IBM Security QRadar Incident Forensics
Version 7.3.0

Administrationshandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen unter „Bemerkungen" auf Seite 35 lesen.

Produktinformationen

Dieses Dokument bezieht sich auf IBM QRadar Security Intelligence Platform V7.3.0 und nachfolgende Releases, bis es durch eine aktualisierte Version dieses Dokuments ersetzt wird.

Inhaltsverzeichnis

Einführung in die Verwaltung von IBM Security QRadar Incident Forensics v

Kapitel 1. Neuerungen für Administratoren in QRadar Incident Forensics V7.3.0 1

Kapitel 2. Verwaltungsworkflow und Benutzerzugriff auf forensische Funktionen 3

Kapitel 3. Server-Management 5
Serverkonfigurationseinstellungen 5
Filter für die Prüffunktionen für Protokolle und Domänen 5
Kategoriefilter für Webinhalte. 6
Unterstützte Protokolle und Dokumenttypen 7

Kapitel 4. Fallmanagement 11
Fälle erstellen. 11
Dateien in Fälle hochladen 12

Kapitel 5. Benutzern Fälle zuordnen 13
Dateien manuell in Forensics-Fälle importieren 13
Benutzern das Hochladen von PCAP-Dateien und Dokumenten via FTP aus externen Systemen in Forensics-Fälle ermöglichen 14
SSL- und TLS-Datenverkehr in QRadar Incident Forensics entschlüsseln 16

Kapitel 6. Geplante Aktionen in QRadar Incident Forensics 19
Aktionen für QRadar Incident Forensics-Hosts planen 19

Kapitel 7. Verdächtige Inhalte verwalten 21
Yara-Regeln importieren 22
Yara-Regeln löschen 22

Kapitel 8. Benutzer und Systembelegung in QRadar Incident Forensics prüfen 25

Kapitel 9. Untersuchen von Bedrohungen mit QRadar Network Insights. 27
Echtzeitorientierte Untersuchungen von Bedrohungen mit QRadar Network Insights 27
QRadar Network Insights-Implementierungen 28
Konfigurationsanforderungen für QRadar Network Insights 29
Format der QFlow-Kollektoren konfigurieren 29
DTLS auf einem verwalteten QRadar Network Insights-Host einrichten 30
QRadar Network Insights-Inspektionsstufen für Datenflüsse 31
Einstellungen von QRadar Network Insights konfigurieren 32
Bedrohungserkennung mit QRadar Network Insights 33

Bemerkungen 35
Marken 36
Nutzungsbedingungen für die Produktdokumentation 37
IBM Online-Datenschutzerklärung 38

Einführung in die Verwaltung von IBM Security QRadar Incident Forensics

Informationen zur Verwaltung von IBM® Security QRadar Incident Forensics.

Zielgruppe

Administratoren erstellen, verwalten und bedienen eine aktive forensische Funktion, damit Benutzer (die sog. Prüfer) sich auf die Überprüfung von Sicherheitsverstößen oder Fällen und auf die Untersuchung von Daten konzentrieren können.

Technische Dokumentation

Wenn Sie im Web nach der Produktdokumentation zu IBM Security QRadar einschließlich der gesamten übersetzten Dokumentation suchen möchten, rufen Sie das IBM Knowledge Center auf (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Informationen zum Zugriff auf weitere technische Dokumentationen in der QRadar-Produktbibliothek finden Sie unter Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Kontaktierung der Kundenunterstützung

Informationen zur Kontaktierung der Kundenunterstützung finden Sie im Dokument Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden gesetzlichen Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter schützen.

Bitte beachten:

Bei der Nutzung dieses Programms muss ggf. eine Reihe von Gesetzen und Bestimmungen beachtet werden, einschließlich solcher, die sich auf den Datenschutz,

die Datensicherheit, arbeitsrechtliche Angelegenheiten sowie die elektronische Kommunikation und die Speicherung beziehen. IBM Security QRadar darf nur für rechtmäßige Zwecke und auf rechtmäßige Weise verwendet werden. Der Kunde verpflichtet sich, dieses Programm gemäß geltendem Recht, geltenden Regelungen und Richtlinien zu verwenden und übernimmt die gesamte Verantwortung für die Einhaltung dieser Bestimmungen. Der Lizenznehmer erklärt, dass er die Zustimmung, Berechtigungen oder Lizenzen einholt bzw. einholen wird, die für die rechtmäßige Verwendung von IBM Security QRadar erforderlich sind.

Hinweis

IBM Security QRadar Incident Forensics soll Unternehmen dabei helfen, ihre Sicherheitsumgebung und Sicherheitsdaten zu verbessern. Insbesondere soll IBM Security QRadar Incident Forensics Unternehmen dabei unterstützen, die Vorgänge bei Sicherheitsverstößen im Netz zu untersuchen und besser zu verstehen. Mit dem Tool können Unternehmen einen Index für erfasste Netzpaketdaten (PCAPs) erstellen und diese durchsuchen und es enthält eine Funktion, mit der diese Daten im ursprünglichen Format wiederhergestellt werden können. Mit dieser Wiederherstellungsfunktion können Daten und Dateien einschließlich E-Mail-Nachrichten, Anhänge von Dateien und Bildern, VoIP-Anrufe und Websites wiederhergestellt werden. Weitere Informationen zu den Funktionen des Programms und der Vorgehensweise bei der Konfiguration der Funktionen finden Sie in den Handbüchern und in der weiteren Dokumentation, die dem Programm beigefügt wurde. Die Verwendung dieses Programms kann verschiedene Gesetze oder Regelungen einschließen. Diese können sich auf die Geheimhaltung, den Datenschutz, die Benutzung und elektronische Kommunikation sowie auf die Speicherung beziehen. IBM Security QRadar Incident Forensics darf nur für gesetzlich zulässige Zwecke und in einer gesetzmäßigen Weise verwendet werden. Der Kunde verpflichtet sich, dieses Programm gemäß geltendem Recht, geltenden Regelungen und Richtlinien zu verwenden, und übernimmt die gesamte Verantwortung für die Einhaltung dieser Bestimmungen. Der Lizenznehmer versichert, dass er alle Zustimmungen, Genehmigungen oder Lizenzen einholen wird oder eingeholt hat, die für eine rechtmäßige Nutzung von IBM Security QRadar Incident Forensics erforderlich sind.

Kapitel 1. Neuerungen für Administratoren in QRadar Incident Forensics V7.3.0

IBM QRadar Network Insights V7.3.0 enthält jetzt eine zusätzliche Option für das QFlow-Format.

TLV-Option für QRadar Network Insights verfügbar

Verwenden Sie QFlow-Kollektoren, um Daten im TLV-Format (Tab-Length-Value) an den QFlow-Prozessor zu exportieren. Bei Neuinstallationen von IBM Security QRadar oder QRadar-Upgrades, bei denen keine QRadar Network Insights-Appliance als Teil der Implementierung vorhanden ist, müssen Sie das Format `TLV` im Menü **QFlow format** (QFlow-Format) auswählen.

 Weitere Informationen zum TLV-Format...

Kapitel 2. Verwaltungsworkflow und Benutzerzugriff auf forensische Funktionen

Nach der Installation und Konfiguration von IBM Security QRadar Incident Forensics kann ein Administrator Fehler im System und den zugehörigen Operationen beheben, das System und die zugehörigen Operationen warten und überwachen und den Benutzerzugriff auf Fälle verwalten.

Zur Anzeige der Verwaltungstools für QRadar Incident Forensics sind Administratorberechtigungen erforderlich.

Beispiel: Workflow für die Verwaltung

Im folgenden Diagramm wird ein Beispielworkflow für die Verwaltung von QRadar Incident Forensics gezeigt.

1. Verwenden Sie das Server-Management, um Webkategorien und Datenverkehr zu filtern, die nicht überwacht werden sollen.
2. Mithilfe der Benutzerberechtigungen für Forensics können Sie Prüfern Fälle zuordnen.
3. Verwenden Sie das Fallmanagement, um Fälle zu erstellen und zu löschen und externe Inhalte in das System zu importieren.
4. Verwenden Sie das Planen von Aktionen, um die Wartung zu planen, also beispielsweise das Löschen alter Dokumente, die Optimierung der Datenbank und das Zurücksetzen des QRadar Incident Forensics-Servers.

Benutzerrollen

Um Benutzerkonten hinzufügen zu können, müssen Sie zuerst Sicherheitsprofile erstellen, damit die jeweiligen Zugriffsanforderungen Ihrer Benutzer erfüllt werden. Weitere Informationen zur Konfiguration von Sicherheitsprofilen finden Sie im *IBM Security QRadar-Verwaltungshandbuch*.

