IBM QRadar User Behavior Analytics (UBA) アプリ

バージョン 3.2.0

ユーザー・ガイド

IBM

注記

本書および本書で紹介する製品をご使用になる前に、 227 ページの『特記事項』に記載されている情報をお読みください。

製品情報

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.2.8 および以降のリリースに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

本書は下記原典を翻訳したものです。

原典： IBM QRadar User Behavior Analytics (UBA) app
Version 3.2.0
User Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

1 User Behavior Analytics for QRadar

User Behavior Analytics for QRadar アプリケーションを使用すると、ネットワーク内部に存在するユーザーのリスク・プロファイルを識別でき、脅威となる動作についてこのアプリケーションからアラートが出された場合に対処できます。

User Behavior Analytics for QRadar (UBA) アプリケーションは、組織内部の脅威を検出するツールです。このアプリケーションは、QRadar 内の既存データを使用するためのアプリケーション・フレームワークに基づいて作成され、ユーザーとリスクに関する新たな洞察を生成します。 UBA では、リスク・プロファイル作成とユーザー・アイデンティティーの統一という 2 つの主要機能が QRadar に追加されます。

リスク・プロファイル作成を行うには、リスクをさまざまなセキュリティー・ユース・ケースに割り当てます。例えば、不正な Web サイトなどに関する単純なルールおよびチェックや、機械学習を利用するより高度なステートフル分析などがあります。リスクは、検出されたインシデントの重大度と信頼性に応じてそれぞれのユース・ケースに割り当てられます。 UBA では、QRadar システム内の既存のイベント・データとフロー・データを使用して必要な洞察が生成され、ユーザーのリスク・プロファイルが作成されます。UBA で使用されるトラフィックには 3 つのタイプがあります。1 つ目は、アクセス、認証、およびアカウント変更に関するトラフィックです。 2 つ目は、ネットワーク上でのユーザー動作です。そのため、プロキシー、ファイアウォール、IPS、VPN などのデバイスが該当します。 3 つ目は、エンドポイントのログとアプリケーション・ログです。Windows や Linux、SAAS アプリケーションなどから取得したものです。この 3 つのタイプのトラフィックによって UBA の能力が向上し、より多くのユース・ケースによってリスク・プロファイルを作成できます。

ユーザー・アイデンティティーの統一は、QRadar 内の 1 ユーザーに対する複数の異なるアカウントを結合することで実現します。Active Directory、LDAP、または CSV ファイルからデータをインポートすると、ユーザー・アイデンティティーにどのアカウントが属するかを UBA に指示できます。これにより、UBA 用に QRadar 内の複数の異なるユーザー名間でリスクとトラフィックを結合できます。

機械学習 (ML) は、UBA アプリケーションを補強するアドオン・ツールです。これを利用すると、時系列のプロファイル作成とクラスター化を実現する、より高度かつ詳細なユース・ケースが得られます。 ML は UBA アプリケーション内から「機械学習の設定」ページを使用してインストールします。 ML を使用することで既存の UBA アプリケーションの可視化項目が増え、学習した動作 (モデル)、現在の動作、およびアラートが表示されます。機械学習では QRadar 内の最大 4 週間分の履歴データを使用して予測モデルが作成され、さらにユーザーにとって何が通常どおりであるかを示すベースラインも作成されます。

Reference Data Import LDAP アプリケーションの使用について詳しくは、 179 ページの『8, Reference Data Import - LDAP アプリケーション』を参照してください。

Machine Learning Analytics アプリケーションの使用について詳しくは、 191 ページの『9, Machine Learning Analytics アプリ』を参照してください。

重要**:** QRadar® UBA アプリをインストールする前に IBM® QRadar V7.2.8 以降をインストールしておく必要があります。

関連概念:

51 ページの『7, UBA アプリのルールおよびチューニング』

IBM QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

25 ページの『User Behavior Analytics アプリの構成』
IBM QRadar User Behavior Analytics (UBA) アプリを使用できるようにするには、追加設定を構成する必要があります。

179 ページの『8, Reference Data Import - LDAP アプリケーション』
Reference Data Import - LDAP アプリケーションを使用して、複数の LDAP ソースからのコンテキスト・アイデンティティー情報を QRadar コンソールに収集します。

191 ページの『9, Machine Learning Analytics アプリ』
Machine Learning Analytics (ML) アプリを使用して機械学習分析用のユース・ケースを追加することにより、QRadar システムと QRadar User Behavior Analytics (UBA) アプリの機能が拡張されます。Machine Learning Analytics のユース・ケースを用いて予測モデリングを行うと、ユーザーの行動をさらに詳しく分析できます。ML アプリにより、ネットワーク内で予期されるユーザーの行動をシステムに学習させることができます。

関連タスク:

19 ページの『User Behavior Analytics アプリのインストール』
IBM QRadar 拡張の管理ツールを使用して、アプリケーション・アーカイブを直接 QRadar コンソールにアップロードおよびインストールします。

23 ページの『User Behavior Analytics アプリのアップグレード』
IBM QRadar 拡張の管理ツールを使用して、アプリケーションをアップグレードします。

User Behavior Analytics アプリの新機能

User Behavior Analytics (UBA) アプリの各リリースにおける新機能について説明します。

V3.2.0 の新機能

- 休止アカウントを持つユーザーをダッシュボードおよびユーザー・プロファイル・ページで特定します。詳しくは、 43 ページの『休止アカウント』を参照してください。
- 欠落しているユーザー・プロパティーに基づいてサービス・アカウントの監視リストを作成します。詳しくは、 39 ページの『監視リストの作成』を参照してください。
- UBA で使用する LDAP 属性を選択できるよう LDAP アプリケーションを向上しました。注: LDAP を構成する際に、「属性マッピング」セクションでの外部キーの選択が必要になりました。詳しくは、 25 ページの『Reference Data Import LDAP アプリの構成』を参照してください。
- CSV ファイルからユーザー情報をインポートする機能が追加されました。詳しくは、 180 ページの『CSV ファイルからのユーザー・データのインポート』を参照してください。
- ユース・ケース「UBA : 複数のホストからのユーザー・アクセス (UBA : User Access from Multiple Hosts)」が追加されました。詳しくは、 66 ページの『UBA : 複数のホストからのユーザー・アクセス (UBA : User Access from Multiple Hosts)』を参照してください。
- ユース・ケース「UBA : ディレクトリー・サービス列挙の可能性 (UBA : Possible Directory Services Enumeration)」が追加されました。詳しくは、 107 ページの『UBA : ディレクトリー・サービス列挙の可能性 (UBA : Possible Directory Services Enumeration)』を参照してください。
- ユース・ケース「UBA : ドメイン・コントローラーに対する SMB セッション列挙の可能性 (UBA : Possible SMB Session Enumeration on a Domain Controller)」が追加されました。詳しくは、 107 ページの『UBA : ドメイン・コントローラーに対する SMB セッション列挙の可能性 (UBA : Possible SMB Session Enumeration on a Domain Controller)』を参照してください。
- ユース・ケース「UBA : 疑わしいアクセスに続くデータ引き出し」が追加されました。詳しくは、 124 ページの『UBA : 疑わしいアクセスに続くデータ引き出し』を参照してください。

- ユース・ケース「UBA : 休止アカウント使用の試み (UBA : Dormant Account Use Attempted)」が追加されました。詳しくは、 83 ページの『UBA : 休止アカウント使用の試み (UBA : Dormant Account Use Attempted)』を参照してください。

V3.1.0 の新機能

- ユーザーのタイムラインでのメトリックの表示をカスタマイズし、そのメトリックで構成されるデータを表示できるようになりました。
- 動的リスクしきい値を設定する機能が追加されました。
- 「ルールおよびチューニング」ページに、「クラウド」と「ドメイン・コントローラー」の 2 つのユース・ケース・カテゴリーが追加されました。詳しくは、 51 ページの『7, UBA アプリのルールおよびチューニング』を参照してください。
- ユース・ケース「UBA : 非標準ユーザーによる AWS リソースへのアクセス」が追加されました。詳しくは、 102 ページの『UBA : 非標準ユーザーによる AWS リソースへのアクセス』を参照してください。
- ユース・ケース「UBA : 無許可ユーザーによる AWS コンソールのアクセス」が追加されました。詳しくは、 102 ページの『UBA : 無許可ユーザーによる AWS コンソールのアクセス』を参照してください。
- ユース・ケース「UBA : 非ドメイン・コントローラーからの複製要求」が追加されました。詳しくは、 109 ページの『UBA : 非ドメイン・コントローラーからの複製要求』を参照してください。
- ユース・ケース「UBA : Kerberos アカウント列挙の検出」が追加されました。詳しくは、 103 ページの『UBA : Kerberos アカウント列挙の検出』を参照してください。
- ユース・ケース「UBA : TGT PAC 偽造の可能性」が追加されました。詳しくは、 109 ページの『UBA : TGT PAC 偽造の可能性』を参照してください。
- ユース・ケース「UBA : DPAPI バックアップのマスター鍵リカバリーの試行」が追加されました。詳しくは、 103 ページの『UBA : DPAPI バックアップのマスター鍵リカバリーの試行』を参照してください。
- ユース・ケース「UBA : アカウント削除による DoS 攻撃 (UBA : DoS Attack by Account Deletion)」が追加されました。詳しくは、 79 ページの『UBA : アカウント削除による DoS 攻撃 (UBA : DoS Attack by Account Deletion)』を参照してください。
- ユース・ケース「UBA : 複数のファイル転送ブロック後のファイル転送」が追加されました。詳しくは、 121 ページの『UBA : 複数のファイル転送ブロック後のファイル転送』を参照してください。

