (für TLS) beginnt.
   b. Geben Sie im Feld **Basis-DN** die Position in der LDAP-Verzeichnisstruktur ein, ab der der Server nach Benutzern suchen soll. Beispiel: Wenn sich Ihr LDAP-Server in der Domäne "example.com" befindet, können Sie zum Beispiel `dc=example,dc=com` eingeben.
   c. Geben Sie im Feld **Filter** das bzw. die Attribute ein, anhand derer die in die Referenztabelle importierten Daten sortiert werden sollen. Beispiel: `cn=*; uid=*; sn=*`. Folgende Standardwerte funktionieren mit Active Directory: `(&(sAMAccountName=*)(samAccountType=805306368))`.
   d. Geben Sie im Feld **Benutzername** den Benutzernamen für die Authentifizierung beim LDAP-Server ein.
   e. Geben Sie im Feld **Kennwort** das Kennwort für den LDAP-Server ein.
8. Klicken Sie auf **Verbindung testen** oder **Weiter**, um sicherzustellen, dass IBM QRadar eine Verbindung zum LDAP-Server herstellen kann. Nach einem erfolgreichen Verbindungsaufbau werden auf der Registerkarte **LDAP-Konfiguration** Informationen vom LDAP-Server angezeigt.



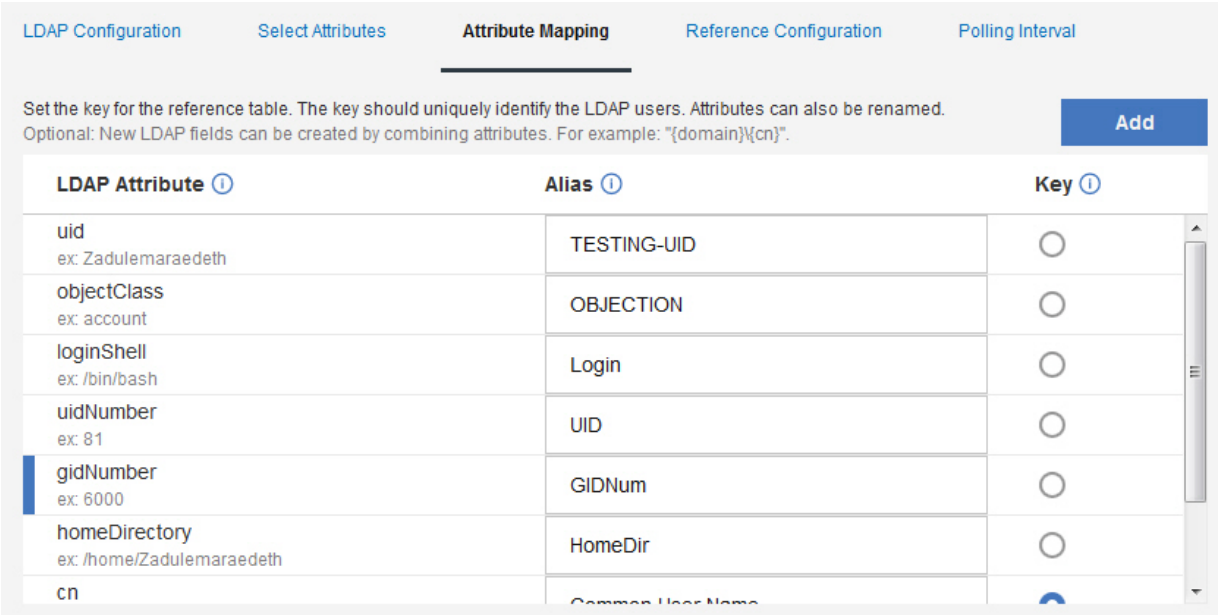
9. Wählen Sie auf der Registerkarte **Select Attributes** (Attribute auswählen) die Attribute aus, die Sie vom LDAP-Server extrahieren möchten. Folgende Standardwerte funktionieren mit Active Directory: `userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.



10. Optional: Legen Sie auf der Registerkarte **Attribute Mapping** (Attributzuordnung) den Schlüssel für die Referenztabelle fest.

    Tipp: Durch das Klicken auf **Add** (Hinzufügen) und die Kombination zweiter Attribute können Sie neue LDAP-Felder erstellen. Sie können zum Beispiel folgende Syntax verwenden: `"Last: {ln}, First: {fn}"`.

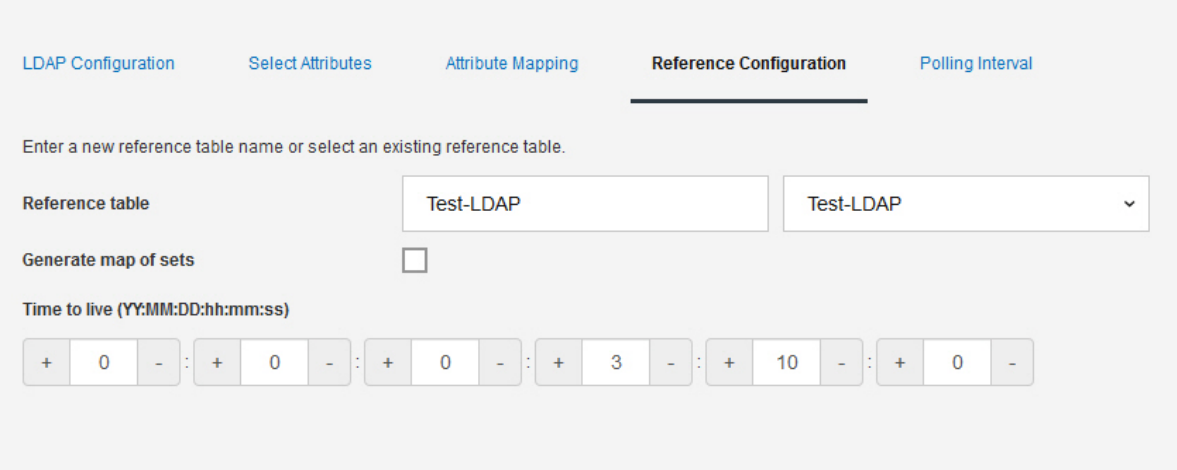
    Tipp: Wenn Sie LDAP-Daten mehrerer Quellen in der gleichen Referenztabelle zusammenführen möchten, können Sie LDAP-Attribute, die in den verschiedenen Quellen gleiche Namen haben, durch benutzerdefinierte Aliasnamen unterscheiden.



11. Erstellen Sie auf der Registerkarte **Referenzkonfiguration** eine Referenzzuordnung von Zuordnungen oder legen Sie eine vorhandene Referenzzuordnung von Zuordnungen fest, der LDAP-Daten hinzugefügt werden sollen.

a. Geben Sie im Feld **Referenztabelle** einen Namen für die neue Referenztabelle ein. Alternativ können Sie aus der Liste auch eine vorhandene Referenztabelle auswählen, der die LDAP-Daten hinzugefügt werden sollen.
b. Das Kontrollkästchen **Zuordnung von Gruppen generieren** ist standardmäßig inaktiviert. Wenn Sie es aktivieren, werden Daten an ein Referenzsetformat gesendet, um die QRadar-Suche zu verbessern, was sich jedoch auf die Leistung auswirken kann.
c. Geben Sie im Bereich **Lebensdauer** an, wie lange die Daten in der Referenztabelle gespeichert werden sollen. Standardmäßig verfallen die hinzugefügten Daten nie. Bei Überschreiten der Lebensdauer wird das Ereignis *ReferenceDataExpiry* ausgelöst.

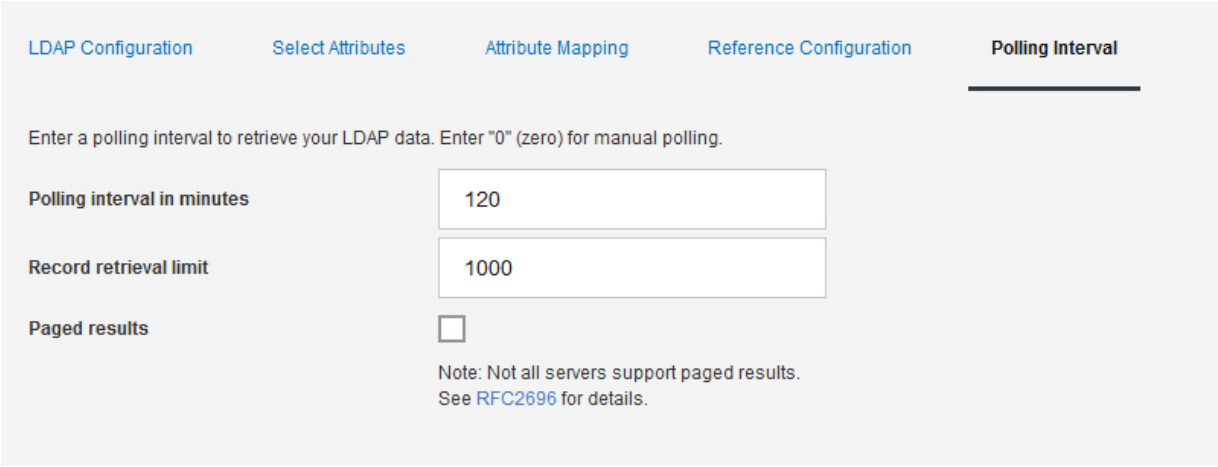
   Anmerkung: Wenn Daten einer vorhandenen Referenzzuordnung von Zuordnungen hinzugefügt werden, übernimmt die App die für diese Zuordnung ursprünglich festgelegten "Time to Live"-Parameter. Diese Parameter können auf der Registerkarte **Referenzkonfiguration** nicht überschrieben werden.



12. Konfigurieren Sie auf der Registerkarte **Abfrage** die Abfrage der Daten vom LDAP-Server.
    a. Geben Sie im Feld **Abfrageintervall in Minuten** an, wie oft die App Daten vom LDAP-Server abfragen soll.

       Anmerkung: Das kürzeste Abfrageintervall beträgt `120` Minuten. Darunter können Sie das Abfrageintervall nur noch auf Null setzen. In diesem Fall müssen Sie die Abfrage manuell mit der Abfrageoption im Feed ausführen.
    b. Geben Sie im Feld **Grenzwert für Datensatzabruf** die Anzahl der Datensätze ein, die die Abfrage zurückgeben kann. Standardmäßig werden 100.000 Datensätze zurückgegeben. Der maximale Wert ist 200.000.
    c. Optional: Das Kontrollkästchen **Seitenweise angezeigte Ergebnisse** ist standardmäßig aktiviert, um eine Begrenzung der Anzahl Datensätze, die der LDAP-Server für jede Abfrage zurückgibt, zu verhindern.

       Anmerkung: Ausgerufene Ergebnisse werden nicht von allen LDAP-Servern unterstützt.



13. Klicken Sie auf **Speichern**.

UBA-Einstellungen konfigurieren

Die IBM QRadar-App "User Behavior Analytics" (UBA) muss zunächst konfiguriert werden, damit sie Daten anzeigt.

Berechtigungstoken in QRadar-Einstellungen konfigurieren

Um die Informationen in der IBM QRadar-App 'User Behavior Analytics' (UBA) anzeigen zu können, müssen Sie in den UBA-Einstellungen ein UBA-Berechtigungstoken konfigurieren.

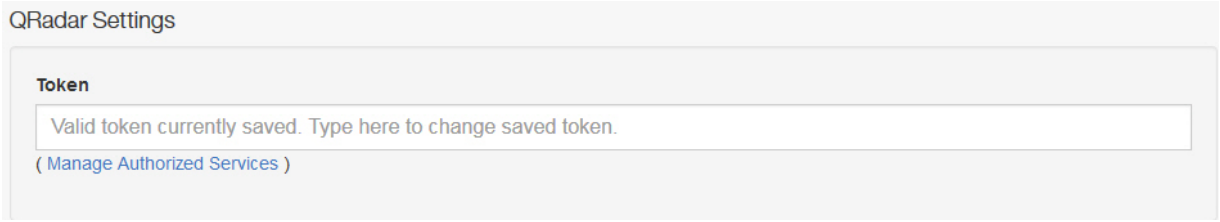
Informationen zu diesem Vorgang

Achtung: Aufgrund eingeschränkter Administratorfunktionen können Administratoren für QRadar on Cloud keine Token für autorisierte Services für QRadar-Apps erstellen. Wenn Sie Kunde von QRadar on Cloud sind, wenden Sie sich an die Kundenunterstützung, damit ein Token für autorisierte Services für Sie erstellt wird.

Führen Sie die folgenden Schritte aus, um ein Berechtigungstoken zu erstellen. Speichern Sie die Konfiguration erst, wenn Sie alle UBA-Einstellungen konfiguriert haben.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü ( ) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **UBA Settings** (UBA-Einstellungen).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **UBA Settings** (Plug-ins > Benutzeranalyse > UBA-Einstellungen).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **UBA Settings** (Apps > Benutzeranalyse > UBA-Einstellungen).
3. Klicken Sie im Abschnitt für die QRadar-Einstellungen auf den Link **Autorisierte Services verwalten**.



4. Klicken Sie auf **Autorisierten Service hinzufügen**
5. Geben Sie im Feld **Servicename** den Namen UBA ein.
6. Wählen Sie in der Liste **Benutzerrolle** die Rolle **Verwaltung** aus.
7. Wählen Sie in der Liste **Sicherheitsprofil** das Sicherheitsprofil aus, das dem autorisierten Service zugewiesen werden soll. Über das Sicherheitsprofil werden die Netze und die Protokollquellen vorgegeben, auf die dieser Service in der QRadar-Benutzerschnittstelle zugreifen kann.
8. Geben Sie in der Liste **Ablaufdatum** das Datum an, an dem der Service ablaufen soll, bzw. wählen Sie ein Datum aus. Ist kein Ablaufdatum erforderlich, wählen Sie **Kein Ablaufdatum** aus.
9. Klicken Sie auf **Service erstellen**.
10. Klicken Sie auf die Zeile mit dem von Ihnen erstellten UBA-Service, wählen Sie im Feld **Ausgewähltes Token** der Menüleiste die Tokenzeichenfolge aus und kopieren Sie sie.
11. Gehen Sie zurück in den Abschnitt mit den **QRadar-Einstellungen** und fügen Sie die Tokenzeichenfolge für den autorisierten Service im Feld **Token** ein.

Nächste Schritte

„Einstellungen für die Inhaltspakete konfigurieren”

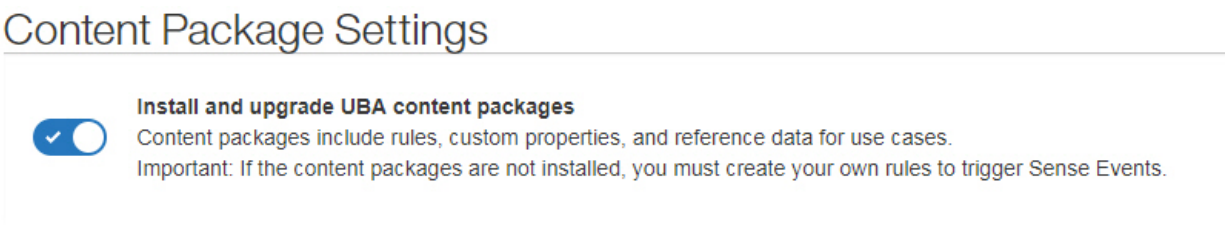
Einstellungen für die Inhaltspakete konfigurieren

Damit Sie Informationen in der IBM QRadar-App 'User Behavior Analytics' (UBA) anzeigen können, müssen die Einstellungen des Inhaltspakets konfiguriert werden.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **UBA Settings** (UBA-Einstellungen).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **UBA Settings** (Plug-ins > Benutzeranalyse > UBA-Einstellungen).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **UBA Settings** (Apps > Benutzeranalyse > UBA-Einstellungen).
3. Im Abschnitt 'Content Package Settings' (Einstellungen für Inhaltspakete) ist das Kontrollkästchen **Install and upgrade UBA content packages** (UBA-Inhaltspakete installieren und aktualisieren) standardmäßig ausgewählt. Wenn Sie die UBA-Inhaltspakete nicht installieren möchten, heben Sie die Auswahl des Kontrollkästchens auf und speichern die Konfiguration. Wenn Sie sich dazu entscheiden, die UBA-Inhaltspakete nicht zu installieren, müssen Sie Ihre eigenen Regeln zum Auslösen von Prüfereignissen erstellen, die Ereignisse an UBA senden.

   Anmerkung: Wenn Sie das Kontrollkästchen **Install and upgrade UBA content packages** abwählen, die Konfiguration speichern und anschließend zur Seite mit den UBA-Einstellungen zurückkehren und dort entscheiden, das Kontrollkästchen auszuwählen und die Konfiguration zu speichern, werden die Inhalte installiert und aktualisiert.



Nächste Schritte

„Anwendungseinstellungen konfigurieren”

Anwendungseinstellungen konfigurieren

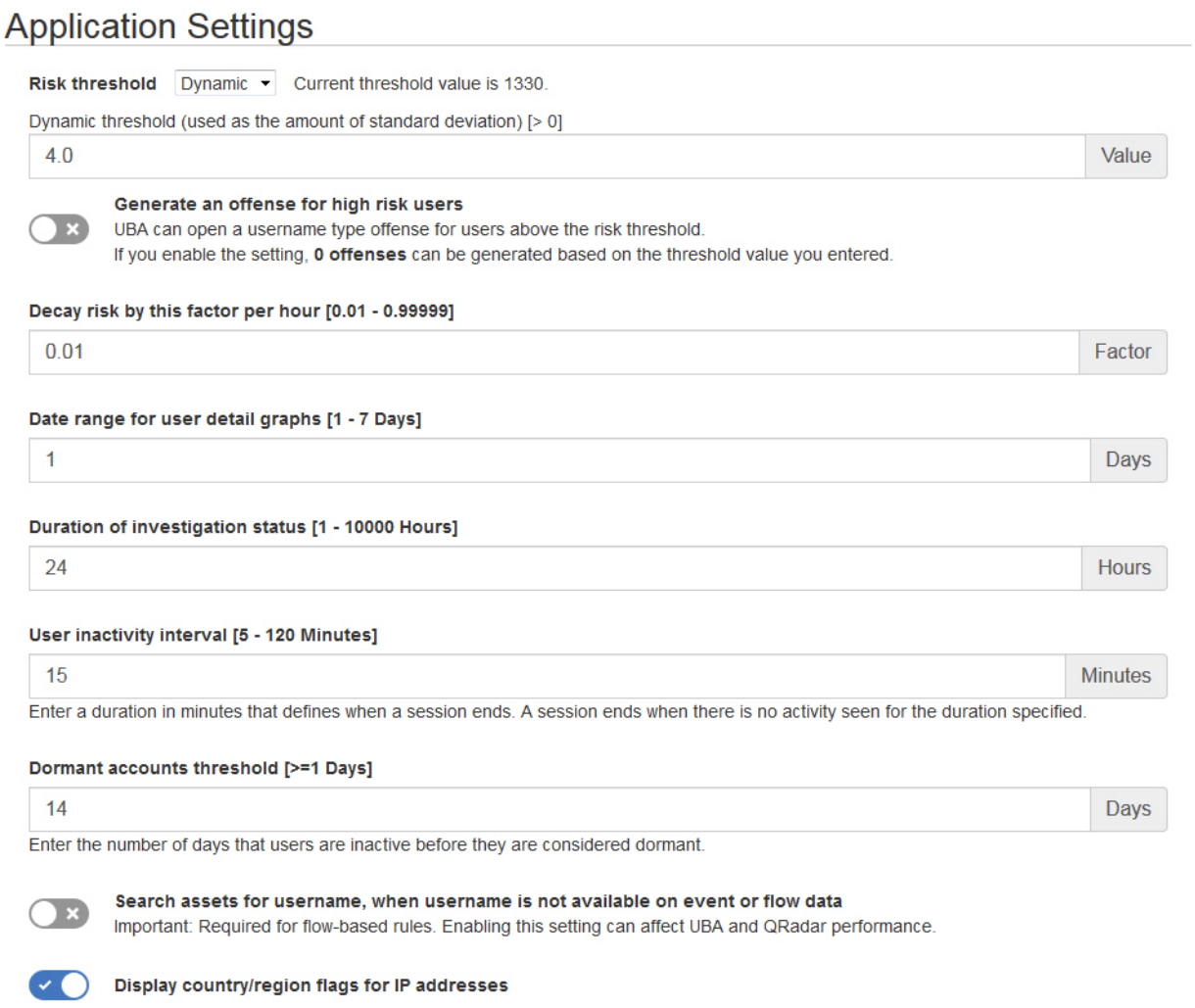
Die IBM QRadar-App "User Behavior Analytics" (UBA) muss zunächst konfiguriert werden, damit sie Daten anzeigt.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **UBA Settings** (UBA-Einstellungen).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **UBA Settings** (Plug-ins > Benutzeranalyse > UBA-Einstellungen).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **UBA Settings** (Apps > Benutzeranalyse > UBA-Einstellungen).
3. Konfigurieren Sie im Bereich "Anwendungseinstellungen" die folgenden Einstellungen:

Option	Bezeichnung
Risk threshold (Risikoschwellenwert)	Gibt an, wie hoch die Risikobewertung eines Benutzers sein muss, bevor ein Angriff gegen den Benutzer ausgelöst wird. Bei einer *Risikobewertung* handelt es sich um die Summe aller Risikoereignisse, die von UBA-Regeln erkannt wurden. Wählen Sie eine der folgenden Optionen aus: • **Dynamic** (Dynamisch): Der Standardwert ist 4,0. Je höher der Wert ist, desto höher ist der dynamische Schwellenwert, was zu weniger Verstößen führt. Sie sollten **Generate an offense for high risk users** (Verstoß für Benutzer mit hohem Risiko generieren) ausschalten, bis die Einstellungen mindestens einen Tag ausgeführt wurden. Der Wert des dynamischen Schwellenwerts wird stündlich auf Basis der Risikobewertungsverteilung im System aktualisiert. Sie können festlegen, ob Sie die Einstellung auf Basis der Anzahl an Verstößen aktivieren möchten, die ausgelöst werden könnten. In den Tipps finden Sie weitere Informationen. **Anmerkung:** Wenn die Bewertungen nicht vielfältig genug sind, wird die Risikobewertung auf +10 ausgehend vom Benutzer mit dem höchsten Risiko gesetzt. Dieser Wert bleibt bestehen, um zu vermeiden, dass unnötigerweise eine große Zahl von Verstößen generiert wird. • **Static** (Statisch): Der Standardwert ist 100.000. Es ist standardmäßig ein hoher Wert eingestellt, um zu verhindern, dass Angriffe ausgelöst werden, bevor die Umgebung analysiert wurde. Sie können **Generate an offense for high risk users** (Verstoß für Benutzer mit hohem Risiko generieren) aktivieren, um einen Verstoß mit einem Benutzernamenstyp für Benutzer zu öffnen, die oberhalb des Risikoschwellenwerts liegen. Sie können festlegen, ob Sie die Einstellung auf Basis der Anzahl an Verstößen aktivieren möchten, die ausgelöst werden könnten. **Tipp:** Es wird empfohlen, bei der UBA-Konfiguration den Standardwert beizubehalten. Beobachten Sie mindestens einen Tag lang, welcher Typ von Bewertungen mit der Standardeinstellung zurückgegeben wird. Überprüfen Sie nach einigen Tagen die Ergebnisse auf dem Dashboard, um ein Muster zu erkennen. Danach können Sie den Schwellenwert anpassen. Wenn Sie beispielsweise sehen, dass es ein oder zwei Personen mit Bewertungen im 500er Bereich gibt, die meisten Bewertungen aber im 100er Bereich liegen, sollten Sie einen Schwellenwert von 200 oder 300 einstellen. Für Ihre Umgebung ist also vielleicht eine Bewertung von 100 "normal" und Sie sollten bei allen höheren Bewertungen Überprüfungen durchführen.
Decay risk by this factor per hour (Risiko um diesen Faktor pro Stunde vermindern)	Die Risikominderung gibt den Prozentsatz an, um den sich die Risikobewertung stündlich verringert. Der Standardwert ist 0,5. **Anmerkung:** Je höher der Wert, desto schneller verringert sich die Risikobewertung; je niedriger der Wert, desto langsamer verringert sich die Risikobewertung.
Datumsbereich für Diagramme mit Benutzerdetails	Der Datumsbereich der Diagramme mit Benutzerdetails auf der Seite **Benutzerdetails**. Der Standardwert ist 1.
Duration of investigation status (Dauer des Untersuchungsstatus)	Die Anzahl Stunden (1 - 10.000), die einer Untersuchung bis zu ihrem Abschluss zugewiesen wird.
User inactivity interval (Benutzerinaktivitätsintervall)	Im Fenster 'User Details' (Benutzerdetails) wird eine Zeitleiste mit nach Sitzungen gruppierter Aktivität angezeigt. Ist ein Benutzer die im Feld **User inactivity interval** eingegebene Zeitdauer inaktiv, wird die Sitzung beendet. Der Standardwert beträgt 15 Minuten.
Schwellenwert für inaktives Konto	Die Anzahl der Tage, die Benutzer inaktiv sind, bevor sie als ruhend betrachtet werden. Der Standardwert ist 14 Tage. Weitere Informationen finden Sie im Abschnitt „Ruhende Konten” auf Seite 41.(Verfügbar in V3.2.0 und höher.)

Option	Bezeichnung
Search assets for username, when username is not available for event or flow data (Assets nach Benutzername durchsuchen, wenn für Ereignis- oder Flussdaten kein Benutzername verfügbar ist)	Aktivieren Sie das Kontrollkästchen, um in der Assettabelle nach Benutzernamen zu suchen. Die UBA-App verwendet Assets für die Suche nach einem Benutzer für eine IP-Adresse, wenn in einem Ereignis kein Benutzer aufgelistet ist. **Wichtig:** Diese Funktion könnte Leistungsprobleme in der UBA-App und Ihrem QRadar-System verursachen. **Tipp:** Falls der Schwellenwert für das Abfragezeitlimit überschritten wird, gibt die App keine Daten zurück. Wenn Sie eine Fehlernachricht im UBA-Dashboard erhalten, heben Sie die Markierung des Kontrollkästchens auf und klicken Sie auf **Aktualisieren**.
Display country/region flags for IP addresses (Landes-/Regionsflaggen für IP-Adressen anzeigen)	Inaktivieren Sie das Kontrollkästchen, wenn keine Landes- und Regionsflaggen für IP-Adressen angezeigt werden sollen.



Nächste Schritte

„Import von Benutzerdaten und Benutzerverbindungen konfigurieren"

Import von Benutzerdaten und Benutzerverbindungen konfigurieren

Zur Anzeige von Informationen in der IBM QRadar-App 'User Behavior Analytics' (UBA) können Sie Benutzerdaten aus einer Referenztabelle importieren.

Vorbereitende Schritte

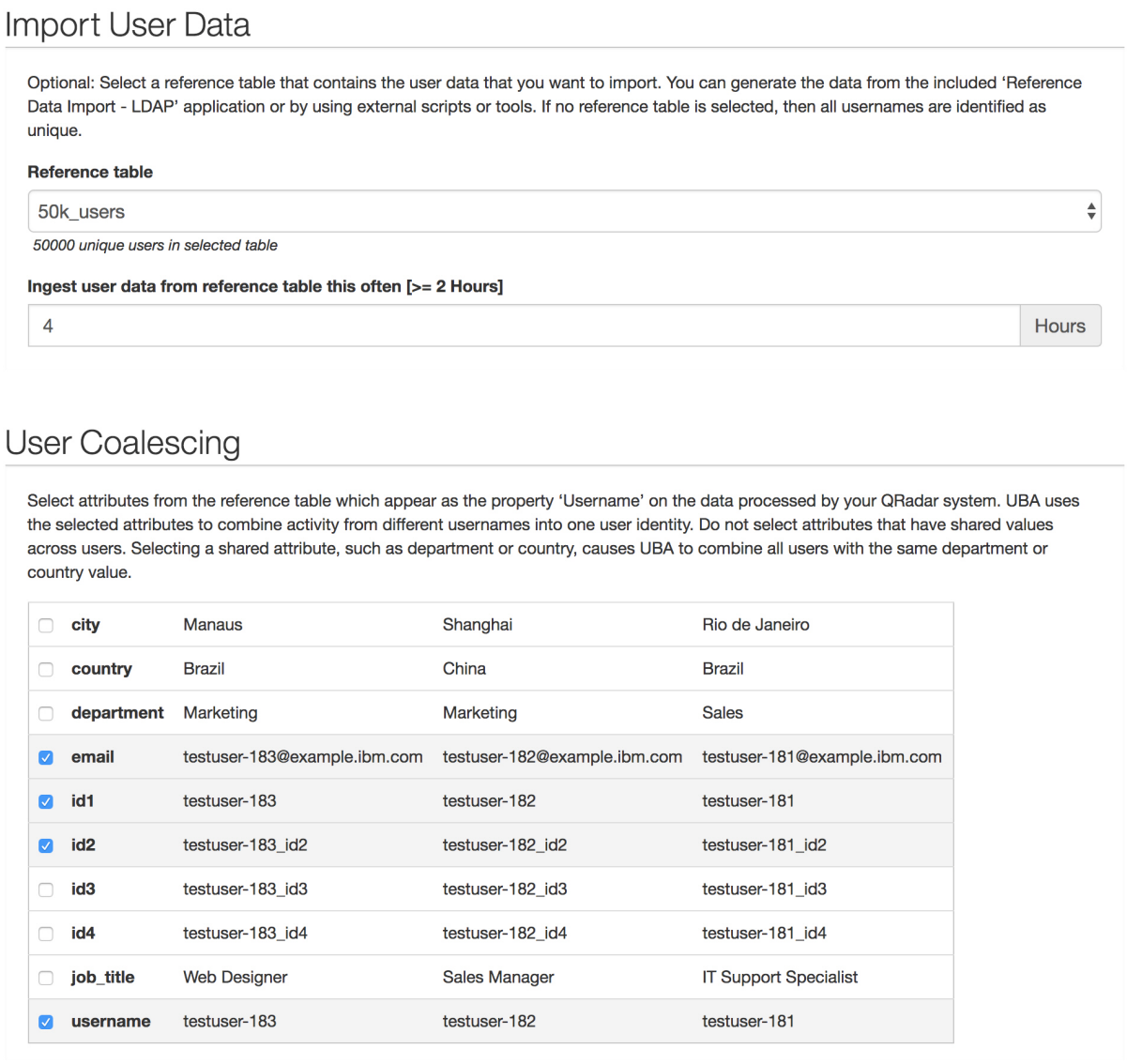
Führen Sie die Anweisungen für „Anwendungseinstellungen konfigurieren" auf Seite 30 aus.

Informationen zu diesem Vorgang

Der Import von Benutzerdaten und die Benutzerverbindungen sind optional.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **UBA Settings** (UBA-Einstellungen).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **UBA Settings** (Plug-ins > Benutzeranalyse > UBA-Einstellungen).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **UBA Settings** (Apps > Benutzeranalyse > UBA-Einstellungen).
3. Wählen Sie im Abschnitt für den Benutzerdatenimport eine **Referenztabelle** aus.
4. Geben Sie die Anzahl Stunden ein, um festzulegen, wie oft Daten in die Referenztabelle aufgenommen werden sollen.
5. Wählen Sie im Abschnitt für Benutzerverbindungen die Attribute aus, die aus der ausgewählten Referenztabelle extrahiert und von Ihrem QRadar-System als "Benutzername" angezeigt werden. Die Risikobewertungen dieser Kennungen werden hinzugefügt und mit der primären Kennung verknüpft. Wählen Sie keine Attribute aus, deren Werte für mehrere Benutzer gemeinsam genutzt werden. Wählen Sie beispielsweise bei vielen Personen in der gleichen Abteilung nicht den Benutzernamen "Abteilung" aus. Durch die Auswahl eines gemeinsam genutzten Attributs wie "Abteilung" oder "Land" verbindet UBA alle Benutzer mit dem gleichen Wert für die Abteilung bzw. das Land.



Nächste Schritte

„Anzeigeattribute konfigurieren"

Anzeigeattribute konfigurieren

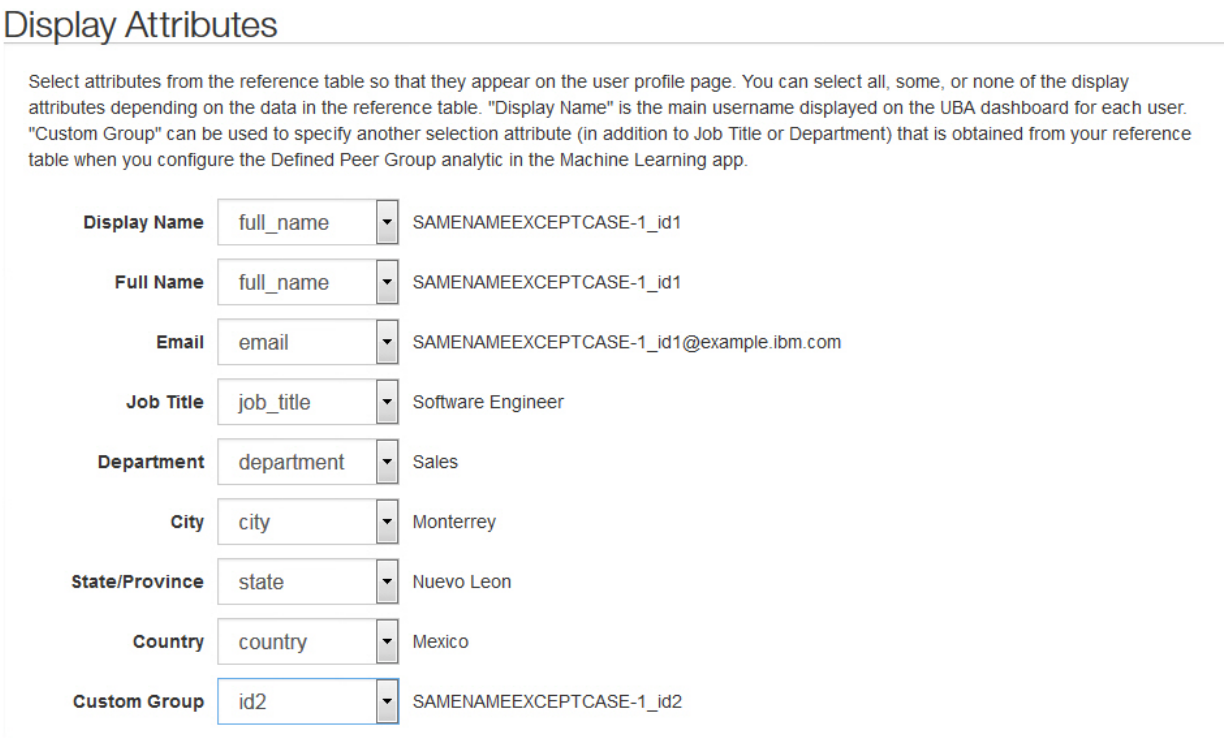
Zur Anzeige von Informationen in der IBM QRadar-App 'User Behavior Analytics' (UBA) können Sie Attribute aus der Referenztabelle auswählen, die Sie auf der Seite **User Details** (Benutzerdetails) anzeigen möchten.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **UBA Settings** (UBA-Einstellungen).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **UBA Settings** (Plug-ins > Benutzeranalyse > UBA-Einstellungen).

- Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **UBA Settings** (Apps > Benutzeranalyse > UBA-Einstellungen).

3. Wählen Sie im Abschnitt für die Attributanzeige die Attribute aus, die auf der Seite **Benutzerdetails** angezeigt werden sollen.



4. Klicken Sie auf **Konfiguration speichern**.

5 Verwaltung

Berechtigungen für die QRadar-App UBA verwalten

Administratoren konfigurieren und verwalten Benutzerkonten mithilfe der Funktion "Benutzerrollenverwaltung" in IBM QRadar. Als Administrator müssen Sie die Berechtigungen "Benutzeranalyse", "Angriffe" und "Protokollaktivität" für jede Benutzerrolle aktivieren, die zur Verwendung der QRadar-App UBA berechtigt ist.

Informationen zu diesem Vorgang

Nach der Installation der QRadar-App UBA müssen die Berechtigungen **Benutzeranalyse**, **Angriffe** und **Protokollaktivität** für die Benutzerrollen aktiviert werden, die Benutzern zugewiesen werden, welche die QRadar-App UBA verwenden möchten.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü () und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie im Abschnitt 'Systemkonfiguration' auf **Benutzerverwaltung** und anschließend auf das Symbol für **Benutzerrollen**.
3. Wählen Sie eine vorhandene Benutzerrolle aus oder erstellen Sie eine neue Rolle.
4. Aktivieren Sie folgende Kontrollkästchen, um die Berechtigungen zur Rolle hinzuzufügen.
   - **Benutzeranalyse**
   - **Angriffe**
   - **Protokollaktivität**
5. Klicken Sie auf **Speichern**.

Beobachtungslisten erstellen

Sie können einen Benutzer zu einer neuen oder vorhandenen Beobachtungsliste hinzufügen.