Im Tool 'User Roles' (Benutzerrollen) auf der Registerkarte **Verwaltung** von QRadar können Sie die folgenden Benutzerrollen zuordnen:

Admin
: Benutzer können alle Fälle, die Benutzern zugeordnet sind, und alle Vorfälle anzeigen und auf diese zugreifen und haben automatisch vollständigen Zugriff auf QRadar Incident Forensics.

Forensics
: Benutzer können die Registerkarte **Forensics** anzeigen und darauf zugreifen, können aber keine Fälle erstellen.

Create cases in Incident Forensics (Fälle in Incident Forensics erstellen)
: Benutzer können automatisch Forensics-Fälle erstellen.

Kapitel 3. Server-Management

Administratoren können das IBM Security QRadar Incident Forensics-System und die zugehörigen Operationen warten und überwachen und dort Fehler beheben.

Öffnen Sie das Server-Management-Tool, um Servereinstellungen zu überwachen oder zu ändern oder um die Benutzer anzuzeigen, die im System angemeldet sind:

1. Melden Sie sich bei QRadar als Administrator an.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Hauptfenster im Abschnitt **Forensics** auf **Server Management** (Server-Management).

Serverkonfigurationseinstellungen

Mit den Servereinstellungen des Server-Management-Tools von IBM Security QRadar Incident Forensics können Sie Systemeinstellungen konfigurieren, die sich auf alle verwalteten Hosts auswirken. Zum Anwenden Ihrer Konfigurationsänderungen klicken Sie auf der Registerkarte **Verwaltung** auf **Änderungen implementieren**.

Suchprotokoll nach Abmeldung löschen
: Das Suchprotokoll wird gelöscht, wenn sich Benutzer abmelden. Die gelöschte Suche wird für die Abfrageprotokollliste im Abfragehilfsprogramm und auf den letzten Benutzer im Feld **Search Criteria Input** (Eingabe der Suchkriterien) auf der Seite **Search and Results** (Suche und Ergebnisse) angewendet.

Standardmäßige Anzahl der Knoten für die Darstellung
: Die maximale Anzahl der Knoten, die im Tool zur Darstellung angezeigt werden. Sie können die Anzahl der Knoten konfigurieren, die nach der ersten Ausgabe ausgegeben werden sollen. Die Anpassung der Anzahl ausgegebener Knoten betrifft nur diese Instanz des Tools zur Darstellung.

Filter für die Prüffunktionen für Protokolle und Domänen

Sie können bestimmte Arten von Datenverkehr aus Untersuchungen ausschließen, indem Sie im Server-Management-Tool die Prüffunktionen für Protokolle oder Domänen inaktivieren. Verwenden Sie dazu die Option **Inspector Filter** (Filter für Prüffunktionen).

Die Prüffunktionen für Protokolle und Domänen verarbeiten die Daten über aufgenommenen Netzverkehr und versuchen, die Daten auf aussagefähige Weise anzugeben und zu indizieren. Durch die Ermittlung und Indexierung dieser Daten erhalten Prüfer mehr Kontrolle über die Suche nach den Informationen.

Bei der Aufnahme von Netzverkehrdaten und der Ermittlung von Protokollen werden die Daten von der entsprechenden Prüffunktion für Protokolle weiter überprüft. Die von der Prüffunktion für HTTP-Protokolle ermittelten Netzverkehrdaten werden weiter von Prüffunktionen für Domänen überprüft und indexiert.

Protocol Inspectors (Prüffunktionen für Protokolle)
: Die Prüffunktionen für Protokolle können Protokolle wie beispielsweise HTTP, POP3, FTP und Telnet ermitteln. Sie können Prüffunktionen für Pro-

tokolle ausschließen. Beim Ausschluss von Prüffunktionen werden weiterhin alle Netzverkehrdaten, die der Prüffunktion zugeordnet sind, aufgenommen, aber der Datenverkehr wird nur auf einer allgemeinen Ebene ermittelt und indexiert.

Domain Inspectors (Prüffunktionen für Domänen)
Prüffunktionen für Domänen überprüfen bestimmte Websites. Sie können Prüffunktionen für Domänen ausschließen. Beim Ausschluss von Prüffunktionen für Domänen werden weiterhin alle HTTP-Netzverkehrdaten, die der Prüffunktion zugeordnet sind, aufgenommen, aber der Datenverkehr wird nur auf der HTTP-Ebene ermittelt und indexiert. Damit Prüffunktionen für Domänen aktiv sein können, muss die Prüffunktion für HTTP-Protokolle ebenfalls aktiv sein.

Standardmäßig sind alle Filter aktiviert und Sie können den Datenverkehr aller Protokolle sehen. Die einzige Ausnahme hiervon ist der über das Session Initiation Protocol (SIP) übertragene Datenverkehr. Dieses auf Anwendungsebene arbeitende Anrufaufbauprotokoll ist standardmäßig inaktiviert.

Hinweis: Änderungen an der Konfiguration der Filter für Prüffunktionen gelten für alle neuen Fälle, die erstellt werden. Die jeweils aktivierten Prüffunktionen geben die Dokumente vor, die für einen Fall erstellt werden, und Prüfer sind nicht mehr in der Lage, nach bestimmten Prüffunktionen zu suchen. Benutzer wissen nicht, welche Prüffunktionen einem Fall zugeordnet sind.

Protokolle, die von keiner Prüffunktion verarbeitet werden, werden als unbekannt eingestuft.

Kategoriefilter für Webinhalte

Über Webkategoriefilter können Sie die Webseiten- und Webservertypen vorgeben, die erkannt werden.

So können Sie beispielsweise bestimmte HTTP-Netzverkehrtypen von Untersuchungen ausschließen. Wenn Daten zum HTTP-Netzverkehr aufgenommen werden, werden diese Daten kategorisiert und die sich daraus ergebenden Dokumente gruppiert.

Administratoren können die Daten zum HTTP-Netzverkehr filtern, um die Aufnahme der Daten zu verhindern.

Für den Ausschluss oder das Filtern des Datenverkehrs für eine Kategorie oder Gruppe inaktivieren Sie die Kategorie oder Gruppe im Server-Management-Tool.

Das Kategorisieren, Gruppieren und Filtern von Webinhalten betrifft während der Aufnahme die Daten zum HTTP-Netzverkehr und hat keine Auswirkung auf Daten, die sich bereits im System befinden.

Wenn ein Gruppenfilter für den Ausschluss von Daten festgelegt ist, werden Daten zum HTTP-Netzverkehr, die Kategorien in dieser Gruppe zugeordnet sind, während der Verarbeitung herausgefiltert, unabhängig von den Filtereinstellungen der zugehörigen Kategorie.

Beispiel: Was geschieht, wenn Sie Datenverkehr mit einem Webkategorienfilter ausschließen?

Sie haben sich entschlossen, Datenverkehr mit Daten von Nachrichten- und Zeitschriften-Sites auszuschließen.

1. Klicken Sie in QRadar auf der Registerkarte **Verwaltung** auf **Server Management** (Server-Management).
2. Klicken Sie auf **Web Category Filter** (Webkategorienfilter) und dann neben dem Filter **News/Magazines** (Nachrichten/Zeitschriften) auf **Off** (Aus).
3. Klicken Sie auf den Filter **Webmail/Unified Messaging** und dann auf **On** (Ein).

Wenn ein Benutzer nun den eingepflegten Datenverkehr auf der Registerkarte **Forensics** untersucht, sieht er, dass weder Datenverkehr mit **News/Magazines**-Daten noch **Webmail/Unified Messaging**-Datenverkehr aufgenommen ist, obwohl der Filter **Webmail/Unified Messaging** aktiviert ist.

Unterstützte Protokolle und Dokumenttypen

In IBM Security QRadar Incident Forensics werden die Inhalte in Netzflusspaketen erfasst und die Nutzdaten und Metadaten werden indexiert und verarbeitet.