V3.0.1 の新機能

- IBM QRadar DNS Analyzer アプリによる DNS トンネリングの検出をサポートするためのユース・ケースが追加されました。詳しくは、 146 ページの『UBA : トンネリング・ドメインへのアクセスの可能性 (UBA : Potential Access to Tunneling Domain)』を参照してください。
- リファレンス・テーブルからユーザーを取り込む機能を妨げる可能性のある問題を修正しました。

V3.0.0 の新機能

- 監視リストを作成および管理して、ユーザーのカスタム・グループをモニターできるようになりました。詳しくは、 39 ページの『監視リストの作成』を参照してください。
- 新規の「ルールおよびチューニング」ページで、UBA ユース・ケースの表示、フィルタリング、およびチューニングが可能になりました。詳しくは、 51 ページの『7, UBA アプリのルールおよびチューニング』を参照してください。

- ユーザー・アクティビティーのタイムラインで、アクティビティーのセッションごとにリスクの高いイベントとメトリックを表示できるようになりました。詳しくは、 10 ページの『UBA ダッシュボードとユーザーの詳細』を参照してください。
- 外部ドメインへの異常なボリュームのデータを検出する機械学習分析が追加されました。詳しくは、 202 ページの『「外部ドメインへの異常ボリューム・データ」分析の構成』を参照してください。
- ユース・ケース「UBA : 高リスク・ユーザーによる大量アウトバウンド転送」が追加されました。詳しくは、 121 ページの『UBA : 高リスク・ユーザーによる大量アウトバウンド転送』を参照してください。
- ユース・ケース「UBA : ハニートークン・アクティビティー」が追加されました。詳しくは、 140 ページの『UBA : ハニートークン・アクティビティー』を参照してください。
- ユース・ケース「UBA : ブルート・フォース認証の試行」が追加されました。詳しくは、 52 ページの『UBA : ブルート・フォース認証の試行』を参照してください。
- ユース・ケース「UBA : 短期間でのユーザー・アカウントの作成と削除」が追加されました。詳しくは、 82 ページの『UBA : 短期間でのユーザー・アカウントの作成と削除』を参照してください。
- ユース・ケース「UBA : 重要なアセットへの高リスク・ユーザー・アクセス」が追加されました。詳しくは、 55 ページの『UBA : 重要なアセットへの高リスク・ユーザー・アクセス』を参照してください。
- ユース・ケース「UBA : 新規ロケーションからの異常なアカウント作成」が追加されました。詳しくは、 125 ページの『UBA : 新規ロケーションからの異常なアカウント作成』を参照してください。
- ユース・ケース「UBA : 新規ロケーションからの異常なクラウド・アカウント作成」が追加されました。詳しくは、 129 ページの『UBA : 新規ロケーションからの異常なクラウド・アカウント作成』を参照してください。

V2.8.0 の新機能

- 機械学習分析設定を構成するときに、「拡張検索フィルター」フィールドで AQL 照会によってフィルタリングできるようになりました。詳しくは、 194 ページの『Machine Learning Analytics 設定の構成』を参照してください。
- 「イベントから検出されたユーザー」および「ディレクトリーからインポートされたユーザー」のダッシュボード統計を表示できるようになりました。詳しくは、 10 ページの『UBA ダッシュボードとユーザーの詳細』を参照してください。
- 機械学習を使用して追跡するユーザーを指定できるようになりました。詳しくは、 10 ページの『UBA ダッシュボードとユーザーの詳細』を参照してください。
- 機械学習分析ごとにグラフを表示するかどうかを構成できるようになりました。詳しくは、 194 ページの『Machine Learning Analytics 設定の構成』を参照してください。
- UBA コンテンツ・パッケージ (QRadar ルール、カスタム・プロパティー、およびユース・ケース用のリファレンス・データ) をインストールまたはアップグレードするかどうかを構成できるようになりました。詳しくは、 31 ページの『コンテンツ・パッケージ設定の構成』を参照してください。
- 異常なアウトバウンド転送の試行を検出するために有効化できる機械学習分析が追加されました。詳しくは、 196 ページの『「異常なアウトバウンド転送の試行」分析の構成』を参照してください。
- アプリケーション・ノード上で Machine Learning を使用して UBA を実行する場合に、より多くのユーザーをサポートするための機械学習メモリーの構成が追加されました。
- 高リスク・ユーザーを識別するリファレンス・セットが追加されました。詳しくは、 49 ページの『リファレンス・セット』を参照してください。

- 「Web サイトをブラウズ」のカテゴリーである「ビジネス/サービス」、「ライフスタイル」、および「未分類」について、ユース・ケースが追加されました。詳しくは、 94 ページの『参照動作』を参照してください。
- ユース・ケース「UBA : ネットワーク共有へのアクセス」が追加されました。詳しくは、 162 ページの『UBA : ネットワーク共有へのアクセス』を参照してください。
- ユース・ケース「UBA : 非管理者によるドメイン・コントローラーへのアクセス」が追加されました。詳しくは、 104 ページの『UBA : 非管理者によるドメイン・コントローラーへのアクセス』を参照してください。
- ユース・ケース「UBA : 禁止された場所からのユーザー・アクセス」が追加されました。詳しくは、 132 ページの『UBA : 禁止された場所からのユーザー・アクセス』を参照してください。
- ユース・ケース「UBA : 制限された場所からのユーザー・アクセス」が追加されました。詳しくは、 117 ページの『UBA : 制限付きプログラムの使用』を参照してください。
- ユース・ケース「UBA : 同一ユーザーの Kerberos 認証の複数回失敗」が追加されました。詳しくは、 104 ページの『UBA : 同一ユーザーの Kerberos 認証の複数回失敗』を参照してください。
- ユース・ケース「UBA : 複数のホストによって使用される TGT チケット (UBA : TGT Ticket Used by Multiple Hosts)」が追加されました。詳しくは、 110 ページの『UBA : 複数のホストによって使用される TGT チケット (UBA : TGT Ticket Used by Multiple Hosts)』を参照してください。

V2.7.0 の新機能

重要: V2.7.0 にアップグレードする場合は、技術情報 http://www.ibm.com/support/docview.wss?uid=swg22005489 に記載されている手順を実行する必要があります。

User Behavior Analytics アプリの V2.7.0 に含まれている新機能は、次のとおりです。

- QRadar Advisor with Watson アプリ内でユーザーを調査できるようになりました。注: QRadar Advisor with Watson V1.13.0 がインストールされている必要があります。詳しくは、 15 ページの『QRadar Advisor with Watson 内でのユーザーの調査』を参照してください。
- ユーザーの一般データ保護規則 (GDPR) 準拠レポートを生成し、ユーザーの追跡を停止することができるようになりました。
- 「ユーザー分析」ダッシュボードから、ユーザーの調査状況にマークを付け、調査対象であるすべてのユーザーを表示することができるようになりました。
- IP アドレスの国および地域フラグを表示するかどうかを構成できるようになりました。
- IBM QRadar DNS Analyzer アプリによって生成されるドメイン・アクセス・イベントのサポートが追加されました。詳しくは、 144 ページの『QRadar DNS Analyzer』を参照してください。
- 19 件の通常ではないスキャンのユース・ケースが新しく追加されました。詳しくは、 152 ページの『スキャン行為』を参照してください。
- 3 件の疑わしいアプリケーションのユース・ケースが新しく追加されました。詳しくは、 111 ページの『エンドポイント』を参照してください。
- 10 件のリスクのあるブラウズのユース・ケースが新しく追加されました。詳しくは、 94 ページの『参照動作』を参照してください。
- 13 件のシステム・モニター (Sysmon) のユース・ケースが新しく追加されました。詳しくは、 161 ページの『システム・モニター (Sysmon)』を参照してください。

V2.6.0 の新機能

重要: V2.6.0 にアップグレードする場合は、技術情報 http://www.ibm.com/support/docview.wss?uid=swg22005489 に記載されている手順を実行する必要があります。

User Behavior Analytics アプリの V2.6.0 に含まれている機能は、次のとおりです。

- LDAP および Active Directory に定義済みのピア・グループに基づいてアノマリを分析するために Machine Learning Analytics (ML) アプリケーションを拡張しました。
- ML アプリケーションの「ピア・グループ」分析が「学習ピア・グループ」に名前変更されました。
- ユース・ケース「UBA : ゴールド・ディスク・ホワイトリスト外のプロセス実行 (Windows/Linux)」が追加されました
- ユース・ケース「UBA : ランサムウェア動作の検出」が追加されました
- ユース・ケース「UBA : Netcat プロセス検出 (Windows/Linux)」が追加されました
- ユース・ケース「UBA : 単一 IP からの複数 VPN アカウントへのログイン失敗」が追加されました
- ユース・ケース「UBA : ボリューム・シャドー・コピーの作成」が追加されました
- ユース・ケース「UBA : 非セキュアまたは非標準プロトコルの検出」が追加されました
- ユース・ケース「UBA : マルウェア・アクティビティー - レジストリーの一括変更」が追加されました
- ユース・ケース「UBA : インターネット設定の変更」が追加されました
- ユース・ケース「UBA : 単一 IP からの複数 VPN アカウントへのログイン」が追加されました
- ユース・ケース「UBA : 疑わしい PowerShell アクティビティー (アセット)」が追加されました
- ユース・ケース「UBA : 疑わしい PowerShell アクティビティー」が追加されました
- ユース・ケース「UBA : 疑わしいコマンド・シェル・アクティビティー (Suspicious Command shell Activity)」が追加されました
- ユース・ケース「UBA : 悪意のあるプロセスの検出」が追加されました