Informationen zu diesem Vorgang

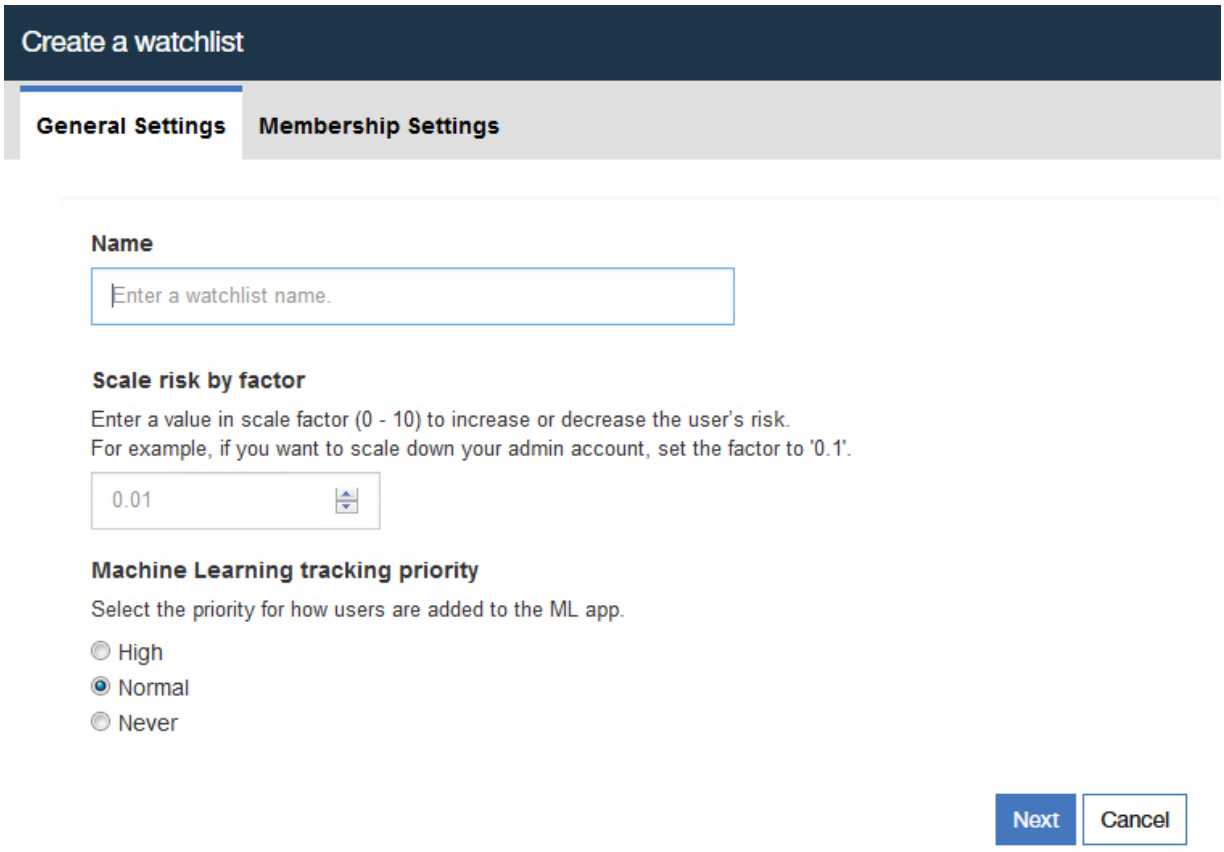
Sie können einen Benutzer im UBA-**Dashboard**, auf der Seite **User Details** (Benutzerdetails) oder auf der Seite **Search Results** (Suchergebnisse) zu einer neuen oder vorhandenen Beobachtungsliste hinzufügen. Ein einzelner Benutzer kann Mitglied mehrerer Beobachtungslisten sein.

Vorgehensweise

1. Klicken Sie im **UBA Dashboard** oder auf der Seite **User Details** (Benutzerdetails) auf das Symbol **Watchlist** (Beobachtungsliste)  .
2. Wählen Sie **Create new watchlist** (Neue Beobachtungsliste erstellen) im Menü aus. Klicken Sie auf **Zur Beobachtungsliste hinzufügen**, um einen Benutzer zu einer vorhandenen Beobachtungsliste hinzuzufügen.
3. Geben Sie auf der Registerkarte **General Settings** (Allgemeine Einstellungen) einen Namen für die Beobachtungsliste ein.

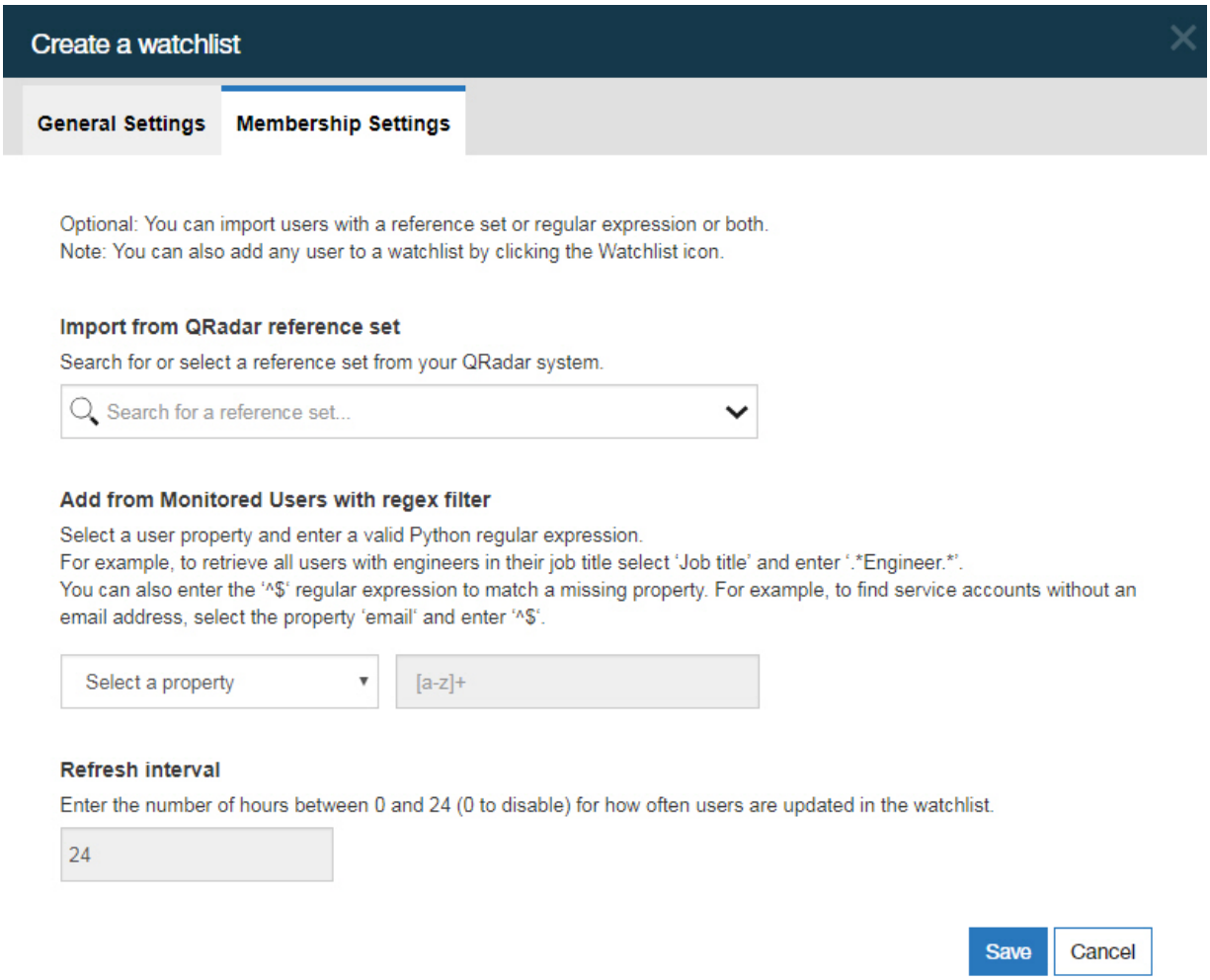
4. Sie können die Risikobewertung eines Benutzers künstlich erhöhen oder senken, indem Sie den Wert im Feld **Scale risk by factor** (Risiko nach Faktor skalieren) ändern. Der Standardfaktor ist '1' und bedeutet, dass die Risikobewertung unverändert bleibt.

   Anmerkung: Wenn ein Benutzer in mehreren Beobachtungslisten enthalten ist, gilt der größte Skalierungsfaktor.
5. Wählen Sie im Abschnitt **Machine Learning tracking priority** (Machine Learning-Überwachungspriorität) die Priorität aus, um anzugeben, wie Benutzer von der Machine Learning-Analyse überwacht werden.
   - High (Hoch) - Benutzer werden immer überwacht, bis zu den maximalen Benutzern pro Machine Learning-Analyse.
   - Normal - Benutzer werden nach dem größten Risiko überwacht, nachdem alle Benutzer mit hoher Priorität eingeschlossen wurden.
   - Never (Nie) - Benutzer werden nicht überwacht.
6. Klicken Sie auf **Next** (Weiter).



7. Auf der Registerkarte **Membership Settings** (Zugehörigkeitseinstellungen) können Sie die Beobachtungsliste automatisch mit Benutzern aus einem Referenzset und/oder einem regulären Ausdruck füllen.
8. Optional: Suchen Sie im Feld **Import from QRadar reference set** (Aus QRadar-Referenzset importieren) nach einem Referenzset oder klicken Sie auf ein Referenzset in der Liste, um alle Einträge aus dem Referenzset zu importieren. Hinweis: Die Liste kann Referenzsets enthalten, für die es keine Benutzernamen gibt. Klicken Sie nach Auswahl eines Referenzsets zur Überprüfung auf den Link.
9. Optional: Sie können im Feld **Add from Monitored Users with regex filter** (Mit Regex-Filter aus überwachten Benutzern hinzufügen) eine Benutzereigenschaft auswählen und einen gültigen regulären Python-Ausdruck eingeben, um Benutzer auszuwählen, die bereits in der UBA-Datenbank enthalten sind.

10. Geben Sie im Feld **Refresh interval** (Aktualisierungsintervall) an, in welchem Stundenintervall die Benutzerliste aktualisiert werden soll. Wenn Sie beispielsweise 10 eingeben, wird die Benutzerliste alle 10 Stunden aktualisiert. Wenn Sie das Feld **Refresh interval** auf den Wert 0 (null) setzen, können Sie die Beobachtungsliste manuell aktualisieren, indem Sie auf **Refresh** (Aktualisieren) klicken.
11. Klicken Sie auf **Save** (Speichern).



Whitelist für vertrauenswürdige Benutzer anzeigen

Sie können die Liste der vertrauenswürdigen Benutzer anzeigen, die in der Referenzsetverwaltungsliste in der Whitelist aufgeführt sind.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie im Abschnitt "Systemkonfiguration" auf **Referenzsetverwaltung**.
3. Wählen Sie im Fenster **Referenzsetverwaltung** das Referenzset **UBA : Trusted Usernames** (UBA: Vertrauenswürdige Benutzernamen) aus.
4. Klicken Sie auf **Inhalt anzeigen**.

Netzüberwachungstools verwalten

Sie können Netzüberwachungstools für die IBM QRadar-App "User Behavior Analytics" (UBA) verwalten.

Informationen zu diesem Vorgang

Wenn Sie die Verwendung von Netzerfassungs-, Überwachungs- oder Analyseprogrammen überwachen möchten, müssen Sie sicherstellen, dass die Programme im Referenzset "UBA : Network Capture, Monitoring and Analysis Program Filenames" (UBA: Netzerfassungs-, Überwachungs- und Analyseprogrammdateinamen) aufgeführt sind. Danach müssen Sie die Regel **UBA : Network Capture, Monitoring and Analysis Program Filenames** aktivieren.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie im Abschnitt "Systemkonfiguration" auf **Referenzsetverwaltung**.
3. Wählen Sie im Fenster **Referenzsetverwaltung** das Referenzset **UBA : Network Capture, Monitoring and Analysis Program Filenames** aus.
4. Klicken Sie auf **Inhalt anzeigen**.
5. Fügen Sie eine zu verwaltende Anwendung hinzu, indem Sie auf **Hinzufügen** klicken und die Werte im Feld eingeben.
6. Entfernen Sie eine Anwendung, indem Sie sie auswählen und auf **Löschen** klicken.

Nächste Schritte

Aktivieren Sie die Regel **UBA : Network Capture, Monitoring and Analysis Program Filenames**.

Eingeschränkte Programme verwalten

Sie können eingeschränkte Programme für die IBM QRadar-App "User Behavior Analytics" (UBA) verwalten.

Informationen zu diesem Vorgang

Wenn Sie die Nutzung bestimmter Anwendungen überwachen möchten, geben Sie im Referenzset "UBA : Restricted Program Filenames" (UBA: Eingeschränkte Programmdateinamen) die Anwendungen ein, die überwacht werden sollen. Danach müssen Sie die Regel "UBA : Restricted Program Filenames" aktivieren.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie im Abschnitt "Systemkonfiguration" auf **Referenzsetverwaltung**.
3. Wählen Sie im Fenster **Referenzsetverwaltung** das Referenzset **UBA : Restricted Program Filenames** aus.
4. Klicken Sie auf **Inhalt anzeigen**.
5. Fügen Sie eine zu verwaltende Anwendung hinzu, indem Sie auf **Hinzufügen** klicken und die Werte im Feld eingeben.

6. Entfernen Sie eine Anwendung, indem Sie sie auswählen und auf **Löschen** klicken.

Nächste Schritte

Aktivieren Sie die Regel **UBA : Restricted Program Filenames**.

Protokollquellen zur Gruppe vertrauenswürdiger Protokollquellen hinzufügen

Wenn bestimmte Protokollquellen nicht von der UBA-App überwacht und gemeldet werden sollen, können Sie diese zur **UBA : Trusted Log Source Group** (UBA: Gruppe vertrauenswürdiger Protokollquellen) hinzufügen. Protokollquellen, die zur Gruppe hinzugefügt wurden, werden nicht mehr von der UBA-App überwacht.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Protokollquellen**.
3. Klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie die allgemeinen Parameter für Ihre Protokollquelle.
5. Konfigurieren Sie die protokollspezifischen Parameter für Ihre Protokollquelle.
6. Aktivieren Sie das Kontrollkästchen **UBA : Trusted Log Source Group**.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf der Registerkarte **Verwaltung** auf **Änderungen implementieren**.

Ruhende Konten

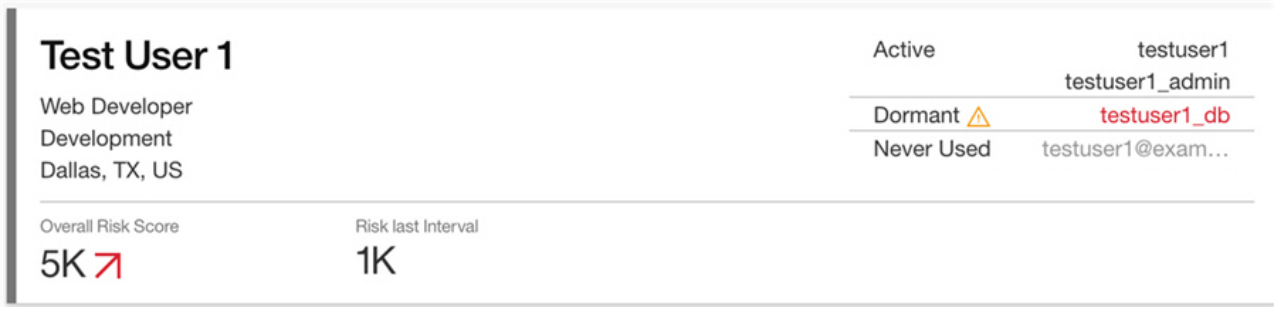
Sie können Benutzer in Ihrem System anzeigen, deren Konten ruhend oder aktiv sind oder nie verwendet wurden.

Ruhende Konten auf der Seite mit den Benutzerdetails anzeigen

In V3.2.0 und höher können Sie den Status der Konten anzeigen, die dem ausgewählten Benutzer auf der Seite mit den Benutzerdetails zugeordnet sind.

Benutzerkontostatus	Beschreibung
Aktiv	Ein Konto, für das UBA Ereignisse aus einer QRadar-Protokollquelle innerhalb des konfigurierten Zeitraums mit dem Schwellenwert für ein ruhendes Konto erkannt hat.
Ruhend	Ein Konto, für das UBA mindestens ein Ereignis in der Vergangenheit erkannt hat, aber keine neuen Ereignisse während des Zeitraums mit dem Schwellenwert für ein ruhendes Konto ermitteln konnte.

Benutzerkontostatus	Beschreibung
Nie verwendet	Ein Konto, für das UBA nie ein Ereignis mit diesem Benutzernamen in einer QRadar-Protokollquelle erkannt hat. Konten, die als "Nie verwendet" angegeben sind, können durch die folgenden Aktivitäten verursacht werden: • Konten, die nie von einer QRadar-Protokollquelle für das Konto mit dem zugeordneten Benutzernamen protokolliert wurden. • Das Ereignis trat auf, bevor UBA V3.2.0 installiert wurde. Hinweis: Bei der ersten Installation der UBA-App werden nur Ereignisse analysiert, die in der letzten Stunde auftraten, um festzustellen, wann zuletzt auf ein Konto zugegriffen wurde. Nach der Anfangsanalyse werden durch UBA Ereignisse abgefragt, die zwischen den Ausführungen der Hintergrundtask auftraten, mit der die Nutzung des Kontos überwacht wird. Hinweis: Konten, die als "Nie verwendet" kategorisiert sind, wurden wahrscheinlich aus der LDAP-App importiert.



Beobachtungsliste 'Users with Dormant Accounts'

Die Beobachtungsliste 'Users with Dormant Accounts' (Benutzer mit ruhenden Konten) wird automatisch generiert, wenn Benutzerdaten von der UBA-App extrahiert werden. Sie können die Beobachtungsliste 'Users with Dormant Accounts' im UBA-Dashboard anzeigen.

Wenn Sie die Beobachtungsliste löschen, wird sie nicht automatisch erneut generiert. Falls Sie sie wieder erstellen müssen, wählen Sie das Referenzset **UBA : Dormant Accounts** auf der Registerkarte **Membership Settings** (Einstellungen der Mitgliedschaft) in der Anzeige 'Create a watchlist' (Beobachtungsliste erstellen) aus.

Schwellenwert für ruhende Konten konfigurieren

Die Standardeinstellung für den Schwellenwert von ruhenden Konten beträgt 14 Tage. Sie können die Anzahl der Tage ändern, die Benutzer inaktiv sein müssen, damit Sie im Abschnitt mit den Anwendungseinstellungen auf der Seite 'UBA Settings' (UBA-Einstellungen) als ruhend betrachtet werden (**Admin Settings** > **User Analytics** > **UBA Settings** (Verwaltungseinstellungen > Benutzeranalyse > UBA-Einstellungen).

Antworten auf ruhende Konten oder Benutzer

Sie können Antworten für ruhende Konten aus den bereitgestellten Regeln generieren. Sie können auch angepasste Antworten erstellen, indem Sie die Ereignisse verwenden, die mit der App ausgelöst werden.

Um die bereitgestellten Regeln zu verwenden, damit die Bewertung eines Benutzers erhöht wird, wenn ein ruhendes Konto wieder verwendet wird oder verwendet werden soll, stellen Sie sicher, dass die folgenden Regeln aktiviert sind:

- „UBA : Dormant Account Use Attempted” auf Seite 77
- „UBA : Dormant Account Used” auf Seite 76

Für die Erstellung von angepassten Antworten können Sie die folgenden generierten Ereignisse in einer Regel oder einer Abfrage verwenden:

- Dormant Account Found (QID 104000012)
- Dormant Account Used (QID 104000013)

Zugehörige Konzepte:

„UBA-Dashboard und Benutzerdetails” auf Seite 9
Die IBM QRadar-App 'User Behavior Analytics' (UBA) gibt Ihnen einen Überblick über die Risikodaten der Benutzer in Ihrem Netz.

Zugehörige Tasks:

„Anwendungseinstellungen konfigurieren” auf Seite 30
Die IBM QRadar-App "User Behavior Analytics" (UBA) muss zunächst konfiguriert werden, damit sie Daten anzeigt.

„Beobachtungslisten erstellen” auf Seite 37
Sie können einen Benutzer zu einer neuen oder vorhandenen Beobachtungsliste hinzufügen.

6 Optimierung

Indizes zur Leistungssteigerung aktivieren

Um die Leistung der IBM QRadar-App 'User Behavior Analytics' (UBA) zu verbessern, können Sie in IBM QRadar Indizes aktivieren.

Informationen zu diesem Vorgang

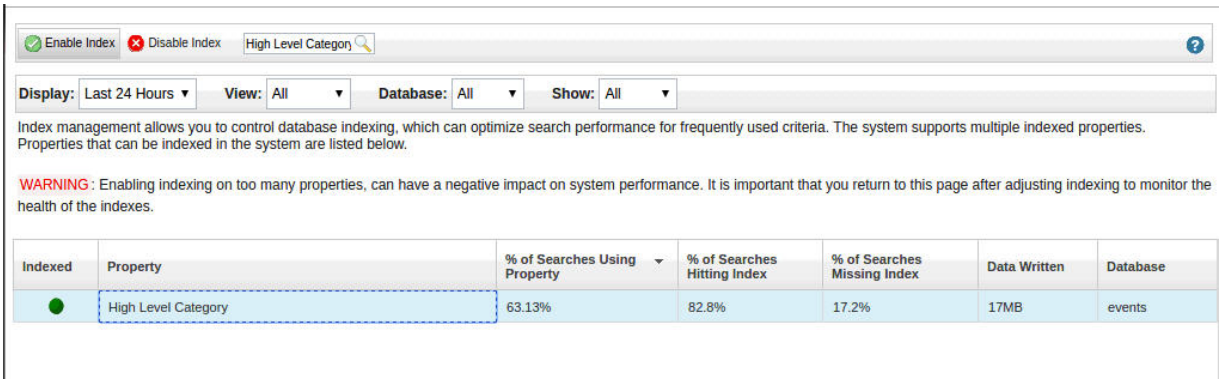
Zur Verbesserung der Suchgeschwindigkeit in IBM QRadar und in der UBA-App können Sie die Datenmenge einschränken, indem Sie die folgenden indizierten Felder zur Suchabfrage hinzufügen:

- High Level Category
- Low Level Category
- senseValue
- senseOverallScore
- Username

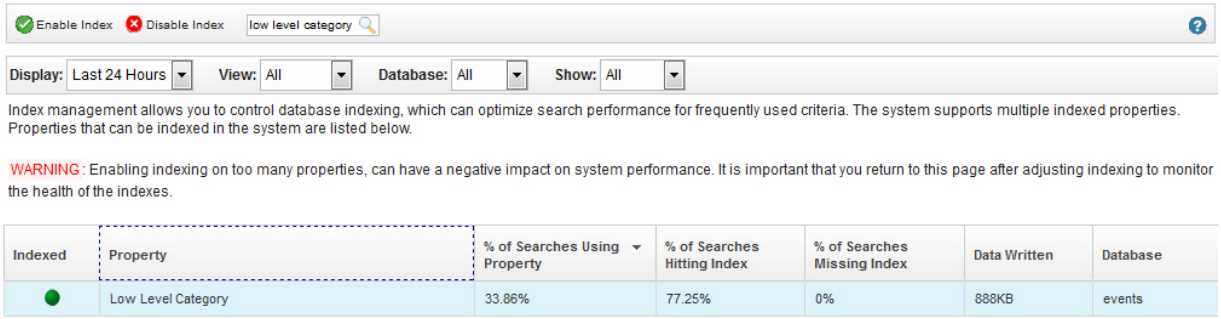
Weitere Informationen zur Indizierung finden Sie im IBM Knowledge Center unter https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_index_mgmt.html.

Vorgehensweise

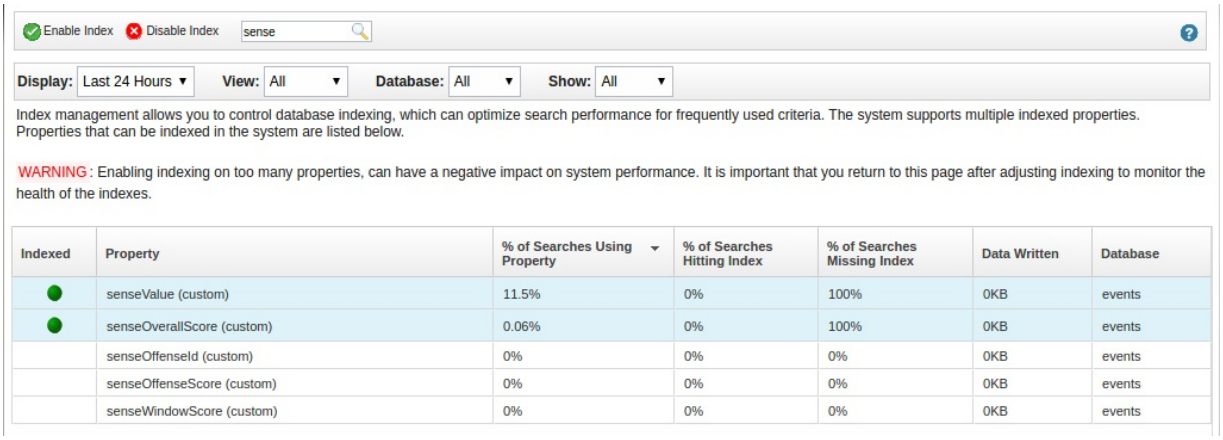
1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie im Abschnitt für die Systemkonfiguration auf das Symbol **Indexverwaltung**.
3. Geben Sie im Suchfeld auf der Seite "Index Management" (Indexverwaltung) `High Level Category` (Übergeordnete Kategorie) ein.
4. Wählen Sie **High Level Category** (Übergeordnete Kategorie) aus und klicken Sie auf **Enable Index** (Index aktivieren).



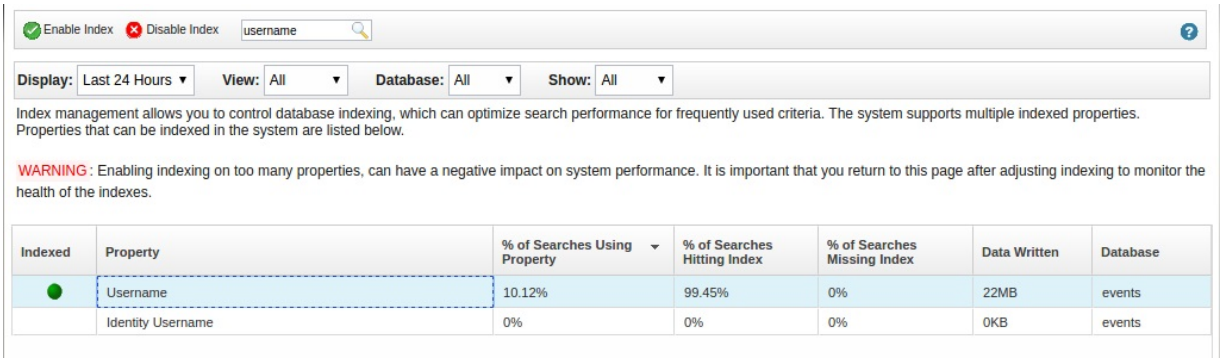
5. Klicken Sie auf **Speichern**.
6. Wählen Sie **Low Level Category** (Untergeordnete Kategorie) aus und klicken Sie auf **Enable Index** (Index aktivieren).



7. Klicken Sie auf **Speichern**.
8. Geben Sie im Suchfeld auf der Seite "Index Management" (Indexverwaltung) `sense` ein.
9. Wählen Sie **senseValue** und **senseOverallScore** aus und klicken Sie auf **Enable Index** (Index aktivieren).



10. Klicken Sie auf **Speichern**.
11. Geben Sie im Suchfeld auf der Seite "Index Management" (Indexverwaltung) `username` (Benutzername) ein.
12. Wählen Sie **Username** (Benutzername) aus und klicken Sie auf **Enable Index** (Index aktivieren).



13. Klicken Sie auf **Speichern**.

Neue oder bestehende QRadar-Inhalte mit der UBA-App integrieren

Mithilfe des Regelassistenten in QRadar können Sie bestehende oder benutzerdefinierte QRadar-Regeln mit der UBA-App integrieren.

Informationen zu diesem Vorgang

Um Ihre spezifischen Anforderungen zu erfüllen, können Sie die in QRadar eingefügten Funktionen verwenden, indem Sie Ihre bestehenden QRadar-Regeln mit der UBA-App integrieren.

Einschränkung: Passen Sie Ihre Regeln nicht für die Verwendung der UBA- und Machine Learning-Referenzsets an. Ein Versuch, die Referenzsets in angepassten Regeln zu verwenden, kann zu Fehlern in der UBA-App führen.

Vorgehensweise

1. Erstellen Sie eine Kopie der bestehenden Regel. Dies verhindert, dass sich Aktualisierungen der Basisregel auf die in der neuen Regel durchgeführten Bearbeitungen auswirken.
2. Öffnen Sie die Regel im Regelassistenten und navigieren Sie zum Abschnitt für Regelantworten.
3. Aktivieren oder bearbeiten Sie die Option **Dispatch New Event** (Neues Ereignis versenden), indem Sie sicherstellen, dass der Text **Event Description** (Ereignisbeschreibung wie folgt formatiert ist: `senseValue=#,senseDesc='sometext',usecase_id='rule UUID'`
4. Setzen Sie **High-Level-Category** (Übergeordnete Kategorie) auf **Sense**.
5. Klicken Sie auf **Fertigstellen**, um die Änderungen zu speichern.

   Anmerkung: Wenn die Regel auf Flussdaten angewendet wird, müssen Sie die Option **Search assets for username, when username is not available for event or flow data** (Assets nach Benutzername durchsuchen, wenn für Ereignis- oder Flussdaten kein Benutzername verfügbar ist) aktivieren, damit Ereignisse ohne Benutzernamen versuchen können, nach der Benutzerzuordnung zu suchen.

Referenzsets

Die User Behavior Analytics-App und die Machine Learning-App benutzen Referenzsets, um Benutzerinformationen zu speichern. Einige Referenzset sind für die Verwendung durch Apps reserviert. Diese sollten Sie nicht ändern und nicht beim Erstellen von angepassten Regeln verwenden.

Referenzset, die angepasst werden können

Referenzset	Beschreibung
UBA : High Risk Users	Das Referenzset *UBA : High Risk Users* (Benutzer mit hohem Risiko) wird aus dem Wert von **Risk threshold to trigger offenses** (Risikoschwelle für Auslösung von Angriffen) auf der Seite **UBA Settings** (UBA-Einstellungen) erstellt. Die maximale Anzahl an Benutzern beträgt 10.000 und das Referenzset wird alle 5 erneut erstellt.
UBA : Trusted Usernames	Sie können dem Referenzset *UBA : Trusted Usernames* (Vertrauenswürdige Benutzernamen) Benutzernamen hinzufügen, es sollte aber nicht für Regeln oder Berichte verwendet werden. Für die Benutzer im Referenzset *UBA : Trusted Usernames* werden keine Verstöße generiert.
UBA : ML Always Tracked Watchlist	Das Referenzset *UBA : ML Always Tracked Watchlist* (Immer überwachte ML-Beobachtungsliste) wird aus den Benutzern erstellt, die mit **Track with Machine Learning** (Mit Machine Learning überwachen) im Abschnitt **Advanced Settings** (Erweiterte Einstellungen) auf der Seite **User Details** (Benutzerdetails) ausgewählt werden. Sie können dem Referenzset *UBA : ML Always Tracked Watchlist* Benutzernamen hinzufügen, es sollte aber nicht für Regeln oder Berichte verwendet werden.

Referenzset, die nicht angepasst werden können

Einschränkung: Die folgenden Referenzsets dürfen nicht geändert oder zum Erstellen von angepassten Regeln verwendet werden.

- UBA - Current ML Tracked Users

- UBA - Previous ML Tracked Users
- UBA - Current Abridged ML Tracked Users
- UBA - Previous Abridged ML Tracked Users
- UBA - Current Peer Group ML Tracked Users
- UBA - Previous Peer Group ML Tracked Users

7 Regeln und Möglichkeiten zur Optimierung für die UBA-App

Die IBM QRadar-App "User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Die App "User Behavior Analytics" (UBA) schließt Anwendungsfälle ein, die auf angepassten Regeln basieren. Anhand dieser Regeln werden Daten für das Dashboard der App UBA generiert. Ab Version 3.0.0 der UBA-App können Sie Regeln innerhalb der App anzeigen, filtern und optimieren. In Version 2.8.0 oder früher können die Regeln in der Benutzerverhaltensanalysegruppe in der Regelliste in QRadar angezeigt und geändert werden.

Anmerkung:

- Standardmäßig sind nicht alle Regeln der UBA-App aktiviert.
- Mindestens eine der Protokollquellen sollte Informationen für die spezifische UBA-Regel bereitstellen. Die Protokollquellen werden in keiner bestimmten Reihenfolge priorisiert.

Einschränkung: Passen Sie Ihre Regeln nicht für die Verwendung der UBA- und Machine Learning-Referenzsets an. Ein Versuch, die Referenzsets in angepassten Regeln zu verwenden, kann zu Fehlern in der UBA-App führen. Weitere Informationen finden Sie im Abschnitt „Referenzsets" auf Seite 47.

Weitere Informationen zum Arbeiten mit Regeln in QRadar finden Sie unter https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_rul_mgt.html

Seite 'Rules and Tuning'

Mit Version 3.0.0 der UBA-App wird die Seite **Rules and Tuning** (Regeln und Optimierung) eingeführt (**Admin Settings (Admin-Einstellungen)** > **User Analytics (Benutzeranalyse)** > **Rules and Tuning (Regeln und Optimierung)**).

Die Seite 'Rules and Tuning' enthält eine Liste aller Regeln, die es in der installierten Version der UBA-App gibt. Außerdem werden der aktuelle aktivierte Status und die zugehörigen Referenzsets angezeigt.

Auf der Seite **Rules and Tuning** haben Sie folgenden Möglichkeiten:

- Regeln aktivieren und inaktivieren
- Schnellzugriff auf den QRadar-Regelassistenten, um Regeln zu überprüfen oder zu bearbeiten
- Schnellzugriff auf Referenzsets, um deren Inhalt zu überprüfen oder zu bearbeiten
- Regeltabelle nach Kategorie, Status, Standardrisikobewertung, erforderliche Referenzsets und Inhaltsabhängigkeiten filtern
- Regeltabelle nach Regelname, Referenzset oder Status sortieren
- Elemente in der Tabelle oder in der Regelbeschreibungs-QuickInfo gefundene Wörter suchen
- Zugriff auf die Hilfedokumentation für einzelne Regeln

Zugriff und Authentifizierung

UBA : Bruteforce Authentication Attempts

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Bruteforce Authentication Attempts (Brute-Force-Authentifizierungsversuche)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Erkennt Authentifizierungsfehler aufgrund von Brute-Force-Attacke (horizontal und vertikal).

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungsfehler
- BB:UBA : Brute-Force-Authentifizierungsversuche erkennen (Horizontal)
- BB:UBA : Brute-Force-Authentifizierungsversuche erkennen (Vertikal)

Datenquellen

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT,Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform,Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security-.com SF-Sherlock, Epic SIEM,Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch,Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing

Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager,Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure,RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security,Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Executive Only Asset Accessed by Non-Executive User

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Executive Only Asset Accessed by Non-Executive User

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es wird erkannt, wenn ein Benutzer ohne Entscheidungsberechtigung sich bei einem Asset anmeldet, das Benutzern mit Entscheidungsberechtigung vorbehalten ist. Mit dieser Regel werden zwei leere Referenzsets importiert: "UBA : Executive Users" und "UBA : Executive Assets". Bearbeiten Sie die Referenzsets, um markierte Konten oder IP-Adressen aus Ihrer Umgebung hinzuzufügen oder zu entfernen. Aktivieren Sie diese Regel nach der Konfiguration der Referenzsets.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg
- BB:CategoryDefinition: Firewall oder ACL akzeptieren

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Executive Users" und "UBA : Executive Assets".

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTO-

Card CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : High Risk User Access to Critical Asset

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : High Risk User Access to Critical Asset (Benutzerzugriff mit hohem Risiko auf kritisches Asset)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt, wenn ein Benutzer in Vorfälle (Angriffe) mit Zugriff auf ein kritisches Asset involviert ist.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "Critical Assets".

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft

Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Multiple VPN Accounts Failed Login From Single IP

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Multiple VPN Accounts Failed Login From Single IP (Fehlgeschlagene Anmeldung mehrerer VPN-Konten aus einzelner IP)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Es werden Anmeldefehler mit dem VPN-Konto vom Referenzset "UBA : Multiple VPN Accounts Failed Login From Single IP" erkannt.

Regeln für die Unterstützung

- UBA : Populate Multiple VPN Accounts Failed Login From Single IP
- BB:UBA : VPN-Anmeldung fehlgeschlagen

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : Populate Multiple VPN Accounts Failed Login From Single IP"

Datenquellen

Cisco Adaptive Security Appliance (ASA)

UBA : Multiple VPN Accounts Logged In From Single IP

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Multiple VPN Accounts Logged In From Single IP (Mehrere VPN-Konten über eine IP angemeldet)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Es werden mehrere VPN-Benutzer zugeordnet, die aus der gleichen IP-Adresse stammen, und anschließend wird die Risikobewertung erhöht. Wenn die Regel erkennt, dass mehrere VPN-Benutzer mit der gleichen IP-Adresse vorhanden sind, wird die IP-Adresse der Regel "UBA : Multiple VPN Accounts Logged In From Single IP" hinzugefügt. Stellen Sie vor dem Aktivieren dieser Regel sicher, dass die Regel "UBA : Populate Multiple VPN Accounts Logged In From Single IP" aktiviert ist und das Referenzset "UBA : Multiple VPN Accounts Logged In From Single IP" Daten enthält.

Regeln für die Unterstützung

- UBA : Populate Multiple VPN Accounts Logged In from Single IP
- BB:UBA : VPN-Anmeldung erfolgreich

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : Populate Multiple VPN Accounts Logged In from Single IP"

Datenquellen

Cisco Adaptive Security Appliance (ASA)

UBA : Repeat Unauthorized Access

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Repeat Unauthorized Access (Wiederholter unbefugter Zugriff)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Zeigt an, dass wiederholte unbefugte Zugriffsaktivitäten gefunden wurden.