In der folgenden Liste werden die unterstützten Protokolle beschrieben, die in QRadar Incident Forensics verarbeitet werden können:

- AIM
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- IMAP
- IRC
- Jabber
- Myspace
- NFS
- SIP
- NetBIOS
- Oracle
- POP3
- SMB (Version 1)
  - Lanman 2.1
  - NT 0.12
- SMTP
- SPDY
- TLS (SSL)
- SSH
- Telnet
- Yahoo Messenger
- MySQL

In der folgenden Liste werden die unterstützten Domänen (Websites) sowie die unterstützten Sprachen für die Domäne beschrieben, die in QRadar Incident Forensics verarbeitet werden können:

- AOL (Barrierefrei, Basis- und Standardversion) (EN)
- Charter (EN)
- Facebook (mobile Version und für Desktop) (AR, CN, DE, EN, ES, FR, RU)
- Gmail (klassische Version und Standardversion) (AR, CN, DE, EN, ES, FR, RU)
- Hotmail (AR, CN, DE, EN, ES, FR, RU)
- LinkedIn (DE, EN, ES, FR, RU)
- MailCom (CN, EN, ES, FR, RU)
- MailRu (RU)
- Maktoob (AR, EN)
- Myspace (EN)
- QQMail (EN, CN)
- Twitter (EN)
- YAHOO Mail (Standardversion, klassische Version) (EN)
- YAHOO Note (EN)
- YouTube (AR, CN, DE, EN, ES, FR, RU)
- Comcast (Zimbra) (EN)

In der folgenden Liste werden die unterstützten Dokumentformate beschrieben, die in QRadar Incident Forensics verarbeitet werden können:

- HyperText Markup Language
- XML und abgeleitete Formate
- Microsoft Office-Dokumentformate
- OpenDocument-Format
- Portable Document Format (PDF)
- EPUB-Format für elektronische Veröffentlichungen
- Rich-Text-Format
- Komprimierungs- und Paketierungsformate
- Textformate
- Audioformate
- Bildformate
- Videoformate
- Dateien und Archive für Java™-Klassen
- mbox-Format

QFlow-Anwendungserkennung

Wenn eine Anwendung, eine Sitzung oder ein Protokoll anhand keiner Prüffunktion ermittelt werden kann, kommt die QFlow-Anwendungserkennung zum Einsatz. Sie überprüft die ersten 64 Bytes eines Pakets auf eine Signatur und versucht, die Anwendung anhand der Signatur und anhand des Ports zu ermitteln. Im Folgenden sind einige der Anwendungen, Sitzungen und Protokolle aufgelistet, die von der QFlow-Anwendungserkennung ermittelt werden können (diese Liste ist nicht vollständig):

- BitTorrent
- Blubster

- CitrixICA
- Google Talk
- Gnucleuslan
- Gnutella
- GSS-SPNEGO
- NTLMMSSP
- OpenNap
- PeerEnabler
- Piolet
- UpdateDaemon
- VNC

Kapitel 4. Fallmanagement

Als Administrator können Sie Fälle und Datensammlungen mithilfe des Fallmanagements verwalten. Sie können Fälle für Sammlungen von Dokumenten oder Paketaufzeichnungen (PCAP-Dateien) erstellen und außerdem externe Dateien in das IBM Security QRadar Incident Forensics-System importieren.

Fallmanagement optimieren

Zur Optimierung des Fallmanagements empfiehlt sich die Option **Flush** (Auf Platte schreiben). Für das *Streaming von PCAP-Daten* (eine Reihe von PCAP-Dateien, die logisch miteinander verbunden sind und eine große PCAP-Datei bilden) können Sie das Schreiben gepufferter Daten auf einen Datenträger erzwingen. Mit der Option **Flush** (Auf Platte schreiben) werden die QRadar Incident Forensics-Hosts gezwungen, nicht abgeschlossene Datenflüsse auf Platte zu schreiben; damit können diese Datenflüsse frühzeitig durchsucht werden.

Verteilungsdiagramme

Wenn Sie das Löschen eines Falles planen, können Sie die Diagramme grafisch darstellen, um die Inhalte des Falles schnell zu prüfen. Sie können den Typ der Dateien, der Protokolle und der Domänen prüfen, die im Fall enthalten sind.

PCAP-Dateien auf verwaltete Hosts hochladen

PCAP-Daten können Sie manuell aus externen Quellen hochladen. Auf welchen von QRadar Incident Forensics verwalteten Host Sie die Daten hochladen, können Sie dabei auswählen. Haben Sie beispielsweise drei verwaltete Hosts und drei PCAP-Dateien, können Sie jede Datei auf einen anderen verwalteten Host hochladen. Für größere PCAP-Dateien sollten Sie zum Hochladen FTP verwenden.

Fälle erstellen

Bei Fällen handelt es sich um logische Container für Ihre Sammlung importierter Dokumente und PCAP-Dateien. Sie können einen einzelnen Fall für alle PCAP-Dateien verwenden oder mehrere Fälle erstellen. Fälle können auf bestimmte Benutzer beschränkt werden.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Verwaltung** auf **Case Management** (Fallmanagement).
2. Klicken Sie auf **Add New Case** (Neuen Fall hinzufügen).
3. Geben Sie im Feld **Case Name** (Fallname) einen eindeutigen Namen ein.

   Einschränkung: Fälle können keine Leerzeichen enthalten.
4. Klicken Sie auf **Save** (Speichern).

Ergebnisse

Es wurde ein neues Verzeichnis erstellt, das auf dem Fallnamen basiert: `/case_input/<Fallname>`. Dieses Verzeichnis wird für den Import Ihrer PCAP-Dateien verwendet.

Dateien in Fälle hochladen

Als Administrator können Sie externe Paketaufzeichnungen (PCAP-Dateien) und Dokumente (z. B. Spreadsheets, Textdateien und Bilddateien) in das Fallmanagement von IBM Security QRadar Incident Forensics hochladen.

Die folgenden Dateitypen werden unterstützt:

- HyperText Markup Language
- XML und abgeleitete Formate
- Microsoft Office-Dokumentformate
- OpenDocument-Format
- Portable Document Format (PDF)
- EPUB-Format für elektronische Veröffentlichungen
- Rich-Text-Format
- Komprimierungs- und Paketierungsformate
- Textformate
- Audioformate
- Bildformate
- Videoformate
- Dateien und Archive für Java-Klassen
- mbox-Format

Mit dem Fallmanagement wird die Anzahl der Dateien, die Sie einem Fall hinzufügen können, sowie die maximale Dateigröße beschränkt.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Verwaltung** im Abschnitt **Forensics** auf **Case Management** (Fallmanagement).
2. Wählen Sie einen Fall aus.
   - Wenn Sie einem vorhandenen Fall externe Dateien hinzufügen möchten, wählen Sie den Fall in der Liste **Cases** (Fälle) aus.
   - Um einem neuen Fall Dateien hinzuzufügen, klicken Sie auf **Add New Case** (Neuen Fall hinzufügen).

     Einschränkung: Fälle können keine Leerzeichen enthalten.
3. Wählen Sie in der Liste **Upload to Host** (Auf Host hochladen) den verwalteten Host aus, von dem die Dateien verarbeitet werden sollen.
4. Sie haben folgende Möglichkeiten, PCAP-Dateien oder andere Dokumenttypen hinzuzufügen:
   - Klicken Sie auf **Add files** (Dateien hinzufügen), wählen Sie die Dateien aus und klicken Sie auf **Start upload** (Upload starten).
   - Ziehen Sie die Dateien in das Upload-Fenster.

   Wenn das Hochladen beendet wurde, werden die Dateien in der Liste **Collections** (Datensammlungen) aufgeführt.

Kapitel 5. Benutzern Fälle zuordnen

Als Administrator können Sie Benutzern den Zugriff auf Forensics-Daten erteilen, Benutzern Fälle zuordnen und Benutzerberechtigungen wie beispielsweise den FTP-Zugriff konfigurieren. Benutzern werden Daten erst angezeigt, wenn sie einem Fall zugeordnet sind, und es werden ihnen nur Daten aus den Fällen angezeigt, denen sie zugeordnet sind.

Weisen Sie Nicht-Administratoren, also Benutzern mit eingeschränkten Zugriffsrechten, Fälle mit Bedacht zu. Durch die ihnen zugewiesenen Fälle könnten sie Einblick in Dokumente von IP-Adressen erhalten, auf die sie normalerweise keinen Zugriff haben. Ordnen Sie einem Nicht-Administrator beispielsweise einen Fall zu, der Finanz- oder Personalinformationen enthält, kann dieser Benutzer diese Daten sehen, wenn er den Fall untersucht.

Informationen zu diesem Vorgang

Administratoren können folgende Tasks ausführen:

- Mehrere Benutzer einem Fall zuordnen.
- Einen Fall von einem Benutzer entfernen.
- Alle Fälle anzeigen und verwalten, die einem Benutzer zugeordnet sind.