V2.5.0 の新機能

重要: V2.5.0 にアップグレードする場合は、技術情報 http://www.ibm.com/support/docview.wss?uid=swg22005489 に記載されている手順を実行する必要があります。

V2.5.0 の User Behavior Analytics アプリは以下の点が向上しています。

- インラインのコンテキスト・イベント・ビューアーを使用して、ユーザーのリスクの高い振る舞いを素早く調査する機能が追加されました。詳しくは、 10 ページの『UBA ダッシュボードとユーザーの詳細』を参照してください。
- 資料、チュートリアル、サポート情報へのリンクに加えて管理機能も提供する「ヘルプおよびサポート」ページが追加されました。詳しくは、 221 ページの『UBA の「ヘルプおよびサポート」ページ』を参照してください。
- 機械学習の正確度とスケーラビリティーが向上し、ダッシュボードの「機械学習モデルの状況」セクションのメッセージが改善されました。詳しくは、 210 ページの『Machine Learning Analytics を使用した UBA ダッシュボード』を参照してください。
- ユース・ケース「UBA : ユーザーによる新規プロセスの実行」が追加されました。詳しくは、 118 ページの『UBA : ユーザーによる新規プロセスの実行』を参照してください。

- ユース・ケース「UBA : ユーザーによる疑わしいアプリケーションのインストール」が追加されました。詳しくは、 118 ページの『UBA : ユーザーによる疑わしいアプリケーションのインストール』を参照してください。
- ユース・ケース「UBA : サービスまたはマシン・アカウントによる UNIX/Linux システム・アクセス」が追加されました。詳しくは、 61 ページの『UBA : サービスまたはマシン・アカウントによる Unix/Linux システム・アクセス』を参照してください。
- ユース・ケース「UBA : ジャンプ・サーバーからの内部サーバーへのユーザー・アクセス」が追加されました。詳しくは、 68 ページの『UBA : ジャンプ・サーバーからの内部サーバーへのユーザー・アクセス』を参照してください。
- ユース・ケース「UBA : 非エグゼクティブ・ユーザーによってアクセスされたエグゼクティブ専用のアセット」が追加されました。詳しくは、 53 ページの『UBA : 非エグゼクティブ・ユーザーによってアクセスされたエグゼクティブ専用のアセット』を参照してください。

V2.4.0 の新機能

重要: V2.4.0 にアップグレードする場合は、技術情報 http://www.ibm.com/support/docview.wss?uid=swg22005489 に記載されている手順を実行する必要があります。

V2.4.0 の User Behavior Analytics アプリは以下の点が向上しています。

- LDAP アプリで LDAP 取得状況を表示できます。
- LDAP アプリで最大 400,000 人までのユーザーをインポートできます。構成を変更する前に、既知の問題を参照してください。
- LDAP/AD データの統合およびマッピングが合理化および単純化されました。
- プライマリー・ユーザー ID に、無制限の数の別名をマップできます。
- 「機械学習の設定」に追加されたメモリー構成設定により、アプリケーション・ノード上で Machine Learning を実行する場合により多くのユーザーをサポートできます。
- フィードバック・サーベイが追加されました。
- ユース・ケース「UBA : サービス・アカウントまたはマシン・アカウントによる Windows アクセス」が追加されました。詳しくは、 75 ページの『UBA : サービスまたはマシン・アカウントによる Windows アクセス』を参照してください。
- ユース・ケース「UBA : D/DoS 攻撃の検出」が追加されました。詳しくは、 139 ページの『UBA : D/DoS 攻撃の検出』を参照してください。
- ユース・ケース「UBA : 持続 SSH セッションの検出」が追加されました。詳しくは、 111 ページの『UBA : 持続 SSH セッションの検出』を参照してください。
- ユース・ケース「UBA : Abnormal data volume to external domain」が追加されました。詳しくは、 119 ページの『UBA : Abnormal data volume to external domain (ADE ルール)』を参照してください。
- ユース・ケース「UBA : Abnormal Outbound Attempts」が追加されました。詳しくは、 120 ページの『UBA : Abnormal Outbound Transfer Attempts (ADE ルール)』を参照してください。

既知の問題

User Behavior Analytics アプリには、アップグレードのための必須情報と既知の問題があります。

注: ADE ルールを有効にすると、UBA アプリおよびご使用の QRadar システムのパフォーマンスに影響を与える可能性があります。

V3.2.0 の既知の問題

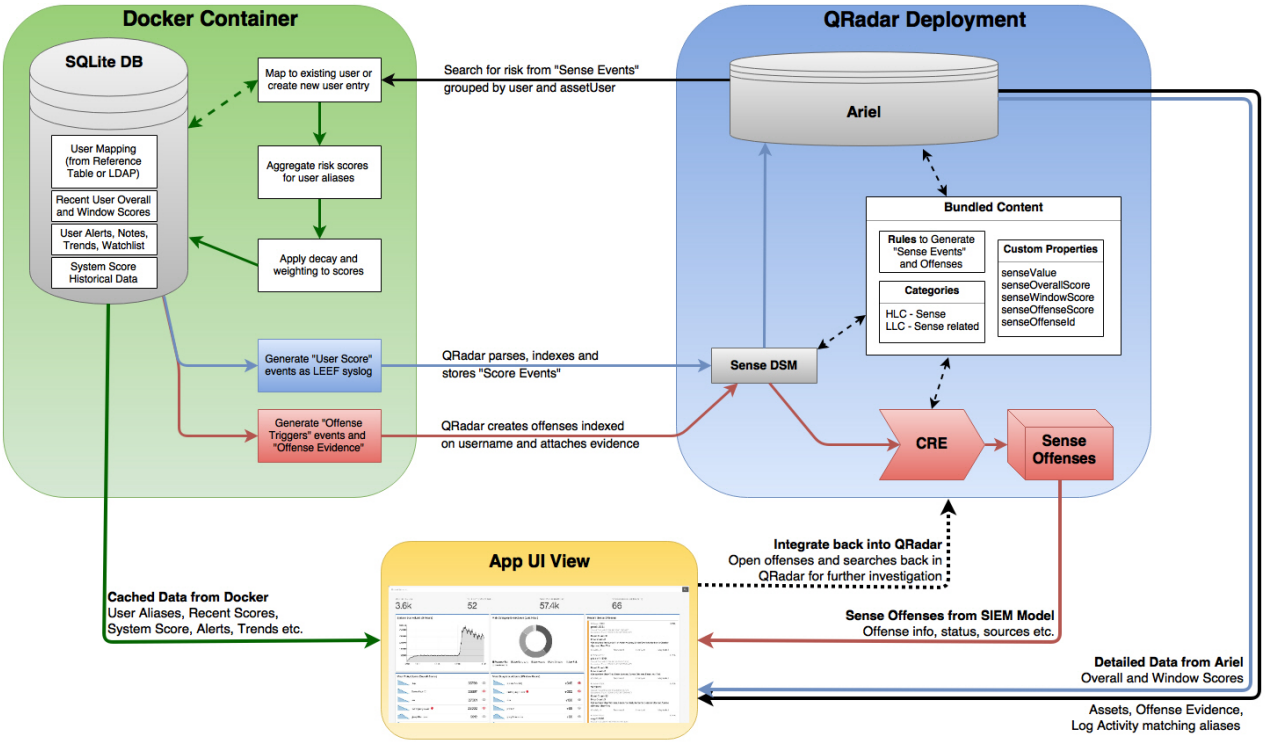
User Behavior Analytics アプリには、以下に示す既知の問題があります。

- QRadar 7.2.8 パッチ 13、QRadar 7.2.8 パッチ 13 IF1、QRadar 7.3.1 パッチ 3、または QRadar 7.3.1 パッチ 4 上で実行している場合に、リファレンス・テーブルからユーザー統合を行うと、UBA ユーザー・レコード内に不完全なユーザー情報が生成されます。この問題は V7.3.1 パッチ 4 IF1 で解決しています。詳しくは APAR IJ06032 を参照してください。
- UBA アプリのアップグレード中に、ルール・セットをロードできなかったことを示す QRadar 通知例外エラーが発生した場合は、これを無視して操作を続行できます。エラーが解決しない場合は、IBM お客様サポートにお問い合わせください。
- QRadar V7.2.8 パッチ 12 および QRadar V7.3.1 パッチ 3 には既知の問題があるため、QRadar V7.2.8 パッチ 13 および QRadar V7.3.1 パッチ 4 にアップグレードする必要があります。
- UBA を V3.2.0 にアップグレードした後、「ユーザーの詳細」ページに「機械学習アクティビティーの分布 (Machine Learning Activity Distribution)」グラフを表示するのに 1 日かかることがあります。
- ユーザー・プロファイル・ページの表示中に、「ホワイトリストに追加」ボタンが表示されない場合があります。これが発生した場合、ページを最新表示することで問題を解決できます。
- UBA 用の LDAP に 100,000 を超えるユーザーをインポートすると、QRadar システムおよび UBA アプリのインストール済み環境に深刻な影響が及ぶことがあります。この問題の原因は、APAR IV98655 の既知の問題です。128 GB のコンソールで QRadar 7.3.0 以降を使用する場合を除き、200,000 を超えるユーザーをインポートすることはお勧めしません。
- QRadar V7.2.8 および V7.3.0 ではまれに、新しく作成した SEC トークンで、その SEC トークンが機能しているように見えるが、後で無効になるという問題が発生することがあります。この問題を修正するには、以下のいずれかのアクションを実行します。
  - QRadar コンソールのコマンド・ラインから Apache Tomcat サービスを再始動します。
  - QRadar の「管理」タブから任意のアクションをデプロイします。
- 「システム・スコア」グラフで、複数の日の日付範囲を選択し、範囲の終了日を現在の日にした場合、最初の 8 データ・ポイントが 0 と表示されます。
- QRadar V7.2.8 を一部のロケールで使用すると、ユーザー・インターフェースの一部で英語のストリングや破損したテキストが表示されます。