Unterstützte Regel

UBA : Unauthorized Access (Unbefugter Zugriff)

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : Unauthorized Access"

Datenquellen

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA SiteMinder, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus,Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform,Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

UBA : Unauthorized Access

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unauthorized Access (Unbefugter Zugriff)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Zeigt an, dass unbefugte Zugriffsaktivitäten gefunden wurden.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Zugriffsverweigerungen
- BB:UBA : Anwendungsverweigerungen

Datenquellen

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA SiteMinder, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus,Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP

Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform,Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

UBA: Unix/Linux System Accessed With Service or Machine Account

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA: Unix/Linux System Accessed With Service or Machine Account

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Erkennt interaktive Sitzungen (über GUI und CLI, lokale Anmeldung und Fernanmeldung), die von einem Service- oder Maschinenkonto in UNIX- und Linux-Servern gestartet werden. Konten und zulässige interaktive Sitzungen werden in den Referenzsets 'UBA : Service, Machine Account' und 'UBA : Allowed Interaction Session' aufgelistet. Bearbeiten Sie die Referenzsets, um zu markierende interaktive Sitzungen aus Ihrer Umgebung hinzuzufügen oder zu entfernen.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Firewall oder ACL akzeptieren
- BB:CategoryDefinition: Authentifizierungserfolg

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgenden Referenzsets hinzu: "UBA : Service, Machine Account" und "UBA : Allowed Interactive Session".

Datenquellen

Linux OS

UBA : User Access - Failed Access to Critical Assets

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Access - Failed Access to Critical Assets (Benutzerzugriff - fehlgeschlagener Zugriff auf kritische Assets)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Diese Regel erkennt Authentifizierungsfehler bei Systemen im Referenzset "Critical Assets" (Kritische Assets).

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungsfehler

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "Critical Assets".

Datenquellen

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT,Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform,Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM,Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch,Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Se-

cure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager,Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure,RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security,Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Access - First Access to Critical Assets

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Unterstützung für:

- UBA : User Access First Access to Critical Assets (Benutzerzugriff - Erster Zugriff auf kritisches Asset)
- UBA : Critical Systems Users Seen Update (Benutzer kritischer Systeme festgestellt - Aktualisierung)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

UBA : User Access First Access to Critical Assets: Zeigt an, dass der Benutzer zum ersten Mal auf ein kritisches Asset zugegriffen hat. Die Referenzsammlung "Critical Systems Users Seen" (Benutzer kritischer Systeme festgestellt) bestimmt die Lebensdauer einer Beobachtung. Standardmäßig erkennt diese Regel den ersten Zugriff in drei Monaten.

UBA : Critical Systems Users Seen Update: Aktualisiert den in der Referenzsammlung 'Critical Systems Users Seen' (Benutzer kritischer Systeme festgestellt) zuletzt festgestellten Wert für bereits vorhandene Ziel-IP/Benutzername-Übereinstimmungen.

Regeln für die Unterstützung

- BB:CategoryDefinition: Authentifizierungserfolg
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "Critical Assets".

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy

Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Access from Multiple Hosts

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : UBA : User Access from Multiple Hosts (Benutzerzugriff aus mehreren Hosts)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt, wenn ein einzelner Benutzer sich aus mehr als der zulässigen Anzahl von Geräten anmeldet.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600,

Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA: User Access to Internal Server From Jump Server

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA: User Access to Internal Server From Jump Server

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es wird erkannt, wenn ein Benutzer über einen Jump-Server auf die VPN-Server oder internen Server zugreift.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgenden Referenzsets hinzu: "UBA : Jump Servers" und "UBA : Internal Servers".

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cis-

co CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Access Login Anomaly

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Access Login Anomaly (Anmeldeanomalie bei Benutzerzugriff)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Zeigt ein Folge von Anmeldefehlern auf einem lokalen Asset an. Die Regel kann auch auf ein kompromittiertes Konto oder Seitenbewegungsaktivität hinweisen. Stellen Sie sicher, dass die Regel "Multiple Login Failures for Single Username" (Mehrere Anmeldefehler für einzelnen Benutzernamen) aktiviert ist. Passen Sie die Abgleich- und Zeitraumparameter für diese Regel an, um die Reaktionsfähigkeit zu optimieren.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- Multiple Login Failures for Single Username (Mehrere Anmeldefehler für einzelnen Benutzernamen)

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: Multiple Login Failures for Single Username

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Accessing Account from Anonymous Source

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Accessing Account from Anonymous Source (Benutzerzugriff auf Konto aus anonymer Quelle)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Zeigt an, dass ein Benutzer auf interne Ressourcen aus einer anonymen Quelle, z. B. TOR oder ein VPN, zugreift.

Regeln für die Unterstützung

- BB:CategoryDefinition: Authentifizierungserfolg
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection,Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile,IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500,Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Time, Access at Unusual Times

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Time, Access at Unusual Times (Benutzerzeit, Zugriff zu ungewöhnlichen Zeiten)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Zeigt an, dass sich Benutzer erfolgreich in Zeiten authentifizieren, die gemäß Definition durch die "UBA: Unusual Times, %"-Bausteine für Ihr Netz ungewöhnlich sind.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg
- BB:UBA : Ungewöhnliche Zeiten (abends)
- BB:UBA : Ungewöhnliche Zeiten (nachts)

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTO-Card CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and

VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : VPN Access By Service or Machine Account

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : VPN Access By Service or Machine Account (VPN-Zugriff durch Service- oder Maschinenkonto)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Es wird erkannt, wenn ein Service- oder Maschinenkonto auf ein Cisco VPN zugreift. Konten werden im Referenzset 'UBA : Service, Machine Account' aufgelistet. Bearbeiten Sie diese Liste, um zu markierende Konten in Ihrer Umgebung hinzuzufügen oder zu entfernen.

Unterstützte Regel

BB:UBA : VPN-Zuordnung (logisch)

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Service, Machine Account".

Datenquellen

Cisco Adaptive Security Appliance (ASA)

UBA : VPN Certificate Sharing

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : VPN Certificate Sharing (Gemeinsame Nutzung eines VPN-Zertifikats)

Standardmäßig aktiviert

Wahr

Anmerkung: Soll die Regel 'UBA : VPN Certificate Sharing' (Gemeinsame Nutzung eines VPN-Zertifikats) verwendet werden, muss das Firewall-DSM von Cisco wie folgt aktualisiert werden:

- Für V7.2.8: `DSM-CiscoFirewallDevices-7.2-20170619124928.noarch.rpm`
- Für V7.3.0 und höher: `DSM-CiscoFirewallDevices-7.3-20170619132427.noarch.rpm`

senseValue-Standardwert

15

Beschreibung

Mit dieser Regel wird festgestellt, ob der Benutzername eines VPN-Ereignisses von 'VPNSubjectcn' abweicht. Ist dies der Fall, kann dies auf die gemeinsame Nutzung eines VPN-Zertifikats hinweisen. Bei einer gemeinsamen Nutzung von Zertifikaten oder Authentifizierungstoken fällt es schwer nachzuvollziehen, welcher Benutzer was getan hat. Dies wiederum erschwert das Ergreifen entsprechender Maßnahmen im Falle von Beeinträchtigungen.

Regeln für die Unterstützung

- BB:UBA : VPN-Zuordnung (logisch)
- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

Durch diese Regeln werden die zugehörigen Referenzsets mit den erforderlichen Daten aktualisiert.

Erforderliche Konfiguration

Aktivieren Sie folgende Regeln:

- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

Datenquellen

Cisco Adaptive Security Appliance (ASA)

UBA : Windows Access with Service or Machine Account

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Windows Access with Service or Machine Account

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Erkennt interaktive Sitzungen (RDP, lokale Anmeldung), die von einem Service- oder Maschinenkonto in Windows Server gestartet werden. Konten werden im Referenzset 'UBA : Service, Machine Account' aufgelistet. Bearbeiten Sie diese Liste, um zu markierende Konten in Ihrer Umgebung hinzuzufügen oder zu entfernen.

Regeln für die Unterstützung

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Service, Machine Account".

Datenquellen

Microsoft Windows Security Event Log (Ereignis-ID: 4776)

Konten und Berechtigungen

UBA : Account or Group or Privileges Added

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Account or Group or Privileges Added (früherer UBA-Name: Account, Group or Privileges Added or Modified)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Erkennt Ereignisse, die ein Benutzer ausführt und die einer der folgenden Kategorien zugeordnet werden können. Die Regel sendet ein IBM Sense-Ereignis, um die Risikobewertung des Ereignisverursachers zu erhöhen.

- Authentifizierung.Gruppe hinzugefügt
- Authentifizierung.Gruppe geändert
- Authentifizierung.Gruppenmitglied hinzugefügt
- Authentifizierung.Computeraccount hinzugefügt
- Authentifizierung.Computeraccount geändert

- Authentifizierung.Richtlinie hinzugefügt
- Authentifizierung.Richtlinienänderung
- Authentifizierung.Vertrauenswürdige Domäne hinzugefügt
- Authentifizierung.Benutzeraccount hinzugefügt
- Authentifizierung.Benutzeraccount geändert
- Authentifizierung.Benutzerrecht zugewiesen

Anmerkung: Um den Einfluss dieser Regel auf die allgemeinen Risikobewertungen von Benutzern zu optimieren, können Sie die Bausteinregel "CategoryDefinition: Authentication User or Group Added or Changed" (Authentifizierungsbenutzer oder -gruppe hinzugefügt oder geändert) ändern, indem Sie Ereigniskategorien hinzufügen, die für Ihr Unternehmen von Interesse sind.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Authentifizierungsbenutzer oder -gruppe oder Richtlinie hinzugefügt

Datenquellen

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System,Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400,Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA,Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X,McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection,

Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss,genua genugate, iT-CUBE agileSI

UBA : Account or Group or Privileges Modified

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Account or Group or Privileges Modified (Konto oder Gruppe oder Berechtigungen geändert) - (früherer UBA-Name: User Account Change)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Zeigt an, wenn ein Benutzerkonto von einer Aktion betroffen wurde, durch die die effektiven Berechtigungen des Benutzers geändert werden (entweder nach oben oder unten).

Hinweis zu 'falsch-positiv'-Situation: Dieses Ereignis ordnet Änderungen eines Kontonamens möglicherweise falsch dem Benutzer zu, der die Änderungen durchführt. Um die Möglichkeit dieses falsch-positiven Alarms zu verringern, können Sie den Test 'and when Username equals AccountName' (und wenn Benutzername gleich Kontoname ist) hinzufügen.

Hinweis zu 'falsch-negativ'-Situation: Dieses Ereignis erkennt möglicherweise nicht alle Fälle von Kontoänderungen für einen Benutzer.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Authentifizierungsbenutzer oder -gruppe oder Richtlinie geändert

Datenquellen

Microsoft Windows Security Event Log (Ereignis-ID: 626, 642, 644, 1300, 1317, 625, 629, 4672, 4722, 4725, 4738, 4765, 4767, 4781, 4737, 4755)

UBA : DoS Attack by Account Deletion

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : DoS Attack by Account Deletion (DoS-Attacke durch Kontolöschung)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt DoS-Attacken, indem die Anzahl der Kontolöschereignisse auf Basis eines festen Schwellenwerts innerhalb eines festgelegten Zeitraums überprüft wird.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Benutzerkonto gelöscht

Datenquellen

Amazon AWS CloudTrail (Ereignis-ID: DeleteUser)

Application Security DbProtect (Ereignis-ID: Login revoked - Windows, Login dropped - standard, Database role - dropped, Database user revoked)

Aruba Mobility Controller (Ereignis-ID: authmgr_user_del)

Box (Ereignis-ID: DELETE_USER)

Brocade FabricOS (Ereignis-ID: SEC-1181, SEC-3028)

CA ACF2 (Ereignis-ID: ACF2-L)

Check Point (Ereignis-ID: user_deleted, device_deleted, User Deleted)

Cilasoft QJRN/400 (Ereignis-ID: C20020)

Cisco Adaptive Security Appliance (ASA) (Ereignis-ID: %PIX|ASA-5-502102, %ASA-5-502102)

Cisco FireSIGHT Management Center (Ereignis-ID: USER_REMOVED_CHANGE_EVENT)

Cisco Firewall Services Module (FWSM) (Ereignis-ID: 502102)

Cisco Identity Services Engine (Ereignis-ID: 86008, 86028)

Cisco NAC Appliance (Ereignis-ID: CCA-1453, CCA-1502)

Cisco Nexus (Ereignis-ID: SECURITYD-6-DELETE_STALE_USER_ACCOUNT)

Cisco Wireless LAN Controllers (Ereignis-ID: 1.3.6.1.4.1.9.9.515.0.1)

CloudPassage Halo (Ereignis-ID: Halo user deleted, Local account deleted (linux only))

CorreLog Agent for IBM zOS (Ereignis-ID: RACF DELUSER: No Violations)

Custom Rule Engine (Ereignis-ID: 3035, 3043)

Cyber-Ark Vault (Ereignis-ID: 276)

EMC VMWare (Ereignis-ID: AccountRemovedEvent)

Extreme Dragon Network IPS (Ereignis-ID: HOST:LINUX:USER-DELETED, HOST:WIN:ACCOUNT-DELETED)

Extreme Matrix K/N/S Series Switch (Ereignis-ID: User Deleted Event, has been deleted)

Extreme NAC (Ereignis-ID: Deleted registered user)

Extreme NetsightASM (Ereignis-ID: UserRemove)

Flow Classification Engine (Ereignis-ID: 3035, 3043)

Forcepoint Sidewinder (Ereignis-ID: passport deletion, all passports revoked)

HBGary Active Defense (Ereignis-ID: DeleteUser)

HP Network Automation (Ereignis-ID: User Deleted)

Huawei S Series Switch (Ereignis-ID: SSH/6/DELUSER_SUCCESS)

IBM AIX Audit (Ereignis-ID: USER_Remove SUCCEEDED)

IBM AIX Server (Ereignis-ID: USER_Remove)

IBM DB2 (Ereignis-ID: DROP_USER SUCCESS)

IBM DataPower (Ereignis-ID: 0x81000136)

IBM IMS (Ereignis-ID: USER DELETED)

IBM Proventia Network Intrusion Prevention System (IPS) (Ereignis-ID: Delete User)

IBM QRadar Packet Capture (Ereignis-ID: UserDeleted)

IBM Resource Access Control Facility (RACF) (Ereignis-ID: 80 17.2, DELUSER_SUCCESS, 80 17.0)

IBM Security Access Manager for Enterprise Single Sign-On (Ereignis-ID: REVOKE_IMS_ID, DELETE_IMS_ID)

IBM Security Directory Server (Ereignis-ID: SDS Audit)

IBM Security Identity Governance (Ereignis-ID: 50, 43, 70005)

IBM Security Identity Manager (Ereignis-ID: Delete SUCCESS, Delete SUBMITTED, Delete Success)

IBM SmartCloud Orchestrator (Ereignis-ID: user)

IBM Tivoli Access Manager for e-business (Ereignis-ID: 13408 - Succeeded, 13408 Command Succeeded)

IBM i (Ereignis-ID: GSL2502, M250100, DO_USRPRF, GSL2602, GSL2601, M260100, MC@0400, GSL2501)

IBM z/OS (Ereignis-ID: 80 1.35)

Juniper Networks Network and Security Manager (Ereignis-ID: adm24473)

Linux OS (Ereignis-ID: userDel, Account Deleted, DEL_USER)

McAfee Application/Change Control (Ereignis-ID: USER_ACCOUNT_DELETED)

McAfee ePolicy Orchestrator (Ereignis-ID: 20793)

Microsoft ISA (Ereignis-ID: user removed)

Microsoft Office 365 (Ereignis-ID: Delete User-PartiallySucceded, Delete user-success, Delete User-success, Delete user-PartiallySucceded)

Microsoft SQL Server (Ereignis-ID: 24129, DR - US, DR - SL, DR - LX, DR - AR,DR - SU, 24076, 24123, 38)

Microsoft Windows Security Event Log (Ereignis-ID: 4743, 630, 1327, 647, 4726)

Netskope Active (Ereignis-ID: Delete Admin, Deleted admin)

Nortel Application Switch (Ereignis-ID: User Deleted)

Novell eDirectory (Ereignis-ID: DELETE_ACCOUNT)

OS Services Qidmap (Ereignis-ID: Account Deleted, User Deleted)

OSSEC (Ereignis-ID: 18112)

Okta (Ereignis-ID: core.user_group_member.user_remove, app.generic.import.details.delete_user)

Oracle Enterprise Manager (Ereignis-ID: Computer Delete (successful), User Delete (successful))

Oracle RDBMS Audit Record (Ereignis-ID: DROP USER-Standard:1, 53:1, 53:0,DROP USER-Standard:0, 53)

PGP Universal Server (Ereignis-ID: ADMIN_DELETED_USER)

Palo Alto Endpoint Security Manager (Ereignis-ID: User Deleted)

Pulse Secure Pulse Connect Secure (Ereignis-ID: SYN24849, ADM20722, ADM24473, SYN24745, SYN24850)

RSA Authentication Manager (Ereignis-ID: unknown, Deleted user, REMOVE_ORPHANED_PRINCIPALS, REMOTE_PRINCIPAL_DELETE, DELETE_PRINCIPAL)

SIM Audit (Ereignis-ID: Configuration-UserAccount-AccountDeleted)

STEALTHbits StealthINTERCEPT (Ereignis-ID: Active DirectorycomputerObject DeletedTrueFalse, Active DirectoryuserObject DeletedTrueFalse, Console user/group deleted, Console user/group deleted)

SafeNet DataSecure/KeySecure (Ereignis-ID: Removed user)

Skyhigh Networks Cloud Security Platform (Ereignis-ID: 10017)

Solaris BSM (Ereignis-ID: delete user)

SonicWALL SonicOS (Ereignis-ID: 559, 1157, 1158)

Trend Micro Deep Security (Ereignis-ID: 651)

Universal DSM (Ereignis-ID: Computer Account Removed, User Account Removed)

VMware vCloud Director (Ereignis-ID: com/vmware/vcloud/event/user/remove, com/vmware/vcloud/event/user/delete)

Vormetric Data Security (Ereignis-ID: DAO0090I)

iT-CUBE agileSI (Ereignis-ID: AU8, U0)

UBA : User Account Created and Deleted in a Short Period of Time

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Account Created and Deleted in a Short Period of Time (Benutzerkonto in kurzem Zeitraum erstellt und gelöscht)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Erkennt, wenn ein Benutzerkonto in einem kurzen Zeitraum erstellt und gelöscht wird.

Regeln für die Unterstützung

- BB:UBA : Benutzerkonto erstellt
- BB:UBA : Benutzerkonto gelöscht
- BB:UBA : Allgemeine Ereignisfilter

Datenquellen

UBA : Dormant Account Used

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Dormant Account Used (Inaktives Konto verwendet)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt die erfolgreiche Anmeldung aus einem Konto, das als ruhend festgelegt wurde.

Unterstützte Regel

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungsfehler

Datenquellen

Alle unterstützten Protokollquellen, die einen Benutzernamen im Ereignis bereitstellen.

UBA : Dormant Account Use Attempted

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Dormant Account Use Attempted (Versuch der Nutzung eines ruhenden Kontos)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Erkennt den fehlgeschlagenen Anmeldeversuch aus einem Konto, das als ruhend festgelegt wurde.

Unterstützte Regel

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungsfehler

Datenquellen

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway,Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Identity Platform, Centrify Infrastructure Services, Check Point,Cilasoft QJRN/400, Cisco ACS,Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center,Cisco Firewall Services Module (FWSM),Cisco IOS,Cisco Identity Services Engine,Cisco Intrusion Prevention System (IPS),Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS,CrowdStrike Falcon Host,Custom Rule Engine, CyberArk Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM,Event CRE Injected,Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch,Extreme Matrix K/N/S Series Switch,Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, Extreme XSR Security Routers, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, Forcepoint Sidewinder, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem,Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM Bluemix Platform, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS,IBM Resource Access Control Facility (RACF),IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager,IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business,IBM WebSphere Application Server,IBM i,IBM z/OS,IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox

NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control,McAfee Network Security Platform,McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta,OpenBSD OS, Open LDAP Software, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Palo Alto PA Series, Pirean Access: One, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sun ONE LDAP, Sybase ASE,Symantec Encryption Management Server, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Expired Account Used

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Expired Account Used (Abgelaufenes Konto verwendet). (Früherer UBA-Name: Orphaned or Revoked or Suspended Account Used)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Zeigt an, dass ein Benutzer versuchte, sich bei einem inaktivierten oder abgelaufenen Konto auf einem lokalen System anzumelden. Diese Regel kann auch darauf hinweisen, dass ein Konto kompromittiert wurde.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierung bei abgelaufenem Konto

Datenquellen

Cisco CatOS for Catalyst Switches, Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Juniper Junos WebApp Secure, Microsoft IAS Server, Microsoft Windows Security Event Log

UBA : First Privilege Escalation

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : First Privilege Escalation (Erste Berechtigungseskalation)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Zeigt an, dass ein Benutzer einen berechtigten Zugriff zum ersten Mal ausgeführt hat. Diese Berichtsregel kann inaktiviert werden, um die Überwachung des Benutzerverhaltens zum Zwecke der Ermittlung von Vergleichsdaten zu ermöglichen.

Unterstützte Regel

BB:UBA : Privilegierter Benutzer, Erstmalige Berechtigungsnutzung (logisch)

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,M-

cAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : New Account Use Detected

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : New Account Use Detected (Neue Kontonutzung erkannt)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Stellt Berichtsfunktionen bereit, die anzeigen, dass sich ein Benutzer zum ersten Mal erfolgreich angemeldet hat. Diese Berichtsregel kann zum Zwecke der Ermittlung von Vergleichsdaten temporär inaktiviert werden.

Unterstützte Regel

BB:UBA : Erstmaliger Benutzerzugriff (logisch)

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection,Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cis-

co ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile,IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500,Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE,Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Suspicious Privileged Activity (First Observed Privilege Use)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Privileged Activity (First Observed Privilege Use) (Verdächtige berechtigte Aktivität (erste beobachtete Berechtigungsnutzung))

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Zeigt an, dass ein Benutzer eine Aktion ausgeführt hat, für die eine Berechtigung erforderlich ist und die er bisher noch nie ausgeführt hat. Beobachtungen werden in der Gruppenzuordnung "UBA : Observed Activities by Low Level Category and Username" (Beobachtete Aktivitäten nach untergeordneter Kategorie und Benutzername) gespeichert.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Berechtigte Aktivität

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch

(SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Suspicious Privileged Activity (Rarely Used Privilege)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Privileged Activity (Rarely Used Privilege) (Verdächtige berechtigte Aktivität (selten genutzte Berechtigung))

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Zeigt an, dass ein Benutzer eine Aktion ausgeführt hat, für die eine Berechtigung erforderlich ist und die er in letzter Zeit nicht ausgeführt hat. Beobachtungen werden in der Gruppenzuordnung "UBA : Recent Activities by Low Level Category and Username" (Kürzliche Aktivitäten nach untergeordneter Kategorie und Benutzername) gespeichert. Die Sensitivität dieses Ereignisses kann durch eine Änderung der Lebensdauer (TTL = time-to-live) der Referenzzuordnung von Gruppen für "UBA : Recent Activities by Low Level Category and Username" modifiziert werden. Eine Erhöhung der TTL verringert die Sensitivität. Eine Verringerung der TTL erhöht die Sensitivität.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Berechtigte Aktivität

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco

Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Attempt to Use a Suspended Account

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Attempt to Use a Suspended Account (Benutzerversuch, ein gesperrtes Konto zu verwenden)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt, dass ein Benutzer versuchte, auf ein gesperrtes oder ein inaktiviertes Konto zuzugreifen.

Regeln für die Unterstützung

- BB:CategoryDefinition: Authentifizierung bei inaktiviertem Konto
- BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Microsoft ISA, Microsoft Windows Security Event Log

UBA : User Has Gone Dormant (ADE rule) (Benutzer ist inaktiv (ADE-Regel))

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wird nicht mehr unterstützt. Informationen zu ruhenden Konten können ab V3.2.0 im UBA-Dashboard angezeigt werden. Weitere Informationen finden Sie im Abschnitt „Ruhende Konten” auf Seite 41.

UBA : User Has Gone Dormant (no activity anomaly rule) (Benutzer ist inaktiv ('keine Aktivität'-Anomalieregel))

UBA : Dormant Account Found (privileged)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Vergewissern Sie sich, dass "UBA : User Has Gone Dormant (no activity anomaly rule)" (Benutzer ist inaktiv (keine Aktivitäts-Anomalieregel) aktiviert ist, um diese Regel zu aktivieren.

Diese Regel weist darauf hin, dass sich die Aktivitätenanzahl eines Benutzernamens um mehr als 80 % geändert hat. "UBA : User Dormant Account Found (privileged)" (Inaktiver Kunde gefunden (privilegiert)) und "UBA : User Has Gone Dormant (no activity anomaly rule)" (UBA: Benutzer ist inaktiv (keine Aktivitäts-Anomalieregel)) sollen deutlich machen, wenn ein Benutzer längere Zeit keine Aktivität gezeigt hat. Diese Bedingung könnte darauf hinweisen, dass der Benutzer keinen Zugriff mehr benötigt, wie aus einer längeren Inaktivität des betreffenden Benutzernamens hervorgeht. Es sind Fehlalarme möglich, wenn die Aktivität eines Benutzernamens während des Zeitraums des kurzen Intervalls (standardmäßig 14 Tage) und vor Festlegung von null als neue Baseline (standardmäßig 28 Tage) auf null fällt Diese Fehlalarme wirken sich nicht auf die Risikobewertung eines Benutzers aus, wenn als Grenzwert für die Antworthäufigkeit für "UBA : User Dormant Account Found (privileged)" ein Zeitraum festgelegt ist, der mindestens so lange wie das lange Intervall für jeden Benutzernamen ist.

Anmerkung: Fehlalarme sind für 'UBA : User Has Gone Dormant (no activity anomaly rule)' möglich, wenn die Aktivität eines Benutzernamens während der kurzen Intervallperiode (standardmäßig 14 Tage) und vor Festlegung von null als neue Baseline (standardmäßig 28 Tage) auf null fällt. Die Fehlalarme beeinflussen nicht die Risikobewertung eines Benutzer, wenn das Antworthäufigkeitslimit für "UBA : User Dormant Account Found (privileged)" auf einen Zeitraum gleich oder größer als das lange Intervall pro Benutzername festgelegt ist.

Unterstützte Regel

UBA : Dormant Account Found (privileged)

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : Dormant Account Found (privileged)".

Datenquellen

Alle unterstützten Protokollquellen.

Navigationsverhalten

UBA : Browsed to Business/Service Website

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Business/Service Website (Geschäfts-/Service-Website wurde aufgerufen)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Communications Website

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Communications Website (Zu Kommunikationswebsite navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Entertainment Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Entertainment Website (Zu Unterhaltungswebsite navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Gambling Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Gambling Website (Zu Spielewebsite navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Information Technology Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Information Technology Website (Zu Informationstechnologiewebsite navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Job Search Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Job Search Website (Zu Jobsuchewebsite navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to LifeStyle Website

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to LifeStyle Website (LifeStyle-Website wurde aufgerufen)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Malicious Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Malicious Website (Zu schädlicher Website navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Mixed Content/Potentially Adult Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Mixed Content/Potentially Adult Website (Zu Website mit gemischtem Inhalt/möglichem Inhalt nur für Erwachsene navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Phishing Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Phishing Website (Zu Phishing-Website navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Pornography Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Pornography Website (Zu Pornografiewebsite navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Scam/Questionable/Illegal Website

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Scam/Questionable/Illegal Website (Zu betrügerischer/fragwürdiger/illegaler Website navigiert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : Browsed to Uncategorized Website

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Browsed to Uncategorized Website (UBA: Nicht kategorisierte Website wurde aufgerufen)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Ein Benutzer hat auf eine URL zugegriffen, die möglicherweise ein erhöhtes Sicherheitsrisiko oder erhöhtes rechtliches Risiko darstellt.

Unterstützte Regel

BB:UBA : URL-Kategoriefilter

Datenquellen

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

UBA : User Accessing Risky URL (Benutzerzugriff auf gefährliche URL)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA: User Accessing Risky URL (früherer Name: X-Force Risky URL)

Standardmäßig aktiviert

Wahr

Beschreibung

Diese Regel erkennt, wenn ein lokaler Benutzer auf fragwürdigen Online-Inhalt zugreift.

Regeln für die Unterstützung

- X-Force Risky URL (Gefährliche URL)
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).
- Aktivieren Sie folgende Regel: X-Force Risky URL.

Datenquellen

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

Cloud

UBA : AWS Console Accessed by Unauthorized User

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : AWS Console Accessed by Unauthorized User (Zugriff auf AWS-Konsole durch nicht berechtigten Benutzer)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt einen unbefugten Zugriffsversuch auf die Amazon Web Services Console (AWS Console) durch einen Benutzer, der nicht in der autorisierten Liste im Referenzset 'AWS - Standardbenutzer' aufgelistet ist.

Regeln für die Unterstützung

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Installieren Sie das folgende Paket aus der IBM Security App Exchange: IBM QRadar Content Extension for Monitoring Amazon AWS.
- Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Domain Controller Administrators". Konfigurieren Sie die folgende Protokollquelle: Amazon AWS Cloudtrail

Datenquellen

Amazon AWS CloudTrail (Ereignis-ID: ConsoleLogin)

UBA : Non-Standard User Accessing AWS Resources

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Non-Standard User Accessing AWS Resources (Zugriff auf AWS-Ressourcen durch einen vom Standard abweichenden Benutzer)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt einen vom Standard abweichenden Benutzer, der versucht, auf Ressourcen von Amazon Web Services (AWS) zuzugreifen.

Datenquelle

Amazon Web Services Extension

Domänencontroller

UBA : DPAPI Backup Master Key Recovery Attempted

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : DPAPI Backup Master Key Recovery Attempted (Versuchte Wiederherstellung eines Hauptschlüssels für DPAPI-Sicherung)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Ermittelt den Versuch einer Wiederherstellung eines DPAPI-Hauptschlüssels.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquelle

Microsoft Windows Security Event Log (Ereignis-ID: 4693)

UBA : Kerberos Account Enumeration Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Kerberos Account Enumeration Detected (Aufzählung von Kerberos-Konto erkannt)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt Aufzählungen von Kerberos-Konten, indem eine große Zahl von Benutzernamen ermittelt wird, mit denen Kerberos-Anforderungen aus der gleichen Quellen-IP vorgenommen werden.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquelle

Microsoft Windows Security Event Log (Ereignis-ID: 4768)

UBA : Multiple Kerberos Authentication Failures from Same User

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Multiple Kerberos Authentication Failures from Same User (Mehrere Kerberos-Authentifizierungsfehler vom gleichen Benutzer)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es werden mehrere Ablehnungen oder Fehler des Tickets für die Kerberos-Authentifizierung erkannt.

Unterstützte Regel

- BB:UBA : Allgemeine Protokollquellenfilter
- BB:UBA : Kerberos-Authentifizierungsfehler

Datenquellen

Microsoft Windows Security Event Log

UBA : Non-Admin Access to Domain Controller

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Non-Admin Access to Domain Controller (Zugriff eines Benutzers ohne Administratorberechtigung auf Domänencontroller)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Der Versuch eines Kontozugriffs durch einen Benutzer ohne Administratorberechtigung auf den Domänencontroller wird erkannt.

Unterstützte Regel

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg
- BB:CategoryDefinition: Authentifizierungsfehler

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgenden Referenzsets hinzu: "UBA : Domain Controllers" und "UBA : Domain Controller Administrators"

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM,

Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Pass the Hash

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Pass the Hash (Pass-the-Hash-Angriff)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt Windows-Anmeldeereignisse, die möglicherweise bei Pass-the-Hash-Exploits generiert werden.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration:

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Trusted Domains.

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4624)

UBA : Possible Directory Services Enumeration

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Possible Directory Services Enumeration (Mögliche Directory Service-Aufzählung)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt Ausspähungsversuche bei der Directory Service-Aufzählung.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Domain Controller Administrators"

Datenquelle

Microsoft Windows Security Event Log (Ereignis-ID: 4661)

UBA : Possible SMB Session Enumeration on a Domain Controller

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Possible SMB Session Enumeration on a Domain Controller (Mögliche Aufzählung einer SMB-Sitzung in einem Domänencontroller)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Versuche bei SMB-Aufzählung für einen Domänencontroller.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgenden Referenzsets hinzu:

- UBA : Domain Controllers
- UBA : Domain Controller Administrators

Datenquelle

Microsoft Windows Security Event Log (Ereignis-ID: 5140)

UBA : Possible TGT Forgery

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Possible TGT Forgery (Mögliche TGT-Fälschung)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt Kerberos-TGTs, die Anomalien beim Domänennamen enthalten. Diese weisen möglicherweise auf Tickets hin, die unter Verwendung von Pass-the-Ticket-Exploits generiert werden.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Trusted Domains.

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4768)

UBA : Possible TGT PAC Forgery

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Possible TGT PAC Forgery (Mögliche TGT PAC-Fälschung)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt die Verwendung eines gefälschten PAC-Zertifikats für den Erhalt eines Service-Tickets von Kerberos TGS.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : TCT PAC Forgery Patched Server
- BB:UBA : TCT PAC Forgery Unpatched Server

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Domain Controller Administrators".

Datenquelle

Microsoft Windows Security Event Log (Ereignis-ID: 4672, 4769)

UBA : Replication Request from a Non-Domain Controller

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Replication Request from a Non-Domain Controller (Replikationsanforderung aus einem Controller außerhalb der Domäne)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Erkennt Replikationsanforderungen von einem unzulässigen Domänencontroller

Regeln für die Unterstützung

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Domain Controller Administrators".

Datenquelle

Microsoft Windows Security Event Log (Ereignis-ID: 4662)

UBA : TGT Ticket Used by Multiple Hosts

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : TGT Ticket Used by Multiple Hosts (UBA: Von mehreren Hosts verwendete TGT-Tickets)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es werden Kerberos-TGT-Tickets erkannt, die von zwei (oder mehr) unterschiedlichen Computern verwendet werden.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

UBA : Kerberos Account Mapping (UBA: Kerberos-Kontozuordnung)

Durch diese Regel werden die zugehörigen Referenzsets mit den erforderlichen Daten aktualisiert.

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : Kerberos Account Mapping"

Datenquellen

Microsoft Windows Security Event Log (Ereignis-ID: 4768)

Endpunkt

UBA : Detect Insecure Or Non-Standard Protocol

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Detect Insecure Or Non-Standard Protocol (Unsicheres oder vom Standard abweichendes Protokoll erkennen)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Es werden alle Benutzer erkannt, die über nicht autorisierte Protokolle kommunizieren, welche als unsichere oder vom Standard abweichende Protokolle betrachtet werden. Autorisierte Protokolle sind im Referenzset 'UBA : Ports of Authorized Protocols' (Ports autorisierter Protokolle) mit dem Standardwert 0 aufgeführt, der für den Port von QRadar-Ereignissen steht. Bearbeiten Sie das zu markierende Referenzset 'UBA : Ports of Authorized Protocols' in Ihrer Umgebung, bevor Sie diese Regel aktivieren.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Unsichere Ports
-

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Ports Of Authorized Protocols.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : Detect Persistent SSH session

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Detect Persistent SSH session (Persistente SSH-Sitzung erkennen)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt SSH-Sitzungen, die länger als zehn Stunden aktiv sind.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : SSH-Sitzung geschlossen
- BB:UBA : SSH-Sitzung geöffnet

Erforderliche Konfiguration

Für diese Regel müssen die Ereignisse 'SSH geöffnet' und 'SSH geschlossen' auftreten, damit eine korrekte Erkennung möglich ist. Wenn die verwendete Protokollquelle über keine Ereignis-ID für beide Ereignisse verfügt, erhalten Sie möglicherweise falsche Ergebnisse. Ermitteln Sie in den Datenquellen die Ereignis-IDs für die verwendete Protokollquelle.

Datenquellen (SSH geöffnet)

Centrify Infrastructure Services (Ereignis-ID: 27100, 27104)

Cisco IOS (Ereignis-ID: %SSH-5-SSH2_SESSION, %SSH-SW2-5-SSH2_SESSION)

Custom Rule Engine (Ereignis-ID: 18037, 3071)

Cyber-Ark Vault (Ereignis-ID: 378)

Extreme XSR Security Routers (Ereignis-ID: NEW_SSH_CONNECTION)

Flow Classification Engine (Ereignis-ID: 3071, 18037)

Huawei S Series Switch (Ereignis-ID: SSH/4/SFTP_REQ_RECORD)

HyTrust CloudControl (Ereignis-ID: AUN0120, unknown)

IBM AIX Server (Ereignis-ID: sshd2 connection established, ssh-server connect, ssh-server session open)

IBM DataPower (Ereignis-ID: 0x8100011e, 0x810001e4, 0x810001e5)

Juniper MX Series Ethernet Services Router (Ereignis-ID: SSH)

Juniper Networks AVT (Ereignis-ID: SSH)

Mac OS X (Ereignis-ID: OSX ssh session started)

OS Services Qidmap (Ereignis-ID: Connection from, pam_open_session, pam_sm_open_session)

Solaris Operating System Authentication Messages (Ereignis-ID: ssh session opened)

Universal DSM (Ereignis-ID: SSH Opened, SSH Session Started)

Datenquellen (SSH geschlossen)

Aruba Mobility Controller (Ereignis-ID: sshd_disconnect)

Centrify Infrastructure Services (Ereignis-ID: 27102)

Cisco IOS (Ereignis-ID: %SSH-5-SSH_CLOSE, %SSH-SW2-5-SSH2_CLOSE, %SSH-5-SSH2_CLOSE)

Custom Rule Engine (Ereignis-ID: 3072, 18038, 18040)

Cyber-Ark Vault (Ereignis-ID: 380, 381)

Flow Classification Engine (Ereignis-ID: 3072, 18038, 18040)

Huawei S Series Switch (Ereignis-ID: SSH/6/RECV_DISCONNECT)

IBM AIX Server (Ereignis-ID: ssh-server disconnect, sshd2 connection lost, SSH Disconnect, sshd2 local disconnect, ssh-server session close)

OS Services Qidmap (Ereignis-ID: Done with connection, pam_sm_close_session, pam_close_session, Did not receive identification string, Connection timed out, Received disconnect from IP, Connection closed)

Pulse Secure Pulse Connect Secure (Ereignis-ID: GWE24572)

Universal DSM (Ereignis-ID: SSH Terminated, SSH Session Finished, SSH Closed)

UBA : Internet Settings Modified

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Internet Settings Modified (Geänderte Interneteinstellungen)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Es werden Änderungen an Interneteinstellungen im System erkannt.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4657)

UBA : Malware Activity - Registry Modified In Bulk

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Malware Activity - Registry Modified In Bulk (Malwareaktivität - Registry im Massenverfahren geändert)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Es werden Prozesse erkannt, mit denen mehrere Registry-Werte im Massenverfahren innerhalb eines kürzeren Intervalls geändert werden.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4657)

UBA : Netcat Process Detection (Linux)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Netcat Process Detection (Linux)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Es wird ein Netcat-Prozess auf einem Linux-System erkannt.