Benutzern werden nur die Fälle angezeigt, die ihnen explizit zugeordnet wurden.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Verwaltung** auf **Forensics User Permissions** (Benutzerberechtigungen für Forensics).
2. Wählen Sie in der Liste **Users** (Benutzer) einen Benutzer aus.
3. Wählen Sie in der Liste **Available** (Verfügbar), in der die Fälle aufgeführt sind, einen oder mehrere Fälle aus und klicken Sie auf den Pfeil (>), um die Fälle in die Liste **Assigned** (Zugeordnet) zu verschieben.

   Tipp: Einem Benutzer mit Administratorberechtigungen sind standardmäßig alle Fälle zugeordnet. Der Linkspfeil (<) und der Rechtspfeil (>) werden nicht angezeigt.

Dateien manuell in Forensics-Fälle importieren

Im Gegensatz zum Tool für das Fallmanagement gibt es keine Einschränkungen bei der Dateigröße oder der Anzahl der Dateien beim manuellen Import von Dateien. Sie können einen Fall manuell erstellen oder Dateien in den Fall kopieren oder Dateien manuell in einen vorhandenen Fall kopieren.

Beispielsweise können Sie mit dem Befehl **scp** Dateien sicher aus einem anderen Host in das Verzeichnis `/opt/ibm/forensics/case_input/case_input/` auf dem IBM Security QRadar Incident Forensics-Host kopieren.

Vorbereitende Schritte

Erstellen Sie eine Sicherungskopie der importierten Dateien. Nach dem Import und der Verarbeitung der Datei wird die ursprüngliche Datei gelöscht.

Vorgehensweise

1. Melden Sie sich in QRadar Incident Forensics über SSH als Rootbenutzer an.
2. Um einen neuen Fall zu erstellen, navigieren Sie zu `/opt/ibm/forensics/case_input` und geben folgenden Befehl ein:

   `mkdir /opt/ibm/forensics/case_input/<Fallname>`
3. Zum Kopieren von Dateien in einem Fall verwenden Sie den Befehl **scp** oder ein anderes Dateiübertragungsprogramm, um die Dateien in das Verzeichnis zu kopieren, das dem Dateityp entspricht.

   In der folgenden Tabelle wird die Verzeichnisstruktur für die importierten Dateien aufgeführt.

Tabelle 1. Verzeichnisstruktur von Falldateien

Verzeichnis	Beschreibung
`/opt/ibm/forensics/case_input/<Fallname>`	Das Verzeichnis, das beim Import einer Reihe von PCAP-Dateien oder eines verbundenen Datenstroms von PCAP-Dateien verwendet wird.
`/opt/ibm/forensics/case_input/<Fallname>/singles`	Das Verzeichnis, das beim Import einzelner PCAP-Dateien verwendet wird.
`/opt/ibm/forensics/case_input/case_input/<Fallname>/import`	Das Verzeichnis, das beim Import einer einzelnen Datei eines anderen Typs als PCAP verwendet wird. Beispiel: Microsoft Word-Dokumente, Adobe Acrobat-PDFs, Textdateien und Abbildungen.

Wichtig: Wenn in einem Dateinamen ein Bindestrich verwendet wird, wird dieser beim Import der Datei in ein Unterstreichungszeichen geändert.

Ergebnisse

Nach dem erfolgreichen Import wird der Name Ihrer Datei automatisch im Fenster **Collections** (Datensammlungen) des von Ihnen erstellten Falls angezeigt.

Benutzern das Hochladen von PCAP-Dateien und Dokumenten via FTP aus externen Systemen in Forensics-Fälle ermöglichen

Für das Hochladen externer Daten zur Integration in bestimmte Fälle können Administratoren den Benutzern sichere FTP-Berechtigungen erteilen und den Fall verwalten, dem die Daten zugeordnet sind. Die Benutzer können selbst auswählen, von welchem IBM Security QRadar Incident Forensics-Host die FTP-Anforderung verarbeitet wird.

Soll ein Kennwort nach Aktivierung des FTP-Zugriffs geändert werden, muss der FTP-Zugriff inaktiviert und der Benutzer gespeichert werden; anschließend kann der FTP-Zugriff wieder aktiviert und ein neues Kennwort eingegeben werden.

Vorbereitende Schritte

Erstellen bzw. weisen Sie forensischen Prüfern mit dem Tool 'User Roles' (Benutzerrollen) auf der Registerkarte **Verwaltung** Rollen zu.

Die Datei /etc/vsftpd/vsftpd.conf ist standardmäßig so konfiguriert, dass fünf Ports offen sind: 55100-55104. Den Portbereich können Sie in der Datei /etc/vsftpd/vsftpd.conf mit den Einstellungen pasv_min_port und pasv_max_port ändern. Zum Anwenden der Konfigurationsänderungen klicken Sie auf der Registerkarte **Verwaltung** auf **Änderungen implementieren**.

Anmerkung: FTP-Clients müssen TLS v1.2 (Datei vsftpd.conf) unterstützen. In der folgenden Liste sind die unterstützten Mindestversionen für FTP-Clients beschrieben:

- WinSCP 5.7
- FileZilla 3.9.0.6

Informationen zu diesem Vorgang

In IBM Security QRadar Incident Forensics können Daten aus allen zugänglichen Verzeichnissen importiert werden, die sich im Netz befinden. Die Daten können verschiedene Formate haben. Dazu gehören u. a. die folgenden Formate:

- Standardmäßige PCAP-Formatdateien aus externen Quellen
- Dokumente wie Textdateien, PDF-Dateien, Spreadsheets und Präsentationen
- Bilddateien
- Streaming-Daten aus Anwendungen
- Streaming-Daten aus externen PCAP-Quellen

Benutzer können mehrere Dateien in einen Fall hochladen und ein Administrator kann mehreren Benutzern Zugriff auf den Fall erteilen.

Einschränkung: Der Name des Falls muss eindeutig sein. Einem Fall ist ein einziger Benutzer zugeordnet, deshalb können nicht zwei Benutzer einen Fall mit dem gleichen Namen erstellen.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Verwaltung** auf **Forensics User Permissions** (Benutzerberechtigungen für Forensics).
2. Wählen Sie in der Liste **Users** (Benutzer) einen Benutzer aus.
3. Aktivieren Sie im Fenster **Edit User** (Benutzer bearbeiten) das Kontrollkästchen **Enable FTP access** (FTP-Zugriff aktivieren).
4. Geben Sie das FTP-Kennwort für den Benutzer ein und bestätigen Sie es.
5. Klicken Sie auf **Save User** (Benutzer speichern), um die Änderungen an den Berechtigungen zu speichern.
6. Gehen Sie im FTP-Client folgendermaßen vor:
   a. Stellen Sie sicher, dass Transport Layer Security (TLS) als Protokoll ausgewählt ist.
   b. Fügen Sie die IP-Adresse des QRadar Incident Forensics-Hosts hinzu.
   c. Erstellen Sie eine Anmeldung, bei der der erstellte Benutzername und das erstellte Kennwort für QRadar Incident Forensics verwendet werden.
7. Stellen Sie eine Verbindung zum QRadar Incident Forensics-Server her und erstellen Sie ein neues Verzeichnis.
8. Für den Zugriff auf FTP und zum Speichern von PCAP-Dateien in dem für den Fall erstellten Verzeichnis erstellen Sie ein Verzeichnis mit der Bezeichnung singles und ziehen die PCAP-Dateien in dieses Verzeichnis.

9. Für den Zugriff auf FTP und zum Speichern anderer Dateitypen, bei denen es sich nicht um PCAP-Dateien handelt, in dem für den Fall erstellten Verzeichnis erstellen Sie ein Verzeichnis mit der Bezeichnung `import` und ziehen die Dateien in dieses Verzeichnis.
10. Geben Sie den folgenden Befehl ein, um den FTP-Server erneut zu starten:
    ```
    etc/init.d/vsftpd restart
    ```
11. Geben Sie den folgenden Befehl ein, um den Server erneut zu starten, mit dem die Dateien aus dem Bereich zum Hochladen in das QRadar Incident Forensics-Verzeichnis verschoben werden:
    ```
    /etc/init.d/ftpmonitor restart
    ```

Ergebnisse

Einem Administrator werden die Daten angezeigt, die in das Fallmanagement hochgeladen werden. Einem Benutzer werden die zugehörigen Fälle in einem der Tools auf der Registerkarte **Forensics** angezeigt.