プロセスの概要

User Behavior Analytics アプリは、QRadar システムと連動して、ネットワーク内のユーザーに関するデータを収集します。

UBA の仕組み



1. QRadar への送信データをログに記録します。
2. UBA 固有のルールで、特定のイベント (有効にされている UBA ルールに依存) を検索し、UBA アプリによって読み取られる新しいセンス・イベントをトリガーします。
3. UBA ルールには、ユーザー名と他のテストが設定されたイベントが必要です (ルールを調べて、ルールによる検索の対象を確認してください)。
4. UBA はセンス・イベントから *senseValue* とユーザー名をプルし、そのユーザーのリスク・スコアを *senseValue* で指定されている量だけ増やします。
5. ユーザーのリスク・スコアが、「UBA の設定」ページで設定したしきい値を超えると、UBA はイベントを送信します。これにより、ルール「UBA : Create Offense」がトリガーされて、そのユーザーに対するオフェンスが作成されます。

リスク・スコア

リスク・スコアは、UBA ルールによって検出されるすべてのリスク・イベントの合計です。リスク・スコアが大きいほど内部ユーザーがセキュリティー上のリスクとなる可能性が高く、ユーザーのネットワーク・アクティビティーをさらに審査する必要があります。新しいイベントが発生しない場合、リスク・スコアは時間の経過につれて減少します。減少量は「UBA の設定」ページの「**1** 時間ごとのリスク減衰の係数」の値によって制御されます。

senseValue を使用してユーザー・リスク・スコアが作成される仕組み

ルールと分析のそれぞれには、検出された問題の重大度を示す値が割り当てられます。ユーザーのアクションによってルールがトリガーされるたびに、そのユーザーのリスク・スコアには、この値が追加されます。ユーザーがルールに「違反」するたびに、スコアが高くなっていきます。

ルールとセンス・イベント

ルールがトリガーされると、ルールによってセンス・イベントが生成され、そのセンス・イベントを使用してユーザーのリスク・スコアが決定されます。

センス・イベントを生成するための QRadar 内の既存のルールは、更新することができます。詳しくは、48 ページの『新規または既存の QRadar コンテンツと UBA アプリの統合』を参照してください。

Machine Learning Analytics とセンス・イベント

Machine Learning Analytics アプリをインストールして機械学習分析を有効にすることで、変則的なユーザー動作を識別できるようになります。分析がトリガーされると、それによってセンス・イベントが生成されます。また、生成されたセンス・イベントによって、ユーザーのリスク・スコアも増加されます。

ビデオによるデモンストレーションとチュートリアル

IBM QRadar User Behavior Analytics (UBA) アプリ、Reference Data Import - LDAP アプリ、および Machine Learning Analytics (ML) アプリの詳細情報を得ることができます。

IBM Security Learning Academy

IBM Security Learning Academy Web サイトで、User Behavior Analytics (UBA) コースに登録してください。

ヒント**:** 登録してビデオを観るには、IBM ID アカウントが必要です。

YouTube でのビデオ・チュートリアル

Machine Learning V2.0.0 を使用した User Behavior Analytics アプリのデモンストレーション: https://www.youtube.com/watch?v=RgF1RztR1yg。

Reference Data Import - LDAP アプリの構成のデモンストレーション: https://www.youtube.com/watch?v=ER-wYxS6wFk

User Behavior Analytics アプリの一般的な概要:

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

UBA ダッシュボードとユーザーの詳細

IBM QRadar User Behavior Analytics (UBA) アプリには、ネットワーク内のユーザーの全体的なリスク・データが表示されます。

ダッシュボード

UBA アプリをインストールおよび構成したら、「ユーザー分析」タブをクリックしてダッシュボードを開きます。

注**:** UBA アプリがモニターできるサポート対象のユーザー数は、400,000 ユーザーです。

「ユーザーの検索」フィールドで、名前、E メール・アドレス、またはユーザー名によりユーザーを検索できます。名前を入力すると、アプリには、上位 5 件の結果が表示されます。

ダッシュボードは、1 分間隔で自動的に最新表示されます。ダッシュボードには、以下のリスク・データが表示されます。

モニター対象ユーザー	UBA アプリがアクティブにモニターしているユーザーの総数を表示します。
高リスク・ユーザー	現在リスク・スコアを超えているユーザー数を表示します。リスク・スコアを決定する値は「UBA の設定」の「オフェンスをトリガーするリスクしきい値」で設定されます。
イベントから検出されたユーザー	イベントから検出されたユーザーの数 (インポートされたユーザーを除く) を表示します。
ディレクトリーからインポートされたユーザー	リファレンス・テーブルからインポートされたユーザーの数を表示します。
アクティブな分析	• UBA ルール: ルール・コンテンツの状況を示します。緑色の状況は、ルールがインストールされ、アクティブであることを示します。グレーは、ルールが無効になっていることを示します。黄色は、インストールが進行中であることを示します。 • フロー・ルール: QNI ルールの状況を示します。緑色の状況は、QNI ルールがインストールされ、アクティブであることを示します。グレーは、QNI ルールがインストールされていないことを示します。 • 振る舞いのアノマリ: 緑色の状況は、ADE ルールがインストールされ、アクティブであることを示します。グレーは、ADE ルールがインストールされていないことを示します。 • Machine Learning Analytics: 緑色の状況は、Machine Learning Analytics アプリがインストールされていることを示します。グレーは、Machine Learning Analytics アプリがインストールされていないことを示します。
モニター対象ユーザー	最もリスクの高い上位 10 人のユーザーを表示します。最初の列には、表示名および役職と市区町村 (取得可能な場合) がリストされます。 • 最近のリスク: 各ユーザーの過去 5 分間における累積リスクを表示します。 • リスク・スコア: ユーザーの過去 1 時間における全体的なリスク・スコアの傾向と現在のリスク・スコアを示すグラフを表示します。グラフの色によって全体的なリスクの高さが示されます。 • 「監視リスト」アイコン: ユーザーを監視リストに追加するか、監視リストを作成します。数値は、そのユーザーがメンバーになっている監視リストの数を示します。 • 「検索」ページですべての追跡対象ユーザーを確認できます。
最新のオフェンス	最新のセンス・オフェンス (ユーザー別)。
[ユーザー] 監視リスト	自分が作成した監視リスト。監視リストは必要な数だけ作成することができ、ダッシュボードに表示されます。「検索」ページで作成済みのカスタムの監視リスト内のすべての追跡対象ユーザーを確認できます。 **ヒント:** 監視リストにユーザーを追加するには、「監視リスト」  アイコンをクリックします。 数値は、そのユーザーがメンバーになっている監視リストの数を示します。
システム・スコア	指定された時点におけるすべてのユーザーの全体的な集計リスク・スコア。1 日より長い日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。選択できる最大期間は、過去 1 年間の任意の 30 日間です。
リスク・カテゴリーの明細	過去 1 時間のハイレベル・リスク・カテゴリー。グラフをクリックしてサブカテゴリーを表示してから、クリックしてイベントを表示します。

休止アカウントを持つユーザー (Users with Dormant Accounts)	休止アカウントを持つとしてフラグが立てられているユーザーの監視リスト。「休止アカウントを持つユーザー (Users with Dormant Accounts)」は自動的に生成されます。 V3.2.0 以降で使用可能です。
アクティブな調査	現在調査対象であるユーザー。自分が開始した調査のみを表示するには、「自分の調査」チェック・ボックスを選択します。V2.7.0 以降で使用可能です。
機械学習モデルの状況	Machine Learning Analytics の状況は、Machine Learning アプリがインストールされている場合に表示されます。詳しくは、 210 ページの『Machine Learning Analytics を使用した UBA ダッシュボード』を参照してください。

「ユーザーの詳細」ページ

アプリ内の任意の場所からユーザー名をクリックして、選択したユーザーの詳細を表示できます。

イベント・ビューアー・ペインでは、ユーザーのアクティビティーの詳細情報を確認できます。イベント・ビューアー・ペインには、選択したアクティビティーまたは選択した時点に関する情報が表示されます。イベント・ビューアー・ペインでイベントをクリックすると、Syslog イベントやペイロード情報などの詳細が表示されます。イベント・ビューアー・ペインは、「ユーザーの詳細」ページの「リスクのあるアクティビティーのタイムライン」のすべてのドーナツ・グラフ、折れ線グラフ、およびアクティビティーで使用できます。