Unterstützte Regel

BB:UBA : Allgemeine Protokollquellenfilter

Datenquellen

Linux-Betriebssystem (Ereignis-ID: SYSCALL)

UBA : Netcat Process Detection (Windows)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Netcat Process Detection (Windows)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Erkennt Netcat-Prozess auf einem Windows-System.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4688)

UBA : Process Executed Outside Gold Disk Whitelist (Linux)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Process Executed Outside Gold Disk Whitelist (Linux) (Prozess wurde außerhalb der Gold Disk-Whitelist ausgeführt (Linux))

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es werden Prozesse erkannt, die auf einem Linux-System erstellt wurden, und es wird eine Benachrichtigung ausgegeben, wenn der Prozess außerhalb der Gold Disk-Whitelist ist.

Anmerkung: Die Regel ist standardmäßig inaktiviert. Aktivieren Sie die Regel erst, nachdem Sie die Prozessnamen so belegt oder geändert haben, dass sie im Referenzset 'UBA : Gold Disk Process Whitelist - Linux' in der Whitelist aufgeführt werden.

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Gold Disk Process Whitelist - Linux".

Unterstützte Regel

BB:UBA : Allgemeine Protokollquellenfilter

Datenquellen

Linux-Betriebssystem (Ereignis-ID: SYSCALL)

UBA : Process Executed Outside Gold Disk Whitelist (Windows)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Process Executed Outside Gold Disk Whitelist (Windows) (Prozess wurde außerhalb der Gold Disk-Whitelist ausgeführt (Windows))

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es werden Prozesse erkannt, die auf einem Windows-System erstellt wurden, und es wird eine Benachrichtigung ausgegeben, wenn der Prozess außerhalb der Gold Disk-Whitelist ist.

Anmerkung: Die Regel ist standardmäßig inaktiviert. Aktivieren Sie die Regel erst, nachdem Sie die Prozessnamen so belegt oder geändert haben, dass sie im Referenzset 'UBA : Gold Disk Process Whitelist - Windows' in der Whitelist aufgeführt werden.

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Gold Disk Process Whitelist - Windows".

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4688)

UBA : Ransomware Behavior Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Ransomware Behavior Detected (Ransomware-Verhalten erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es wird ein Verhalten erkannt, das typisch für das Verhalten während einer Infektion mit Ransomware ist.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Windows Common Processes".

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4663)

UBA : Restricted Program Usage

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Restricted Program Usage (Eingeschränkte Programmnutzung)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Zeigt an, dass ein Prozess erstellt wird und der Prozessname mit einem der binären Namen übereinstimmt, die im Referenzset "UBA : Restricted Program Filenames" aufgeführt sind. Das Referenzset ist standardmäßig leer, d. h., es kann angepasst werden. Sie können das Referenzset mit Dateinamen füllen, die im Rahmen des Risikomanagements überwacht werden sollen.

Weitere Informationen zum Hinzufügen oder Entfernen von Programmen für die Überwachung finden Sie im Abschnitt Eingeschränkte Programme verwalten.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Restricted Program Filenames".

Datenquellen

Microsoft Windows Security Event Log

UBA : User Installing Suspicious Application

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Unterstützt die folgenden Regeln:

- UBA : User Installing Suspicious Application
- UBA : Populate Authorized Applications

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es werden Ereignisse von Anwendungsinstallationen erkannt und Benachrichtigungen ausgegeben, wenn verdächtige Anwendungen ermittelt werden. Hinweis: Füllen Sie das Referenzset "UBA : Authorized Applications" mit den Namen der für das Unternehmen berechtigten Anwendungen aus. Die Regel "UBA : Populate Authorized Applications" kann für einen kurzen Zeitraum aktiviert werden, um dieses Referenzset auszufüllen.

Die Regel "UBA : Populate Authorized Applications" füllt das Referenzset "UBA : Authorized Applications" mit den Namen der Anwendungen, die installiert sind, während diese Regel aktiviert ist. Hinweis: Die Regel ist standardmäßig inaktiviert. Aktivieren Sie die Regel für einen kurzen Zeitraum, um die Namen auszufüllen, während die Anwendungen von Benutzern installiert werden.

Datenquellen

Microsoft Windows Security Event Logs

UBA : User Running New Process

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Unterstützt die folgenden Regeln:

- UBA : User Running New Process
- UBA : Populate Process Filenames

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es werden Prozesse erkannt, die vom Benutzer erstellt werden, und es wird eine Benachrichtigung ausgegeben, wenn ein Benutzer einen neuen Prozess ausführt.

Die Regel "UBA: Populate Process Filenames" füllt das Referenzset "UBA : Process Filenames" aus, das als Regel von Dienstprogrammen für "UBA : User Running New Process" verwendet wird. Hinweis: Die Regel ist standardmäßig inaktiviert. Aktivieren Sie die Regel für einen kurzen Zeitraum, um die Dateinamen auszufüllen.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter, UBA : Populate Process Filenames

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: "UBA : Process Filenames".

Datenquellen

Microsoft Windows System Event Logs (Ereignis-ID: 4688)

UBA : Volume Shadow Copy Created

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Volume Shadow Copy Created (Spiegelkopie eines Datenträgers erstellt)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Es werden Spiegelkopien erkannt, die mit 'vssadmin.exe' oder dem Kommandozeilenprogramm Windows Management Instrumentation Command-line (WMIC) erstellt wurden.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 1 oder 4688)

Daten-Exfiltration

UBA : Abnormal data volume to external domain (ADE-Regel)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wurde durch folgende Machine Learning-Analyse ersetzt: Abnormal Volume of Data to External Domains.

- UBA : Abnormal data volume to external domain (Abnormales Datenvolumen an externe Domäne)
- UBA : Abnormal data volume to external domain Found (Abnormales Datenvolumen an externe Domäne gefunden)

Anmerkung: Das Aktivieren von ADE-Regeln kann die Leistung der UBA-App und Ihres QRadar-Systems beeinträchtigen.

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

UBA : Abnormal data volume to external domain Diese Regel verwendet die Anomalieerkennungsengine, um den Datenverkehr eines Benutzers zu überwachen und bei einem abnormalen Datenvolumen im Datenverkehr mit externen Domänen zu warnen.

UBA : Abnormal data volume to external domain Found Dies ist eine CRE-Regel, die die identische entsprechende ADE-Regel 'UBA: Abnormal data volume to external domain' unterstützt, die mithilfe der Anomalieerkennungsengine den Datenverkehr eines Benutzers überwacht und bei einem abnormalen Datenvolumen im Datenverkehr mit externen Domänen eine Warnung ausgibt.

Datenquellen

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

UBA : Abnormal Outbound Transfer Attempts (ADE-Regel)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wurde durch folgende Machine Learning-Analyse ersetzt: Abnormal Outbound Transfer Attempts. Weitere Informationen finden Sie im Abschnitt „Analyse *Abnormal Outbound Transfer Attempts* (Abnormale abgehende Übertragungsversuche) konfigurieren" auf Seite 182.

UBA: Abnormal Outbound Transfer Attempts (in V2.4.0 unter der Bezeichnung 'UBA: Abnormal Outbound Attempts')

UBA : Abnormal Outbound Transfer Attempts Found (Abnormale Ausgangsverkehrsversuche gefunden)

Anmerkung: Das Aktivieren von ADE-Regeln kann die Leistung der UBA-App und Ihres QRadar-Systems beeinträchtigen.

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

UBA : Abnormal Outbound Transfer Attempts (ADE-Regel) Diese Regel verwendet die Anomalieerkennungsengine, um den abgehenden Datenverkehr zu überwachen und bei einer abnormalen Anzahl an Versuchen zu warnen.

UBA : Abnormal Outbound Transfer Attempts Found Dies ist eine CRE-Regel, die die identische entsprechende ADE-Regel 'UBA : Abnormal Outbound Attempts' unterstützt, die mithilfe der Anomalieer-

kennungsengine den abgehenden Datenverkehr überwacht und bei einer abnormalen Anzahl an Versuchen eine Warnung ausgibt.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : Large Outbound Transfer by High Risk User

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Large Outbound Transfer by High Risk User (Umfangreiche abgehende Übertragung durch Hochrisikobenutzer)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt eine abgehende Übertragung von 200.000 Bytes oder mehr durch einen Hochrisikobenutzer.

Regeln für die Unterstützung

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Protokollquellen, für die CEP BytesSent definiert ist.

UBA : Multiple Blocked File Transfers Followed by a File Transfer

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Multiple Blocked File Transfers Followed by a File Transfer (Mehrere blockierte Dateiübertragungen nach einer Dateiübertragung)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt eine Exfiltration durch die Überprüfung von Dateiuploads, die ursprünglich blockiert wurden, auf die aber ein erfolgreicher Upload innerhalb einer Zeitspanne von 5 Minuten erfolgte.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Blocked File Transfer
- BB:UBA : Successful File Transfer

Erforderliche Konfiguration

Für diese Regel sind Ereignisse für blockierte Dateiübertragungen und für erfolgreiche Dateiübertragungen erforderlich, damit eine korrekte Erkennung möglich ist. Wenn die verwendete Protokollquelle über keine Ereignis-ID für beide Ereignisse verfügt, erhalten Sie möglicherweise falsche Ergebnisse. Ermitteln Sie in den Datenquellen die Ereignis-IDs für die verwendete Protokollquelle.

Datenquellen (Blockierte Dateiübertragungen)

Cilasoft QJRN/400 (Ereignis-ID: C21020)

Cisco Call Manager (Ereignis-ID: %UC_DRF-3-DRFSftpFailure)

Cisco IOS (Ereignis-ID: %UPDATE-3-SFTP_TRANSFER_FAIL)

Custom Rule Engine (Ereignis-ID: 18014, 18071, 18187, 4032)

Extreme Stackable and Standalone Switches (Ereignis-ID: FFTP request failed)

Flow Classification Engine (Ereignis-ID: 4032, 18187, 18014, 18071)

Forcepoint Sidewinder (Ereignis-ID: FTP Permits, denied ftp command)

IBM i (EventID: UNR0907, UNR0908, UNR2302, GSL0118, GSL0119, GSL0318, GSL0319, GSL3718, GSL3719, GSL0618,UNR0701, UNR0707, UNR0901, UNR0910, UNR2301, UNR0705, UNR0706, UNR0708, UNR0710, UNR0801, UNR0802, UNR0905, UNR0906, GSL0619)

Juniper Networks Intrusion Detection and Prevention (IDP) (Ereignis-ID: TFTP:AUDIT:READ-FAILED)

Microsoft IIS (Ereignis-ID: 530)

Microsoft Operations Manager (Ereignis-ID: 22095)

OSSEC (Ereignis-ID: 11504, 11512)

Universal DSM (Ereignis-ID: FTP Action Denied, TFTP Session Denied,FTP Denied,FileTransfer Denied)

WatchGuard Fireware OS (Ereignis-ID: 1CFF0002,1CFF0006,1CFF0007,1CFF0009, 1CFF0001,1CFF0019, 1CFF0000, 1CFF0003)

Datenquellen (Erfolgreiche Dateiübertragungen)

Cilasoft QJRN/400 (Ereignis-ID: C21031)

Cisco FireSIGHT Management Center (Ereignis-ID: FILE_EVENT, FILE_EVENT_0)

Cisco IOS (Ereignis-ID: %FTPSERVER-6-NEWCONN)

Cisco IronPort (Ereignis-ID: FTP_connection)

Custom Rule Engine (Ereignis-ID: 18010, 4031,18431, 18183)

DG Technology MEAS (Ereignis-ID: 119-003, 119-070)

Flow Classification Engine (Ereignis-ID: 18010, 4031,18431, 18183)

Flow Device Type (Ereignis-ID: 21984, 21879, 51337, 51336, 35159, 21910)

Huawei S Series Switch (Ereignis-ID: FTPS/5/REQUEST)

IBM Proventia Network Intrusion Prevention System (IPS) (Ereignis-ID: FTP, TFTP)

IBM i (Ereignis-ID: MLD1200, MLD2100, MO10300,MO10400, MO11800, MO12100, MO12400, MO20200, MO20300. MO21300, MO21800, MO21900, GSL0101, GSL0102, GSL0301, GSL0302, GSL3701,GSL3702, M090100, UNA0705, UNA0706, UNA0708, UNA0710, UNA0801, UNA0802, UNA0905, UNA0906, UNA0907,UNA0908, UNA2302,UNA0601, UNA0604, UNA0605, UNA0607, UNA0701, UNA0707, UNA0901, UNA0902, UNA0910, UNA2301, M030100, MLD1100)

Juniper MX Series Ethernet Services Router (Ereignis-ID: TFTP, FTP)

Juniper Networks AVT (Ereignis-ID: TFTP, FTP)

Microsoft IIS (Ereignis-ID: 150, 125, 225)

ProFTPD Server (Ereignis-ID: FTP session opened)

Solaris Operating System Authentication Messages (Ereignis-ID: ftp connection)

SonicWALL SonicOS (Ereignis-ID: 1112, 1113)

Squid Web Proxy (Ereignis-ID: 3C0002_ALLOWED)

Trend InterScan VirusWall (Ereignis-ID: Trend ftpconnect)

Universal DSM (Ereignis-ID: File Transfer, FTP Opened, FTP Action Allowed, TFTP Session Opened)

Verdasys Digital Guardian (Ereignis-ID: Network Transfer Upload, Network Transfer Download)

WatchGuard Fireware OS (Ereignis-ID: 2AFF0004, 1CFF0019)

UBA : Suspicious Access Followed by Data Exfiltration

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Access Followed by Data Exfiltration (Verdächtiger Zugriff nach Datenexfiltration)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Zugriff aus unüblichen, eingeschränkten oder beschränkten Positionen nach einer versuchten Datenexfiltration.

Unterstützte Regel

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Data Exfiltration
- UBA : User Access from Restricted Location (UBA: Benutzerzugriff aus eingeschränkter Position)
- UBA : User Access from Prohibited Location (UBA: Benutzerzugriff aus unzulässiger Position)
- UBA : User Geography, Access from Unusual Locations (Benutzergeografie, Zugriff von ungewöhnlichen Standorten)

Erforderliche Konfiguration

Aktivieren Sie folgende Regeln:

- UBA : User Access from Restricted Location (UBA: Benutzerzugriff aus eingeschränkter Position)
- UBA : User Access from Prohibited Location (UBA: Benutzerzugriff aus unzulässiger Position)
- UBA : User Geography, Access from Unusual Locations (Benutzergeografie, Zugriff von ungewöhnlichen Standorten)

Datenquelle

Cisco Stealthwatch (Ereignis-ID: 45)

IBM Security Trusteer Apex Advanced Malware Protection (Ereignis-ID: ConnectionCreate.Connection_Test, CerberusNG.ent_create_remote_thread, ConnectionCreate.in_suspend_state, ConnectionCreate.orphant_thread_connect, close.file_inspection, processcreate.file_inspection)

Skyhigh Networks Cloud Security Platform (Ereignis-ID: 10003, 10004)

UBA : User Volume Activity Anomaly - Traffic to External Domains (ADE-Regel)

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wird nicht mehr unterstützt.

- UBA : User Volume Activity Anomaly - Traffic to External Domains (Anomalie bei Benutzeraktivitätsvolumen - Datenverkehr an externe Domänen)
- UBA : User Volume Activity Anomaly - Traffic to External Domains Found (Anomalie bei Benutzeraktivitätsvolumen - Gefundener Datenverkehr an externe Domänen)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

UBA : User Volume Activity Anomaly - Traffic to External Domains Hierbei handelt es sich um eine CRE-Regel, die die identische entsprechende ADE-Regel 'UBA : User Volume of Activity Anomaly - Traffic' unterstützt, die mithilfe der Anomalieerkennung den Datenverkehr eines Benutzers überwacht und bei einem ungewöhnlichen Datenverkehrsvolumen eine Warnung ausgibt.

UBA : User Volume Activity Anomaly - Traffic to External Domains Found Hierbei handelt es sich um eine CRE-Regel, die die identische entsprechende Regel 'UBA : User Volume Activity Anomaly - Traffic to External Domains' unterstützt, die mithilfe der Anomalieerkennung den abgehenden Datenverkehr überwacht und bei einer abnormalen Anzahlen an Versuchen eine Warnung ausgibt.

Datenquellen

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

Land/Region

UBA : Anomalous Account Created From New Location

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Anomalous Account Created From New Location (Anomales Konto von neuem Standort erstellt)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Erkennt Aktivität zum Erstellen eines anomalen Kontos von einem neuen Standort aus.

Regeln für die Unterstützung

- BB:UBA : Cloudendpunkte
- BB:UBA : Benutzerkonto erstellt
- BB:UBA : Allgemeine Ereignisfilter
- UBA : User Geography Change

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : User Geography Change".

Datenquellen

AhnLab Policy Center APC (Ereignis-ID: Administrator Account Add:Succeeded, ADD_ADMIN_ACCOUNT_SUCCESS)

Application Security DbProtect (Ereignis-ID: Database user created, Login created - standard, Login added - Windows, Database role - created)

Aruba Mobility Controller (Ereignis-ID: authmgr_user_add)

Bit9 Security Platform (Ereignis-ID: User_group_created, User_group_modified, User_group_deleted, Console_user_created, Console_user_modified, Console_user_deleted)

Box (Ereignis-ID: NEW_USER)

Brocade FabricOS (Ereignis-ID: SEC-1180,SEC-3025, SEC-1182)

CA ACF2 (Ereignis-ID: ACF2-L)

Check Point (Ereignis-ID: User Added, device_added)

Cilasoft QJRN/400 (Ereignis-ID: C20010, C20011)

Cisco Adaptive Security Appliance (ASA) (Ereignis-ID: %PIX|ASA-5-502101, %ASA-5-502101)

Cisco Firewall Services Module (FWSM) (Ereignis-ID: 502101, 504001)

Cisco IOS (Ereignis-ID: %APF-6-USER_NAME_CREATED)

Cisco Identity Services Engine (Ereignis-ID: 86006)

Cisco NAC Appliance (Ereignis-ID: CCA-1500)

Cisco PIX Firewall (Ereignis-ID: %PIX-0-502101, %PIX-1-502101, %PIX-2-502101, %PIX-3-502101, %PIX-4-502101, %PIX-5-502101, %PIX-6-502101, %PIX-7-502101)

Cisco PIX Firewall (Ereignis-ID: 502101)

Cisco Wireless LAN Controllers (Ereignis-ID: %APF-6-USER_NAME_CREATED, 1.3.6.1.4.1.9.9.515.0.2)

Cisco Wireless Services Module (WiSM) (Ereignis-ID: %AAA-6-GUEST_ACCOUNT_CREATE, %APF-6-USER_NAME_CREATED)

CloudPassage Halo (Ereignis-ID: Halo user added, Halo user re-added, Local account created (linux only))

CorreLog Agent for IBM zOS (Ereignis-ID: RACF ADDUSER: No Violations)

Cyber-Ark Vault (Ereignis-ID: 180, 2)

EMC VMWare (Ereignis-ID: AccountCreatedEvent)

Extreme Dragon Network IPS (Ereignis-ID: HOST:WIN:ACCOUNT-CREATED)

Extreme Matrix K/N/S Series Switch (Ereignis-ID: created with, User Created Event)

Extreme NAC (Ereignis-ID: Added registered user, Add Registered User)

Flow Classification Engine (Ereignis-ID: 3031, 3041)

Forcepoint Sidewinder (Ereignis-ID: passport addition)

Fortinet FortiGate Security Gateway (Ereignis-ID: add, auth-logon)

Foundry Fastiron (Ereignis-ID: SNMP_USER_ADDED)

HBGary Active Defense (Ereignis-ID: CreateUser)

HP Network Automation (Ereignis-ID: User Added)

IBM AIX Audit (Ereignis-ID: USER_Create SUCCEEDED)

IBM AIX Server (Ereignis-ID: USER_Create)

IBM DB2 (Ereignis-ID: ADD_USER SUCCESS)

IBM IMS (Ereignis-ID: USER CREATED)

IBM QRadar Packet Capture (Ereignis-ID: UserAdded)

IBM Resource Access Control Facility (RACF) (Ereignis-ID: 80 10.0, 80 10.2)

IBM Security Access Manager for Enterprise Single Sign-On (Ereignis-ID: PRE_PROVISION_IMS_USER, AA_SCR_REGISTRATION, REGISTER_MAC_IDENTITY, REGISTER_IDENTITY)

IBM Security Directory Server (Ereignis-ID: SDS Audit)

IBM Security Identity Governance (Ereignis-ID: 49, 70004, 42)

IBM Security Identity Manager (Ereignis-ID: Add Success, Add SUBMITTED, Add SUCCESS)

IBM SmartCloud Orchestrator (Ereignis-ID: user)

IBM Tivoli Access Manager for e-business (Ereignis-ID: 13402 - Succeeded, 13401 - Succeeded, 13402 Command Succeeded, 13401 Command Succeeded)

IBM i (Ereignis-ID: GSL2401,MC@0300, GSL2402, M240100, CP_CRT)

Imperva SecureSphere (Ereignis-ID: NEW_USERS_ACCOUNT, SOX_NEW_USERS, SOX - New users, New Users Account)

Itron Smart Meter (Ereignis-ID: CEUI-AUDIT-27, CEUI.AUDIT.26)

Juniper Networks Network and Security Manager (Ereignis-ID: adm23303, aut20167, adm30407, aut20168, adm20716, adm20717)

Linux OS (Ereignis-ID: ADD_USER)

McAfee Application/Change Control (Ereignis-ID: USER_ACCOUNT_CREATED)

McAfee ePolicy Orchestrator (Ereignis-ID: 20792)

Microsoft ISA (Ereignis-ID: user added)

Microsoft SQL Server (Ereignis-ID: CR - SU, CR - US, CR - SL, CR - LX, CR - AR, CR - WU, 24127, 24121, 24075)

Microsoft SharePoint (Ereignis-ID: 37)

Microsoft Windows Security Event Log (Ereignis-ID: 624, 645, 1318, 4720, 4741)

NCC Group DDos Secure (Ereignis-ID: 1003)

Netskope Active (Ereignis-ID: Create Admin, Created new admin)

Novell eDirectory (Ereignis-ID: CREATE_ACCOUNT)

OS Services Qidmap (Ereignis-ID: User Account Added)

OSSEC (Ereignis-ID: 5902, 18110)

Okta (Ereignis-ID: app.user_management.push_new_user_success, app.generic.import.details.add_user, app.generic.import.new_user, app.user_management.provision_user, app.user_management.push_new_user, app.user_management.push_profile_success, core.user.config.user_creation.success, core.user_group_member.user_add, cvd.user_profile_bootstrapped, cvd.appuser_profile_bootstrapped)

OpenBSD OS (Ereignis-ID: add user)

Oracle Enterprise Manager (Ereignis-ID: User Create (successful), Computer Create (successful))

Oracle RDBMS Audit Record (Ereignis-ID: 51:1, 51:0, CREATE USER-Standard:1, CREATE USER-Standard:0)

Oracle RDBMS OS Audit Record (Ereignis-ID: 51)

Pirean Access: One (Ereignis-ID: IsimUserRegistration;*;1)

Pulse Secure Pulse Connect Secure (Ereignis-ID: ADM23303, ADM20265, AUT20167, ADM30407, AUT20168)

RSA Authentication Manager (Ereignis-ID: Added user, unknown, REMOTE_PRINCIPAL_CREATE, CREATE_PRINCIPAL, CREATE_AM_PRINCIPAL)

SIM Audit (Ereignis-ID: Configuration-UserAccount-AccountAdded)

STEALTHbits StealthINTERCEPT (Ereignis-ID: Active DirectorycomputerObject AddedTrueFalse, Console ? user/group added, Console ⌂ user/group added, Active DirectoryuserObject AddedTrueFalse, Console - user/group added)

SafeNet DataSecure/KeySecure (Ereignis-ID: Added user)

Salesforce Security Auditing (Ereignis-ID: Created new Customer User, Created new user)

Skyhigh Networks Cloud Security Platform (Ereignis-ID: 10016)

Solaris BSM (Ereignis-ID: create user)

SonicWALL SonicOS (Ereignis-ID: 558)

Symantec Encryption Management Server (Ereignis-ID: ADMIN_IMPORTED_USER)

ThreatGRID Malware Threat Intelligence Platform (Ereignis-ID: user-account-creation)

Trend Micro Deep Discovery Email Inspector (Ereignis-ID: SYSTEM_EVENT_ACCOUNT_CREATED)

Trend Micro Deep Security (Ereignis-ID: 650)

Universal DSM (Ereignis-ID: Computer Account Added, User Account Added)

VMware vCloud Director (Ereignis-ID: com/vmware/vcloud/event/user/create, com/vmware/vcloud/event/user/import)

Vormetric Data Security (Ereignis-ID: DAO0089I)

iT-CUBE agileSI (Ereignis-ID: U0, AU7)

UBA : Anomalous Cloud Account Created From New Location

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Anomalous Cloud Account Created From New Location (Anomales Cloudkonto von neuem Standort erstellt)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt Aktivitäten zum Erstellen eines Cloudkontos von einem neuen Standort aus.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:UBA : Cloudendpunkte
- BB:UBA : Benutzerkonto erstellt
- UBA : User Geography Change

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: "UBA : User Geography Change".

Datenquellen

Amazon AWS CloudTrail (Ereignis-ID: CreateUser)

Microsoft Office 365 (Ereignis-ID: Add User-success, Add user-PartiallySucceded)

UBA : User Access from Multiple Locations

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Access from Multiple Locations (Benutzerzugriff aus mehreren Positionen)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Zeigt an, dass mehrere Standorte oder Quellen dasselbe Benutzerkonto gleichzeitig verwenden. Passen Sie die Abgleich- und Zeitraumparameter an, um die Reaktionsfähigkeit zu optimieren.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile,IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/

Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Access from Prohibited Location

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Access from Prohibited Location (UBA: Benutzerzugriff aus unzulässiger Position)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es wird ein Benutzerzugriff aus einer Position erkannt, die nicht in der Regel 'UBA : Allowed Location List' aufgeführt ist.

Regeln für die Unterstützung:

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg
-

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Allowed Location List

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix

K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Access from Restricted Location

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Access from Restricted Location (UBA: Benutzerzugriff aus eingeschränkter Position)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Es wird ein Benutzerzugriff aus einer Position erkannt, die nicht in der Regel 'UBA : Restricted Location List' aufgeführt ist. Sie können Länder aus "geographic location" (Standort) zu "UBA : Restricted Location List" hinzufügen.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg
-

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Restricted Location List

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle

Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Geography Change

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Geography Change (Änderung der Benutzergeografie)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

5

Beschreibung

Eine Übereinstimmung bedeutet, dass sich ein Benutzer über Fernzugriff aus einem Land angemeldet hat, das sich von dem Land unterscheidet, aus dem er sich zuletzt über Fernzugriff angemeldet hat. Diese Regel kann auch auf ein kompromittiertes Konto hinweisen, vor allem wenn die Regelübereinstimmungen kurz hintereinander auftreten.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Ereignisfilter
- BB:CategoryDefinition: Authentifizierungserfolg
- UBA : Benutzerlandkarte

Erforderliche Konfiguration

Aktivieren Sie folgende Regel: UBA : User Geography Map

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cis-

co CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile,IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Unterstützte Regel

User Geography Map (Landkarte für den Benutzer)

Durch diese Regel werden die zugehörigen Referenzsets mit den erforderlichen Daten aktualisiert.

UBA : User Geography, Access from Unusual Locations

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Geography, Access from Unusual Locations (Benutzergeografie, Zugriff von ungewöhnlichen Standorten)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

15

Beschreibung

Zeigt an, dass sich Benutzer in Ländern authentifizieren konnten, die gemäß der Definition durch die Bausteinregel "UBA : BB : Unusual Source Locations" (Ungewöhnliche Quellenstandorte) für Ihr Netz ungewöhnlich sind.

Regeln für die Unterstützung

- BB:UBA : Ungewöhnliche Quellenstandorte
- BB:CategoryDefinition: Authentifizierungserfolg
- BB:UBA : Allgemeine Ereignisfilter

Datenquellen

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller,Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection,Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA),Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort,Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile,IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP,

Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500,Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/ Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Netzverkehr und Angriffe

UBA : D/DoS Attack Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : D/DoS Attack Detected (D/DoS-Attacke erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt Denial-of-Service-(DoS-)Attacken im Netz durch einen Benutzer.

Anmerkung: Um diese Regel verwenden zu können, müssen Sie zunächst Folgendes tun:

1. Klicken Sie auf der Registerkarte **Verwaltung** auf **UBA Settings** (UBA-Einstellungen).
2. Aktivieren Sie das Kontrollkästchen **Search assets for username, when username is not available for event or flow data** (Assets nach Benutzername durchsuchen, wenn für Ereignis- oder Flussdaten kein Benutzername verfügbar ist), um in der Assettabelle nach Benutzernamen zu suchen. Die UBA-App verwendet Assets für die Suche nach einem Benutzer für eine IP-Adresse, wenn in einem Ereignis kein Benutzer aufgelistet ist.
3. Für die Ereignisregel muss Protokollquelle 'Snort Open Source IDS' aktiv sein.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Protokollquellenfilter
- BB:CategoryDefinition: DDoS-Attackenereignisse

- BB:CategoryDefinition: Netz-DoS-Attacke
- BB:CategoryDefinition: Service-DoS

Datenquellen

Akamai KONA, Application Security DbProtect, Aruba Mobility Controller, Barracuda Web Application Firewall, Brocade FabricOS, CRE System, Check Point, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Intrusion Prevention System (IPS), Cisco PIX Firewall, Cisco Stealthwatch, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Custom Rule Engine, CyberGuard TSP Firewall/VPN, Enterprise-IT-Security.com SF-Sherlock, Event CRE Injected, Extreme Dragon Network IPS, Extreme HiPath, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Fair Warning, FireEye, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, Huawei AR Series Router, IBM Proventia Network Intrusion Prevention System (IPS), IBM Security Network IPS (GX), Imperva Incapsula, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Motorola SymbolAP, NCC Group DDos Secure, Niksun 2005 v3.5, Nortel Application Switch, OS Services Qidmap, OSSEC, Palo Alto PA Series, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, SonicWALL SonicOS, Squid Web Proxy, Stonesoft Management Center, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), Top Layer IPS, Trend Micro Deep Security, Universal DSM, Vectra Networks Vectra, Venustech Venusense Security Platform, WatchGuard Fireware OS

UBA : Honeytoken Activity

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Honeytoken Activity (Honeytoken-Aktivität)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt eine Aktivität, bei der ein Honeytoken-Konto verwendet wird.

Regeln für die Unterstützung

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Honeytoken Accounts

Fügen Sie die entsprechenden Protokollquellen zu folgenden Protokollquellengruppen hinzu: UBA : Systems with Honeytoken Accounts.

Datenquellen

Alle Protokollquellen zur Protokollquellengruppe 'UBA : Systems with Honeytoken Accounts' hinzugefügt.

UBA : Network Traffic : Capture, Monitoring and Analysis Program Usage

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Network Traffic : Capture, Monitoring and Analysis Program Usage (Netzverkehr: Erfassungs-, Überwachungs- und Analyseprogrammnutzung)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Zeigt an, dass ein Prozess erstellt wird und der Prozessname mit einem der binären Namen übereinstimmt, die im Referenzset "UBA : Network Capture, Monitoring and Analysis Program Filenames" aufgeführt sind. Dieses Referenzset enthält die binären Namen von Netzpaketaufzeichnungssoftware. Das Referenzset wird vorab mit den Namen von allgemeinen Netzprotokollanalysesoftwaredateien gefüllt.

Weitere Informationen zum Hinzufügen oder Entfernen von Programmen für die Überwachung finden Sie im Abschnitt Netzüberwachungstools verwalten.

Unterstützte Regel

BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

Fügen Sie die entsprechenden Werte zu folgendem Referenzset hinzu: UBA : Network Capture, Monitoring and Analysis Program Filenames.

Datenquellen

Microsoft Windows Security Event Log

UBA : User Behavior, Session Anomaly by Destination (ADE-Regel)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wird nicht mehr unterstützt.

UBA : User Behavior, Session Anomaly by Destination (Benutzerverhalten, Sitzungsanomalie bei Zielen)

UBA : User Behavior, Session Anomaly by Destination Found (Benutzerverhalten, Sitzungsanomalie nach Ziel gefunden)

Anmerkung: Das Aktivieren von ADE-Regeln kann die Leistung der UBA-App und Ihres QRadar-Systems beeinträchtigen.

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

UBA : User Behavior, Session Anomaly by Destination (Benutzerverhalten, Sitzungsanomalie nach Ziel) Zeigt an, dass ein Benutzer auf IP-Zieladressen zugreift, die sich erheblich von den Adressen unterscheiden, auf die er in der Vergangenheit zugegriffen hat. Das Ereignis ist nicht zwangsläufig ein Hinweis auf eine Kompromittierung. Die Verhaltensänderung kann auf eine erhebliche Änderung der Zuständigkeit oder Arbeitsgewohnheiten des Benutzers hindeuten.

UBA : User Behavior, Session Anomaly by Destination Found Hierbei handelt es sich um eine CRE-Regel, die die identische entsprechende ADE-Regel 'UBA : User Behavior, Session Anomaly by Destination (Benutzerverhalten, Sitzungsanomalie nach Ziel) unterstützt, die darauf hinweist, dass ein Benutzer auf IP-Zieladressen zugreift, die sich erheblich von den Adressen unterscheiden, auf die er sonst zugreift. Das Ereignis ist nicht zwangsläufig ein Hinweis auf eine Kompromittierung. Die Verhaltensänderung kann auf eine erhebliche Änderung der Zuständigkeit oder Arbeitsgewohnheiten des Benutzers hindeuten.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Event Frequency Anomaly Categories (ADE-Regel)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wurde durch folgende Machine Learning-Analyse ersetzt: Activity by Category. Weitere Informationen finden Sie im Abschnitt „Analyse *Activity by Category* (Aktivität nach Kategorie) konfigurieren” auf Seite 184.

UBA : User Event Frequency Anomaly Categories (ADE-Regel)

UBA : User Event Frequency Anomaly - Categories Found (Anomalie bei der Benutzerereignishäufigkeit - Gefundene Kategorien)

Anmerkung: Das Aktivieren von ADE-Regeln kann die Leistung der UBA-App und Ihres QRadar-Systems beeinträchtigen.

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

UBA : User Event Frequency Anomaly Categories (Anomalie bei der Benutzerereignishäufigkeit - Kategorien) Verwendet die Anomalieerkennungsengine zur Überwachung der Kategorieverteilung von Ereignissen eines Benutzers. Bei ungewöhnlichen Häufigkeitsänderungen erfolgt eine Warnung.

UBA : User Event Frequency Anomaly - Categories Found (Anomalie bei der Benutzerereignishäufigkeit - Gefundene Kategorien) Hierbei handelt es sich um eine CRE-Regel, die die identische entsprechende ADE-Regel 'UBA : User Event Frequency Anomaly - Categories' unterstützt, die mithilfe der Anomalieerkennungsengine die Verteilung der Ereignisse eines Benutzers überwacht. Mit dieser Regel wird auf ungewöhnliche Änderungen in der Häufigkeit aufmerksam gemacht.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Volume Activity Anomaly - Traffic to Internal Domains (ADE-Regel)

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wird nicht mehr unterstützt.

- UBA : User Volume Activity Anomaly - Traffic to Internal Domains (Anomalie bei Benutzeraktivitätsvolumen - Datenverkehr an interne Domänen)
- UBA : User Volume Activity Anomaly - Traffic to Internal Domains Found (Anomalie bei Benutzeraktivitätsvolumen - Gefundener Datenverkehr an interne Domänen)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Hierbei handelt es sich um eine CRE-Regel, die die identische entsprechende Regel 'UBA : User Volume of Activity Anomaly - Traffic to Internal Domains' unterstützt, die mithilfe der Anomalieerkennung den Datenverkehr eines Benutzers überwacht und bei einem ungewöhnlichen Datenverkehrsvolumen eine Warnung ausgibt.

Datenquellen

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

QRadar DNS Analyzer

Weitere Informationen finden Sie unter IBM QRadar DNS Analyzer.

UBA : Potential Access to Blacklist Domain

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Potential Access to Blacklist Domain (Potenzieller Zugriff auf Blacklist-Domäne)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt Ereignisse, die darauf hinweisen, dass der Benutzer möglicherweise auf eine Blacklist-Domäne zugegriffen hat. Hierfür ist die App IBM QRadar DNS Analyzer erforderlich.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie die App 'IBM QRadar DNS Analyzer' installieren. Weitere Informationen finden Sie unter IBM QRadar DNS Analyzer.

Datenquellen

IBM QRadar DNS Analyzer

UBA : Potential Access to DGA Domain

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Potential Access to DGA Domain (Potenzieller Zugriff auf DGA-Domäne)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt Ereignisse, die darauf hinweisen, dass der Benutzer möglicherweise auf eine Domain Generated by Algorithm-(DGA-)Domäne zugegriffen hat. Hierfür ist die App IBM QRadar DNS Analyzer erforderlich.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie die App 'IBM QRadar DNS Analyzer' installieren. Weitere Informationen finden Sie unter IBM QRadar DNS Analyzer.

Datenquellen

IBM QRadar DNS Analyzer

UBA : Potential Access to Squatting Domain

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Potential Access to Squatting Domain (Potenzieller Zugriff auf Squatting-Domäne)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt Ereignisse, die darauf hinweisen, dass der Benutzer möglicherweise auf eine Squatting-Domäne zugegriffen hat. Hierfür ist die App IBM QRadar DNS Analyzer erforderlich.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie die App 'IBM QRadar DNS Analyzer' installieren. Weitere Informationen finden Sie unter IBM QRadar DNS Analyzer.