SSL- und TLS-Datenverkehr in QRadar Incident Forensics entschlüsseln

Für die Ermittlung verdeckter Sicherheitsrisiken kann in IBM Security QRadar Incident Forensics SSL-Datenverkehr entschlüsselt werden. Wenn Sie den privaten Schlüssel und die IP-Adresse des Servers oder einen Schlüssel für die Browsersitzung und einige andere Sitzungsdaten angeben, kann die Prüffunktion für Protokolle den SSL-Datenverkehr entschlüsseln.

Wenn der Sitzungsschlüssel von externen Sites oder einem anderen Browser generiert wurde, kann die Prüffunktion für Protokolle den SSL-Datenverkehr aus einer Browsersitzung nicht entschlüsseln.

Einschränkung: Der `Diffie Hellman`-Schlüsselaustauschmechanismus wird nicht unterstützt, wenn verschlüsselter Datenverkehr über einen privaten Schlüssel entschlüsselt wird. Bei der Verwendung eines privaten Schlüssels werden andere Schlüsselaustauschverfahren unterstützt, beispielsweise RSA.

Die `Diffie Hellman`-Einschränkung gilt nicht, wenn Datenverkehr mit Informationen entschlüsselt wird, die sich in einem Keylogger befinden.

Informationen zu diesem Vorgang

Die Entschlüsselung wird für die folgenden Protokolle unterstützt:

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

Schlüsselprotokolldateien werden von Chrome-, Firefox- und Opera-Browsern mit der Umgebungsvariablen SSLKEYLOGFILE unterstützt. Die folgenden Schlüsselformate werden für den Sitzungsschlüssel SSLKEYLOGFILE unterstützt:

- RSA
- DH

Vorgehensweise

1. Verwenden Sie SSH, um sich im primären QRadar Incident Forensics-Host als Rootbenutzer anzumelden.
2. Überprüfen Sie die Position der Schlüssel in der Datei `/opt/qradar/forensics.conf`.

   ```
   <sslkeys
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

3. Kopieren Sie die Schlüssel in das Verzeichnis, das in der Datei `/opt/qradar/forensics.conf` angegeben ist.
   - Kopieren Sie für private Schlüssel den Schlüssel in das Verzeichnis `/opt/ibm/forensics/decapper/keys`.

     Beispiel:

     ```
     <keys>
      <key file=" /opt/ibm/forensics/decapper/keys/Schlüsselname">
         <address> 1.2.3.4</address>
         <range> 1.2.3.0-1.2.3.255</range>
       </key></keys>
     ```

   - Kopieren Sie für Schlüsselprotokolldateien, die vom Browser generiert wurden, die Schlüsselprotokolldateien in das Verzeichnis `/opt/ibm/forensics/decapper/keylogs/default`.

   Wenn Sie die Unterverzeichnisse in das Verzeichnis `/opt/ibm/forensics/decapper/keys` oder `/opt/ibm/forensics/decapper/keylogs` ändern, müssen Sie den Decapper-Service erneut starten.

   Geben Sie für den Neustart des Decapper-Service den folgenden Befehl ein: `service decapper restart`

Kapitel 6. Geplante Aktionen in QRadar Incident Forensics

Sie können die Wartung planen, also beispielsweise das Löschen alter Dokumente, die Optimierung der Datenbank und das Zurücksetzen des IBM Security QRadar Incident Forensics-Servers.

Wenn viele Dokumente vorhanden sind, kann das Durchführen geplanter Aktionen wie das Löschen alter Dokumente sehr lange dauern. Zum Löschen eines gesamten Falles verwenden Sie das Case Management-Tool.

Dokumente löschen

Administratoren können veraltete Dokumente auf Basis der Zeitmarke des Dokuments im Netz löschen.

Sie können Dokumente (einschließlich PCAP-Dateien und andere Dateitypen) aus einem Fall oder vom Server löschen. Durch das Löschen veralteter Dokumente wird die Geschwindigkeit beim Suchen von Dokumenten verbessert.

Flush Case (Fall auf Platte schreiben)

Mithilfe der Option **Flush Case** (Fall auf Platte schreiben) können Sie das Fallmanagement optimieren. Für das *Streaming von PCAP-Daten* (eine Reihe von PCAP-Dateien, die logisch miteinander verbunden sind und eine große PCAP-Datei bilden) können Sie das Schreiben gepufferter Daten auf einen Datenträger erzwingen. Mit der Option **Flush Case** (Fall auf Platte schreiben) werden die QRadar Incident Forensics-Hosts gezwungen, nicht abgeschlossene Datenflüsse auf Platte zu schreiben; damit können diese Datenflüsse frühzeitig durchsucht werden.

Datenbank optimieren

Administratoren können die Datenbank optimieren, um den Index der Suchmaschine in Segmente zu reorganisieren und gelöschte Dokumente zu löschen.

Die geplante Aktion **Optimize Database** (Datenbank optimieren) entspricht weitgehend dem Befehl **`defrag`**.

Beim Optimieren der Datenbank wird ein neuer Index erstellt. Nachdem der Index erstellt wurde, wird der alte Index durch den neuen Index ersetzt. Da bis zum Ersetzen des alten Index zwei Indizes vorhanden sind, ist für den Befehl zur Indexoptimierung die doppelte Menge an Festplattenspeicherplatz erforderlich.

Stellen Sie vor dem Optimieren Ihrer Datenbank sicher, dass die Größe Ihres Index nicht 50 Prozent des verfügbaren Speicherplatzes auf Ihrer Festplatte überschreitet.

Aktionen für QRadar Incident Forensics-Hosts planen

Sie können auf den IBM Security QRadar Incident Forensics-Hosts Verwaltungstasks terminieren.

Folgende Tasks können terminiert werden:

- Neuen Index für die aktuell verfügbaren Fälle erstellen.

- Dokumente entfernen, die nach Ablauf eines angegebenen Zeitraums nicht mehr beibehalten werden sollen.
- Schreiben von Daten auf Platte erzwingen.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Verwaltung** im Abschnitt **Forensics** auf **Schedule Actions** (Aktionen planen).
2. Klicken Sie auf **Add New Action** (Neue Aktion hinzufügen).
3. Wählen Sie in der Liste **Select Action** (Aktion auswählen) eine Aktion aus und geben Sie die Einstellungen an.
   - Soll ein neuer Index für aktuelle Fälle erstellt werden, wählen Sie **Optimize Index** (Index optimieren) aus.

     Für den neuen Index ist ungefähr doppelt so viel Speicher wie für den bereits vorhandenen Index erforderlich. Stellen Sie daher sicher, dass ausreichend Speicherplatz verfügbar ist.
   - Sollen Dokumente gelöscht werden, deren Netzzeitmarke das angegebene Alter überschritten hat, wählen Sie **Age Out Documents** (Dokumente löschen) aus.

     Beim Löschen der Dokumente werden auch die Indizes gelöscht.
   - Sollen nicht abgeschlossene Datenflüsse auf Platte geschrieben werden, wählen Sie **Flush Case** (Fall auf Platte schreiben) aus.
4. Klicken Sie auf **Save** (Speichern).
5. Soll eine Aktion ausgeführt, bearbeitet oder gelöscht werden, wählen Sie die Aktion für die Liste **Actions** (Aktionen) aus und klicken Sie auf **run** (Ausführen), **edit** (Bearbeiten) oder **delete** (Löschen).

Kapitel 7. Verdächtige Inhalte verwalten

Als Administrator können Sie verdächtige Inhalte mithilfe der Funktion 'Management verdächtiger Inhalte' markieren.

Yara-Regeln

Für die Markierung von verdächtigen Inhalten in den Dateien, die im Netzverkehr von QRadar Incident Forensics gefunden werden, können Sie bestehende Yara-Regeln importieren und verwenden. Damit können Sie angepasste Regeln angeben, die für die Dateien ausgeführt werden.

Jede Yara-Regel beginnt mit der Schlüsselwortregel, gefolgt von einer Regel-ID. Yara-Regeln bestehen aus zwei Abschnitten:

1. Zeichenfolgedefinition: Im Abschnitt für Zeichenfolgedefinitionen müssen Sie die Zeichenfolgen angeben, die einen Teil der Regel bilden sollen. Jede Zeichenfolge verwendet eine ID, die aus einem Dollarzeichen ($) gefolgt von einer Folge alphanumerischer Zeichen besteht, die durch Unterstriche getrennt werden.
2. Bedingung: Im Abschnitt für Bedingungen müssen Sie die Logik der Regel definieren. Dieser Abschnitt muss einen booleschen Ausdruck enthalten, der die Bedingungen definiert, zu denen eine Datei die Regel erfüllt.

Das folgende Beispiel zeigt eine einfache Yara-Regel:

```
rule simple_forensics : qradar
{
    meta:
        description = "This rule will look for str1 at an offsets of 25 bytes
                       into the file."
    strings:
        $str1 = "pattern of interest"

    condition:
        $a at 25
}
```

Das folgende Beispiel zeigt eine etwas komplexere Yara-Regel:

```
rule ibm_forensics : qradar
{
    meta:
        description = "This rule will flag content that contains the hex
                       sequence as well as str1 at least 3 times."

    strings:
        $hex1 = {4D 2B 68 00 ?? 14 99 F9 B? 00 30 C1 8D}
        $str1 = "IBM Security!"


    condition:
        $hex1 and (#str1 > 3)
}
```

Wenn die Yara-Regel hochgeladen wird, verwendet der Decapper angegebene Regeln, wenn er eine Datei in einer Fehlerbehebung oder in einem PCAP-Upload findet. Falls passende Inhalte gefunden werden, wird unter der Registerkarte **Attribu-**

te ein **SuspectContent**-Feld hinzugefügt. Das Feld **SuspectContent** wird mit dem Yara-Regelnamen und eventuellen Tags gefüllt, die von der Regel angegeben werden.

Einschränkung: Die Implementierung von Yara-Modulen ist derzeit nicht verfügbar.

Yara-Regeln importieren

Sie können Ihre bestehenden Yara-Regeln in IBM Security QRadar Incident Forensics importieren und diese Regeln für den Abgleich und die Markierung von böswilligen Inhalten verwenden. Eine importierte Datei kann mehrere Yara-Regeln enthalten.

Vorgehensweise

1. Wählen Sie auf der Registerkarte **Verwaltung** die Option **Management verdächtiger Inhalte** aus.
2. Klicken Sie auf **Datei auswählen**.
3. Navigieren Sie im Fenster **Hochladen von Datei** zu der Datei, die Sie importieren möchten, und klicken Sie auf **Öffnen**.

   Wichtig: Yara-Regelnamen müssen eindeutig sein.

Ergebnisse

Sie werden in einer angezeigten Nachricht informiert, sobald die Yara-Regel erfolgreich importiert wurde.

Nächste Schritte

Neu importierte Yara-Regeln werden nicht rückwirkend angewendet. Nachdem Sie die Yara-Regeln importiert haben, müssen Sie eine vollständige Implementierung durchführen, damit die Änderungen wirksam werden.

Yara-Regeln löschen

Sie können alle vorhandenen Yara-Regeln aus IBM Security QRadar Incident Forensics löschen. Sie laden eine Datei hoch, die eine einzelne leere Regel enthält, um Yara-Regeln zu inaktivieren.

Vorbereitende Schritte

Vorgehensweise

1. Führen Sie die folgenden Schritte aus, um eine neue Datei zu erstellen, die eine einzelne leere Regel enthält:
   a. Kopieren Sie die folgende Regel in einen Texteditor Ihrer Wahl:

   ```
   rule empty
   {
    condition:
              false
   }
   ```

   b. Speichern Sie dies als Textdatei.
2. Wählen Sie auf der Registerkarte **Verwaltung** die Option **Management verdächtiger Inhalte** aus.

3. Klicken Sie auf **Datei auswählen**.
4. Navigieren Sie im Fenster **Hochladen von Datei** zu der Datei, die Sie in Schritt 1 erstellt haben, und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Speichern**.

Ergebnisse

Die einzelne Regel gibt stets das Ergebnis **`false`** zurück, was ihr das Bestehen des Validators ermöglicht. Die einzelne Regel löscht alle vorhandenen Regeln und wird in die Datenbank eingefügt. Die einzelne Regel markiert Inhalte niemals als verdächtig.

Kapitel 8. Benutzer und Systembelegung in QRadar Incident Forensics prüfen

Prüfprotokolle sind chronologisch angeordnete Datensätze, die die Benutzerkonten angeben, die mit einem Datenzugriff in Verbindung stehen. Anhand dieser Protokolle können ungewöhnliche oder unbefugte Zugriffe und Probleme wie beispielsweise fehlgeschlagene Jobs erkannt werden.

Prüfprotokollereignisse werden bei den folgenden Aktivitäten erstellt:

- Fall erstellen
- Fall zuweisen
- Fall löschen
- Datensammlungen löschen
- Sämtliche Benutzerabfragen
- Dokument anzeigen
- Dokument exportieren

Einschränkung: Die Protokollierung von Ereignissen in Zusammenhang mit der Erstellung von Datensammlungen wird nicht unterstützt.

Vorgehensweise

1. Melden Sie sich über SSH als Administrator bei der QRadar-Konsole oder QRadar Incident Forensics Standalone an.
2. Navigieren Sie zum Verzeichnis `/var/log/audit`.
3. Öffnen Sie die Datei `audit.log` in einem Editor (beispielsweise vi) und überprüfen Sie ihren Inhalt oder suchen Sie mit dem Befehl **`grep`** nach einem bestimmten Eintrag.

Kapitel 9. Untersuchen von Bedrohungen mit QRadar Network Insights

Mit IBM QRadar Network Insights können Sie Ihre Netzdaten in Echtzeit analysieren und erhalten so einen Einblick in das Bedrohungsverhalten in Ihrem Netz.

QRadar Network Insights ist eine Lösung für die Analyse von Bedrohungen im Netz, die schnell und ohne großen Aufwand interne Bedrohungen, Daten-Exfiltration und Malwareaktivität erkennt. Wichtige Bedrohungsindikatoren werden gesammelt und bei vollständiger Transparenz des Datenaustauschs im Netz verfolgt.

Echtzeitorientierte Untersuchungen von Bedrohungen mit QRadar Network Insights

IBM QRadar Network Insights stellt eine Echtzeitanalyse von Netzdaten und eine intelligente Bedrohungserkennung und -analyse zur Verfügung.

Ausgeklügelte Bedrohungen der Cybersicherheit sind immer schwieriger zu erkennen und zu verhindern. Schädliche Aktivität wird häufig als normale Nutzung getarnt. Dadurch können Bedrohungen ungehindert in Netzen wandern und kommunizieren, um ihre Ziele zu erreichen. Durch "Morphen" kann sich Malware beispielsweise verändern, um eine signaturbasierte Erkennung zu umgehen, und Social Engineering-Verfahren wie Phishing sind ein effektives Mittel, um diesen Angriffen den Zugang zu ermöglichen.

Suchfunktion

Die Suchfunktion von QRadar Network Insights sucht wichtige Indikatoren und extrahiert diese aus den Paketdaten, beispielsweise Datenflussinformationen, Metadaten, extrahierte Inhalte und verdächtige Inhalte. Sie können die extrahierten Inhalte für die langfristige Rückschauanalyse verwenden.

Integration in IBM Security QRadar Incident Forensics

QRadar Network Insights zeichnet Anwendungsaktivitäten auf, erfasst Artefakte und ermittelt Assets, Anwendungen und Benutzer, die an der Netzkommunikation beteiligt sind. QRadar Network Insights ist nahtlos in IBM Security QRadar Incident Forensics integriert, um Untersuchungen nach einem Vorfall und Aktivitäten zum Aufspüren von Bedrohungen zu ermöglichen. QRadar Incident Forensics und IBM QRadar Network Packet Capture erfassen und rekonstruieren die gesamte Konversation und spielen diese erneut durch. QRadar Network Insights sorgt für die Erkennung von Vorfällen und informiert Sie, ob in der Konversation irgendwann verdächtige Elemente oder interessante Thema behandelt wurden.

Verdächtiger Inhalt kann aus vielen verschiedenen Quellen stammen, er kann sich beispielsweise aufgrund von Malware, vom Standard abweichenden Ports, regex oder Yara-Regeln ergeben.

Wert der Datenflüsse

Datenflüsse bieten QRadar einen Einblick in die Netzaktivität, da sie eine Asseterkennung ermöglichen, wenn sich Geräte mit einem Netz verbinden. Mit QRadar

Network Insights können Sie die Flussdaten mit Ereignisdaten korrelieren, um Bedrohungen zu erkennen, die nicht ausschließlich über Protokolle ermittelt werden können. IBM Security QRadar QFlow Collector stellt Netzflüsse bereit und erkennt außerdem Layer-7-Anwendungen und Sie können den Beginn der Sitzungen aufzeichnen. QRadar Network Insights macht zuvor verdeckte Bedrohungen und schädliches Verhalten sichtbar.

Zugehörige Konzepte:

„QRadar Network Insights-Inspektionsstufen für Datenflüsse" auf Seite 31
Zur Leistungssteigerung müssen Sie die richtige Datenflussrate wählen, die erforderlich ist. Hierfür wird die Einstellung **Inspektionsstufe für Fluss** konfiguriert.