「ユーザーの詳細」ページには、以下のユーザー情報が含まれています。

- 選択されたユーザーの名前と別名、および LDAP からインポートされた属性からの追加の詳細情報を表示します。
- V3.2.0 以降では、対象のユーザーに関連付けられているすべてのアカウントの状況 (「休止 (Dormant)」、「アクティブ」、「未使用 (Never Used)」) を表示できます。
- QRadar Advisor with Watson V1.13.0 以降がインストールされている場合は、ユーザーに関連する情報を検索できます。QRadar の管理者特権が必要です。「**Watson** で検索」アイコンをクリックします。(V2.7.0 以降で使用可能。)
- ユーザーに対する調査を開始するには、「調査の開始」  アイコンをクリックします。調査が完了したら、「調査の終了」アイコンをクリックします。(V2.7.0 以降で使用可能。)
- 監視リストにユーザーを追加する、または監視リストを作成するには、「監視リスト」  アイコンをクリックします。

「拡張アクション」リストには、以下のアクションが含まれています。

カスタム・アラートの追加	ユーザー名別に表示されるカスタム・アラートを設定できます。「カスタム・アラートの追加」をクリックし、アラート・メッセージを入力し、「設定 **(Set)**」をクリックします。選択したユーザーに関するカスタム・アラートを削除するには、「カスタム・アラートの削除」をクリックします。
ホワイトリストに追加	QRadar の管理者特権が必要です。選択したユーザーをホワイトリストに追加して、そのユーザーがリスク・スコアやオフェンスを生成しないようにします。選択したユーザーをホワイトリストから削除するには、「ホワイトリストに追加済み」をクリックします。ホワイトリストに追加したユーザーの完全なリストを表示するには、 41 ページの『信頼できるユーザーのホワイトリストの参照』を参照してください。

ユーザーの **GDPR** 準拠レポートの生成	ユーザーの一般データ保護規則 (GDPR) 準拠レポートを生成できます。 **重要:** 「ユーザーのトラッキングの削除および停止」をクリックする前にレポートを生成します。
ユーザーのトラッキングの削除および停止	QRadar の管理者特権が必要です。一般データ保護規則 (GDPR) に準拠するには、「ユーザーのトラッキングの削除および停止」をクリックします。ユーザーの追跡を完全に削除および停止するには、「はい」を選択します。ユーザーの追跡を再度開始するには、リファレンス・セット「**UBA : 追跡されないユーザー (UBA : Users Not Tracked)**」からユーザーの別名を削除します。ユーザーの別名をすべて表示するには、ユーザーを削除する前に GDPR レポートをダウンロードします。
常に **Machine Learning** で追跡	QRadar の管理者特権が必要です。「常に **Machine Learning** で追跡」をクリックして、ユーザーを 「*UBA: ML 常に追跡される監視リスト (UBA: ML Always Tracked Watchlist)*」リファレンス・セットに追加できます。ユーザーをリファレンス・セットに追加することにより、そのユーザーが機械学習モデルに含められる可能性が最も高くなります。UBA のリファレンス・セットについて詳しくは、 49 ページの『リファレンス・セット』を参照してください。選択したユーザーをリファレンス・セットから削除するには、「**Machine Learning** で追跡」 をクリックします。 **注:** V2.8.0 以降で Machine Learning がインストール済みであり、QRadar 管理者特権がある場合にのみ使用できます。

選択されたユーザーに関して、以下の情報を見ることができます。

全体のリスク・スコア	「全体のリスク・スコア」には、ユーザーのリスク・トレンドが表示されます。
タイムライン	タイムライン・グラフには、リスクの高いイベントとユーザー・イベントが表示されます。リスクの高いイベントとは、リスク・スコアを上げる要因となるリスク・イベントです。ユーザー・イベントとは、リスクのないイベントです。Y 軸はイベント数、X 軸は時間です。タイムライン上の任意のアクティビティーをクリックすると、ユーザーのアクティビティーに関連付けられたサポート・ログ・イベントをリストするイベント・ビューアー・ペインを開くことができます。イベントをクリックすると、Syslog イベントやペイロード情報などの詳細が表示されます。 • V2.8.0 以前では、「リスクのあるアクティビティーのタイムライン」セクションで「アクティビティーでグループ化」または「時間でグループ化」をクリックすると、ユーザー・アクティビティーのリストが表示され、タイムライン上の任意の列を基準としてフィルタリングや検索を実行できるようになります。 • V3.0.0 以降では、タイムラインのアクティビティーはセッションおよび日数ごとにグループ化されます。セッションは、「**UBA** の設定」ページの「アプリケーション設定」セクションで定義します。色によってセッションの全体的なリスクの高さが示されます。日付範囲 (1 日から 14 日) を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 • 3.1.0 以降では、「メトリック設定」アイコンをクリックして、タイムラインに関して表示されるメトリック設定をカスタマイズできます。表示するカテゴリーの追加や削除が可能です。「メトリック設定」画面の「サンプル・メトリック」セクションに表示されるデータは実際の値を表しているわけではありません。 **注:** 「リスクのあるイベント」と「ユース・ケース」には、「リスクのあるイベント」が特定のユース・ケースに関するイベントの総数である場合、同じデータが表示されます。「URL カテゴリー」と「URL」には、「URL」が特定の URL カテゴリーに関するイベントの総数である場合、同じデータが表示されます。「イベント ID」と「イベント」には、「イベント」が特定のイベント ID に関するイベントの総数である場合、同じデータが表示されます。

最新のオフェンス	ユーザー名が選択したユーザーの別名のいずれかに一致するユーザー・タイプ・オフェンスを表示します。最新の 5 件のオフェンスが表示されます。QRadar で「オフェンス」タブを開くには、オフェンスをクリックします。
リスク・カテゴリーの明細	選択したユーザーの過去 1 時間のリスク・カテゴリーを表示します。
メモの追加	「追加」アイコン  をクリックして、選択したユーザーのメモを追加します。メモは、30 日間の保存期間が経過すると自動的に削除されます。 **ヒント:** メモを無期限に保存するには、「フラグ **(Flag)**」アイコンをクリックしてメモに重要のマークを付けます。

Machine Learning アプリがインストールされており、かつ指定された分析が有効になっている場合は、「ユーザーの詳細」ページに以下のグラフが表示されます。詳しくは、 210 ページの『Machine Learning Analytics を使用した UBA ダッシュボード』を参照してください。

合計アクティビティー	ユーザー・アクティビティーの実際の量と学習済みの量が終日にわたって時間でグループ化されて表示されます。
ユーザー・アクティビティー (カテゴリー別)	ユーザー・アクティビティーの実際の行動パターンと予期される行動パターンが上位カテゴリー別に表示されます。
リスク状況	ユーザーのリスク・スコアが予期されるリスク・スコア・パターンから逸脱している場合に表示されます。
異常なアウトバウンド転送の試行	各ユーザーのアウトバウンド・トラフィック使用量を表示し、異常な動作についてアラートを出します。この分析のグラフは、デフォルトでは有効になっていないことに注意してください。「異常なアウトバウンド転送の試行」分析は、Machine Learning アプリがインストールされ、分析が有効であり、かつ「機械学習の設定」で「ユーザーの詳細ページにグラフを表示」が選択されている場合にのみダッシュボードに表示されます。V2.8.0 以降で使用可能です。
外部ドメインへの異常ボリューム・データ	各ユーザーの外部ドメインのデータ使用量を表示し、異常な動作に対するアラートを表示します。「外部ドメインへの異常ボリューム・データ」分析は、Machine Learning アプリがインストールされ、分析が有効であり、かつ「機械学習の設定」で「ユーザーの詳細ページにグラフを表示」が選択されている場合にのみダッシュボードに表示されます。V3.0.0 以降で使用可能です。
アクティビティーの分布	機械学習によってモニターされているすべてのユーザーの動的な振る舞いの集合体を表示します。V2.2.0 以降で使用可能です。
学習ピア・グループ	ユーザーが属すると予期される推定ピア・グループから、そのユーザーがどれほど逸脱しているかを表示します。V2.2.0 以降で使用可能です。
定義済みピア・グループ	ユーザーのイベント・アクティビティーが定義済みのピア・グループからどの程度逸脱しているかを示します。V2.6.0 以降で使用可能です。

メインのダッシュボードに戻るには、「ダッシュボード」をクリックします。

関連概念:

210 ページの『Machine Learning Analytics を使用した UBA ダッシュボード』
Machine Learning Analytics を使用した IBM QRadar User Behavior Analytics (UBA) アプリには、Machine Learning Analytics の状況と、選択されたユーザーの追加の詳細情報が含まれます。

43 ページの『休止アカウント』
休止アカウント、アクティブ・アカウント、またはまったく未使用のアカウントを持つ、システム内のユーザーを表示できます。

関連タスク:

39 ページの『監視リストの作成』
新規監視リストまたは既存の監視リストにユーザーを追加できます。

41 ページの『信頼できるユーザーのホワイトリストの参照』
「リファレンス・セット管理」リストで、ホワイトリストに登録されている信頼できるユーザーのリストを確認できます。

43 ページの『信頼できるログ・ソース・グループへのログ・ソースの追加』
UBA アプリで特定のログ・ソースをモニターおよび報告しない場合、それらのログ・ソースを「**UBA : Trusted Log Source Group**」に追加できます。このグループにログ・ソースを追加すると、UBA アプリはそれらのログ・ソースのモニターを停止します。