Datenquellen

IBM QRadar DNS Analyzer

UBA : Potential Access to Tunneling Domain

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Potential Access to Tunneling Domain (Potenzieller Zugriff auf Tunnelung-Domäne)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt Ereignisse, die darauf hinweisen, dass der Benutzer möglicherweise auf eine Tunnelung-Domäne zugegriffen hat. Hierfür ist die App 'IBM DNS Analyzer' erforderlich.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie die App 'IBM QRadar DNS Analyzer' installieren. Weitere Informationen finden Sie unter IBM QRadar DNS Analyzer.

Datenquellen

IBM QRadar DNS Analyzer

QRadar Network Insights (QNI)

Weitere Informationen zur Installation von QNI-Regeln in QRadar V7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8.

Informationen zu QRadar V7.3.0 und höher finden Sie unter QRadar Network Insights Content v7.3.0+.

UBA : QNI - Access to Improperly Secured Service - Certificate Expired

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Access to Improperly Secured Service - Certificate Expired (Zugriff auf nicht ordnungsgemäß gesicherten Service - Zertifikat abgelaufen)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

QRadar Network Insights (QNI) hat eine SSL-/TLS-Sitzung erkannt, die ein abgelaufenes Zertifikat verwendet. Server und Clients verwenden Zertifikate beim Aufbau der Kommunikation mithilfe von Secure Sockets Layer (SSL) oder Transport Layer Security (TLS). Zertifikate werden mit einem Ablaufdatum ausgegeben, das angibt, wie lange das Zertifikat gültig bleibt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Access to Improperly Secured Service - Certificate Invalid

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Access to Improperly Secured Service - Certificate Invalid (Zugriff auf nicht ordnungsgemäß gesicherten Service - Zertifikat ungültig)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

QRadar Network Insights (QNI) hat eine SSL-/TLS-Sitzung erkannt, die ein ungültiges Zertifikat verwendet. Server und Clients verwenden X.509-Zertifikate beim Aufbau der Kommunikation mithilfe von Secure Sockets Layer (SSL). Zertifikate werden mit einem Datum "Not Before" (Nicht vor) ausgegeben, welches das früheste Gültigkeitsdatum des Zertifikats angibt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length (Zugriff auf nicht ordnungsgemäß gesicherten Service - geringe Länge des öffentlichen Schlüssels)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

QRadar Network Insights (QNI) hat eine SSL-/TLS-Sitzung erkannt, die ein Zertifikat mit einer niedrigen Bitzahl des öffentlichen Schlüssels von weniger als 2048 verwendet. Ein Server, der ein schwaches Zertifikat für öffentlichen Schlüssel (weniger als 1024 Bit) bereitstellt, kann ein Sicherheitsrisiko darstellen. Laut NIST-Veröffentlichung 800-57 liegt die empfohlene minimale RSA-Schlüssellänge ab 2011 bei 2048 Bit.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate (Zugriff auf nicht ordnungsgemäß gesicherten Service - selbst signiertes Zertifikat)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

QRadar Network Insights (QNI) hat eine SSL-/TLS-Sitzung erkannt, die ein selbst signiertes Zertifikat verwendet. Ein selbst signiertes Zertifikat in einer öffentlichen Anwendung oder einer Produktionsserveranwendung könnte dazu führen, dass ein Remote-Angreifer eine Man-in-the-Middle-Attacke starten kann.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Confidential Content Being Transferred to Foreign Geography

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Confidential Content Being Transferred to Foreign Geography (An ausländische Regionen übertragene vertrauliche Inhalte)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Erkennt vertrauliche Inhalte, die an Länder und Regionen mit eingeschränktem Zugriff übertragen werden. Beachten Sie, dass diese Länder und Regionen in folgendem Baustein definiert sind: "Länder/

Regionen mit eingeschränktem Zugriff". Stellen Sie vor Aktivierung dieser Regel sicher, dass der Baustein Ihrem Geschäftsanwendungsfall entsprechend konfiguriert wird.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Observed File Hash Associated with Malware Threat

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Observed File Hash Associated with Malware Threat (Festgestellter Datei-Hash in Zusammenhang mit Bedrohung durch Malware)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Diese Regel wird ausgelöst, wenn Datenflussinhalte einen Datei-Hash enthalten, der mit bekannten schlechten Datei-Hashes übereinstimmt, die in einem Bedrohungsdatenfeed enthalten sind. Weist darauf hin, dass Malware über das Netz übertragen wurde.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Observed File Hash Seen Across Multiple Hosts

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Observed File Hash Seen Across Multiple Host (Datei-Hash auf mehreren Hosts festgestellt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Diese Regel wird ausgelöst, wenn festgestellt wird, dass derselbe zu Malware zugehörige Datei-Hash auf mehrere Ziele übertragen wird.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient (Potenzieller Spam-/Phishing-Versuch bei abgelehntem E-Mail-Empfänger erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Diese Regel wird ausgelöst, wenn im System abgelehnte E-Mail-Ereignisse gefunden werden, die an eine nicht vorhandene Empfängeradresse gesendet werden. Dies kann auf einen Spam- oder Phishing-Versuch hinweisen. Konfigurieren Sie den Baustein "BB:CategoryDefinition: Rejected Email Recipient" (BB: Kategoriedefinition: abgelehnter E-Mail-Empfänger), um für Ihr Unternehmen relevante QIDs einzubeziehen. Er ist bereits vorab mit den folgenden QIDs belegt, die für die Überwachung gut geeignet sind: Microsoft Exchange, Linux-Betriebssystem [mit sendmail], Sendmail-Protokolle des Solaris-Betriebssystems und Barracuda Spam and Virus Firewall.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers (Potenzieller Spam-/Phishing-Betreff von mehreren sendenden Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

5

Beschreibung

Diese Regel wird ausgelöst, wenn mehrere sendende Server in einem bestimmten Zeitraum denselben E-Mail-Betreff senden, was ein Zeichen für Spam oder Phishing sein kann.

Erforderliche Konfiguration

Vor dem Aktivieren dieser QNI-Regel müssen Sie das QRadar Network Insights Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Informationen zu QRadar 7.2.8 finden Sie unter QRadar Network Insights Content v7.2.8. Informationen zu QRadar 7.3.0 oder höher finden Sie unter QRadar Network Insights Content v7.3.0+.

Datenquellen

QRadar Network Insights (QNI)

Ausspähung

Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of DHCP Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of DHCP Servers Detected (Ungewöhnliches Scannen von DHCP-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu DHCP-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Database Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Database Servers Detected (Ungewöhnliches Scannen von Datenbankservern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Datenbankservern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of DNS Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of DNS Servers Detected (Ungewöhnliches Scannen von DNS-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu DNS-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of FTP Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of FTP Servers Detected (Ungewöhnliches Scannen von FTP-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu FTP-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Game Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Game Servers Detected (Ungewöhnliches Scannen von Spieleservern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Spieleservern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Generic ICMP Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Generic ICMP Detected (Ungewöhnliches Scannen von generischen ICMP-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz auf Servern, die das ICMP-Protokoll verwenden.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Generic TCP Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Generic TCP Detected (Ungewöhnliches Scannen von generischem TCP erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz auf Servern, die allgemeine TCP-Ports verwenden.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Generic UDP Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Generic UDP Detected (Ungewöhnliches Scannen von generischem UDP erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz auf Servern, die allgemeine UDP-Ports verwenden.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of IRC Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of IRC Servers Detected (Ungewöhnliches Scannen von IRC-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu IRC-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of LDAP Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of LDAP Servers Detected (Ungewöhnliches Scannen von LDAP-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu LDAP-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Mail Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Mail Servers Detected (Ungewöhnliches Scannen von Mail-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Mail-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Messaging Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Messaging Servers Detected (Ungewöhnliches Scannen von Messaging-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Messaging-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of P2P Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of P2P Servers Detected (Ungewöhnliches Scannen von P2P-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu P2P-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Proxy Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Proxy Servers Detected (Ungewöhnliches Scannen von Proxy-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Proxy-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of RPC Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of RPC Servers Detected (Ungewöhnliches Scannen von RPC-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu RPC-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of SNMP Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of SNMP Servers Detected (Ungewöhnliches Scannen von SNMP-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu SNMP-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of SSH Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of SSH Servers Detected (Ungewöhnliches Scannen von SSH-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu SSH-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Web Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Web Servers Detected (Ungewöhnliches Scannen von Web-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Web-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

UBA : Unusual Scanning of Windows Servers Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Unusual Scanning of Windows Servers Detected (Ungewöhnliches Scannen von Windows-Servern erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Erkennt ungewöhnliches Scannen im Netz zu Windows-Servern.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM Security Reconnaissance Content-Paket installieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM Security Reconnaissance Content.

Systemüberwachung (Sysmon)

Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

UBA : Common Exploit Tools Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Common Exploit Tools Detected (Gängige Exploit-Tools erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt die Verwendung gängiger Exploit-Tools wie Keylogger und PsExec.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Common Exploit Tools Detected (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Common Exploit Tools Detected (Gängige Exploit-Tools erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt die Verwendung gängiger Exploit-Tools wie Keylogger und PsExec.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Malicious Process Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Malicious Process Detected (Schädlicher Prozess erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden Prozesse erkannt, durch die ein schädliches Verhalten auf Windows-Hosts angezeigt wird.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Network Share Accessed

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Network Share Accessed (Zugriff auf gemeinsam genutzten Netzbereich)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden verdächtige Aktivitäten zu Netzfreigaben erkannt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Regeln für die Systemüberwachung

UBA : Process Creating Suspicious Remote Threads Detected (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Process Creating Suspicious Remote Threads Detected (Prozess erkannt, der verdächtige ferne Threads erstellt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Prozesse, die verdächtige Threads auf einer fernen Maschine erstellen.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Activities on Compromised Hosts

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Activities on Compromised Hosts (Verdächtige Aktivitäten auf kompromittierten Hosts)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Aktivitäten, die auf einem kompromittierten Host stattfinden.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Activities on Compromised Hosts (Assets)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Activities on Compromised Hosts (Verdächtige Aktivitäten auf kompromittierten Hosts)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Aktivitäten, die auf einem kompromittierten Host stattfinden.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Administrative Activities Detected

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Administrative Activities Detected (Verdächtige Verwaltungsaktivitäten erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt selten durchgeführte Verwaltungsaktivitäten, die verdächtig erscheinen.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Command Prompt Activity

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Command Prompt Activity

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden Aktivitäten im Zusammenhang mit Scripts in der Eingabeaufforderung erkannt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Entries in System Registry (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Entries in System Registry (Verdächtige Einträge in Systemregistry)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt verdächtige Aktivitäten, die Änderungen oder Aktualisierungen der Windows-Registrierung einschließen.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Image Load Detected (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Image Load Detected (Verdächtige Image-Uploads erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt verdächtige Images, die an sensible Speicherpositionen hochgeladen werden.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Pipe Activities (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Pipe Activities (Verdächtige Pipe-Aktivitäten)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt verdächtige Aktivitäten, die Prozesspipes auf Windows-Hosts einschließen.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious PowerShell Activity

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious PowerShell Activity

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden Aktivitäten im Zusammenhang mit Microsoft PowerShell-Scripts erkannt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious PowerShell Activity (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious PowerShell Activity (Asset)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden Aktivitäten im Zusammenhang mit Microsoft PowerShell-Scripts erkannt. Für diese Regel muss die Funktion "Search assets for username, when username is not available for event or flow data" (Assets nach Benutzername durchsuchen, wenn für Ereignis- oder Flussdaten kein Benutzername verfügbar ist) aktiviert sein.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Scheduled Task Activities

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Scheduled Task Activities (Verdächtige geplante Taskaktivitäten)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt die verdächtige Erstellung von geplanten Tasks auf Windows-Hosts.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Service Activities

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Service Activities (Verdächtige Serviceaktivitäten)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden verdächtige Service-Aktivitäten auf Windows-Computern erkannt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : Suspicious Service Activities (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Suspicious Service Activities (Verdächtige Serviceaktivitäten)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Es werden verdächtige Service-Aktivitäten auf Windows-Computern erkannt.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

UBA : User Access Control Bypass Detected (Asset)

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Access Control Bypass Detected (Umgehung von Benutzerzugriffssteuerung erkannt)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Prozessaktivitäten, die auf eine Umgehung der Benutzerzugriffssteuerung (UAC) hinweisen.

Erforderliche Konfiguration

Vor dem Aktivieren dieser Regel müssen Sie das IBM QRadar Content Extension for Sysmon-Paket aktivieren und die zugehörigen Regelinhalte aktivieren. Weitere Informationen finden Sie unter IBM QRadar Content Extension for Sysmon.

Datenquellen

Microsoft Windows Security Event Logs

Bedrohungsdaten

UBA : Abnormal visits to Risky Resources (ADE-Regel)

Die QRadar-App 'User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wird nicht mehr unterstützt.

- UBA : Abnormal visits to Risky Resources (Abnormale Besuche bei gefährlichen Ressourcen)
- UBA : Abnormal visits to Risky Resources Found (Abnormale Besuche bei gefährlichen Ressourcen gefunden)

Anmerkung: Das Aktivieren von ADE-Regeln kann die Leistung der UBA-App und Ihres QRadar-Systems beeinträchtigen.

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

UBA : Abnormal visits to Risky Resources Diese Regel verwendet die Anomalieerkennungsengine, um die Anzahl der Zugriffe eines Benutzers auf eine gefährliche Ressource (z. B. verdächtige URLs, Anonymizer und Malware-Host) zu überwachen und zu warnen, wenn sich die Anzahl der Besuche abnormal ändert.

UBA : Abnormal visits to Risky Resources Found Dies ist eine CRE-Regel, die die identische entsprechende ADE-Regel 'UBA : Abnormal visits to Risky Resources' unterstützt, die die Anomalieerkennungsengine verwendet, um die Anzahl der Zugriffe eines Benutzers auf gefährliche Ressourcen (z. B. verdächtige URLs, Anonymizer, Malware-Host) zu überwachen und zu warnen, wenn sich die Anzahl der Besuche abnormal ändert.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : Detect IOCs For Locky

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Detect IOCs For Locky (IOCs für Locky erkennen)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Benutzercomputer, die Indicators of Compromise (IOCs) für Locky aufweisen, anhand von URLs oder IPs, die aus X-Force-Kampagnenfeeds gespeist werden.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Protokollquellenfilter
- BB:UBA : Locky anhand von IP erkennen
- BB:UBA : Locky anhand von URL erkennen

Erforderliche Konfiguration

- Fügen Sie die entsprechenden Werte zu folgenden Referenzsets hinzu: UBA : IOCs-Locky IP und UBA : IOCs-Locky URL.
- Aktivieren Sie 'User Lookup from Asset' (Benutzersuche von Asset) in **Admin Settings** > **UBA Settings** (Admin-Einstellungen > UBA-Einstellungen).

Datenquellen

Alle unterstützten Protokollquellen.

UBA : Detect IOCs for WannaCry

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : Detect IOCs For WannaCry (IOCs für WannaCry erkennen)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

10

Beschreibung

Erkennt Benutzercomputer, die Indicators of Compromise (IOCs) für WannaCry aufweisen, anhand von URLs, IPs oder Hashwerten, die aus X-Force-Kampagnenfeeds gespeist werden.

Regeln für die Unterstützung

- BB:UBA : Allgemeine Protokollquellenfilter
- BB:UBA : WannaCry anhand von Hashes erkennen
- BB:UBA : WannaCry anhand von IP erkennen
- BB:UBA : WannaCry anhand von URL erkennen

Erforderliche Konfiguration:

- Fügen Sie die entsprechenden Werte zu folgenden Referenzsets hinzu: UBA : Malware Activity WannaCry - Hash, UBA : Malware Activity WannaCry - IP und UBA : Malware Activity WannaCry - URL.
- Aktivieren Sie 'User Lookup from Asset' (Benutzersuche von Asset) in **Admin Settings** > **UBA Settings** (Admin-Einstellungen > UBA-Einstellungen).

Datenquellen

Alle unterstützten Protokollquellen.

UBA : ShellBags Modified By Ransomware

Die App 'QRadar User Behavior Analytics' (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : ShellBags Modified By Ransomware (ShellBags geändert durch Ransomware)

Standardmäßig aktiviert

Wahr

senseValue-Standardwert

10

Beschreibung

Erkennt ShellBag-Registrierungsänderungen, die auf ein typisches Malware- oder Ransomware-Verhalten hinweisen.

Regeln für die Unterstützung

BB:UBA : Allgemeine Ereignisfilter

Datenquellen

Microsoft Windows Security Event Logs (Ereignis-ID: 4657)

UBA : User Accessing Risky Resources

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

Anmerkung: Diese Regel wird nicht mehr unterstützt.

'UBA : User Accessing Risky Resources' (Benutzerzugriff auf gefährliche Ressourcen) ist ab V2.3.0 standardmäßig inaktiviert. Die Regeln werden jetzt nach folgenden Typen aufgelistet und sind standardmäßig aktiviert:

- UBA : User Accessing Risky IP, Anonymization (Benutzerzugriff auf gefährliche IP, Anonymisierung)
- UBA : User Accessing Risky IP, Botnet (Benutzerzugriff auf gefährliche IP, Botnet)
- UBA : User Accessing Risky IP, Dynamic (Benutzerzugriff auf gefährliche IP, Dynamisch)
- UBA : User Accessing Risky IP, Malware (Benutzerzugriff auf gefährliche IP, Malware)
- UBA : User Accessing Risky IP, Spam (Benutzerzugriff auf gefährliche IP, Spam)

Standardmäßig aktiviert

Falsch

senseValue-Standardwert

15

Beschreibung

Zeigt an, dass ein Benutzer auf eine externe Ressource zugegriffen hat, die als ungeeignet oder gefährlich betrachtet wird oder Anzeichen einer Infizierung aufweist.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Accessing Risky IP, Anonymization (Benutzerzugriff auf gefährliche IP, Anonymisierung)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Accessing Risky IP, Anonymization (früherer Name: X-Force Risky IP, Anonymization)

Standardmäßig aktiviert

Wahr

Beschreibung

Diese Regel erkennt, wenn ein lokaler Benutzer oder Host eine Verbindung zu einem externen Anonymisierungsservice herstellt.

Regeln für die Unterstützung

- X-Force Risky IP, Anonymization (Gefährliche IP, Anonymisierung)
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).
- Aktivieren Sie folgende Regel: X-Force Risky IP, Anonymization.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Accessing Risky IP, Botnet (Benutzerzugriff auf gefährliche IP, Botnet)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Accessing Risky IP, Botnet (früherer Name: X-Force Risky IP, Botnet)

Standardmäßig aktiviert

Wahr

Beschreibung

Diese Regel erkennt, wenn ein lokaler Benutzer oder Host eine Verbindung zu einem Botnet-Befehls- und -Steuerungsserver herstellt.

Regeln für die Unterstützung

- X-Force Risky IP, Botnet (Gefährliche IP, Botnet)
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).
- Aktivieren Sie folgende Regel: X-Force Risky IP, Botnet.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Accessing Risky IP, Dynamic (Benutzerzugriff auf gefährliche IP, Dynamisch)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Accessing Risky IP, Dynamic (früherer Name: X-Force Risky IP, Dynamic)

Standardmäßig aktiviert

Wahr

Beschreibung

Diese Regel erkennt, wenn ein lokaler Benutzer oder Host eine Verbindung zu einer dynamisch zugewiesenen IP-Adresse herstellt.

Regeln für die Unterstützung

- X-Force Risky IP, Dynamic (Gefährliche IP, Dynamisch)
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).
- Aktivieren Sie folgende Regel: X-Force Risky IP, Dynamic.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Accessing Risky IP, Malware (Benutzerzugriff auf gefährliche IP, Malware)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Accessing Risky IP, Malware (früherer Name: X-Force Risky IP, Malware)

Standardmäßig aktiviert

Wahr

Beschreibung

Diese Regel erkennt, wenn ein lokaler Benutzer oder Host eine Verbindung zu einem Malware-Host herstellt.

Regeln für die Unterstützung

- X-Force Risky IP, Malware (Gefährliche IP, Malware)
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).
- Aktivieren Sie folgende Regel: X-Force Risky IP, Malware.

Datenquellen

Alle unterstützten Protokollquellen.

UBA : User Accessing Risky IP, Spam (Benutzerzugriff auf gefährliche IP, Spam)

Die App "QRadar User Behavior Analytics" (UBA) unterstützt Anwendungsfälle auf Basis von Regeln für bestimmte Verhaltensabweichungen.

UBA : User Accessing Risky IP, Spam (früherer Name: X-Force Risky IP, Spam)

Standardmäßig aktiviert

Wahr

Beschreibung

Diese Regel erkennt, wenn ein lokaler Benutzer oder Host eine Verbindung zu einem Host herstellt, der als Spamverteiler bekannt ist.

Regeln für die Unterstützung

- X-Force Risky IP, Spam (Gefährliche IP, Spam)
- BB:UBA : Allgemeine Ereignisfilter

Erforderliche Konfiguration

- Setzen Sie 'Enable X-Force Threat Intelligence Feed' (X-Force-Bedrohungsdatenfeed aktivieren) in **Admin Settings** > **System Settings** (Admin-Einstellungen > Systemeinstellungen) auf 'Yes' (Ja).
- Aktivieren Sie folgende Regel: X-Force Risky IP, Spam.

Datenquellen

Alle unterstützten Protokollquellen.

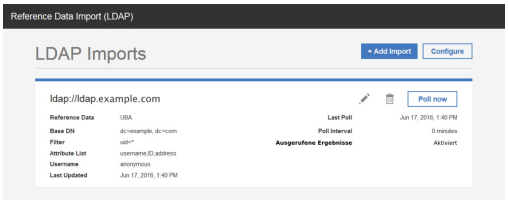
8 App 'Reference Data Import - LDAP'

Mit der App 'Reference Data Import - LDAP' (Referenzdatenimport - LDAP) können Sie kontextbezogene Identitätsinformationen aus mehreren LDAP-Quellen in Ihrer QRadar-Konsole zusammenstellen.

Achtung: Die App 'Reference Data Import - LDAP' wird unter QRadar on Cloud nicht unterstützt.

Bei der Installation der IBM® QRadar®-App 'User Behavior Analytics' (UBA) wird auch die App 'Import von Referenzdaten - LDAP' installiert. Mit dieser App können Sie Benutzerdaten von einem LDAP/AD-Server oder aus einer CSV-Datei in eine QRadar-Referenztabelle importieren. Die Referenztabelle wird anschließend von der UBA-App genutzt oder für QRadar-Suchvorgänge oder -Regeln verwendet.

Anmerkung: Für die App 'Reference Data Import - LDAP' ist QRadar V7.2.8 oder höher erforderlich.



LDAP-Daten in QRadar verwenden

Bei jeder Aktualisierung der Referenztabelle wird ein Ereignis `ReferenceDataUpdated` ausgelöst. Sie können einen Wert für die Lebensdauer der LDAP-Daten in der Referenztabelle festlegen. Bei Überschreiten der Lebensdauer wird das Ereignis `ReferenceDataExpiry` ausgelöst. Sie können Regeln erstellen, die auf diese Ereignisse antworten, oder Suchvorgänge generieren, um die Nutzdaten dieser Ereignisse auf der QRadar-Registerkarte **Protokollaktivität** abzufragen.

Auf die App 'Reference Data Import - LDAP' zugreifen

Der Zugriff auf die QRadar-App 'Reference Data Import - LDAP' erfolgt durch Klicken auf das Symbol **Reference Data Import LDAP** (Referenzdatenimport LDAP) in den Einstellungen für **Verwaltung**.

Weitere Informationen zu Referenzdatensammlungen in QRadar finden Sie im *IBM QRadar SIEM Verwaltungshandbuch*.

Unterstützte Browser für die LDAP-App

Um die Funktionen in IBM Security QRadar-Produkten uneingeschränkt nutzen zu können, müssen Sie einen unterstützten Web-Browser verwenden.

In der folgenden Tabelle werden die unterstützten Versionen von Web-Browsern aufgelistet.

Tabelle 1. Unterstützte Web-Browser für die QRadar-App "Import von Referenzdaten - LDAP"

Web-Browser	Unterstützte Versionen
Mozilla Firefox	45.2 Extended Support Release
Google Chrome	Neueste

Benutzerdaten aus einer CSV-Datei importieren

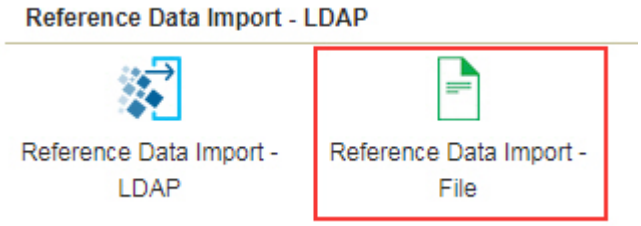
Sie können mit der App 'Reference Data Import - LDAP' eine CSV-Datei mit Benutzerdaten hochladen.

Informationen zu diesem Vorgang

Wenn die Benutzerdaten ein standardmäßiges CSV-Format haben, können Sie die Daten aus einer CSV-Datei in die UBA-App importieren.

Vorgehensweise

1. Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **Reference Data Import - LDAP** > **Reference Data Import - File** (Apps > Import von Referenzdaten - LDPA > Import von Referenzdaten - Datei).



3. Klicken Sie im Fenster 'Reference Data Import (File)' auf **Configure** (Konfigurieren), um ein Token für autorisierte Services zu erstellen.
4. Klicken Sie im Fenster 'Reference Data Import (File)' auf **Import**.
5. Suchen Sie in der Anzeige **Add user data** (Benutzerdaten hinzufügen) eine CSV-Datei mit Benutzerdaten.

   Anmerkung:

   Die Datei muss eine Größe von maximal 5 MB haben, eine Kopfzeile mit den Spaltennamen enthalten und über mindestens eine Spalte mit eindeutigen Daten verfügen.
6. Klicken Sie auf **Next** (Weiter) und geben Sie an, ob die Daten in einer vorhandenen Referenztabelle zusammengeführt werden sollen oder ob eine Referenztabelle erstellt werden soll.
   - Wenn Sie auswählen, dass die Daten in einer vorhandenen Referenztabelle zusammengeführt werden sollen, klicken Sie auf **Next** und wählen eine vorhandene Referenztabelle aus.
   - Wenn eine Referenztabelle erstellt werden soll, klicken Sie auf **Next** und erstellen eine Referenztabelle.

7. Klicken Sie auf **Next**.
8. Legen Sie in der Anzeige 'Attribute Mapping' (Attributzuordnung) die Attributnamen und den Schlüssel für die Referenztabelle fest und klicken Sie auf **Import**.

Token für autorisierten Service erstellen

Bevor Sie den LDAP-Server konfigurieren können, um Daten zu einer Referenztabelle hinzuzufügen, müssen Sie ein Token für autorisierten Service erstellen.

Vorbereitende Schritte

Achtung: Aufgrund eingeschränkter Administratorfunktionen können Administratoren für QRadar on Cloud keine Token für autorisierte Services für QRadar-Apps erstellen. Wenn Sie Kunde von QRadar on Cloud sind, wenden Sie sich an die Kundenunterstützung, damit ein Token für autorisierte Services für Sie erstellt wird.

Informationen zu diesem Vorgang

Anmerkung: Nach der Übergabe des Token für autorisierten Service müssen Sie Änderungen für das neue Token für autorisierten Service implementieren, damit diese wirksam werden.
IBM QRadar verlangt die Verwendung eines Authentifizierungstokens zur Authentifizierung der API-Aufrufe der App "Import von Referenzdaten - LDAP". Über das Fenster **Autorisierte Services verwalten** in den Einstellungen für **Verwaltung** können Sie Tokens für autorisierte Services erstellen.

Vorgehensweise

1. Klicken Sie im Fenster der App "Import von Referenzdaten - LDAP" auf **Konfigurieren**.
2. Klicken Sie im Dialogfenster **Autorisiertes Service-Token konfigurieren** auf **Autorisierte Services verwalten**.
3. Klicken Sie im Fenster **Autorisierte Services verwalten** auf **Autorisierten Service hinzufügen**.
4. Geben Sie in den folgenden Feldern die relevanten Informationen an und klicken Sie auf **Service erstellen**.
   a. Geben Sie im Feld **Servicename** einen Namen für den autorisierten Service ein. Der Name kann bis zu 255 Zeichen umfassen.
   b. Wählen Sie in der Liste **Benutzerrolle Admin** (Verwaltung) aus.
   c. Wählen Sie in der Liste **Sicherheitsprofil** das Sicherheitsprofil aus, das dem autorisierten Service zugewiesen werden soll. Über das Sicherheitsprofil werden die Netze und die Protokollquellen vorgegeben, auf die dieser Service in der QRadar-Benutzerschnittstelle zugreifen kann.
   d. Geben Sie in der Liste **Ablaufdatum** das Datum an, an dem der Service ablaufen soll, bzw. wählen Sie ein Datum aus. Ist kein Ablaufdatum erforderlich, wählen Sie **Kein Ablaufdatum** aus.
5. Klicken Sie auf die Zeile mit dem von Ihnen erstellten Service, wählen und kopieren Sie die Tokenzeichenfolge im Feld **Ausgewähltes Token** in der Menüleiste und schließen Sie das Fenster **Autorisierte Services verwalten**.
6. Fügen Sie im Dialogfenster **Autorisiertes Service-Token konfigurieren** die Tokenzeichenfolge in das Feld **Token** ein und klicken Sie auf **OK**.
7. Implementieren Sie Änderungen für das neue Token für autorisierten Service, damit diese wirksam werden.

Nächste Schritte

„LDAP-Konfiguration hinzufügen” auf Seite 168

Private Stammzertifizierungsstelle hinzufügen

Sie können ein Paket mit einer privaten Stammzertifizierungsstelle auf IBM QRadar hochladen, das mit der LDAP-App verwendet werden soll.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü () und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Reference Data Import LDAP**.
3. Klicken Sie im Hauptfenster der App **Reference Data Import LDAP** auf **Configure** (Konfigurieren).
4. Klicken Sie auf **Choose File** (Datei auswählen) und anschließend auf **Hochladen**. Nur der Dateityp `.pem` wird unterstützt.
5. Klicken Sie auf **OK**.

LDAP-Konfiguration hinzufügen

Fügen Sie die LDAP-Serverinformationen hinzu, die Sie zum Einfügen von Benutzerdaten in eine Referenzzuordnung von Zuordnungen verwenden.

Vorbereitende Schritte

Sie können erst eine LDAP-Konfiguration hinzufügen, nachdem Sie ein Authentifizierungstoken für die App "Import von Referenzdaten - LDAP" erstellt und hinzugefügt haben.

Vorgehensweise

1. Klicken Sie im Fenster der App "Import von Referenzdaten - LDAP" auf **Add Import** (Import hinzufügen).
2. Geben Sie auf der Registerkarte **LDAP-Konfiguration** folgende Informationen ein:
   a. Geben Sie im Feld **LDAP-URL** eine URL ein, die mit `ldap://` oder `ldaps://` (für TLS) beginnt.
   b. Geben Sie im Feld **Basis-DN** die Position in der LDAP-Verzeichnisstruktur ein, ab der der Server nach Benutzern suchen soll.

      Wenn sich Ihr LDAP-Server beispielsweise in der Domäne `example.com` befindet, können Sie `dc=example,dc=com` eingeben.
   c. Geben Sie im Feld **Filter** das bzw. die Attribute ein, anhand derer die in die Referenztabelle importierten Daten sortiert werden sollen. Beispiel:

      ```
      cn=*; uid=*; sn=*
      ```

      Folgende Standardwerte funktionieren mit Active Directory:
      `(&(sAMAccountName=*)(samAccountType=805306368))`.
   d. Geben Sie die Attribute, die Sie in die Referenztabelle importieren möchten, in das Feld **Attributliste** ein.

      Folgende Standardwerte funktionieren mit Active Directory:
      `userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.
   e. Geben Sie im Feld **Benutzername** den Benutzernamen für die Authentifizierung beim LDAP-Server ein.
   f. Geben Sie im Feld **Kennwort** das Kennwort für den LDAP-Server ein.
3. Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass IBM QRadar eine Verbindung zum LDAP-Server herstellen kann, bevor Sie fortfahren.

Nach einem erfolgreichen Verbindungsaufbau werden auf der Registerkarte **LDAP-Konfiguration** Informationen vom LDAP-Server angezeigt.

4. Klicken Sie auf **Weiter**.

Nächste Schritte

„Attribute auswählen".

Zugehörige Tasks:

„Private Stammzertifizierungsstelle hinzufügen" auf Seite 168
Sie können ein Paket mit einer privaten Stammzertifizierungsstelle auf IBM QRadar hochladen, das mit der LDAP-App verwendet werden soll.

„Token für autorisierten Service erstellen" auf Seite 167
Bevor Sie den LDAP-Server konfigurieren können, um Daten zu einer Referenztabelle hinzuzufügen, müssen Sie ein Token für autorisierten Service erstellen.

„LDAP-Attributzuordnungen hinzufügen"
Sie können Aliasnamen hinzufügen und den Schlüssel für die Referenztabelle festlegen.

Attribute auswählen

Wählen Sie die Attribute aus, die aus Ihrem LDAP-Server extrahiert werden sollen.

Vorgehensweise

1. Suchen Sie auf der Registerkarte **Select Attributes** (Attribute auswählen) bestimmte Attribute und wählen Sie die Attribute aus, die Sie vom LDAP-Server extrahieren möchten.
2. Klicken Sie auf **Next** (Weiter).

Nächste Schritte

Fügen Sie LDAP-Attributzuordnungen hinzu.

LDAP-Attributzuordnungen hinzufügen

Sie können Aliasnamen hinzufügen und den Schlüssel für die Referenztabelle festlegen.

Informationen zu diesem Vorgang

Wenn Sie LDAP-Daten mehrerer Quellen in derselben Referenztabelle zusammenführen möchten, können Sie zur Unterscheidung von LDAP-Attributen, die in verschiedenen Quellen denselben Namen haben, benutzerdefinierte Aliasse verwenden.

Vorgehensweise

1. Legen Sie auf der Registerkarte **Attribute Mapping** (Attributzuordnung) den Schlüssel für die Referenztabelle fest.

   Tipp: Durch das Klicken auf **Add** (Hinzufügen) und die Kombination zweiter Attribute können Sie neue LDAP-Attributfelder erstellen. Sie können zum Beispiel folgende Syntax verwenden: `"Last: {ln}, First: {fn}"`.
2. Klicken Sie auf **Weiter**.

Nächste Schritte

Konfigurieren Sie eine Referenzdatentabelle zum Speichern von LDAP-Daten.

Zugehörige Tasks:

„Referenzdatenkonfiguration hinzufügen”
Richten Sie über die Registerkarte "Referenzkonfiguration" eine Referenzdatentabelle zum Speichern von LDAP-Daten ein.

„Erstellen einer Regel, die auf LDAP-Datenaktualisierungen antwortet” auf Seite 172
Nachdem Sie die IBM QRadar-App "Import von Referenzdaten - LDAP" für das Speichern von Daten von Ihrem LDAP-Server in einer Referenztabelle in QRadar konfiguriert haben, können Sie die Daten zum Erstellen von Ereignisregeln verwenden.

Referenzdatenkonfiguration hinzufügen

Richten Sie über die Registerkarte "Referenzkonfiguration" eine Referenzdatentabelle zum Speichern von LDAP-Daten ein.

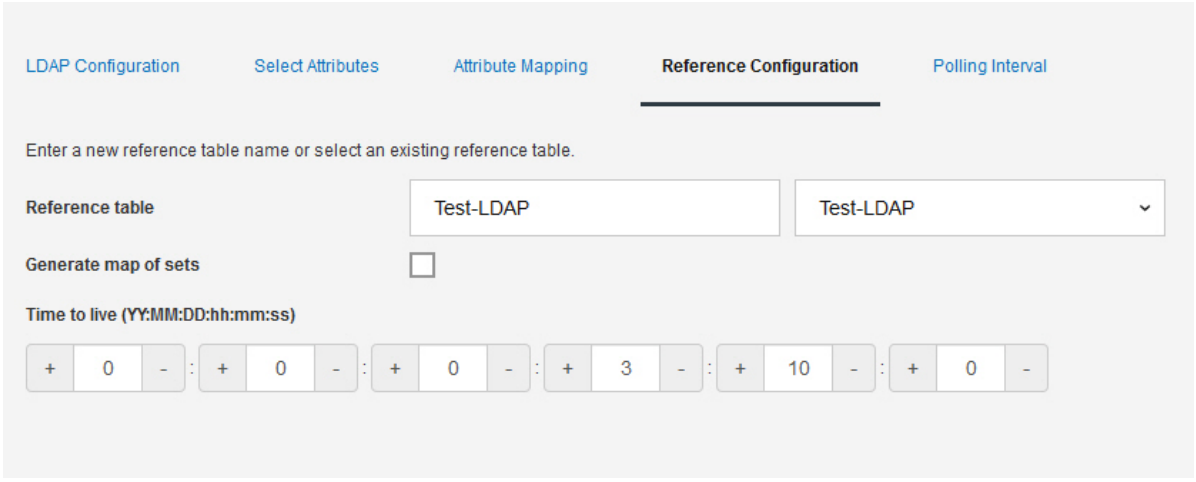
Vorbereitende Schritte

Nach der Konfiguration der LDAP-Serverinformationen müssen Sie eine Referenztabelle einrichten, in der die an die App übergebenen LDAP-Daten gespeichert werden sollen. Mithilfe der gespeicherten Daten können Sie Regeln in QRadar erstellen oder Suchvorgänge und Berichte generieren.