QRadar Network Insights-Implementierungen

IBM QRadar Network Insights ist ein verwalteter Host, den Sie der QRadar-Konsole zuordnen.

Für eine QRadar Network Insights-Implementierung müssen Sie während der Installation die Applianceoption `6200` auswählen. Sie finden weitere Informationen zur Installation der QRadar Network Insights-Appliance im *IBM Security QRadar Incident Forensics-Installationshandbuch*.

Für eine QRadar Network Insights-Implementierung müssen Sie der Applianceoption `6200` eine Lizenz zuordnen. QRadar Network Insights erfordert eine separate Lizenz für die Appliance `6200`. Auf der QRadar-Konsole benötigen Sie jedoch keine QRadar Network Insights-Lizenz.

Beziehung zwischen der QRadar Network Insights-Appliance und IBM Security QRadar Incident Forensics

Sie können QRadar Network Insights gesondert von der IBM Security QRadar Incident Forensics Processor-Implementierung implementieren. QRadar Network Insights benötigt lediglich eine Verbindung mit der QRadar-Konsole. Es wird keine Verbindung mit der QRadar Incident Forensics-Appliance benötigt.

QRadar Network Insights-Appliance

Die QRadar Network Insights 1920-Appliance ist mit zwei Netzkarten der dritten Generation ausgestattet. Die Netzkarten werden direkt in das Netz eingebunden, um die echtzeitorientierte Paketuntersuchung zu erleichtern.

Die konfigurierbare Funktion für die Datenflussweiterleitung ermöglicht den Lastausgleich zwischen mehreren Appliances. Die Hardwarekonfiguration erleichtert die speicherinterne Verarbeitung, um eine Echtzeitanalyse der Netzdaten bereitstellen zu können.

Tabelle 2. Spezifikationen der Netzkarte

1920-Appliance	**Beschreibung**
`Server`	X3650 M5
`CPU`	2 x E5-2680 v4 14C 2,4 GHz 35 MB 2.400 MHz 120 W
`RAM`	8 x 16 GB
`HDD`	2 x 200 GB SSD
`ServeRAID`	M1215

Tabelle 2. Spezifikationen der Netzkarte (Forts.)

1920-Appliance	Beschreibung
E/A-Karten	Intel X520 2P 10 GbE + 2 x 10G SR 2 x NT40E3 4P 40G + 2 x 10G SR + 2 x 10G LR
P/S	2 x 900 W

Konfigurationsanforderungen für QRadar Network Insights

Nachdem Sie IBM QRadar Network Insights installiert und als verwalteten Host der QRadar-Konsole zugeordnet haben, müssen Sie Ihre Appliance konfigurieren, damit Sie das Produkt für die Untersuchung von Bedrohungen in Ihrem Netz verwenden können. Die QRadar Network Insights-Appliance liest die rohen Pakete aus einem Netz-TAP oder Span-Port und generiert dann IPFIX-Pakete. Die IPFIX-Pakete werden an den QFlow-Prozess auf der QRadar-Konsole gesendet.

Format der QFlow-Kollektoren konfigurieren

Als Manager eines von QRadar verwalteten Host-Clusters können Sie das Format wählen, das Ihre QFlow-Kollektoren für den Export von Daten an den QFlow-Prozessor verwenden: TLV oder Nutzdaten.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

__ • Installieren Sie eine QRadar-Konsole-Konsole, der eine QRadar Network Insights-Instanz als verwalteter Host zugeordnet wird.

__ • Nehmen Sie nach der Zuordnung von IBM QRadar Network Insights als verwalteten Host eine vollständige Implementierung vor.

Vorgehensweise

1. Melden Sie sich bei QRadar an: `https://`*`IP-Adresse_QRadar`*

   Der Standardbenutzername lautet `admin`. Das Kennwort ist das Kennwort des Rootbenutzerkontos.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Navigationsfenster auf **Systemeinstellungen**.
4. Klicken Sie auf das Menü **QFlow-Einstellungen** und wählen Sie das QFlow-Format aus.

Tabelle 3. QFlow-Formatoptionen

QFlow-Format	Beschreibung
TLV	Dies ist die standardmäßige QFlow-Formateinstellung. Wählen Sie **TLV** (Tab-Length-Value) bei Neuinstallationen oder für Upgrades, bei denen keine QRadar Network Insights-Appliance als Teil der Implementierung vorhanden ist.
Nutzdaten	Wählen Sie **Nutzdaten** für Upgrades, bei denen eine QRadar Network Insights-Appliance als Teil der Implementierung vorhanden ist. Dies bedeutet, dass die Implementierung genau wie vorher funktionsfähig ist.

5. Klicken Sie auf **Speichern**.
6. Klicken Sie in der Menüleiste der Registerkarte **Verwaltung** auf **Vollständige Konfiguration implementieren** und bestätigen Sie die Änderungen.

7. Aktualisieren Sie Ihren Web-Browser zur Anzeige der Registerkarte **Forensics**.

DTLS auf einem verwalteten QRadar Network Insights-Host einrichten

Um ein Ausspionieren und eine Manipulation des Systems zu verhindern, müssen Sie Datagram Transport Layer Security (DTLS) auf einem verwalteten QRadar Network Insights-Host einrichten. Zunächst müssen Sie eine Datenflussquelle konfigurieren.

Vorgehensweise

1. Fügen Sie QRadar Network Insights als verwalteten Host hinzu:
   a. Klicken Sie auf die Registerkarte **Verwaltung**.
   b. Klicken Sie im Navigationsfenster unter dem Abschnitt **Systemkonfiguration** auf **System- und Lizenzverwaltung**.
   c. Wählen Sie den verwalteten QRadar Network Insights-Host aus. Der Appliance-Typ ist `6200`.
   d. Klicken Sie auf das Symbol **Implementierungsaktionen** und wählen Sie **Host hinzufügen** aus.
   e. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse und das Rootkennwort des verwalteten QRadar Network Insights-Hosts ein und klicken Sie auf **Hinzufügen**.
2. Führen Sie folgende Schritte aus, um eine Datenflussquelle zu konfigurieren:
   a. Melden Sie sich bei QRadar als Administrator an.
   b. Klicken Sie auf die Registerkarte **Verwaltung**.
   c. Klicken Sie im Navigationsfenster unter dem Abschnitt **Flüsse** auf **Datenflussquellen**.
   d. Klicken Sie auf das Symbol **Hinzufügen**.
   e. Geben Sie in **Flussquellenname** einen beschreibenden Namen an.
   f. Wählen Sie einen **Zielflusskollektor** aus oder akzeptieren Sie den angegebenen Wert.
   g. Wählen Sie **Netflow v.1/v.5/v.7/v.9/IPFIX** als **Flussquellentyp** aus.
   h. Geben Sie einen Wert für den **Überwachungsport** ein oder akzeptieren Sie den angegebenen Wert.
   i. Wählen Sie `DTLS` in der Liste **Verbindungsprotokoll** aus.
   j. Klicken Sie auf **Speichern**.
   k. Klicken Sie in der Menüleiste der Registerkarte **Verwaltung** auf **Vollständige Konfiguration implementieren** und bestätigen Sie die Änderungen.
   l. Aktualisieren Sie Ihren Web-Browser.
3. Führen Sie folgende Schritte aus, um die DTLS-Kommunikation zu konfigurieren:

   Anmerkung: Wenn Sie den QRadar-Datenflusskollektor oder die Datenflussquelle eines verwalteten QRadar Network Insights-Hosts in Ihrer Implementierung ändern, müssen Sie das DTLS-Setup-Script erneut ausführen.
   a. Klicken Sie auf das Symbol **Implementierungsaktionen** und wählen Sie **Hostverbindung bearbeiten** aus.
   b. Wählen Sie auf der Seite **QRadar Network Insights ändern** den QRadar-Datenflusskollektor und die Datenflussquelle aus.
   c. Klicken Sie auf **Speichern**.
   d. Schließen Sie die Seite **System- und Lizenzverwaltung**.

e. Klicken Sie auf der Registerkarte **Verwaltung** auf das Symbol **Änderungen implementieren**.
f. Melden Sie sich über **SSH** als Rootbenutzer bei der QRadar-Konsole an.
g. Führen Sie folgenden Befehl aus, um das DTLS-Zertifikat einzurichten:
```
python /opt/qradar/bin/qflow_dtls_cert_setup.py
```
h. Melden Sie sich bei QRadar als Administrator an.
i. Wählen Sie auf der Registerkarte **Verwaltung** nacheinander **Erweitert** > **Gesamte Konfiguration implementieren** aus.

QRadar Network Insights-Inspektionsstufen für Datenflüsse

Zur Leistungssteigerung müssen Sie die richtige Datenflussrate wählen, die erforderlich ist. Hierfür wird die Einstellung **Inspektionsstufe für Fluss** konfiguriert.