193 ページの『Machine Learning Analytics アプリのインストール』
Extension Manager から UBA アプリをインストールした後に、Machine Learning Analytics アプリをインストールします。

『QRadar Advisor with Watson 内でのユーザーの調査』
User Behavior Analytics (UBA) アプリからユーザーを選択して、調査のために QRadar Advisor with Watson に送信できます。

QRadar Advisor with Watson 内でのユーザーの調査

User Behavior Analytics (UBA) アプリからユーザーを選択して、調査のために QRadar Advisor with Watson に送信できます。

始める前に

- User Behavior Analytics (UBA) アプリ V2.7.0 以降がインストールされ、ユーザー・データを指定して構成されている必要があります。
- 管理者特権が必要です。
- QRadar Advisor with Watson V1.13.0 以降がインストールされている必要があります。

詳しくは、https://developer.ibm.com/qradar/advisorを参照してください。

このタスクについて

注**:** この機能は、User Behavior Analytics V2.7.0 以降および QRadar Advisor with Watson V1.13.0 以降でのみ使用可能です。

手順

1. 「ユーザー分析」タブをクリックして UBA ダッシュボードを開きます。
2. ユーザーを選択するか、ユーザーを検索すると、「ユーザーの詳細」ページが開きます。
3. 「**Watson** で検索」アイコンをクリックします。 アイコンの回転が停止したら、QRadar Advisor with Watson アプリ内で結果を確認できます。
4. 「**Watson**」タブから、「Incident Overview」ページで、ユーザー調査を選択します。ユーザー調査は、「**UBA** から開始された調査 **(Investigation initiated from UBA)**」  アイコン付きで表示されます。

User Behavior Analytics アプリのインストール前提条件

User Behavior Analytics (UBA) アプリをインストールする前に、要件を満たしていることを確認してください。

- IBM Security QRadar V7.2.8 以降がインストール済みであることを確認します。

  最適なエクスペリエンスを得るには、QRadar システムを以下のバージョンにアップグレードしてください。

  – QRadar 7.2.8 パッチ 13 (7.2.8.20180529210357) 以降
  – QRadar 7.3.1 パッチ 6 (7.3.1.20180912181210) 以降
- IBM App Exchange からのコンテンツ・パックのインストール
- User Behavior Analytics (UBA) アプリ用の IBM Sense DSM を追加します。

コンテンツの依存関係

他のアプリから UBA にイベントをフィードするために、いくつかのルールが設計されています。これらのルールを正しく機能させるために、他のアプリ用のコンテンツをインストールする必要があります。

UBA コンテンツおよび必須アプリについて詳しくは、以下の表を参照してください。

UBA コンテンツ	必須アプリ
144 ページの『QRadar DNS Analyzer』	IBM QRadar DNS Analyzer
UBA QRadar Network Insights	QRadar Network Insights Content v7.2.8 QRadar Network Insights Content for V7.3.0+
スキャン行為	IBM Security Reconnaissance Content
システム・モニター (Sysmon)	IBM QRadar Content for Sysmon

注**:** これらのルールを編集すると、予期したとおりに機能しない場合があります。

IBM Sense DSM の手動インストール

User Behavior Analytics (UBA) アプリでは、IBM Sense DSM を使用して、ユーザーのリスク・スコアおよびオフェンスを QRadar に追加します。DSM は、自動更新を通じてインストールするか、QRadar にアップロードしてから手動でインストールすることができます。

注**:** システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

制約事項**:** デバイス・サポート・モジュール (DSM) のアンインストールは、QRadar ではサポートされていません。

1. DSM RPM ファイルを IBM サポート Web サイトからダウンロードします。
   - QRadar V7.2.8 の場合: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
   - QRadar V7.3.1 以降の場合: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`
2. RPM ファイルを QRadar コンソールにコピーします。
3. SSH を使用して QRadar ホストに root ユーザーとしてログインします。
4. ダウンロードしたファイルが格納されているディレクトリーに移動します。
5. 以下のコマンドを入力します。

```
rpm -Uvh <rpm_filename>
```

6. 「管理」設定から「変更のデプロイ」をクリックします。
7. 「管理」設定から、「拡張」 > 「**Web** サービスの再始動 **(Restart Web Services)**」を選択します。

UBA アプリでサポートされるブラウザー

IBM Security QRadar 製品の機能が正しく動作するためには、サポート対象の Web ブラウザーを使用する必要があります。

以下の表に、サポートされる Web ブラウザーのバージョンをリストします。

Web ブラウザー	サポートされるバージョン
Mozilla Firefox	45.2 延長サポート版
Google Chrome	最新版

注**:** UBA を最大限に活用するには、以下のいずれかを行ってください。

- ブラウザーのポップアップ・ブロッカーを無効にする
- QRadar コンソールの IP アドレスから送信されるポップアップに対する例外を許可するようにブラウザーを構成する

UBA アプリに関連するログ・ソース・タイプ

User Behavior Analytics (UBA) アプリおよび ML アプリは、特定のログ・ソースからイベントを受け入れて分析できます。

基本的に、UBA アプリおよび ML アプリでは、ユーザー名を提供するログ・ソースが必要です。UBA の場合、ユーザー名が存在しない場合は、「UBA の設定」の「イベント・データまたはフロー・データにユーザー名がない場合、ユーザー名を探してアセットを検索します」チェック・ボックスを有効にして、UBA がアセット・テーブルからユーザーを検索できるようにします。ユーザーが判別できない場合、UBA はイベントを処理しません。

特定のユース・ケースおよび対応するログ・ソース・タイプについて詳しくは、 51 ページの『7, UBA アプリのルールおよびチューニング』を参照してください。

関連タスク:

30 ページの『UBA 設定の構成』
IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、UBA アプリケーション設定を構成する必要があります。

2 インストールとアンインストール

User Behavior Analytics アプリのインストール

IBM QRadar 拡張の管理ツールを使用して、アプリケーション・アーカイブを直接 QRadar コンソールにアップロードおよびインストールします。

始める前に

16 ページの『User Behavior Analytics アプリのインストール前提条件』を完了します。

重要: アプリをインストールする前に、IBM QRadar が最小メモリー (RAM) 要件を満たしていることを確認してください。UBA アプリには、メモリーのアプリケーション・プールに 1 GB の空きメモリーが必要です。アプリケーション・プールに十分な空きメモリーがない場合、UBA アプリのインストールは失敗します。

このタスクについて

インストールは V2.8.0 から変更されました。オフェンスのトリガーのルールを含む UBA 固有のコンテンツ・パッケージは、別個の拡張機能としてインストールされるようになりました。コンテンツ・パッケージはデフォルトでインストールされます。UBA でオフェンスをトリガーするための独自のカスタム・ルールを作成することを選択した場合は、UBA 設定を構成するときに、「コンテンツ・パッケージのインストールおよびアップグレード」設定を変更できます。

重要: アプリをインストールした後、以下を行う必要があります。

- 索引を有効化します。
- すべての構成をデプロイします。
- ブラウザーのキャッシュをクリアし、ブラウザー・ウィンドウを最新表示します。
- 「ユーザー分析」タブにアクセスして表示する必要があるユーザーの権限をセットアップします。このアプリへのアクセス権限が必要な各ユーザー・ロールに対して、以下の権限を割り当てる必要があります。
  - ユーザー分析
  - オフェンス
  - ログ・アクティビティー

IBM Security App Exchange からアプリケーションをダウンロードしたら、IBM QRadar 拡張の管理ツールを使用して、QRadar コンソールでアプリケーションをインストールします。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「システム構成」 > 「拡張の管理」をクリックします。

3. 「拡張の管理」ウィンドウで「追加」をクリックし、コンソールにアップロードする UBA アプリのアーカイブを選択します。
4. 「即時にインストール」チェック・ボックスを選択し、「追加」をクリックします。
5. プロンプトで、「上書き」を選択します。

   重要**:** アプリがアクティブになるまでに数分かかる場合があります。UBA アプリがインストールされた後、コンテンツ・パッケージはバックグラウンドでインストールされます。アプリのインストール直後は、コンテンツが QRadar に表示されない場合があります。
6. 「管理」設定から「システム構成」 > 「索引管理」をクリックし、以下の索引を有効にします。
   - 上位カテゴリー
   - 下位カテゴリー
   - ユーザー名
   - senseValue
7. 「管理」設定から、「拡張」 > 「すべての構成のデプロイ」をクリックします。

   注**:** UBA のインストールと構成が完了すると、以下のコンテンツ・パッケージがインストールされます。
   - User Behavior Analytics Access and Authentication コンテンツ
   - User Behavior Analytics Accounts and Privileges コンテンツ
   - User Behavior Analytics Browsing Behavior コンテンツ
   - User Behavior Analytics DNS Analyzer コンテンツ
   - User Behavior Analytics Endpoint コンテンツ
   - User Behavior Analytics Exfiltration コンテンツ
   - User Behavior Analytics Geography コンテンツ
   - User Behavior Analytics Network Traffic and Attacks コンテンツ
   - User Behavior Analytics QRadar Network Insights コンテンツ
   - User Behavior Analytics Reconnaissance コンテンツ
   - User Behavior Analytics Sysmon コンテンツ
   - User Behavior Analytics Threat Intelligence コンテンツ