Vorgehensweise

1. Geben Sie auf der Registerkarte **Referenzkonfiguration** eine neue Referenztabelle ein oder legen Sie eine vorhandene Referenztabelle fest, der LDAP-Daten hinzugefügt werden sollen.
   a. Geben Sie einen Namen für die Referenzdatensammlung in das Feld **Referenzdaten** ein oder wählen Sie eine vorhandene Referenzdatensammlung aus der Liste aus.
   b. Das Kontrollkästchen **Zuordnung von Gruppen generieren** ist standardmäßig inaktiviert. Wenn Sie es aktivieren, werden Daten an ein Referenzsetformat gesendet, um die QRadar-Suche zu verbessern, was sich auf die Leistung auswirken kann.
   c. Geben Sie in den Feldern **Lebensdauer** an, wie lange die Daten in der Referenztabelle gespeichert werden sollen. Standardmäßig verfallen die hinzugefügten Daten nie. Bei Überschreiten der Lebensdauer wird das Ereignis `ReferenceDataExpiry` ausgelöst.

      Anmerkung: Wenn Daten einer vorhandenen Referenzzuordnung von Zuordnungen hinzugefügt werden, übernimmt die App die für diese Zuordnung ursprünglich festgelegten "Time to Live"-Parameter. Diese Parameter können auf der Registerkarte **Referenzkonfiguration** nicht überschrieben werden.



2. Klicken Sie auf **Next** (Weiter).

Nächste Schritte

Legen Sie das Abfrageintervall fest.

Zugehörige Tasks:

„Abfrage konfigurieren”
Konfigurieren Sie auf der Registerkarte **Abfrageintervall** die Häufigkeit, mit der die App Ihren LDAP-Server nach neuen Informationen abfragen soll.

Abfrage konfigurieren

Konfigurieren Sie auf der Registerkarte **Abfrageintervall** die Häufigkeit, mit der die App Ihren LDAP-Server nach neuen Informationen abfragen soll.

Vorbereitende Schritte

Nach der Konfiguration der LDAP-Serverinformationen und der Referenzdatensammlung müssen Sie konfigurieren, wie oft die App Daten vom LDAP-Server abrufen soll.

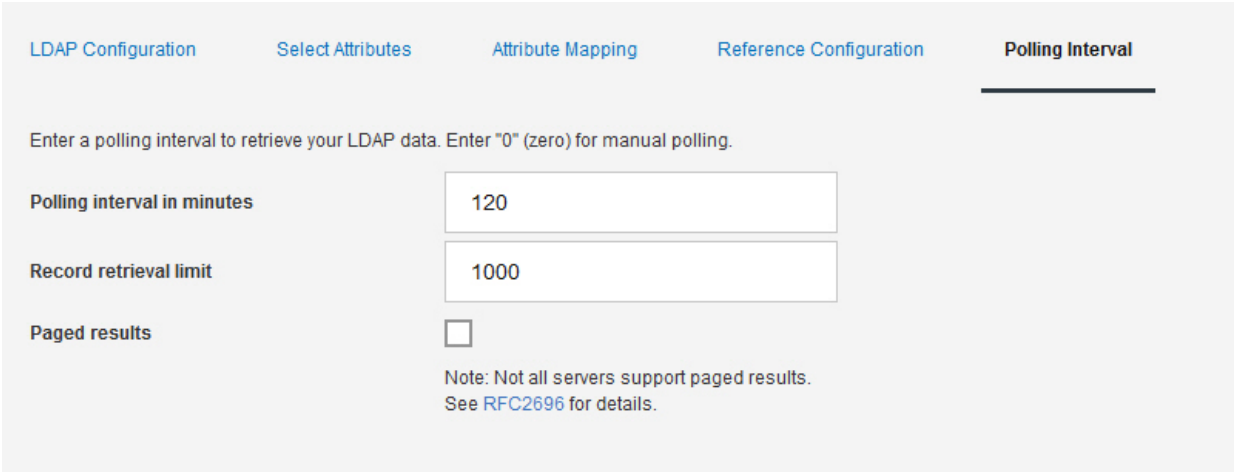
Vorgehensweise

1. Geben Sie im Feld **Abfrageintervall in Minuten** in Minuten an, wie oft die APP Ihren LDAP-Server nach Daten abfragen soll.

   Das kürzeste zulässige Abfrageintervall beträgt `120` Minuten.
2. Geben Sie im Feld **Grenzwert für Datensatzabruf** an, wie viele Datensätze die Abfrage melden soll.

   Standardmäßig werden 100.000 Datensätze zurückgegeben. Der maximale Wert ist 200.000.
3. Das Kontrollkästchen **Seitenweise angezeigte Ergebnisse** ist standardmäßig aktiviert, um eine Begrenzung der Anzahl Datensätze, die der LDAP-Server für jede Abfrage zurückgibt, zu verhindern.

   Anmerkung: Ausgerufene Ergebnisse werden nicht von allen LDAP-Servern unterstützt.
4. Klicken Sie auf **Speichern**.



Ergebnisse

Daten von Ihrem LDAP-Server werden zu dem von Ihnen konfigurierten Intervall zu der von Ihnen ausgewählten Referenzdatensammlung hinzugefügt. Über die API-Seite Ihrer IBM QRadar-Konsole können Sie prüfen, ob der Referenzdatensammlung Daten hinzugefügt wurden.

Zugehörige Tasks:

„Prüfung, ob der Referenzdatensammlung Daten hinzugefügt werden” auf Seite 172
Über die IBM QRadar-Seite "API Documentation" (API-Dokumentation) können Sie testen, ob der von Ih-

nen erstellten Referenzdatensammlung Daten hinzugefügt wurden.

Prüfung, ob der Referenzdatensammlung Daten hinzugefügt werden

Über die IBM QRadar-Seite "API Documentation" (API-Dokumentation) können Sie testen, ob der von Ihnen erstellten Referenzdatensammlung Daten hinzugefügt wurden.

Informationen zu diesem Vorgang

Auf der Seite **API Documentation** in Ihrer QRadar-Konsole können die Daten angezeigt werden, die in der Referenztabelle gespeichert sind, welche Sie in der App "Import von Referenzdaten - LDAP" erstellt haben. Über die Seite **API Documentation** können Sie prüfen, ob die LDAP-Informationen von der App aktualisiert wurden.

Vorgehensweise

1. Melden Sie sich bei der QRadar-Seite **API Documentation** an.

   `https://<Konsolen-IP>/api_doc`
2. Öffnen Sie in der Navigationsstruktur die neueste API.
3. Wechseln Sie zu **/reference_data** > **/table** > **/name** > **GET**.
4. Geben Sie in das Feld **Wert** des Parameters **`Name`** den Namen der Referenzdatensammlung ein, die Sie zum Speichern von LDAP-Informationen erstellt haben, und klicken Sie auf **Probieren Sie es aus!**.

   Die von der App hinzugefügten Daten werden im Feld **Response Body** (Antworthauptteil) zurückgegeben.

Erstellen einer Regel, die auf LDAP-Datenaktualisierungen antwortet

Nachdem Sie die IBM QRadar-App "Import von Referenzdaten - LDAP" für das Speichern von Daten von Ihrem LDAP-Server in einer Referenztabelle in QRadar konfiguriert haben, können Sie die Daten zum Erstellen von Ereignisregeln verwenden.

Informationen zu diesem Vorgang

Wenn Sie Ihren LDAP-Server abfragen und der Referenztabelle Daten hinzugefügt werden, werden Ereignisse `ReferenceDataUpdated` ausgelöst. Bei Überschreiten der Lebensdauer, die Sie auf der Registerkarte **Referenzkonfiguration** konfiguriert haben, wird ein Ereignis `ReferenceDataExpiry` ausgelöst. Sie können Regeln erstellen, die auf Inhalte in Ereignisnutzdaten `ReferenceDataUpdated` oder `ReferenceDataExpiry` antworten.

LDAP-Daten, die von der App in einer Referenzdatensammlung gespeichert werden, sind für Regeln verfügbar, die Sie über den **Regelassistent** von QRadar konfigurieren können. Der Zugriff auf den **Regelassistent** kann über die Registerkarten **Angriffe**, **Protokollaktivität** oder **Netzaktivität** erfolgen.

Vorgehensweise

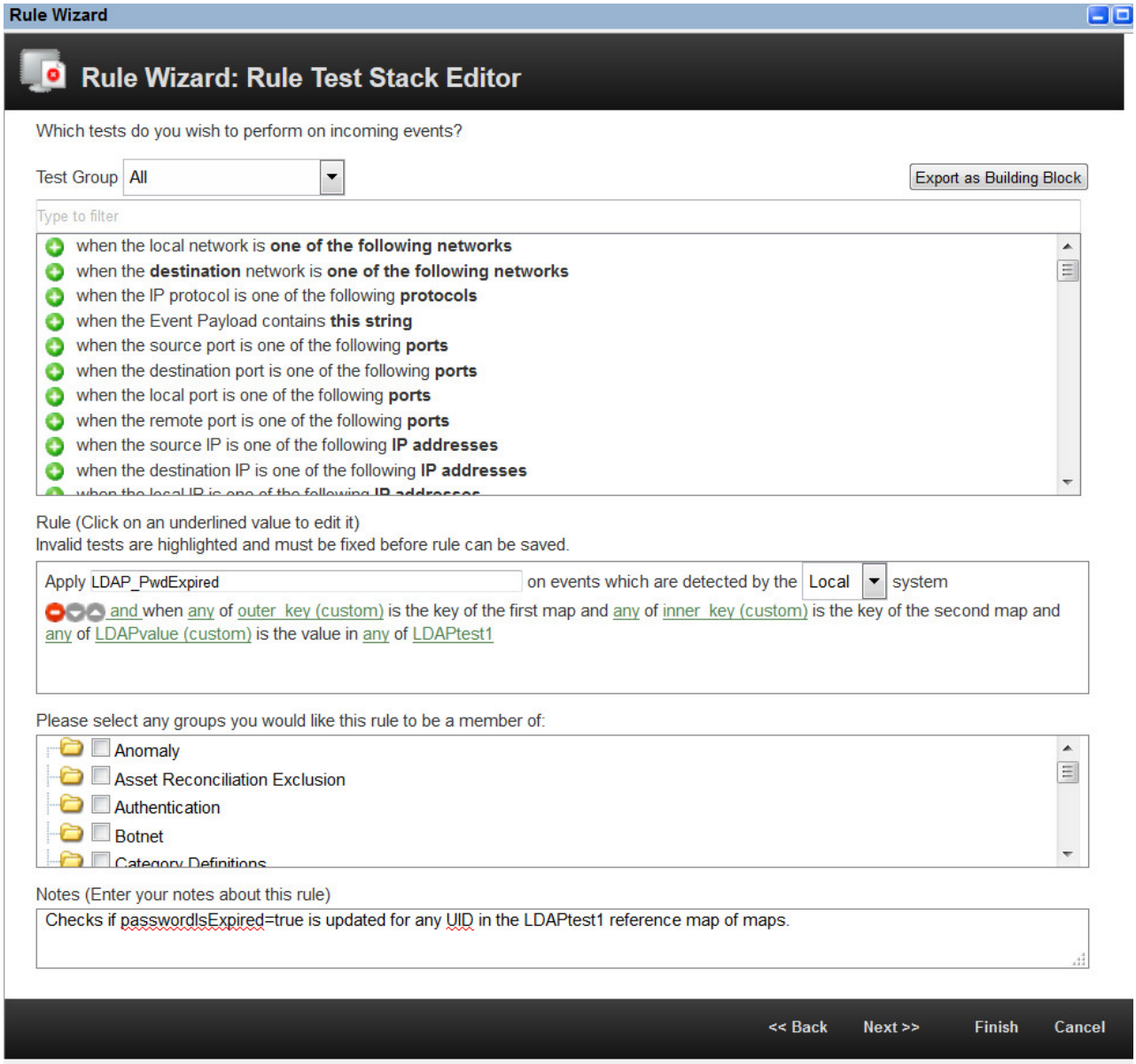
1. Klicken Sie auf **Protokollaktivität** > **Regeln** > **Aktionen** > **Neue Ereignisregel**.
2. Klicken Sie im **Regelassistent** auf der Einführungsseite auf **Weiter**.
3. Stellen Sie sicher, dass das Optionsfeld **Ereignisse** ausgewählt ist, und klicken Sie auf **Weiter**.
4. Geben Sie einen Namen für die Regel in das entsprechende Feld ein.
5. Wählen Sie in der Liste **Testgruppe** einen Test aus und klicken Sie auf das Plussymbol (+) neben dem zu verwendenden Test:

   Welchen Regeltest Sie auswählen, hängt davon ab, welche Informationen Sie aus der Referenzdatensammlung, in der Ihre LDAP-Daten gespeichert sind, abrufen möchten.

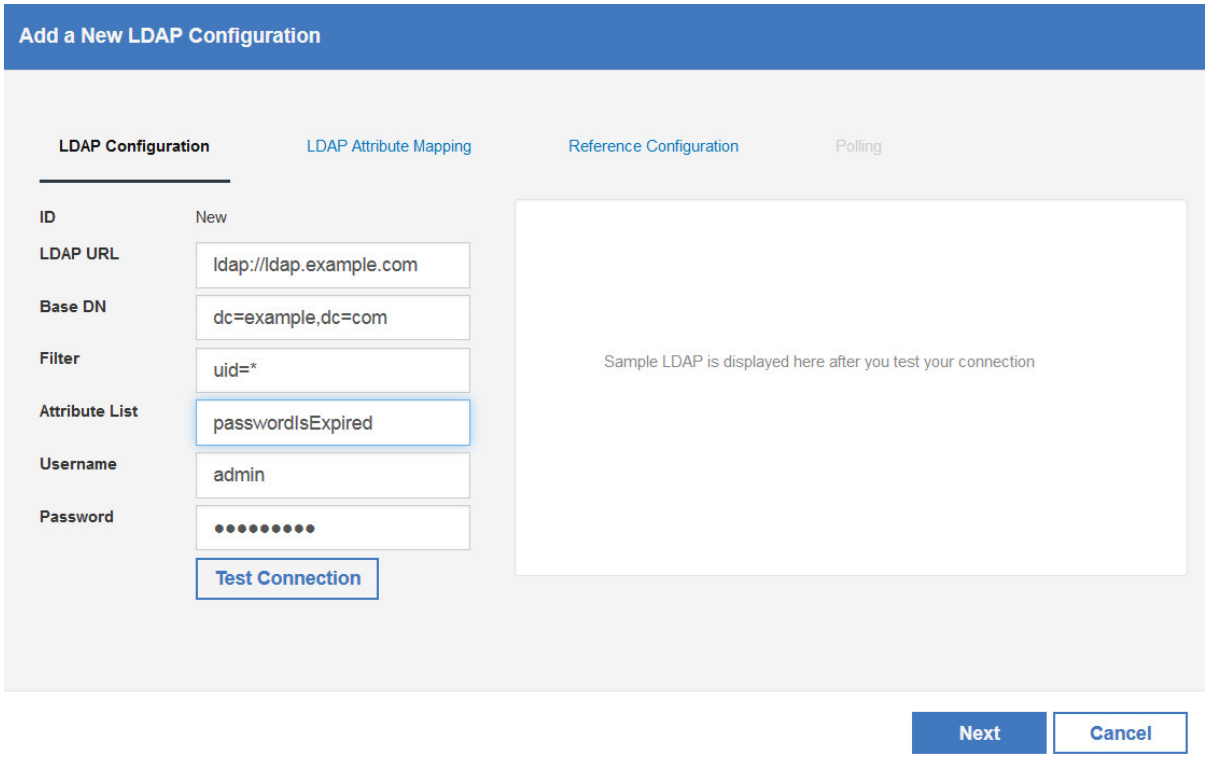
Der folgende Ereigniseigenschaftentest der Referenzzuordnungen von Zuordnungen ist zum Testen von Ereignissen vorgesehen, die bei der Aktualisierung der Referenztabelle der App "Import von Referenzdaten - LDAP" ausgelöst wurden.

```
when any of these event properties is the key of the first map
 and any of these event properties is the key of the second map
 and any of these event properties is the value
 in any of these reference map of maps.
```

Es wird eine Regel konfiguriert, um die Ereignisnutzdaten `ReferenceDataExpiry` zu testen, wenn das LDAP-Attribut **`PasswordIsExpired`** für jede Benutzer-ID in der Referenzdatensammlung **LDAPtest1** aktualisiert und auf `true` (wahr) gesetzt wird.



Um diesen Ereigniseigenschaftstest verwenden zu können, müssen Sie benutzerdefinierte Ereigniseigenschaften für die Felder **`outer key`** (äußerer Schlüssel, der Schlüssel der ersten Zuordnung), **`interner Schlüssel`** (der Schlüssel der zweiten Zuordnung) und **`Wert`** erstellen. Im folgenden Beispiel wurde die App "Import von Referenzdaten - LDAP" so konfiguriert, dass Daten zu Benutzern, deren Kennwort abgelaufen ist, von einem LDAP-Server unter `example.com` importiert werden.



Outer Key (Äußerer Schlüssel)

Diese Eigenschaft enthält die Daten, die in die LDAP-Felder eingegeben wurden, welche in den Feldern **Basis-DN** und **Filter** auf der Registerkarte "LDAP-Konfiguration" der App angegeben wurden. Der reguläre Ausdruck (Regex) für die benutzerdefinierte Ereigniseigenschaft könnte wie folgt aussehen:

```
(uid=(.*?),dc=example,dc=com)
```

Interner Schlüssel

Diese Eigenschaft enthält die Daten, die in die LDAP-Felder eingegeben wurden, welche im Feld **Attribute** (Attribut) auf der Registerkarte "LDAP-Konfiguration" der App angegeben wurden. In diesem Feld können Sie Attributaliasse verwenden. Der reguläre Ausdruck (Regex) für die benutzerdefinierte Ereigniseigenschaft könnte wie folgt aussehen:

```
(passwordIsExpired)
```

Wert Diese Eigenschaft enthält die Daten, die für jeden einzelnen Benutzer für das LDAP-Attribut **`passwordIsExpired`** abgerufen werden. Der reguläre Ausdruck (Regex) für die benutzerdefinierte Ereigniseigenschaft könnte wie folgt aussehen:

```
(\['true'\])
```

Weitere Informationen zu benutzerdefinierten Ereigniseigenschaften finden Sie im *IBM QRadar SIEM Benutzerhandbuch*.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Regelaktion, die Regelantwort und den Regelbegrenzer aus, die auf die Regel angewendet werden sollen, und klicken Sie auf **Beenden**.

   Weitere Informationen zu benutzerdefinierten Ereignisregeln finden Sie im *IBM QRadar SIEM Benutzerhandbuch*.

Ergebnisse

Wenn Sie Ihren LDAP-Server das nächste Mal abfragen und die von Ihnen erstellte Referenzdatensammlung aktualisiert wird, wird Ihre Regel ausgelöst.

Zugehörige Tasks:

„LDAP-Attributzuordnungen hinzufügen" auf Seite 169
Sie können Aliasnamen hinzufügen und den Schlüssel für die Referenztabelle festlegen.

„Referenzdatenkonfiguration hinzufügen" auf Seite 170
Richten Sie über die Registerkarte "Referenzkonfiguration" eine Referenzdatentabelle zum Speichern von LDAP-Daten ein.

9 App 'Machine Learning Analytics'

Die ML-App (Machine Learning Analytics) erweitert durch Hinzufügen von Anwendungsfällen für 'Machine Learning Analytics' das Leistungsspektrum des QRadar-Systems sowie der QRadar-App 'User Behavior Analytics' (UBA). Mit den Anwendungsfällen für 'Machine Learning Analytics' erhalten Sie zusätzliche Einblicke in das Benutzerverhalten mit Vorhersagemodellierung. Mithilfe der ML-App erlernt Ihr System das erwartete Verhalten der Benutzer in Ihrem Netz.

Achtung: Vor der Installation der UBA-App und der ML-App müssen Sie IBM QRadar V7.2.8 oder höher installieren.

Wichtig:

- Es wird empfohlen, die Einstellungen für 'Machine Learning Analytics' erst einen Tag nach der Erstkonfiguration der UBA-App zu aktivieren. Durch diese Wartezeit von einem Tag wird sichergestellt, dass für die UBA-App ausreichend Zeit zur Erstellung der Risikoprofile für Benutzer zur Verfügung steht.
- Das Modell wird alle 7 Tage aktualisiert. Damit wird sichergestellt, dass die App 'Machine Learning Analytics' die aktuellsten risikoreichen Benutzer überwacht.
- Durch die QRadar-Konsole wird die Speicherkapazität begrenzt, die von Apps verwendet werden kann. Die Optionen zur Größe der ML-App-Installation basieren auf dem aktuellen Speicherplatz von QRadar für Anwendungen.
  - Für die Installation der ML-App auf einer QRadar-Konsole sind mindestens 2 GB und auf einem App-Knoten mindestens 5 GB freier Speicher erforderlich.
  - Die Anzahl der durch die ML-App überwachten Benutzer ist von der Größe der ML-App-Installation und der entsprechenden Machine Learning-Analyse abhängig. Die maximale Anzahl an Benutzern, die von einer Machine Learning-Analyse überwacht werden können, beträgt 500 Benutzer pro GB der Größe der Machine Learning-Installation. Beispielsweise können bei einer Größe von 2 GB bis zu 1.000 Benutzer und bei 50 GB bis zu 25.000 Benutzer überwacht werden.
- Die Installation kann aufgrund von Speichermangel fehlschlagen. Diese Situation kann eintreten, wenn der für Anwendungen verfügbare Speicherplatz zu klein ist, weil bereits andere Anwendungen installiert sind.

Bekannte Probleme bei 'Machine Learning Analytics'

Für die App 'Machine Learning Analytics' liegen erforderliche Informationen zur Installation und zu bekannten Problemen vor.

In der App 'Machine Learning Analytics' gibt es folgende bekannte Probleme:

- Die App 'Machine Learning' zeigt möglicherweise Warnhinweise im Abschnitt 'Status of Machine Learning' (Status von Machine Learning). Weitere Informationen finden Sie im Abschnitt „Warnung in Statusanzeige für App 'Machine Learning' im Dashboard” auf Seite 208.
- Die Installation kann aufgrund von Speichermangel fehlschlagen. Dieser Fall kann bei Konsolen mit 128 GB eintreten, wenn bereits mehrere andere Apps installiert sind und für die Installation der ML-App weniger als 10 GB verfügbar sind. Wenn die Installation fehlschlägt, wird die Fehlernachricht 'FEHLGESCHLAGEN' angezeigt. Deinstallieren Sie zur Behebung dieses Problems einige andere Apps und wiederholen Sie den Vorgang.

Voraussetzungen für die Installation der App "Machine Learning Analytics"

Stellen Sie vor der Installation der App "Machine Learning Analytics" sicher, dass die Voraussetzungen erfüllt sind.

Sie können die App "Machine Learning Analytics" erst installieren, wenn die folgenden Systemvoraussetzungen erfüllt sind und die App "User Behaviour Analytics" (UBA) vollständig installiert und konfiguriert wurde.

Komponente	Mindestvoraussetzungen
Systemspeicher	• Konsole: 64 GB • App-Knoten: 5 GB
Version von IBM QRadar	V7.2.8 oder höher
Sense DSM	Installieren Sie die DSM-RPM-Datei.
UBA-App	• Installieren Sie die App 'UBA V3.1.0'. • Konfigurieren Sie die UBA-Einstellungen. • Klicken Sie auf die Registerkarte **Benutzeranalyse** und vergewissern Sie sich, dass im UBA-Dashboard Benutzerdaten enthalten sind.

IBM Sense-DSM manuell installieren

Die UBA-App und die App 'Machine Learning Analytics' fügen mithilfe der folgenden Sense-DSM-Dateien Benutzerrisikobewertungen und Verstöße zu QRadar hinzu.

- Für V7.2.8: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
- Für QRadar V7.3.1 und höher: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`

Einschränkung: Die Deinstallation eines DSM wird in QRadar nicht unterstützt.

1. Kopieren Sie die DSM-RPM-Datei in die QRadar-Konsole.
2. Melden Sie sich mit SSH als Rootbenutzer beim QRadar-Host an.
3. Wechseln Sie in das Verzeichnis, in das Sie die Datei heruntergeladen haben.
4. Geben Sie den folgenden Befehl ein:
   `rpm -Uvh <RPM-Dateiname>`
5. Klicken Sie in den Einstellungen für **Verwaltung** auf **Erweitert** > **Gesamte Konfiguration implementieren**.

Anmerkung: Anweisungen zur Installation und Konfiguration der UBA-App finden Sie im IBM Knowledge Center.

Zugehörige Tasks:

„App 'User Behavior Analytics' installieren” auf Seite 17
Sie können das Archiv, das die App enthält, mit dem IBM QRadar-Tool für das Erweiterungsmanagement direkt in die QRadar-Konsole hochladen und dort installieren.

„UBA-Einstellungen konfigurieren” auf Seite 28
Die IBM QRadar-App "User Behavior Analytics" (UBA) muss zunächst konfiguriert werden, damit sie Daten anzeigt.

App 'Machine Learning Analytics' installieren

Installieren Sie nach der Installation der UBA-App die App 'Machine Learning Analytics' über Extension Manager.

Vorbereitende Schritte

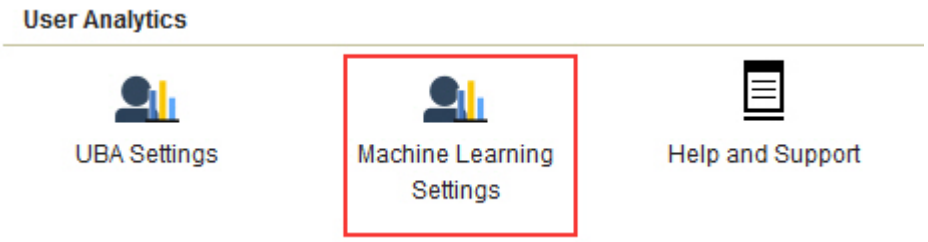
Vergewissern Sie sich, dass Sie alle Voraussetzungen für die Installation der App 'Machine Learning Analytics' erfüllt haben.

Informationen zu diesem Vorgang

Nach der Installation der UBA-App V2.1.0 können Sie über die Seite 'Machine Learning Settings' (ML-Einstellungen) die App 'Machine Learning Analytics' installieren.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).



3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Install ML App** (ML-App installieren).
4. Klicken Sie in der Eingabeaufforderung auf **Yes** (Ja), um die App zu installieren. Die Installation der ML-App dauert mehrere Minuten.

Nächste Schritte

Nach Abschluss der Installation können Sie ML-Anwendungsfälle aktivieren; klicken Sie anschließend auf **Save Configuration** (Konfiguration speichern).

Upgrade für die App 'Machine Learning Analytics' durchführen

Ein Upgrade für die App 'Machine Learning Analytics' wird über die Seite **Machine Learning Settings** (ML-Einstellungen) vorgenommen.

Vorbereitende Schritte

Ab UBA mit ML V2.2.0 gibt es keine Upgradeprozeduren. Das Upgrade der ML-App erfolgt automatisch zusammen mit dem Upgrade der UBA-App. Nach der Installation der UBA-App bzw. im Anschluss an ein Upgrade der UBA-App auf V2.1.0 können Sie über die Seite **Machine Learning Settings** (ML-Einstellungen) ein Upgrade der App 'Machine Learning Analytics' durchführen.

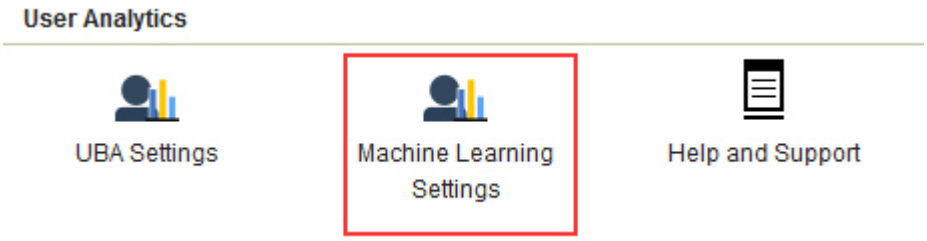
Achtung: Wenn die ML-App (Machine Learning Analytics) V2.0.0 installiert ist und ein Upgrade auf die neueste Version der UBA-App vorgenommen wird, sollte die App 'Machine Learning Analytics' nicht

über QRadar Extension Manager deinstalliert werden. Bei dem Versuch, die App 'Machine Learning Analytics' über Extension Manager zu entfernen, können möglicherweise Probleme in Zusammenhang mit der ML-App-Installation auftreten.

Anmerkung: Wenn Sie ein Upgrade der App 'Machine Learning Analytics' der Version 2.1.0 oder früher ausführen, wird der Wert **Risk Value of Sense Event** (Risikowert des Prüfereignisses) für jede Benutzeranalyse auf den aktuellen Machine Learning-Standardwert aktualisiert.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).



3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Upgrade ML App** (ML-App aktualisieren).
4. Klicken Sie in der Eingabeaufforderung auf **Yes** (Ja). Das Upgrade der ML-App dauert mehrere Minuten.
5. Nach Abschluss des Upgrades wird die Modellerstellung erneut gestartet.

Nächste Schritte

Überprüfen Sie, ob die Einstellungen für die ML-App korrekt konfiguriert wurden. Wenn Einstellungen geändert werden, müssen Sie diese über **Save Configuration** (Konfiguration speichern) speichern.

Einstellungen für Machine Learning Analytics konfigurieren

Um in der App "Machine Learning Analytics" Informationen anzeigen zu können, müssen Sie die Anwendungseinstellungen für Machine Learning Analytics konfigurieren.

Analyse *Total Activity* (Gesamtaktivität) konfigurieren

Konfigurieren Sie die Machine Learning-App *Total Activity* (Gesamtaktivität), um die tatsächliche und erwartete (erlernte) Aktivitätsauslastung der Benutzer über den ganzen Tag im **UBA-Dashboard** anzuzeigen.

Informationen zu diesem Vorgang

Achtung: Nach der Konfiguration oder Änderung der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Wichtig: Mit V2.2.0 wurden die Standardwerte für **Risk value of sense event** (Risikowert des Prüfereignisses) geändert. Da die neuen Standardwerte deutlich unter den vorherigen Standardwerten liegen, überschreiben die neuen Standardwerte die bestehenden Standardwerte bzw. alle zuvor von Ihnen geänderten Werte.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü ( ) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).
3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Total Activity** (Gesamtaktivität).
4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Total Activity* zu aktivieren.

   Wichtig: Sie benötigen Daten von 7 Tagen, damit die Analyse ein Modell erstellt.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig aktiviert, um die Grafik *Total Activity* auf der Seite **User Details** anzuzeigen. Wenn Sie die Grafik *Total Activity* auf der Seite **User Details** nicht anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk value of sense event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 5.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

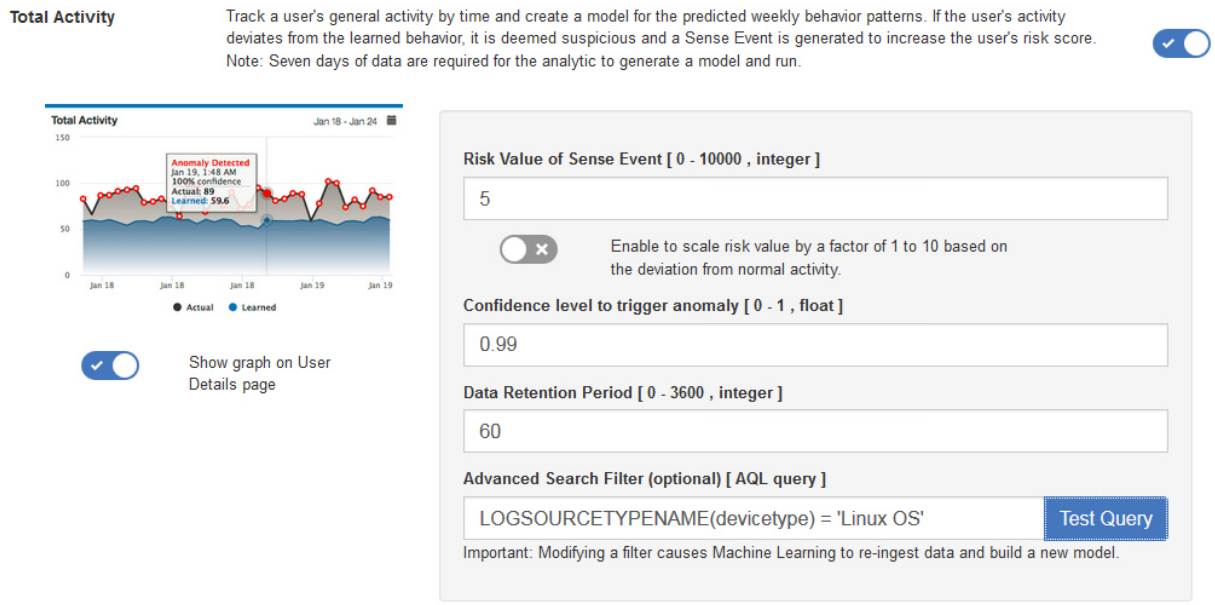
    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:
    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`

- **INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)**

Weitere Informationen finden Sie unter Ariel Query Language.

11. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Abnormal Outbound Transfer Attempts* (Abnormale abgehende Übertragungsversuche) konfigurieren

Konfigurieren Sie die Machine Learning-Analyse *Abnormal Outbound Transfer Attempts* (Abnormale abgehende Übertragungsversuche), um die abgehende Datenverkehrsnutzung für jeden Benutzer im **UBA-Dashboard** anzuzeigen.

Informationen zu diesem Vorgang

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Die Machine Learning-App *Abnormal Outbound Transfer Attempts* ist in V2.8.0 und höher verfügbar.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).

- Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).

3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Abnormal Outbound Transfer Attempts**.
4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Abnormal Outbound Transfer Attempts* zu aktivieren.

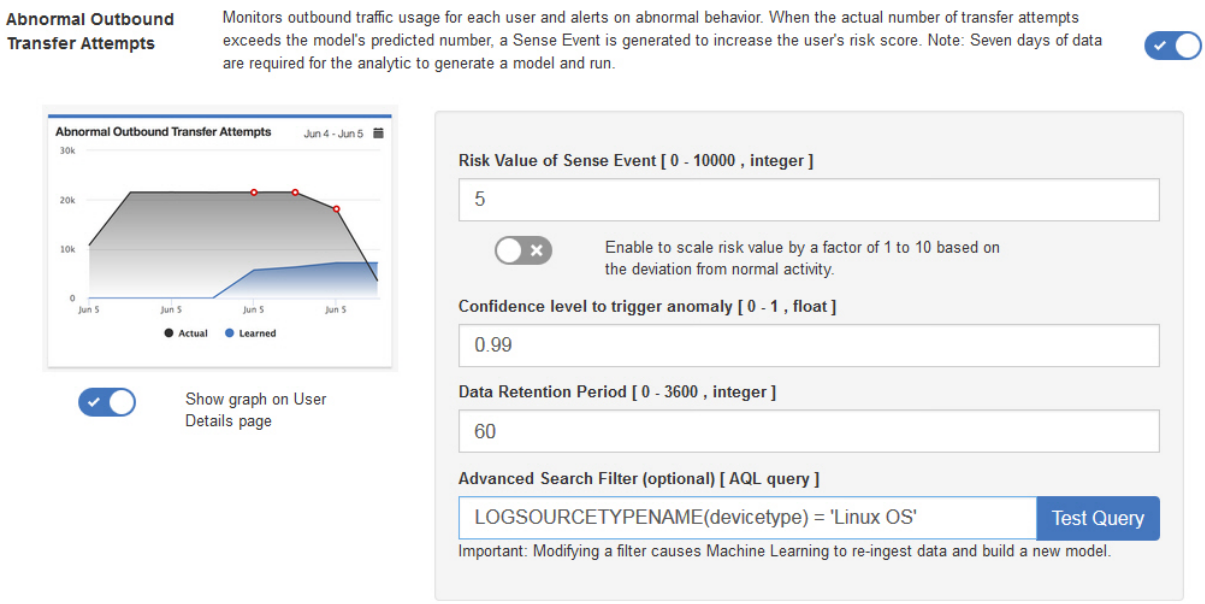
   Wichtig: Sie benötigen Daten aus 7 Tagen nach der Aktivierung von UBA-Inhalten auf dem System.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig inaktiviert. Wenn Sie die Grafik *Abnormal Outbound Transfer Attempts* auf der Seite **User Details** anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 5.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:

    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`

    Weitere Informationen finden Sie unter Ariel Query Language.
11. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Activity by Category* (Aktivität nach Kategorie) konfigurieren

Konfigurieren Sie die Machine Learning-Analyse *Activity by Category* (Aktivität nach Kategorie), um Muster für das tatsächliche und das erwartete Benutzerverhalten nach übergeordneter Kategorie im **UBA-Dashboard** anzuzeigen.

Informationen zu diesem Vorgang

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Wichtig: Mit V2.2.0 wurden die Standardwerte für **Risk value of sense event** (Risikowert des Prüfereignisses) geändert. Da die neuen Standardwerte deutlich unter den vorherigen Standardwerten liegen, überschreiben die neuen Standardwerte die bestehenden Standardwerte bzw. alle zuvor von Ihnen geänderten Werte.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).
3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Activity by Category** (Aktivität nach Kategorie).

4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Activity by Category* zu aktivieren und die Grafik *Activity by Category* auf der Seite **User Details** (Benutzerdetails) anzuzeigen.