Die Datenflussrate hängt mit der Transparenzstufe des verfügbaren Inhalts wie Quelle, Ziel, Protokoll und bestimmten Dateitypen zusammen.

Die Inspektionsstufen für Datenflüsse sind kumulativ, jede Stufe übernimmt also die Eigenschaften der vorherigen Stufe.

Flüsse

'Flüsse' ist die niedrigste Inspektionsstufe. Datenflüsse werden nach dem 5-Tupel-Prinzip erkannt und die Anzahl der Bytes und Pakete, die in jede Richtung fließen, werden gezählt. Diese Art von Informationen ähnelt den Informationen aus einem Router oder Netzswitch, der keine Deep Packet Inspection ausführt. Diese Stufe unterstützt die höchste Bandbreite, generiert aber auch die geringste Menge an Datenflussinformationen.

Folgende Attribute werden von QRadar Network Insights mit der Inspektionsstufe 'Flüsse' generiert: 5-Tupel-Werte, eine Datenfluss-ID, Paket- und Oktettzahlen in jeder Richtung sowie die Start- und Endzeiten von Datenflüssen.

Aufbereitete Flüsse

Jeder Datenfluss wird von einem der Protokoll- oder Domänenprüfer ermittelt und untersucht. Diese Inspektion kann zahlreiche Arten von Attributen generieren.

In der folgenden Liste werden die Attribute beschrieben, die von QRadar Network Insights mit der Inspektionsstufe 'Aufbereitete Flüsse' generiert werden:

- HTTP-Metadatenwerte - einschließlich der Kategorisierung von URLs
- Anwendungs-ID und Aktion
- Dateiinformationen (Name, Größe, Hash)
- Benutzernamen der Sender und Empfänger
- Begrenzte verdächtige Inhaltswerte

Inhaltlich aufbereitete Flüsse

'Inhaltlich aufbereitete Flüsse' ist die Standardeinstellung und höchste Inspektionsstufe. Sie liefert alle Attribute der Stufe 'Aufbereitete Flüsse', scannt und untersucht zusätzlich aber auch die Inhalte der gefundenen Dateien. Dies ermöglicht eine genauere Feststellung des Inhaltstyps und kann als Folge der Inspektion des Dateiinhalts mehr verdächtige Inhaltswerte ergeben.

In der folgenden Liste werden die Attribute beschrieben, die von QRadar Network Insights mit der Inspektionsstufe 'Inhaltlich aufbereitete Flüsse' generiert werden:

- Persönliche Informationen
- Vertrauliche Daten
- Eingebettete Scripts
- Umleitungen
- Konfigurierbare inhaltsbasierte verdächtige Inhalte

Tabelle 4. Leistungsaspekte

Einstellung der Inspektionsstufe für Datenflüsse	Leistung
`Flüsse`	10 Gb/s
`Aufbereitete Flüsse`	Ungefähr 10 Gb/s. Die Leistung variiert je nach festgelegter Inspektionsstufe, Suche, Extraktionskriterien und Netzdaten.
`Inhaltlich aufbereitete Flüsse (Erweitert)`	Ungefähr 3,5 Gb/s. Eine Leistung von 10 Gb/s kann mit mehreren Appliances erreicht werden.

Zugehörige Konzepte:

„Echtzeitorientierte Untersuchungen von Bedrohungen mit QRadar Network Insights" auf Seite 27
IBM QRadar Network Insights stellt eine Echtzeitanalyse von Netzdaten und eine intelligente Bedrohungserkennung und -analyse zur Verfügung.

Einstellungen von QRadar Network Insights konfigurieren

Zur Leistungssteigerung können Sie die Stufen für die Datenflüsse konfigurieren, die von den QRadar Network Insights-Appliances in Ihren Implementierungen erstellt werden. Jede Inspektionsstufe bietet einen noch genaueren Einblick und extrahiert noch mehr Inhalte.

Vorgehensweise

1. Melden Sie sich bei QRadar als Administrator an.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Navigationsfenster auf **Systemeinstellungen**.
4. Klicken Sie auf das Menü **Network Insights-Einstellungen**.
5. Wählen Sie in **Inspektionsstufe für Fluss** die erforderliche Datenflussrate aus. In der folgenden Tabelle werden die Inspektionsstufen für Datenflüsse erläutert:

Tabelle 5. Inspektionsstufen für Datenflüsse

Inspektionsstufe für Datenflüsse	Beschreibung
`Flüsse`	Dies ist die niedrigste Inspektionsstufe. Datenflüsse werden nach dem 5-Tupel-Prinzip erkannt und die Anzahl der Bytes und Pakete, die in jede Richtung fließen, werden gezählt.
`Aufbereitete Flüsse`	Jeder Datenfluss wird von einem der Protokoll- oder Domänenprüfer ermittelt und untersucht. Diese Inspektion kann zahlreiche Arten von Attributen generieren.
`Inhaltlich aufbereitete Flüsse`	Dies ist die Standardeinstellung. Hierbei handelt es sich um die höchste Inspektionsstufe. Sie führt alle Aktionen der Stufen vom Typ 'Aufbereitete Flüsse' aus, scannt und untersucht zusätzlich aber auch die Inhalte der gefundenen Dateien.

6. Klicken Sie auf **Speichern**.
7. Klicken Sie in der Menüleiste der Registerkarte **Verwaltung** auf **Vollständige Konfiguration implementieren**.
8. Aktualisieren Sie Ihren Web-Browser.

Nächste Schritte

Implementieren Sie den verwalteten QRadar Incident Forensics Processor-Host.

Bedrohungserkennung mit QRadar Network Insights

Damit Sie einen echtzeitorientierten Einblick in bedrohliche Aktivitäten in Ihrem Netz erhalten, verwenden Sie QRadar Network Insights, um Indikatoren für Cyberangriffe und ihre schädliche Aktivität zu finden.

QRadar Network Insights-Inhalte herunterladen

Sie laden die QRadar Network Insights-Inhalte (Erweiterung) von der Website IBM Security App Exchange (http://exchange.xforce.ibmcloud.com/hub/extension/522bf1095f047b0b37225d8efc5d4877) herunter. Diese werden mit dem Tool **Extensions Management** installiert.

Sie finden Informationen zur Verwendung des Tools **Extensions Management** im *IBM Security QRadar Administration Guide*.

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 die in diesem Handbuch beschriebenen 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 in diesem Dokument beschriebenen 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 Leistungsdaten und Kundenbeispiele dienen allein der Veranschaulichung. Die tatsächliche Leistung ist von der jeweiligen Konfiguration und den Betriebsbedingungen abhängig.

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 den Namen real existierender Einzelpersonen 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- und 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 Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Nutzungsbedingungen 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 weder weitergeben oder anzeigen noch 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.

Rechte

Abgesehen von den hier gewährten Rechten werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin 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 Software-Produkte, einschließlich "Software as a Service"-Lösungen (Softwareangebote) verwenden möglicherweise Cookies oder andere Technologien, um Nutzungsinformationen zum Produkt zu erfassen, die Erfahrung der Endbenutzer zu verbessern, Interaktionen mit dem Endbenutzer zu optimieren usw. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Manche Softwareangebote helfen Ihnen dabei, personenbezogene Daten zu erfassen. Wenn dieses Softwareangebot Cookies verwendet, um personenbezogene Daten zu erfassen, sind Informationen zur Verwendung von Cookies in diesem Angebot unten dargelegt.

Je nachdem, welche Konfigurationen implementiert wurden, ist es möglich, dass dieses Softwareangebot Sitzungscookies zum Erfassen der Sitzungs-IDs einzelner Benutzer für die Sitzungsverwaltung und Authentifizierung verwendet. Diese Cookies können inaktiviert werden, dabei wird jedoch auch die Funktionalität inaktiviert, die diese Cookies ermöglichen.

Wenn die für dieses Softwareangebot genutzten 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, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der IBM Datenschutzrichtlinie unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzrichtlinie unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und im "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Gedruckt in Deutschland