次のタスク

- インストールが完了したら、アプリケーションを使用する前に、ブラウザー・キャッシュをクリアし、ブラウザー・ウィンドウを最新表示します。
- UBA アプリのユーザー・ロールについて、権限の管理を行います。

関連タスク:

47 ページの『パフォーマンス改善のための索引の有効化』
IBM QRadar User Behavior Analytics (UBA) アプリのパフォーマンスを向上させるために、IBM QRadar で索引を有効にします。

39 ページの『QRadar UBA アプリの権限の管理』
管理者は、IBM QRadar の「ユーザー・ロール管理」機能を使用して、ユーザー・アカウントを構成および管理します。管理者は、QRadar UBA アプリの使用を許可されている各ユーザー・ロールに対して、「ユーザー分析」権限、「オフェンス」権限、および「ログ・アクティビティー」権限を有効にする必要があります。

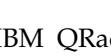
UBA アプリのアンインストール

IBM QRadar 拡張の管理ツールを使用して、QRadar コンソールからアプリケーションをアンインストールします。

始める前に

Machine Learning Analytics (ML) アプリがインストール済みである場合、「拡張の管理」ウィンドウから UBA アプリをアンインストールする前に、「機械学習の設定」ページから ML アプリをアンインストールする必要があります。UBA アプリをアンインストールする前に ML アプリを削除しない場合、対話式 API 資料インターフェースから ML アプリを削除する必要があります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「拡張の管理」をクリックします。
3. 「拡張の管理」ウィンドウの「インストール済み」タブで、User Behavior Analytics アプリを選択して「アンインストール」をクリックします。

   アプリケーションをアンインストールすると、そのアプリケーションはシステムから削除されます。アプリケーションを再インストールするには、再度追加する必要があります。
4. V2.8.0 以降では、UBA アプリを構成するときに、以下のコンテンツ・パッケージがインストールされます。アプリを完全に削除するには、各コンテンツ・パッケージをアンインストールする必要があります
   - User Behavior Analytics Access and Authentication コンテンツ
   - User Behavior Analytics Accounts and Privileges コンテンツ
   - User Behavior Analytics Browsing Behavior コンテンツ
   - User Behavior Analytics DNS Analyzer コンテンツ
   - User Behavior Analytics Endpoint コンテンツ
   - User Behavior Analytics Exfiltration コンテンツ
   - User Behavior Analytics Geography コンテンツ
   - User Behavior Analytics Network Traffic and Attacks コンテンツ
   - User Behavior Analytics QRadar Network Insights コンテンツ
   - User Behavior Analytics Reconnaissance コンテンツ
   - User Behavior Analytics Sysmon コンテンツ
   - User Behavior Analytics Threat Intelligence コンテンツ

3 アップグレード

User Behavior Analytics アプリのアップグレード

IBM QRadar 拡張の管理ツールを使用して、アプリケーションをアップグレードします。

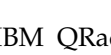
始める前に

重要: V2.8.0 からはメモリー所要量が増加しました。アプリをアップグレードする前に、IBM QRadar が最小メモリー (RAM) 要件を満たしていることを確認してください。UBA アプリには、メモリーのアプリケーション・プールに 1 GB の空きメモリーが必要です。アプリケーション・プールに十分な空きメモリーがない場合、UBA アプリのアップグレードは失敗します。

最適なエクスペリエンスを得るには、QRadar システムを以下のバージョンにアップグレードしてください。

- QRadar 7.2.8 パッチ 13 (7.2.8.20180529210357) 以降
- QRadar 7.3.0 パッチ 7 (7.3.0.20171205025101) 以降
- QRadar 7.3.1 パッチ 6 (7.3.1.20180912181210) 以降

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「拡張の管理」をクリックします。
3. 「拡張の管理」ウィンドウで「追加」をクリックし、コンソールにアップロードする UBA アプリのアーカイブを選択します。
4. プロンプトで、「上書き」を選択します。すべての既存の UBA アプリのデータはそのまま維持されます。

   重要: アプリがアクティブになるまでに数分かかる場合があります。UBA アプリがアップグレードされた後、コンテンツ・パッケージはバックグラウンドでアップグレードされます。アプリのアップグレード直後は、コンテンツが QRadar に表示されない場合があります。

   注: UBA のアップグレードと構成が完了すると、以下のコンテンツ・パッケージがアップグレードされます。
   - User Behavior Analytics Access and Authentication コンテンツ
   - User Behavior Analytics Accounts and Privileges コンテンツ
   - User Behavior Analytics Browsing Behavior コンテンツ
   - User Behavior Analytics DNS Analyzer コンテンツ
   - User Behavior Analytics Endpoint コンテンツ
   - User Behavior Analytics Exfiltration コンテンツ
   - User Behavior Analytics Geography コンテンツ

- User Behavior Analytics Network Traffic and Attacks コンテンツ
- User Behavior Analytics QRadar Network Insights コンテンツ
- User Behavior Analytics Reconnaissance コンテンツ
- User Behavior Analytics Sysmon コンテンツ
- User Behavior Analytics Threat Intelligence コンテンツ

次のタスク

アップグレードが完了したら、アプリケーションを使用する前に、ブラウザー・キャッシュをクリアし、ブラウザー・ウィンドウを最新表示します。

4 構成

User Behavior Analytics アプリの構成

IBM QRadar User Behavior Analytics (UBA) アプリを使用できるようにするには、追加設定を構成する必要があります。

UBA アプリをインストールすると、IBM QRadar Reference Data Import LDAP (LDAP) アプリもインストールされます。この LDAP アプリを使用することを選択する場合、UBA アプリをセットアップする前に LDAP アプリを構成する必要があります。UBA アプリが使用するデータは、LDAP 照会により取得されます。LDAP 照会は、UBA アプリにデータを設定するために使用するユーザーのリストを取得します。

UBA アプリと LDAP アプリの両方に、別個の許可トークンが必要です。許可トークンは、各アプリを構成するときに作成できます。

以下のセットアップ手順を実行します。

- Reference Data Import LDAP アプリを構成します (LDAP を使用する場合)
- UBA アプリの UBA 設定を構成します

Reference Data Import LDAP アプリの構成

IBM® QRadar® User Behavior Analytics (UBA) アプリケーションをインストールすると、Reference Data Import - LDAP アプリケーションもインストールされます。LDAP アプリケーションを使用すると、ユーザー・データを LDAP/AD サーバーまたは CSV ファイルから QRadar リファレンス・テーブルにインポートできます。インポートされたリファレンス・テーブルは、UBA アプリケーションで利用され、QRadar の検索やルールに使用されることもあります。

始める前に

重要: 以前にスタンドアロンの Reference Data Import LDAP アプリをインストールしている場合、UBA アプリのインストール時に置換されます。更新されたバージョンの Reference Data Import LDAP アプリに構成が追加されます。

このタスクについて

注: リファレンス・テーブル名および属性に設定したカスタム別名 (ある場合) を必ず記録してください。UBA アプリをセットアップする際に、Reference Data Import LDAP アプリで作成したリファレンス・テーブルを選択します。

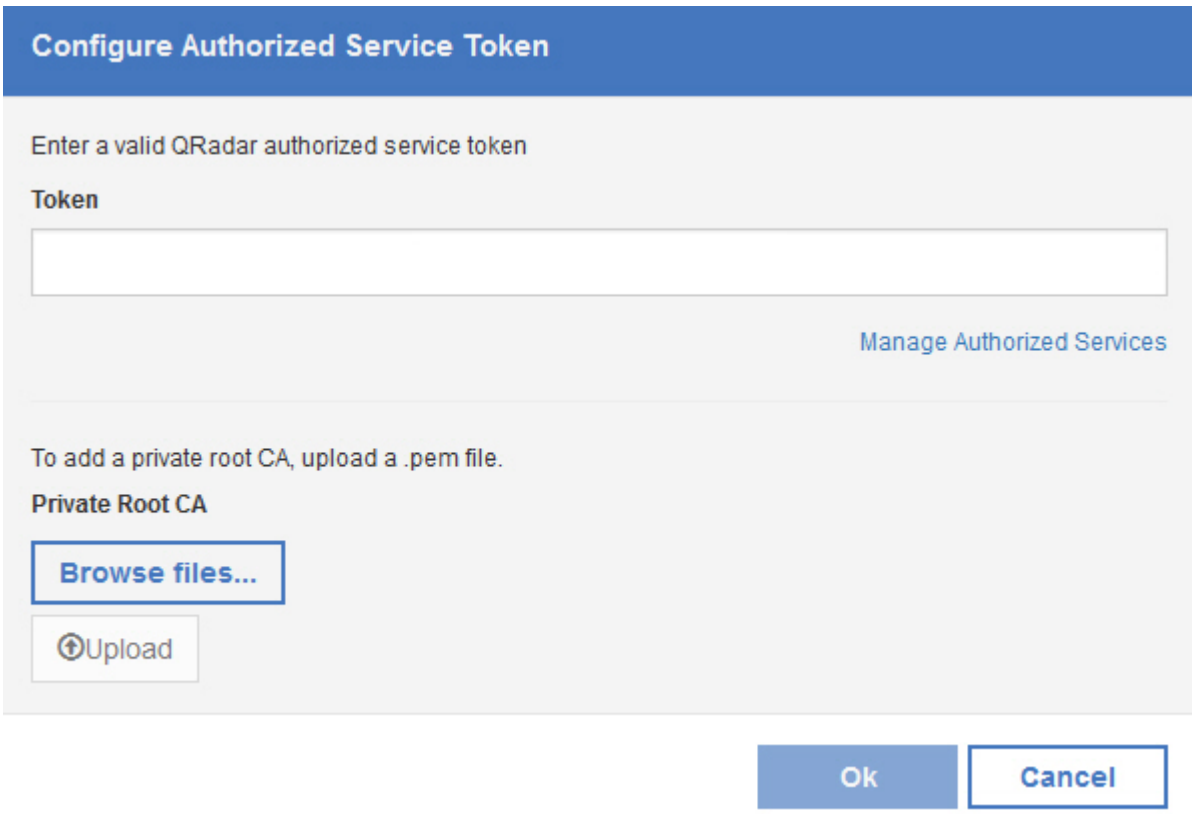
Reference Data Import LDAP アプリについて詳しくは、IBM Knowledge Center の次のセクションを参照してください。http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.apps.doc/c_Qapps_LDAP_intro.html