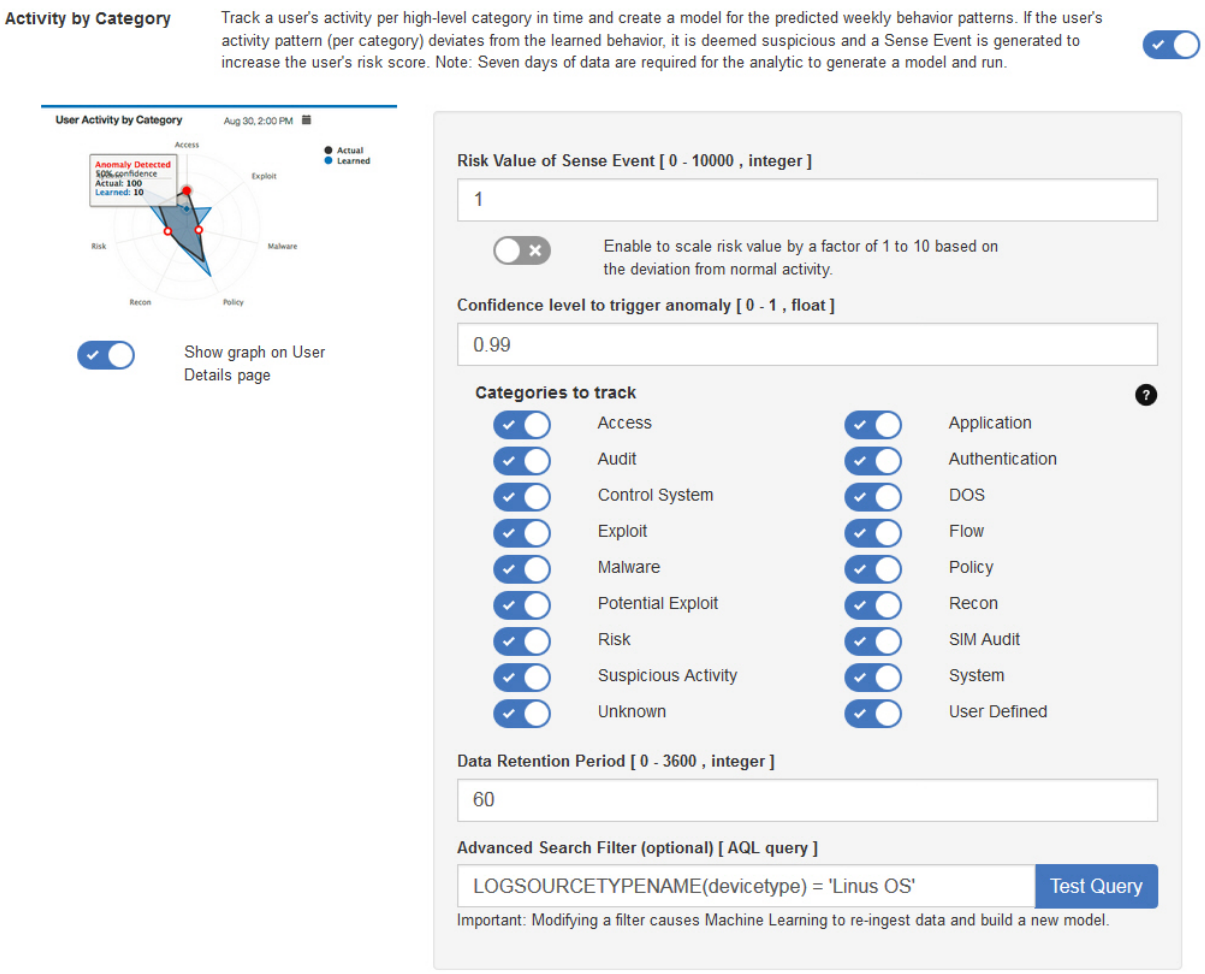
   Wichtig: Sie benötigen Daten aus 7 Tagen, damit die Analyse ein Modell erstellt. Wenn noch keine Benutzerdaten aus 7 Tagen für dieses QRadar-System vorliegen, wird das erste Modell erstellt, sobald Benutzerdaten aus 7 Tagen aufgelaufen sind.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig aktiviert, um die Grafik *Activity by Category* auf der Seite **User Details** anzuzeigen. Wenn Sie die Grafik *Activity by Category* auf der Seite 'User Details' nicht anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 1.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Im Abschnitt **Categories to track** (Zu verfolgende Kategorien) sind die übergeordneten Ereigniskategorien standardmäßig aktiviert. Klicken Sie auf eine Kategorie, um ihre Überwachung zu deaktivieren. Weitere Informationen über Kategorien finden Sie im Abschnitt High-level categories im IBM Knowledge Center.
10. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
11. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:

    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`

    Weitere Informationen finden Sie unter Ariel Query Language.
12. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Risk Posture* (Risikoneigung)

Konfigurieren Sie die Machine Learning-App *Risk Posture* (Risikoneigung), um die Abweichung der Risikobewertung des Benutzers im **UBA-Dashboard** anzuzeigen.

Informationen zu diesem Vorgang

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Wichtig: Mit V2.2.0 wurden die Standardwerte für **Risk value of sense event** (Risikowert des Prüfereignisses) geändert. Da die neuen Standardwerte deutlich unter den vorherigen Standardwerten liegen, überschreiben die neuen Standardwerte die bestehenden Standardwerte bzw. alle zuvor von Ihnen geänderten Werte.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.

- Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü ( ) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.

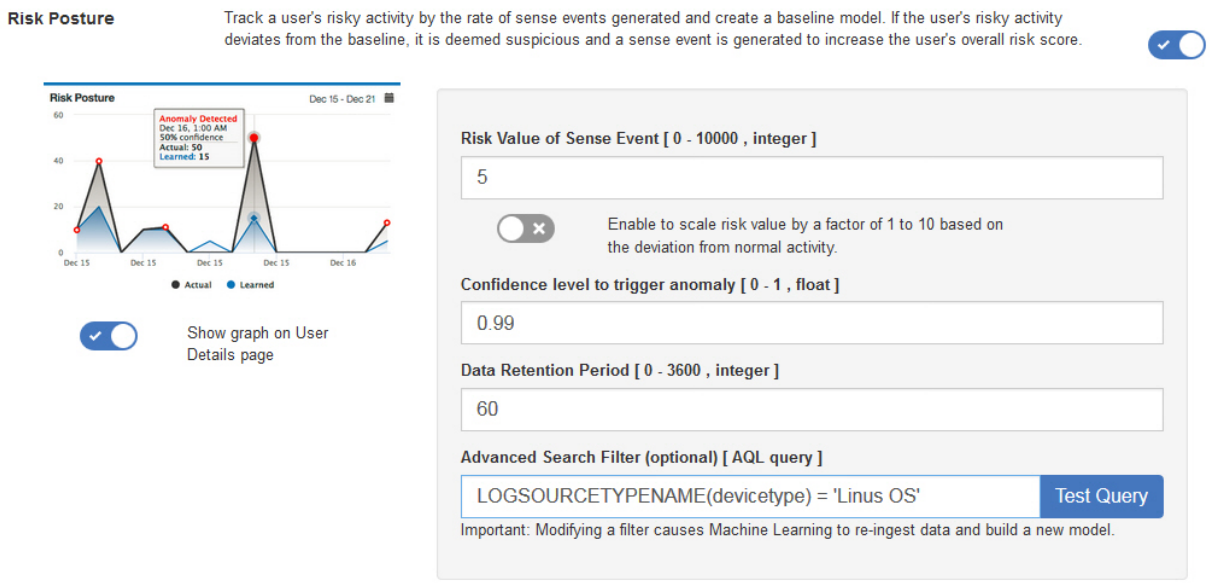
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).
3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Risk Posture** (Risikoneigung).
4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Risk Posture* zu aktivieren.

   Wichtig: Sie benötigen Daten von 7 Tagen, damit die Analyse ein Modell erstellt.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig aktiviert, um die Grafik *Risk Posture* auf der Seite **User Details** anzuzeigen. Wenn Sie die Grafik *Risk Posture* auf der Seite 'User Details' nicht anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 5.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:
    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`

    Weitere Informationen finden Sie unter Ariel Query Language.
11. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Abnormal Volume of Data to External Domains* konfigurieren

Konfigurieren Sie die Machine Learning-App *Abnormal Volume of Data to External Domains* (Abnormales Datenvolumen an externe Domänen), um das tatsächliche und erwartete (erlernte) Datenvolumen, das vom lokalen an einen fernen Standort hochgeladen wurde, für jeden Benutzer im **UBA-Dashboard** anzuzeigen.

Informationen zu diesem Vorgang

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Die Machine Learning-App *Abnormal Volume of Data to External Domains* ist in V3.0.0 und höher verfügbar.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).
3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Abnormal Volume of Data to External Domains**.

4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Abnormal Volume of Data to External Domains* zu aktivieren.

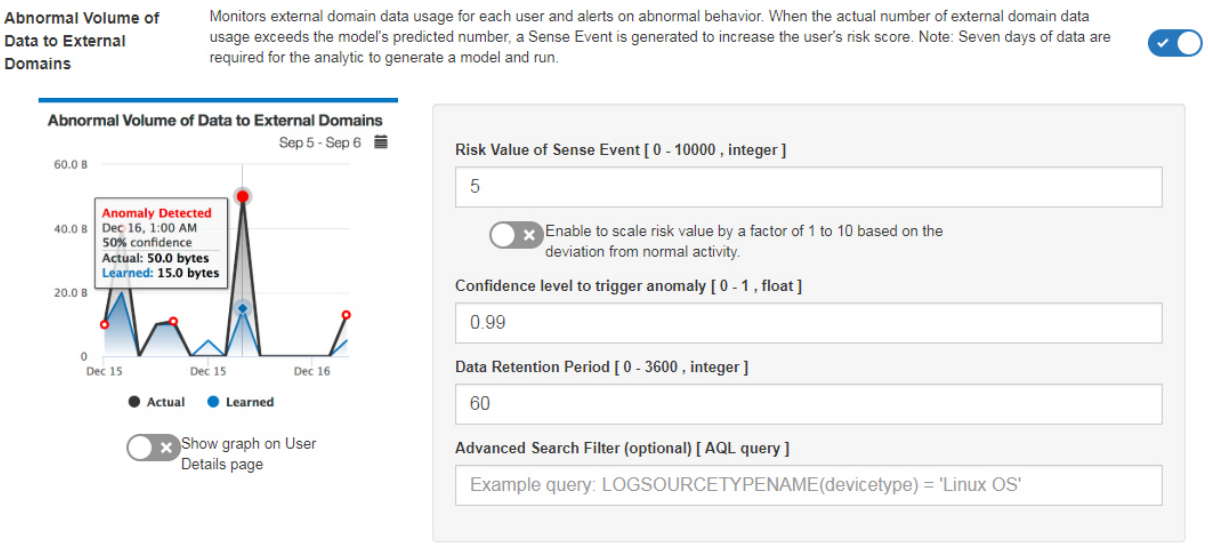
   Wichtig: Sie benötigen Daten aus 7 Tagen nach der Aktivierung von UBA-Inhalten auf dem System.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig inaktiviert. Wenn Sie die Grafik *Abnormal Volume of Data to External Domains* auf der Seite **User Details** anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 1.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:

    - **`REFERENCESETCONTAINS('Important People', Benutzername)`**
    - **`LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`**
    - **`INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`**

    Weitere Informationen finden Sie unter Ariel Query Language.
11. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Activity Distribution* (Aktivitätsverteilung) konfigurieren

Konfigurieren Sie die Machine Learning-Analyse *Activity Distribution* (Aktivitätsverteilung), um dynamische Verhaltenscluster für alle Benutzer anzuzeigen, die von Machine Learning im **UBA-Dashboard** überwacht werden.

Informationen zu diesem Vorgang

Die Machine Learning-Analyse *Activity Distribution* ist in V2.2.0 und höher verfügbar.

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü ( ) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).
3. Klicken Sie auf der Seite **Machine Learning Settings** auf **Activity Distribution** (Aktivitätsverteilung).
4. Klicken Sie auf **Enabled** (Aktiviert) , um die Analyse *Activity Distribution* zu aktivieren und die Grafik *Activity Distribution* auf der Seite **User Details** (Benutzerdetails) anzuzeigen.

   Wichtig: Sie benötigen Daten von 7 Tagen, damit die Analyse ein Modell erstellt.

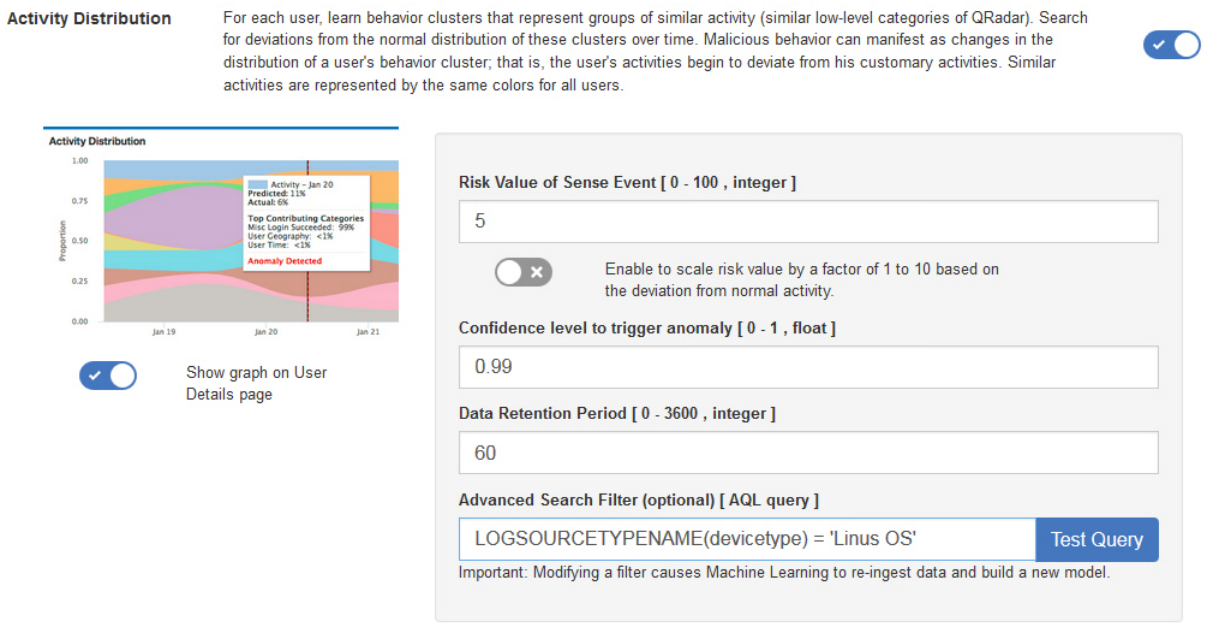
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig aktiviert, um die Grafik *Activity Distribution* auf der Seite **User Details** anzuzeigen. Wenn Sie die Grafik *Activity Distribution* auf der Seite 'User Details' nicht anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 5.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:

    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`

    Weitere Informationen finden Sie unter Ariel Query Language.
11. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Defined Peer Group* (Definierte Peergruppe) konfigurieren

Konfigurieren Sie die Machine Learning-App *Defined Peer Group* (Definierte Peergruppe), um anzuzeigen, in welchem Maß die Ereignisaktivität eines Benutzers von der Ereignisaktivität der zugehörigen definierten Peergruppe im **UBA-Dashboard** abweicht.

Vorbereitende Schritte

- Zum Aktivieren der Analyse *Defined Peer Group* müssen gültige Benutzergruppen in einer Referenztabelle vorhanden sein. Sie müssen **UBA Settings** > **Display Attributes** > **Custom Groups** (UBA-Einstellungen > Attribute anzeigen > Angepasste Gruppen) konfigurieren, damit Sie die Referenztabelle verwenden können. Weitere Informationen finden Sie im Abschnitt „Benutzergruppen für die Analyse 'Defined Peer Group'" auf Seite 204.
- Sie benötigen Ereignisdaten von 7 Tagen, damit die Analyse ein Modell erstellt.

Informationen zu diesem Vorgang

Die Machine Learning-Analyse *Defined Peer Group* ist in V2.6.0 und höher verfügbar.

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).

- Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
- Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).

3. Klicken Sie auf der Seite **Machine Learning Settings** auf *Defined Peer Group*.
4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Defined Peer Group* zu aktivieren.

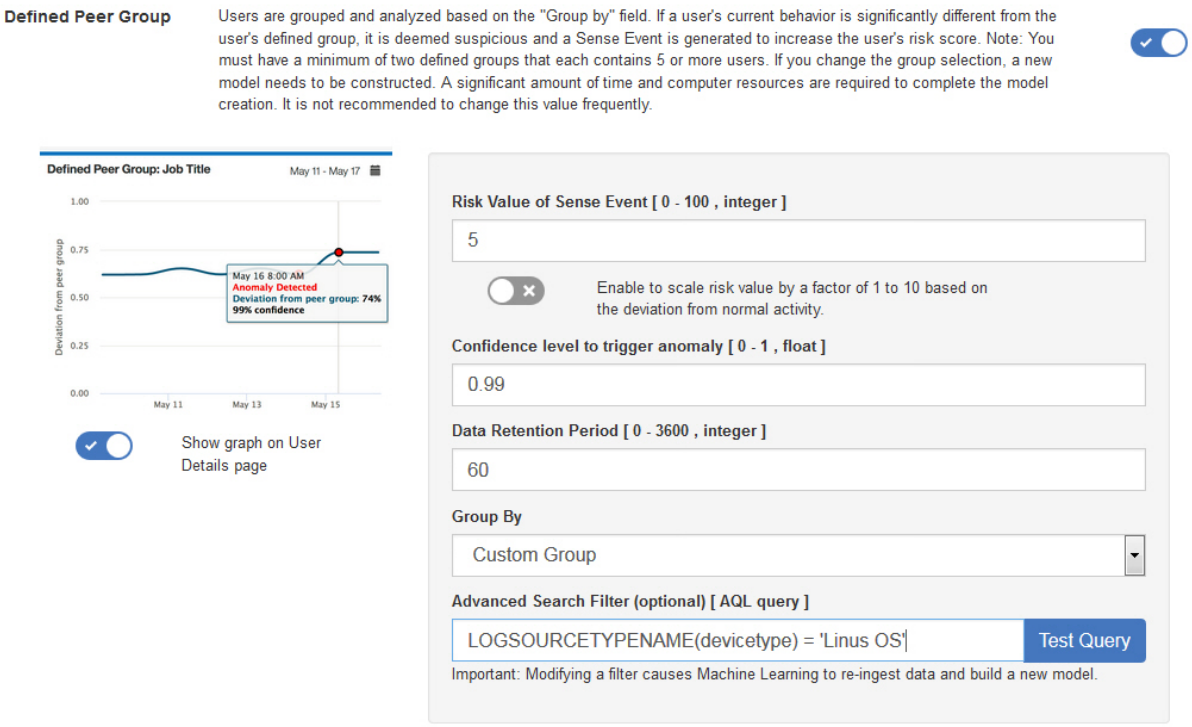
   Wichtig: Sie benötigen Daten von 7 Tagen, damit die Analyse ein Modell erstellt.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig aktiviert, um die Grafik *Defined Peer Group* auf der Seite **User Details** anzuzeigen. Wenn Sie die Grafik *Defined Peer Group* auf der Seite **User Details** nicht anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 5.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Wählen Sie im Feld **Group By** (Gruppieren nach) die Gruppe aus, die die Analyse *Defined Peer Group* anwenden soll.
11. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:

    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`

    Weitere Informationen finden Sie unter Ariel Query Language.
12. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

Analyse *Learned Peer Group* (Erlernte Peergruppe) konfigurieren

Konfigurieren Sie die Machine Learning-Analyse *Learned Peer Group* (Erlernte Peergruppe), um im **UBA-Dashboard** anzuzeigen, in welchem Maß der Benutzer von der abgeleiteten Peergruppe abweicht, der er als zugehörig betrachtet wurde.

Vorbereitende Schritte

- Sie müssen einen App-Knoten installieren, um die Analyse *Learned Peer Group* zu aktivieren. Weitere Informationen finden Sie im Abschnitt https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_adm_appnode_intro.html.
- Sie benötigen Ereignisdaten aus 7 Tagen, damit die Analyse *Learned Peer Group* ein Modell erstellt.

Informationen zu diesem Vorgang

Die Machine Learning-Analyse *Learned Peer Group* ist in V2.2.0 und höher verfügbar.

Achtung: Nach der Konfiguration der Einstellungen dauert es mindestens eine Stunde, Daten aufzunehmen, ein erstes Modell zu erstellen und erste Ergebnisse für Benutzer zu sehen.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.

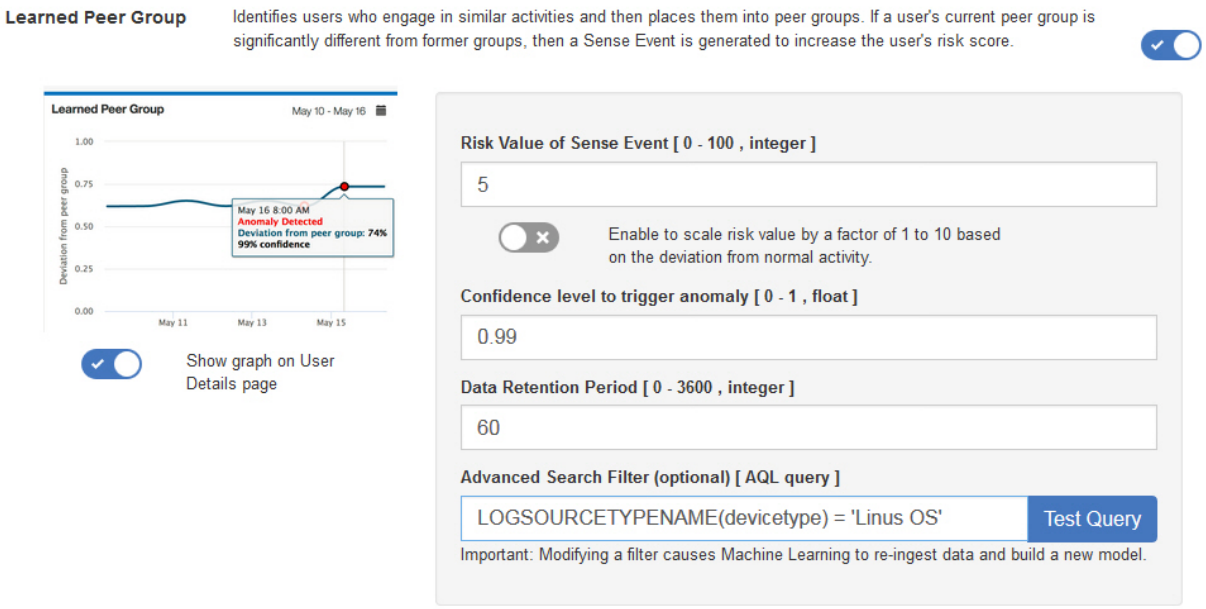
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).
3. Klicken Sie auf der Seite **Machine Learning Settings** auf *Learned Peer Group*.
4. Klicken Sie auf **Enabled** (Aktiviert)  , um die Analyse *Learned Peer Group* zu aktivieren.

   Wichtig: Sie benötigen Daten von 7 Tagen, damit die Analyse ein Modell erstellt.
5. Die Umschaltfunktion **Show graph on User Details page** (Grafik auf Seite mit Benutzerdetails anzeigen) ist standardmäßig aktiviert, um die Grafik *Learned Peer Group* auf der Seite **User Details** anzuzeigen. Wenn Sie die Grafik *Learned Peer Group* auf der Seite **User Details** nicht anzeigen möchten, klicken Sie auf das Umschaltsymbol.
6. Geben Sie im Feld **Risk Value of Sense Event** (Risikowert des Prüfereignisses) an, um wie viel die Risikobewertung des Benutzers erhöht werden soll, wenn ein Prüfereignis ausgelöst wird. Der Standardwert ist 5.
7. Aktivieren Sie den Umschalter, um den Risikowert zu skalieren. Ist er aktiviert, wird der Basisrisikowert mit einem Faktor (von 1 - 10) multipliziert. Dieser Faktor wird dadurch bestimmt, um stark der Benutzer von seinem erwarteten Verhalten abweicht, nicht nur dadurch, dass er davon abweicht.
8. Geben Sie im Feld **Confidence interval to trigger anomaly** (Konfidenzintervall für das Auslösen einer Anomalie) in Prozent an, wie sicher der Machine Learning-Algorithmus sein sollte, bevor er ein Anomalieereignis auslöst. Der Standardwert ist 0,99.
9. Legen Sie im Feld **Data Retention Period** (Datenaufbewahrungszeitraum) fest, wie viele Tage die Modelldaten gespeichert werden sollen. Der Standardwert ist 60. Wenn Sie die automatische Bereinigung von Daten deaktivieren möchten, legen Sie den Wert 0 (null) fest.
10. Optional: Im Feld **Advanced Search Filter** (Filter für erweiterte Suche) können Sie einen AQL-Filter hinzufügen, um die Daten einzugrenzen, die von der Analyse in QRadar abgefragt werden. Durch das Filtern mit einer AQL-Abfrage können Sie die Anzahl der Benutzer oder die Datentypen reduzieren, die in der Analyse analysiert werden. Vor dem Speichern der Konfiguration klicken Sie auf **Test Query** (Abfrage testen), um eine vollständige AQL-Abfrage in QRadar zu starten, damit Sie die Abfrage überprüfen und die Ergebnisse bestätigen können.

    Wichtig: Wenn Sie den AQL-Filter ändern, wird das vorhandene Analysemodell als ungültig markiert und erneut erstellt. Die Dauer der Neuerstellung ist von der Datenmenge abhängig, die vom geänderten Filter zurückgegeben wird.

    Sie können für das Filtern bestimmte Protokollquellen, Netznamen oder Referenzsets verwenden, die spezifische Benutzer enthalten. Hier finden Sie Beispiele dazu:
    - `REFERENCESETCONTAINS('Important People', Benutzername)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', Quellen-IP) oder INCIDR('10.0.0.0/8', Quellen-IP) oder INCIDR('192.168.0.0/16', Quellen-IP)`

    Weitere Informationen finden Sie unter Ariel Query Language.
11. Klicken Sie auf **Save Configuration** (Konfiguration speichern).



Ergebnisse

Es kann mindestens eine Stunde dauern, bis die App Daten aufgenommen und ein erstes Modell erstellt hat.

UBA-Dashboard mit Machine Learning Analytics

Die IBM QRadar-App "User Behavior Analytics" (UBA) mit Machine Learning Analytics umfasst den Status von Machine Learning Analytics sowie weitere Details für den ausgewählten Benutzer.

Dashboard

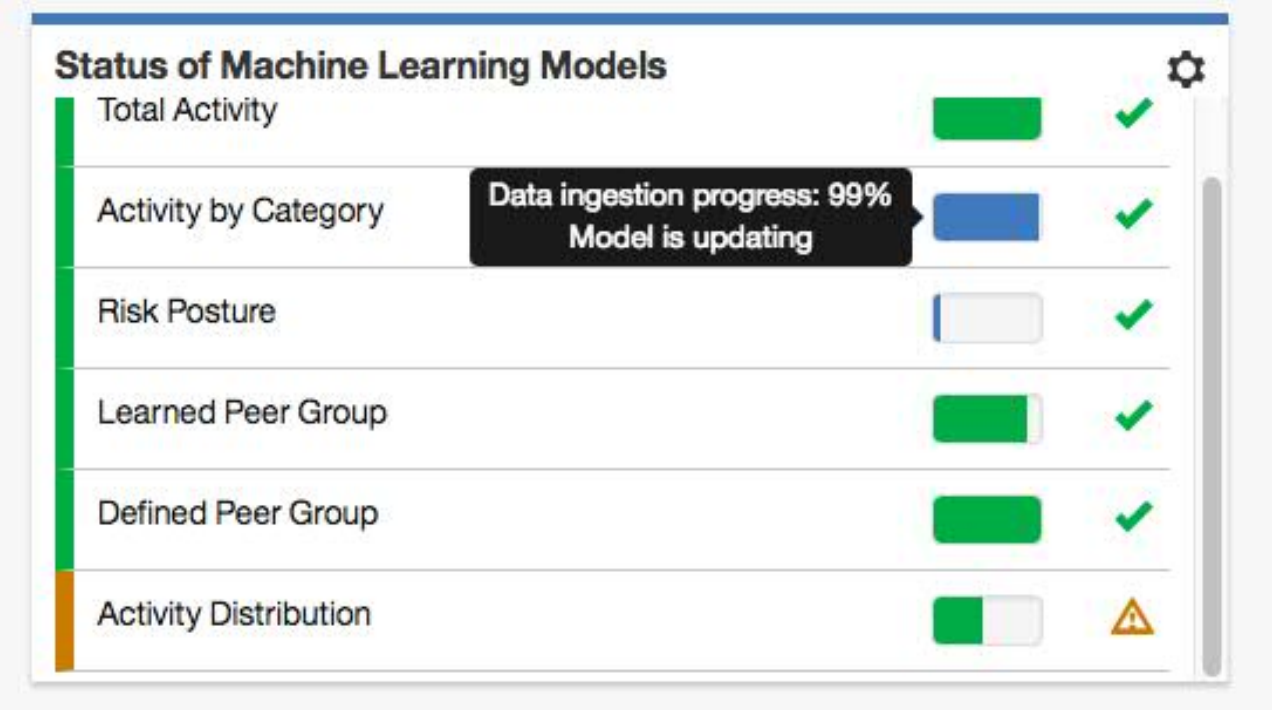
Klicken Sie nach Aktivierung von Machine Learning Analytics auf die Registerkarte **Benutzeranalyse**, um das Dashboard zu öffnen.

Im Abschnitt 'Status of Machine Learning Models' (Status der Machine Learning-Modelle) wird der Fortschritt bei der Modellaufnahme und Modellerstellung für jede von Ihnen aktivierte Analyse gezeigt. Beachten Sie, dass die Modelle alle sieben Tage aktualisiert werden.

- Die blaue Fortschrittsleiste zeigt an, dass Daten in die Analyse aufgenommen werden.
- Die grüne Fortschrittsleiste zeigt an, dass das Modell in der Analyse erstellt wird.
- Das grüne Häkchen zeigt an, dass die Analyse aktiviert ist.
- Das gelbe Warnsymbol zeigt an, dass in der Modellerstellungsphase ein Problem erkannt wurde. Weitere Informationen finden Sie im Abschnitt „Warnung in Statusanzeige für App 'Machine Learning' im Dashboard" auf Seite 208

Klicken Sie auf das Symbol **ML Settings** (ML-Einstellungen) , um die Seite 'Machine Learning Analytics' zu öffnen, und bearbeiten Sie die Konfiguration für die Anwendungsfälle von Machine Learning Analytics.

Anmerkung: Wenn Sie die Konfiguration bearbeiten, nachdem sie gespeichert wurde, wird ein neues Modell erstellt und die Wartezeit für die Aufnahme von Daten und die Modellerstellung wird zurückgesetzt.

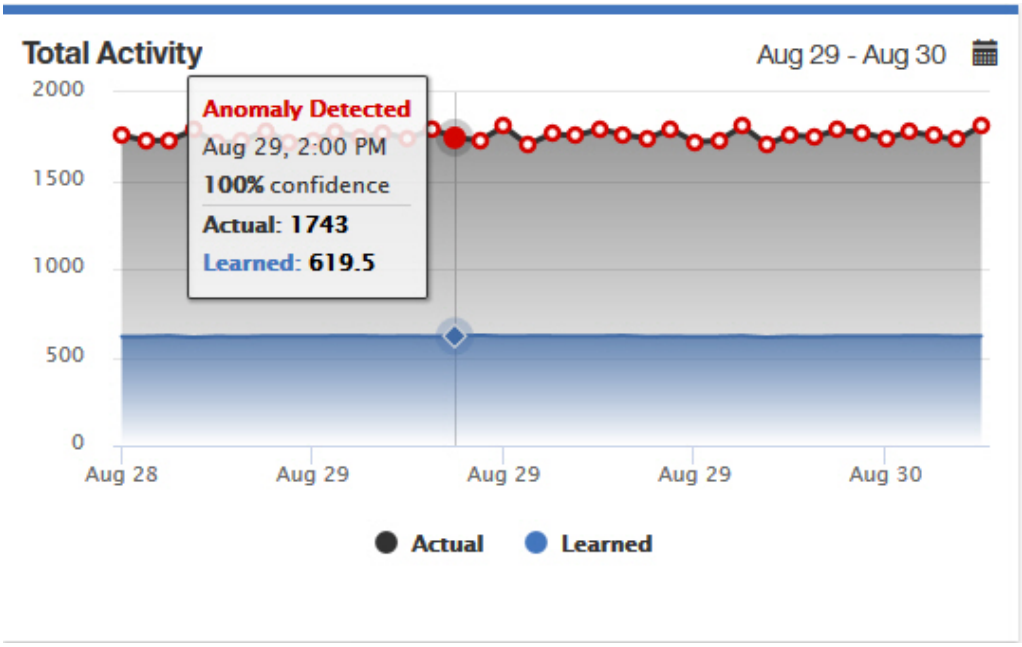


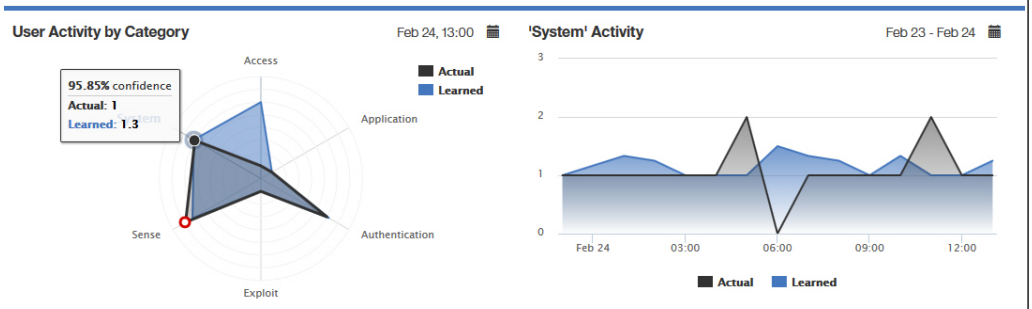
Seite mit den Benutzerdetails

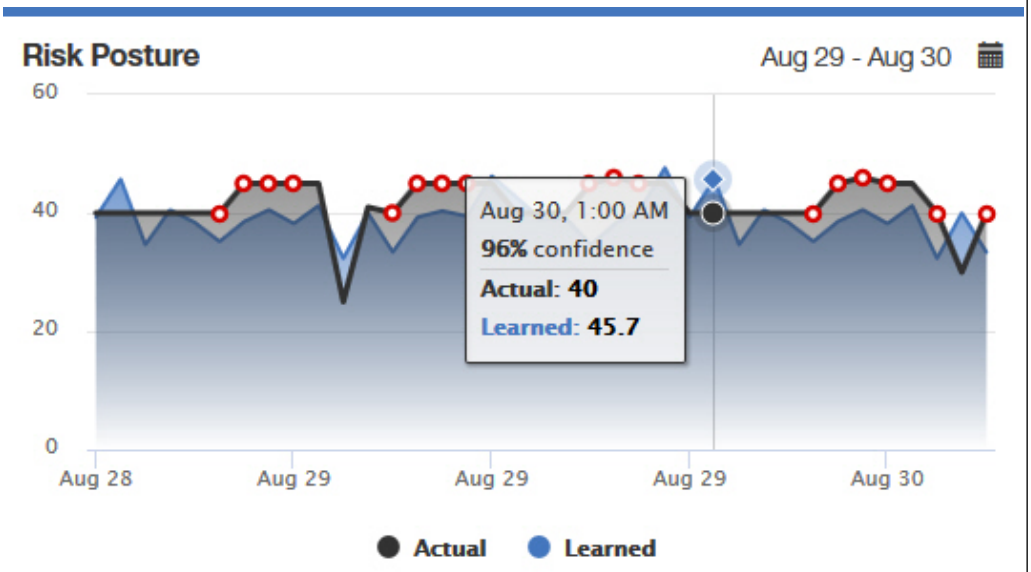
Die Details eines Benutzers können Sie überall in der App anzeigen, indem Sie auf dessen Benutzernamen klicken.

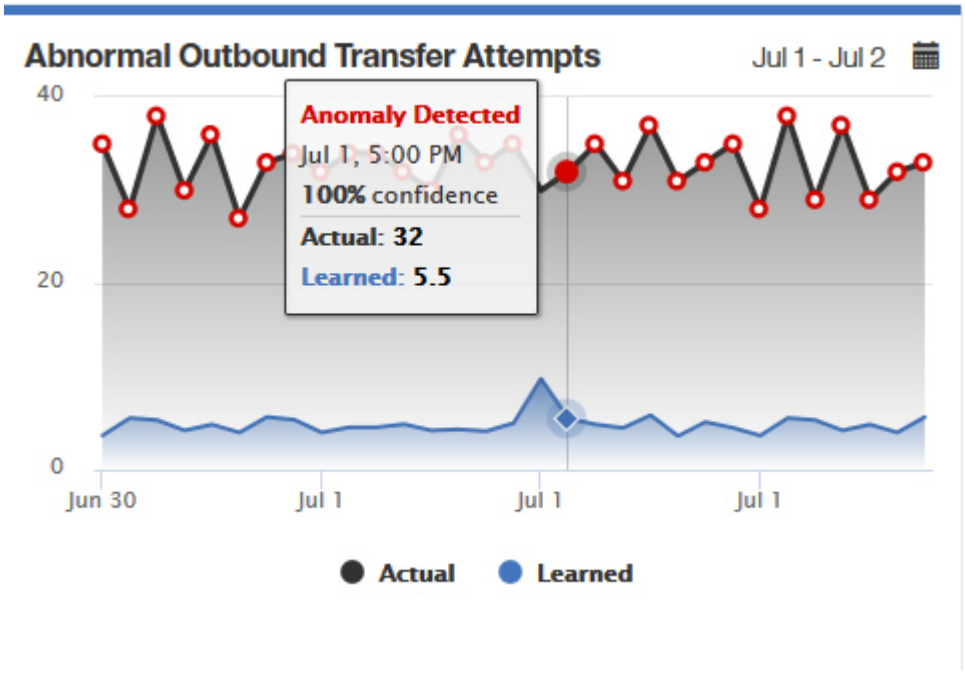
Ab V2.5.0 erhalten Sie im Fenster *Event Viewer* (Ereignisanzeige) weitere Informationen zu den Aktivitäten von Benutzern. In der Ereignisanzeige werden Details zu einer ausgewählten Aktivität oder einem Zeitpunkt angezeigt. Wenn Sie auf ein Ereignis im Fenster 'Event Viewer' klicken, finden Sie weitere Einzelheiten wie Syslog-Ereignisse und Nutzdaten. Das Fenster mit der Ereignisanzeige ist für alle Ring- und Kurvendiagramme auf der Seite **Benutzerangaben** verfügbar.

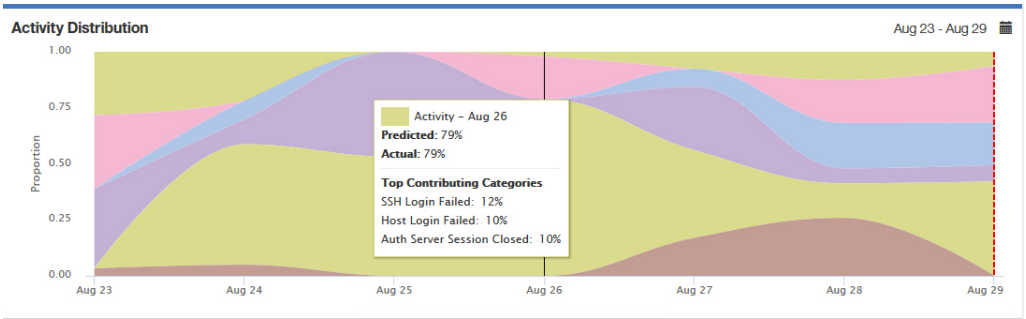
In der folgenden Tabelle werden die Machine Learning Analytics-Grafiken beschrieben, die auf der Seite **User Details** (Benutzerdetails) verfügbar sind.

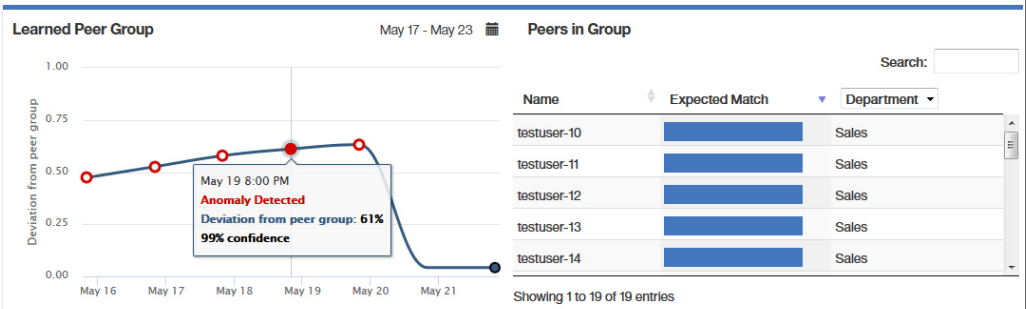
Total Activity (Gesamtaktivität)	Zeigt die tatsächliche und erwartete (erlernte) Aktivitätsauslastung der Benutzer über den ganzen Tag an. Die tatsächlichen Werte entsprechen der Anzahl Ereignisse für den Benutzer während des ausgewählten Zeitraums. Die erwarteten Werte entsprechen der Anzahl Ereignisse, die für den Benutzer während des ausgewählten Zeitraums vorhergesagt wurden. Ein roter Kreis zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. In der Grafik 'Total Activity' (Gesamtaktivität) haben Sie folgende Möglichkeiten: • Sie können auf einen Datenknoten klicken und eine Abfrageliste der Ereignisse abrufen, die die Anomalie ausmachen. • Sie können auf das Kalendersymbol klicken, um einen benutzerdefinierten Zeitraum anzugeben. 

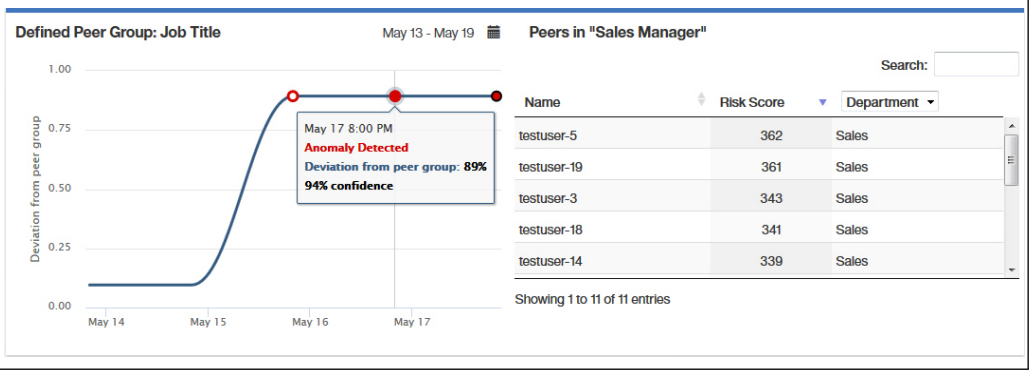
User Activity by Category (Benutzeraktivität nach Kategorie)	Zeigt die tatsächlichen und erwarteten Verhaltensmuster der Benutzeraktivität nach High-Level-Kategorie an. Die tatsächlichen Werte entsprechen der Anzahl Ereignisse pro High-Level-Kategorie für den Benutzer während des ausgewählten Zeitraums. Die erwarteten Werte entsprechen der vorhergesagten Anzahl Ereignisse pro High-Level-Kategorie für den Benutzer während des ausgewählten Zeitraums. Ein roter Kreis zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. In der Grafik 'User Activity by Category' (Benutzeraktivität nach Kategorie) haben Sie folgende Möglichkeiten: • Sie können auf das Kalendersymbol klicken, um ein Datum und eine Uhrzeit anzugeben. • Sie können auf eine Kategorie klicken, um die Zeitleistengrafik für die ausgewählte Kategorie zu öffnen. In der Zeitleistengrafik für die ausgewählte Kategorie haben Sie folgende Möglichkeiten: • Sie können auf einen Datenknoten klicken und eine Abfrageliste der Ereignisse abrufen, die den Knoten repräsentieren. • Sie können auf das Kalendersymbol klicken, um einen benutzerdefinierten Zeitraum anzugeben. 

Risk Posture (Risikoneigung)	Zeigt an, ob die Risikobewertung für einen Benutzer vom erwarteten Risikobewertungsmuster abweicht. Die tatsächlichen Werte entsprechen der Summe der Prüfwerte für die Prüfereignisse für den Benutzer während des ausgewählten Zeitraums. Die erwarteten Werte entsprechen der vorhergesagten Summe der Prüfwerte für die Prüfereignisse für den Benutzer während des ausgewählten Zeitraums. Ein roter Kreis zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. In der Grafik 'Risk Posture' (Risikoneigung) haben Sie folgende Möglichkeiten: • Sie können auf einen Knoten klicken und eine Abfrageliste der Ereignisse abrufen. • Sie können auf das Kalendersymbol klicken, um einen benutzerdefinierten Zeitraum anzugeben. 

Abnormal Outbound Transfer Attempts (Abnormale abgehende Übertragungsversuche)	Es wird angezeigt, ob die abgehende Datenverkehrsnutzung eines Nutzer vom erwarteten Verhalten abweicht. Die tatsächlichen Werte entsprechen der Anzahl der Übertragungsversuche für diesen Benutzer während des ausgewählten Zeitraums. Die erlernten Werte sind die vorhergesagte Anzahl an Übertragungsversuchen im Modell. Ein roter Kreis zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. In der Grafik 'Abnormal Outbound Transfer Attempts' haben Sie folgende Möglichkeiten: • Sie können auf einen Knoten klicken und eine Abfrageliste der Ereignisse abrufen. • Sie können auf das Kalendersymbol klicken, um einen benutzerdefinierten Zeitraum anzugeben. 

Activity Distribution (Aktivitätsverteilung, V2.2.0 oder höher)	Zeigt dynamische Verhaltenscluster für alle Benutzer an, die von Machine Learning überwacht werden. Die Cluster werden von den Low-Level-Aktivitätskategorien für alle Benutzer, die von Machine Learning überwacht werden, abgeleitet. Die tatsächlichen Werte entsprechen der Übereinstimmung in Prozent für den jeweiligen Cluster. Die erwarteten Werte entsprechen der vorhergesagten Übereinstimmung in Prozent für den jeweiligen Cluster. Jede Farbe in der Grafik steht für einen eindeutigen dynamischen Verhaltenscluster für alle von Machine Learning überwachten Benutzer. Eine Farbe, die zur Bezeichnung einer einzelnen Gruppe verwendet wird, ist für alle Benutzer dieselbe. Eine rote vertikale Linie zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. In der Grafik 'Activity Distribution' (Aktivitätsverteilung) haben Sie folgende Möglichkeiten: • Sie können den Mauszeiger über jeden einzelnen Cluster bewegen, um die tatsächlichen und vorhergesagten Aktivitätsperzentile und die wichtigsten drei beitragenden Low-Level-Kategorien anzuzeigen. • Über das Kalendersymbol können Sie auch einen anderen Zeitraum angeben. 

Learned Peer Group (Erlernte Peergruppe, V2.2.0 oder höher)	Zeigt an, wie stark der Benutzer von der abgeleiteten Peergruppe abwich, der er als zugehörig betrachtet wurde. Die 'Learned Peer Group' wird von den Low-Level-Aktivitätskategorien für den Benutzer abgeleitet. Ein roter Kreis zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. **Deviation from peer group** (Abweichung von Peergruppe) zeigt die Abweichung eines Benutzers von seiner abgeleiteten Peergruppe in Prozent an. **Confidence** (Konfidenz) ist die Perzentile der Abweichung in Bezug auf die Protokolldaten, auf denen das Modell basiert. Es wird eine Benachrichtigung ausgelöst, wenn sowohl die Abweichung als auch die Konfidenz den jeweiligen Schwellenwert überschreiten. In der Grafik 'Learned Peer Group' (Erlernte Peergruppe) haben Sie folgende Möglichkeiten: • Sie können auf einen Datenpunkt klicken, um die Tabelle 'Peers in Group' (Peers in der Gruppe) anzuzeigen. • Über das Kalendersymbol können Sie auch einen anderen Zeitraum angeben. In der Tabelle 'Peers in Group' werden alle Benutzer angezeigt, die in der Gruppe erwartet werden und die tatsächlich in der Gruppe enthalten sind. Sie haben folgende Möglichkeiten: • Klicken Sie auf einen Benutzernamen, um die Seite **User Details** (Benutzerdetails) zu öffnen. • **Expected match** (Erwartete Übereinstimmung) zeigt an, wie sicher sich die Analyse ist, dass der Benutzer in der Gruppe enthalten ist. • Sie können auf die Dropdown-Liste klicken, um die anzuzeigenden Benutzerattribute auszuwählen. • Sie können eine Suche durchführen, um die Benutzernamen zu filtern. 

Defined peer group (Definierte Peergruppe, V2.6.0 oder höher)	Es wird gezeigt, in welchem Maß die Ereignisaktivität eines Benutzers von der der zugehörigen definierten Peergruppe abweicht. Die Analyse verwendet die Low-Level-Aktivitätskategorien der Ereignisse des Benutzers, um die Abweichung des Benutzers von der zugehörigen definierten Peergruppe zu bestimmen. Ein roter Kreis zeigt an, dass eine Anomalie erkannt wurde und Machine Learning ein Prüfereignis generiert hat. **Deviation from peer group** (Abweichung von Peergruppe) zeigt die Abweichung eines Benutzers von seiner definierten Peergruppe in Prozent an. **Confidence** (Konfidenz) ist die Perzentile der Abweichung in Bezug auf die Protokolldaten, auf denen das Modell basiert. Es wird eine Benachrichtigung ausgelöst, wenn sowohl die Abweichung als auch die Konfidenz den jeweiligen Schwellenwert überschreiten. Zur Anzeige der Analyse 'Defined peer group' müssen Sie Benutzergruppen definieren. Weitere Informationen finden Sie im Abschnitt „Benutzergruppen für die Analyse 'Defined Peer Group'". In der Grafik 'Defined Peer Group' (Definierte Peergruppe) haben Sie folgende Möglichkeiten: • Klicken Sie auf einen Datenpunkt, um die Peers in der Tabelle 'Your defined peer group' (Ihre definierte Peergruppe) anzuzeigen. • Über das Kalendersymbol können Sie auch einen anderen Zeitraum angeben. Die Peers in der Tabelle 'Your defined peer group' zeigen den bedenklichsten Benutzer in der Gruppe des aktuellen Benutzers. Sie haben folgende Möglichkeiten: • Klicken Sie auf einen Benutzernamen, um die Seite **User Details** (Benutzerdetails) zu öffnen. • Sie können auf die Dropdown-Liste klicken, um die anzuzeigenden Benutzerattribute auszuwählen. • Sie können eine Suche durchführen, um die Benutzernamen zu filtern. 

Benutzergruppen für die Analyse 'Defined Peer Group'

Sie können die Analyse 'Defined Peer Group' (Definierte Peergruppe) in der Machine Learning-App aktivieren, wenn UBA für die Verwendung einer Referenztabelle konfiguriert ist, die mindestens zwei Gruppierungen mit mindestens fünf Benutzern enthält, wobei eine der Gruppen ausgewählt ist.

Anmerkung: In V2.6.0 oder höher können Sie Benutzergruppen in UBA extrahieren und die Analyse 'Defined Peer Group' aktivieren.

Bei der Auswahl für die Gruppierung handelt es sich um **Job Title** (Jobbezeichnung), **Department** (Abteilung) oder um eine angepasste Eigenschaft, die Sie auf der Seite **UBA Settings** (UBA-Einstellungen) unter 'Display Attributes' (Attribute anzeigen) im Feld **Custom Group** (Angepasste Gruppe) definieren. Wenn UBA mehr als zwei eindeutige Gruppen mit jeweils mindestens fünf Benutzern erkennt, kann die Analyse 'Defined Peer Group' aktiviert werden. Um gültige Benutzergruppen zu erhalten, können Sie die App 'Reference Data Import LDAP' konfigurieren, damit die Benutzereigenschaften ('Job Title','Department' oder

eine andere Gruppierung für LDAP-Attribute) als Referenztabelle extrahiert werden können. Anschließend können Sie UBA für die Verwendung der erstellten Referenztabelle konfigurieren.

Mit der Analyse 'Defined Peer Group' können bis zu 20 Gruppen überwacht werden. Es werden die 20 größten Gruppen im konfigurierten Feld **Group By** (Gruppieren nach) ausgewählt. Die Anzahl der zu überwachenden Benutzern wird proportional von jeder Gruppe reduziert, um den Grenzwert für die überwachten Benutzern entsprechend der Größe Ihrer Machine Learning-Installation zu erreichen.

Hinweis: Beim Import der Referenztabelle wird ein Intervall für die Wiederholungen von mindestens 2 Stunden eingehalten, wie auf der Seite **UBA Settings** konfiguriert wurde. Alle neuen Benutzergruppierungsattribute werden importiert, sobald der Importvorgang nach dem Zeitplan ausgeführt wird.

App 'Machine Learning Analytics' deinstallieren

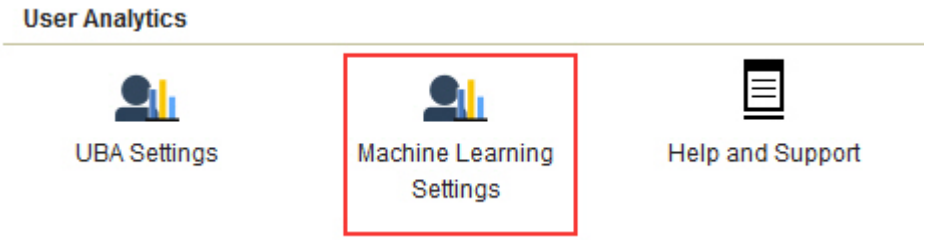
Die App 'Machine Learning Analytics' wird über die Seite 'Machine Learning Settings' (ML-Einstellungen) deinstalliert.

Informationen zu diesem Vorgang

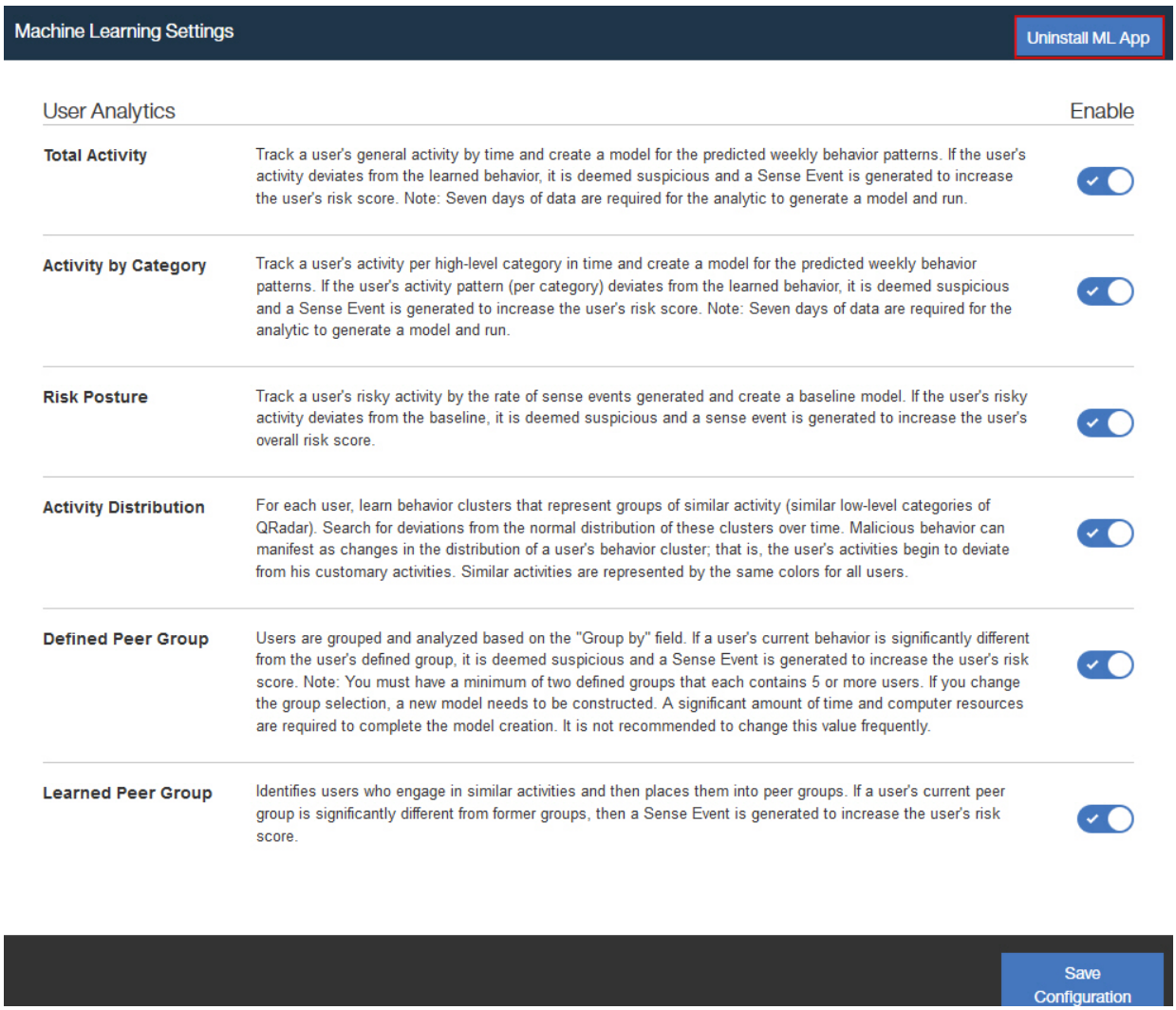
Bevor Sie die UBA-App deinstallieren, müssen Sie die unten beschriebene Prozedur zur Deinstallation der ML-App ausführen. Wenn Sie die ML-App nicht vor der Deinstallation von UBA deinstallieren, müssen Sie sie aus der interaktiven API-Dokumentationsschnittstelle entfernen.

Vorgehensweise

1. Öffnen Sie die Einstellungen für **Verwaltung**:
   - Klicken Sie in IBM QRadar V7.3.0 oder früher auf die Registerkarte **Verwaltung**.
   - Klicken Sie in IBM QRadar V7.3.1 und höher auf das Navigationsmenü (☰) und anschließend auf **Verwaltung**, um die Verwaltungsregisterkarte zu öffnen.
2. Klicken Sie auf das Symbol **Machine Learning Settings** (Einstellungen für Machine Learning).
   - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Machine Learning Settings** (Plug-ins > Benutzeranalyse > Einstellungen für Machine Learning).
   - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Machine Learning Settings** (Apps > Benutzeranalyse > Einstellungen für Machine Learning).



3. Klicken Sie in der Anzeige 'Machine Learning Settings' (ML-Einstellungen) auf **Uninstall ML App** (ML-App deinstallieren).



4. Klicken Sie in der Eingabeaufforderung für die Deinstallation auf **Yes** (Ja).

Nächste Schritte

Sie müssen zunächst den Browser-Cache löschen, bevor Sie sich an der QRadar-Konsole erneut anmelden.

10 Fehlerbehebung und Unterstützung

Sie können mithilfe der Fehlerbehebungs- und Unterstützungsinformationen Probleme mit Ihrem IBM Produkt eingrenzen und lösen.

Antworten auf allgemeine Unterstützungsfragen zu den Apps 'User Behavior Analytics' und 'Machine Learning Analytics' finden Sie unter https://developer.ibm.com/answers/topics/uba/

Seite mit Hilfe und Unterstützung für UBA

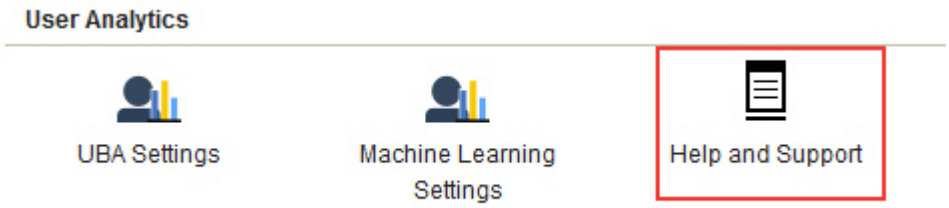
Die UBA-App (V2.5.0) beinhaltet einen Abschnitt mit Hilfe und Unterstützung bei der Verwendung der UBA-App, der LDAP-App und der Machine Learning Analytics-App.

Zugriff auf die Seite Help and Support für UBA

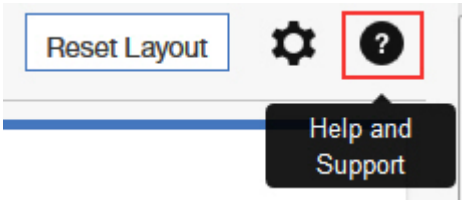
Auf der Seite **Help and Support** (Hilfe und Unterstützung) finden Sie Links zur Dokumentation, Fehlerbehebung und Unterstützung sowie Schulungsvideos, Protokolldateien und Verwaltungsfunktionen. Sie benötigen QRadar®-Administratorberechtigungen, um Protokolldateien anzeigen und Verwaltungsfunktionen auf der Seite **Help and support** ausführen zu können.

Nach der Installation der UBA-App können Sie auf die Seite **Help and Support** aus den folgenden Positionen zugreifen:

- Von den Einstellungen für **Verwaltung**:
  - Klicken Sie in QRadar V7.3.0 oder früher auf **Plugins** > **User Analytics** > **Help and Support** (Plug-ins > Benutzeranalyse > Hilfe und Unterstützung).
  - Klicken Sie in QRadar 7.3.1 oder höher auf **Apps** > **User Analytics** > **Help and Support** (Apps > Benutzeranalyse > Hilfe und Unterstützung).



- Klicken Sie auf der Registerkarte **User Analytics** (Benutzeranalyse) auf das Symbol **Help and Support**.



Verwaltungsfunktionen

Sie benötigen QRadar®-Administratorberechtigungen, um Protokolldateien anzeigen und Verwaltungsfunktionen ausführen zu können.

Zu den Verwaltungsfunktionen gehört die Funktion zum Ausführen der folgenden Aktionen:

- Klicken Sie auf **#Clear UBA Data** (UBA-Daten löschen), um alle UBA-Benutzerdaten zu löschen, aber sämtlichen aktuellen UBA-Konfigurationseinstellungen beizubehalten. Durch das Löschen der UBA-Daten verhält sich die UBA-App, wie wenn Sie die **UBA-Einstellungen** gerade erst installiert und konfiguriert hätten. Wenn die Machine Learning-App installiert ist, wird die ML-App ebenfalls über die Schaltfläche **Clear UBA Data** zurückgesetzt.
- Klicken Sie auf **Reset ML Setting** (ML-Einstellung zurücksetzen), wenn die Machine Learning-App installiert ist und Sie alle Machine Learning-Einstellungen zurücksetzen und die aktivierten Analysen inaktivieren möchten.

Serviceanforderungen

Serviceanforderungen sind auch als PMRs (Problem Management Records) bekannt.

Es gibt mehrere Methoden, um Diagnoseinformationen an den IBM Software Technical Support zu übergeben. Um eine Serviceanforderung zu öffnen oder um Informationen mit dem Technical Support auszutauschen, rufen Sie die Seite 'IBM Software Support - Informationen mit dem Technical Support austauschen (http://www.ibm.com/software/support/exchangeinfo.html) auf. Serviceanforderungen können mit dem Tool für Serviceanforderungen (PMRs) unter http://www.ibm.com/support/entry/portal/Open_service_request auch direkt übergeben werden.

Warnung in Statusanzeige für App 'Machine Learning' im Dashboard

Wenn in 'Status of Machine Learning Models (Status der Machine Learning-Modelle) im UBA-Dashboard Warnhinweise anzeigt, überprüfen Sie die Prozeduren zum Beheben des Problems.

Wenn in 'Status of Machine Learning Models' für eine Analyse die Fehlernachricht **Model failed to build** (Modell konnte nicht erstellt werden) angezeigt wird, können Sie einen der folgenden Vorschläge zur Behebung des Problems ausprobieren:

- Überprüfen Sie die Fehlerprotokolle für die ML-App.
- Überprüfen Sie den Plattenspeicherplatz auf dem System, auf dem die Machine Learning-App aktiv ist.
- Stellen Sie sicher, dass die UBA-App Benutzer mit Ereignissen enthält.
- Wenden Sie sich an die IBM Kundenunterstützung.

Zugehörige Konzepte:

„UBA- und Machine Learning-Protokolle extrahieren” auf Seite 210
Verwenden Sie die UBA- und Machine Learning-Protokolldateien bei der Behebung von Problemen.

Status der Machine Learning-App zeigt keinen Fortschritt bei der Datenaufnahme

Wenn 'Status of Machine Learning Models' (Status der Machine Learning-Modelle) im UBA-Dashboard während der Phase der Datenaufnahme scheinbar blockiert ist, überprüfen Sie den Vorgang, um das Problem zu beheben.

Wenn in 'Status of Machine Learning Models' für eine Analyse kein Fortschritt bei der Datenaufnahme angezeigt wird, können Sie folgende Vorschläge zur Behebung des Problems ausprobieren:

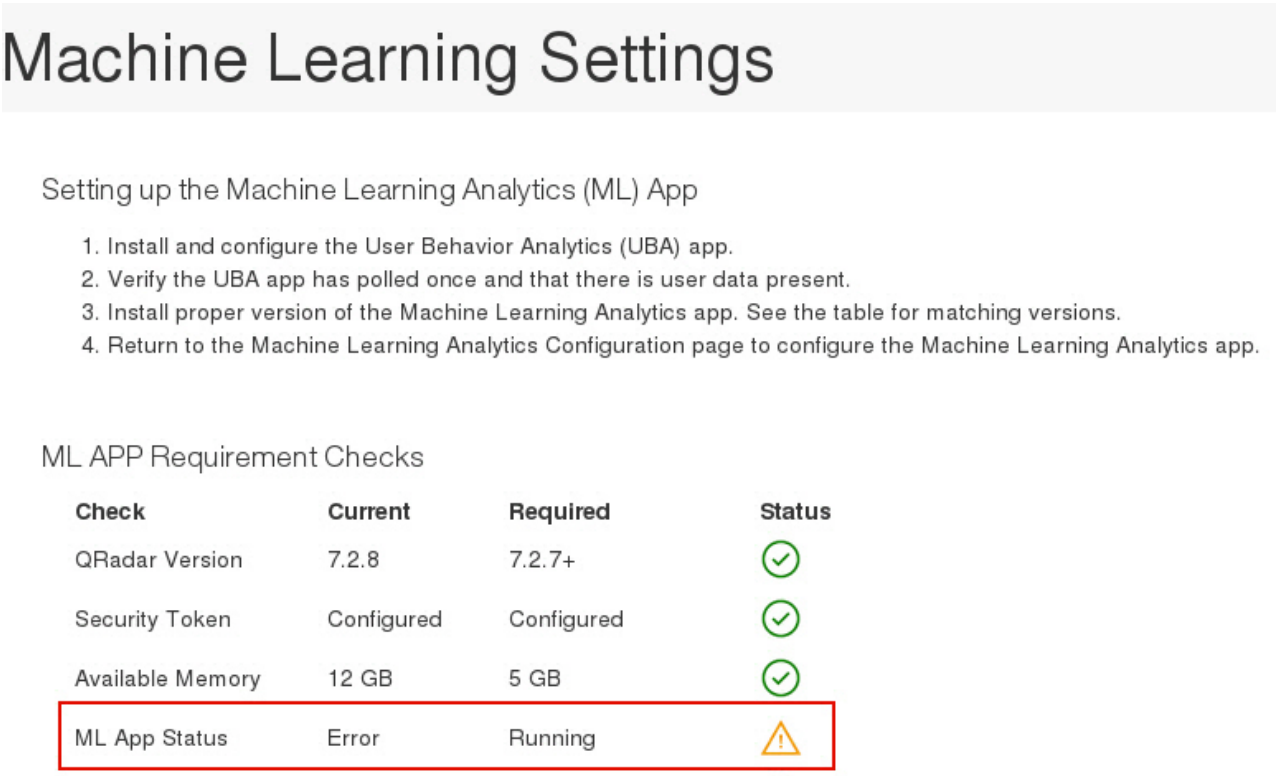
- Starten Sie den Ariel Server-Service erneut
- Überprüfen Sie den Plattenspeicherplatz auf dem System, auf dem die ML-App aktiv ist.
- Überprüfen Sie im ML-Container, ob der Prozess **UBAController** ausgeführt wird.
- Wenden Sie sich an die IBM Kundenunterstützung.

ML-App ist in einem Fehlerstatus

Wenn die Installation der App 'Machine Learning Analytics' (ML) fehlschlägt und die ML-Einstellungen einen Fehlerstatus anzeigen, können Sie die ML-App mithilfe des Befehlszeilentools **cURL** und der API-Dokumentationseinstellungen deinstallieren.

Vorgehensweise

Wenn auf der Seite 'Machine Learning Settings' (ML-Einstellungen) für die ML-App der Status 'Error' (Fehler) angezeigt wird, gehen Sie wie unten beschrieben vor, um die fehlgeschlagene App zu deinstallieren.



Anmerkung: Sie müssen über ein gültiges Authentifizierungstoken verfügen. Sie können die Liste der konfigurierten Authentifizierungstokens im Abschnitt 'Autorisierte Services' in den Verwaltungseinstellungen der QRadar-Konsole einsehen.

1. Melden Sie sich über SSH bei der QRadar-Konsole an.
2. Führen Sie folgenden Befehl aus:

   # psql -U qradar -c 'select id,name,status from installed_application'

   Beispielausgabe:

```
 id  |  name  |  status
-----+--------------------------------+---------
1356 | User Analytics | RUNNING
1358 | Machine Learning Analytics | ERROR
1357 | dataimport.ldap.applicationname | RUNNING
```

3. Suchen Sie den *id*-Wert für Machine Learning Analytics in der Ausgabe des Befehls und notieren Sie sich den Wert.

4. Ersetzen Sie im folgenden Befehl *<gültiges Token>* durch ein gültiges Authentifizierungstoken und *<id>* durch den notierten ID-Wert und führen Sie den Befehl aus, um die fehlgeschlagene ML-App zu deinstallieren: **# curl -X DELETE -k -H 'SEC:<gültiges Token>' https://127.0.0.1/api/gui_app_framework/applications/<id>**

App 'Machine Learning' (ML) entfernen

Gehen Sie wie folgt vor, um die ML-App über die API gui_app_framework zu entfernen:

1. Öffnen Sie die QRadar-Konsole und navigieren Sie zur API-Dokumentationsseite an der folgenden Adresse: https://*<Host_Adresse_Port>*/api_doc
2. Öffnen Sie den Ordner für die höchste API-Versionsnummer (die Nummer ist von der QRadar-Version abhängig, z. B. 7.0 für QR 7.2.8).
3. Öffnen Sie den Ordner `/gui_app_framework` und wählen Sie dann `/applications` aus.
4. Sie sollten jetzt bei der **GET API** angelangt sein. Klicken Sie auf die Schaltfläche **"Probieren Sie es aus!"**, um die Liste der installierten Anwendungen abzurufen.
5. Suchen Sie in den Ergebnissen aus Schritt 4 nach `Machine Learning Analytics` und rufen Sie den Attributwert `application_id` ab.
6. Erweitern Sie das Menü `/applications` in der API-Dokumentation (dieselbe Adresse wie in Schritt 3), wählen Sie die API `/application_id` aus und klicken Sie auf die Registerkarte **DELETE** (Löschen).
7. Geben Sie den Wert der Anwendungs-ID aus Schritt 5 ein und klicken Sie dann auf die Schaltfläche **"Probieren Sie es aus!"**, um die Anwendung zu entfernen.
8. Die API sollte den HTTP-Statuscode 204 zurückgeben, um anzuzeigen, dass die Anwendung erfolgreich entfernt wurde.

UBA- und Machine Learning-Protokolle extrahieren

Verwenden Sie die UBA- und Machine Learning-Protokolldateien bei der Behebung von Problemen.

Protokolldateien für die App herunterladen

Protokolldateien für die UBA-App und die Machine Learning-App können ohne großen Aufwand von der „Seite mit Hilfe und Unterstützung für UBA" auf Seite 207 heruntergeladen werden.

Protokolldateien der UBA-App

Gehen Sie wie hier beschrieben vor, um die Protokolldateien der UBA-App manuell aus dem Docker-Container zu extrahieren.

1. Navigieren Sie auf dem QRadar-Host, auf dem UBA aktiv ist, zu einem Verzeichnis mit genug Speicherplatz zum Erstellen einer ZIP-Datei, die alle Protokolldateien der App enthält.
2. Führen Sie folgenden Befehl aus:

   find /store/docker/v* -name uba.db
3. Kopieren Sie den Verzeichnispfad, der vor `uba.db` steht.

   Wenn der Verzeichnispfad beispielsweise
   /store/docker/volumes/qapp-1001/uba.db
   lautet, dann kopieren Sie
   /store/docker/volumes/qapp-1001/
4. Führen Sie folgenden Befehl aus und fügen Sie dabei den Verzeichnispfad aus Schritt 1 ein:

   zip -qr uba_logs.zip <Ihr_Pfad>log*

Beispiel:
zip -qr uba_logs.zip /store/docker/volumes/qapp-1001/log*

Protokolldateien der App 'Machine Learning'

Gehen Sie wie hier beschrieben vor, um die Protokolldateien der App 'Machine Learning' manuell aus dem Docker-Container zu extrahieren.

1. Navigieren Sie auf dem QRadar-Host, auf dem UBA aktiv ist, zu einem Verzeichnis mit genug Speicherplatz zum Erstellen einer ZIP-Datei, die alle Protokolldateien der App enthält.
2. Führen Sie folgenden Befehl aus:

   find /store/docker/v* -name itproot
3. Kopieren Sie den Verzeichnispfad, der vor `itproot` steht.

   Wenn der Verzeichnispfad beispielsweise
   /store/docker/volumes/qapp-1003/itproot
   lautet, dann kopieren Sie
   /store/docker/volumes/qapp-1003/
4. Führen Sie folgenden Befehl aus und fügen Sie dabei den Verzeichnispfad aus Schritt 1 ein:

   zip -qr ml_logs.zip <Ihr_Pfad>log*

   Beispiel:
   zip -qr ml_logs.zip /store/docker/volumes/qapp-1003/log*

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in dieser Dokumentation beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Défense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die genannten Leistungsdaten und Kundenbeispiele dienen lediglich Darstellungszwecken. Tatsächliche Leistungsergebnisse können je nach bestimmten Konfigurationen und Betriebsbedingungen abweichen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können unter Umständen von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Personen oder Unternehmen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- oder Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind entweder eingetragene Marken oder Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Java™ und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken von Oracle und/oder dessen verbundenen Unternehmen.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Bedingungen für die Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit

Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

IBM Online-Datenschutzerklärung

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Je nach implementierten Konfigurationen verwendet dieses Softwareangebot auch Sitzungscookies, die zum Zwecke der Sitzungsverwaltung und Authentifizierung die Sitzungs-IDs der Benutzer aufzeichnen. Diese Cookies können inaktiviert werden, damit wird aber zugleich die dadurch ermöglichte Funktionalität inaktiviert.

Wenn die für dieses Softwareangebot bereitgestellten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung rechtlich beraten lassen, insbesondere Meldepflichten sowie die Einforderung von Einwilligungen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter http://www.ibm.com/

privacy, in der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und auf der Seite "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Datenschutz-Grundverordnung (DSGVO)

Kunden sind dafür verantwortlich, die Einhaltung verschiedener Gesetze und Verordnungen sicherzustellen, einschließlich der Datenschutz-Grundverordnung der Europäischen Union. Es obliegt allein den Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Auslegung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die ihre Geschäftstätigkeit und die von ihnen eventuell einzuleitenden Maßnahmen zur Einhaltung dieser Gesetze und Bestimmungen betreffen. Die hier beschriebenen Produkte, Services und sonstigen Funktionen sind nicht für alle Kunden geeignet und möglicherweise nur eingeschränkt verfügbar. IBM erteilt keine Rechts- oder Steuerberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen und gesetzlichen Bestimmungen.

Weitere Informationen zur Umsetzung der DSGVO durch IBM und unseren Funktionen und Angeboten zur DSGVO finden Sie hier: https://ibm.com/gdpr.

Gedruckt in Deutschland