手順

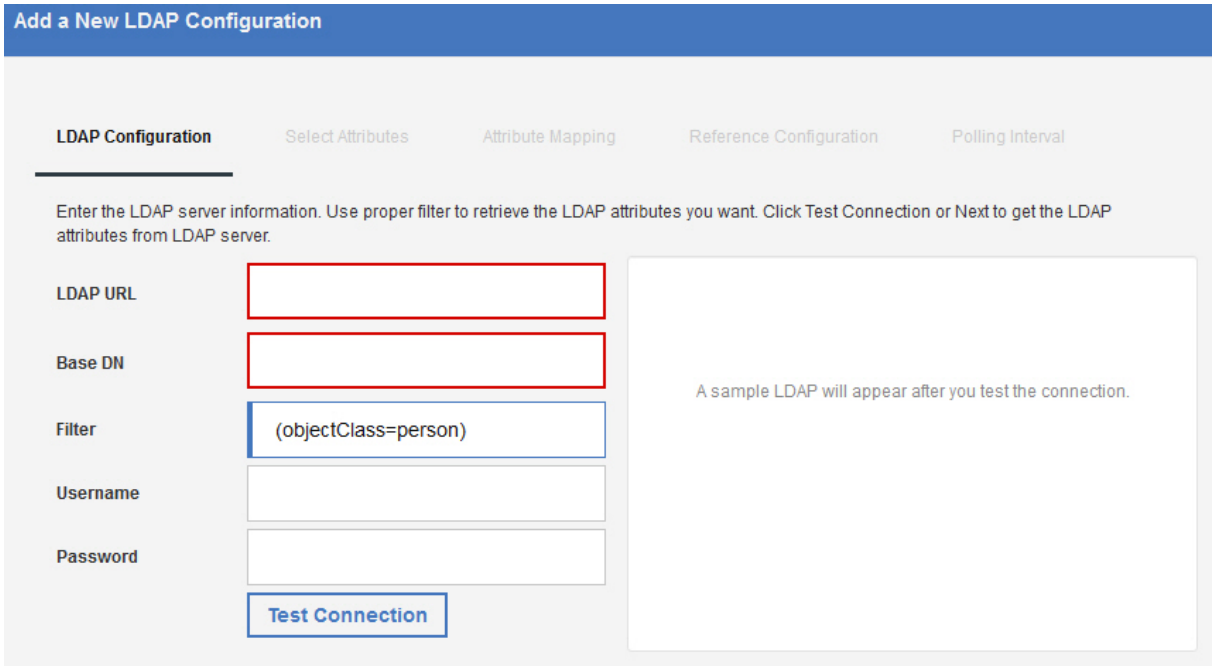
1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。

- IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。

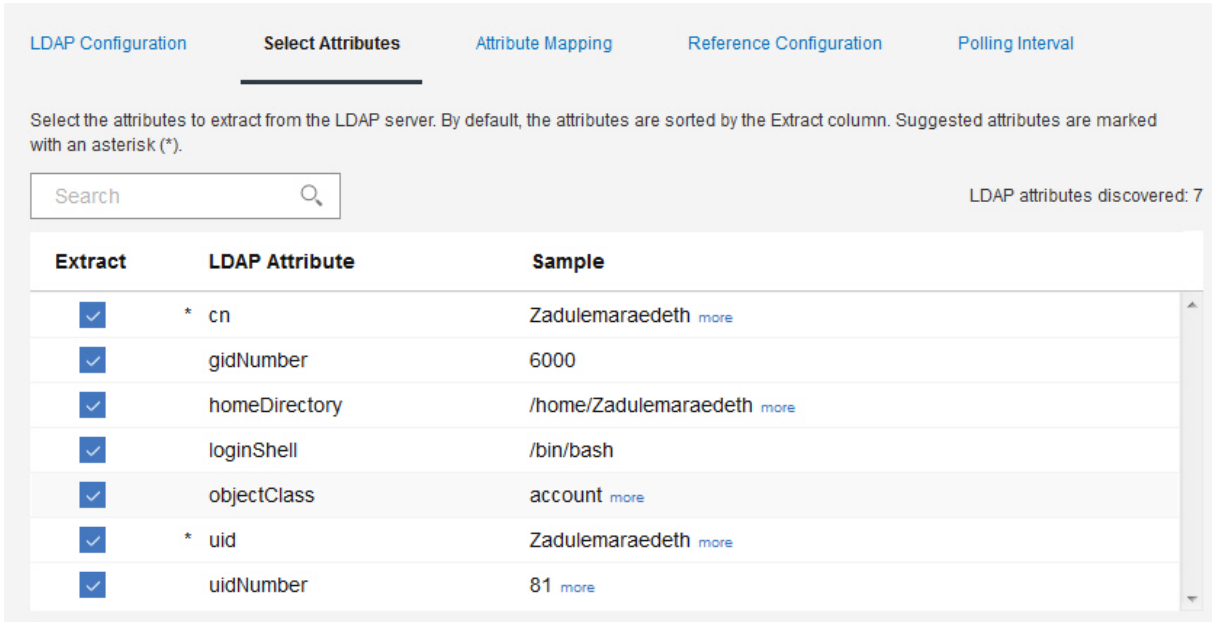
2. 「**Reference Data Import - LDAP**」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「参照データのインポート **- LDAP**」 > 「参照データのインポート **- LDAP**」をクリックします。
3. 「構成」」をクリックして、LDAP の許可サービス・トークンを作成します。「許可サービス・トークンの構成」ボックスが開きます。
   a. 「許可サービスの管理」リンクをクリックし、「許可サービスの追加」をクリックします。
   b. 「サービス名」フィールドに `LDAP` と入力します。これは、LDAP アプリケーションからの API 要求の実行に使用されるユーザーです。
   c. 「ユーザー・ロール」リストから「管理」ユーザー・ロールを選択します。
   d. 「セキュリティー・プロファイル」リストで、この許可サービスに割り当てるセキュリティー・プロファイルを選択します。セキュリティー・プロファイルは、当該サービスが QRadar ユーザー・インターフェースでアクセスできるネットワークおよびログ・ソースを決定します。
   e. 「有効期限日付」リストで、このサービスが期限切れになる日付を入力または選択します。有効期限日付が不要な場合は、「期限なし」を選択します。
   f. 「サービスの作成」をクリックします。
   g. 作成したサービスを含む行をクリックし、メニュー・バーの「選択したトークン」フィールドからトークン・ストリングを選択してコピーします。
   h. 「許可サービス・トークンの構成」ボックスで、「トークン」フィールドに許可サービス・トークン・ストリングを貼り付けます。
4. オプション: プライベート・ルート認証局ファイルを追加するには、「ファイルの参照」をクリックし、サポートされるファイルを開き、「オープン」をクリックして「アップロード」をクリックします。サポートされるファイル・タイプは `.pem` です。
5. 「**OK**」をクリックします。



6. 「Reference Data Import (LDAP)」アプリのメイン・ウィンドウで、「インポートの追加」をクリックします。「新しい LDAP 構成の追加」ダイアログ・ボックスが開きます。
7. 「**LDAP** 構成」タブで、LDAP サーバーの接続情報を追加します。「フィルター」フィールドには、Active Directory の属性が自動的に取り込まれます。
   a. `ldap://` または `ldaps://` (TLS の場合) で始まる URL を「**LDAP URL**」フィールドに入力します。
   b. 「基本 **DN**」フィールドに、LDAP ディレクトリー・ツリー内で、サーバーがユーザーの検索を開始すべきポイントを入力します。例えば、LDAP サーバーがドメイン example.com にある場合は、以下を使用できます。`dc=example,dc=com`
   c. 「フィルター」フィールドに、リファレンス・テーブルにインポートされたデータをソートするために使用する 1 つまたは複数の属性を入力します。例: `cn=*; uid=*; sn=*`。以下のデフォルト値は Active Directory で機能します。`(&(sAMAccountName=*)(samAccountType=805306368))`
   d. 「ユーザー名」フィールドに、LDAP サーバーの認証に使用されるユーザー名を入力します。
   e. 「パスワード」フィールドに、LDAP サーバーのパスワードを入力します。
8. 「接続のテスト」または「次へ」をクリックして、IBM QRadar が LDAP サーバーに接続できることを確認します。接続試行が成功した場合は、LDAP サーバーからの情報が「**LDAP** 構成」タブに表示されます。



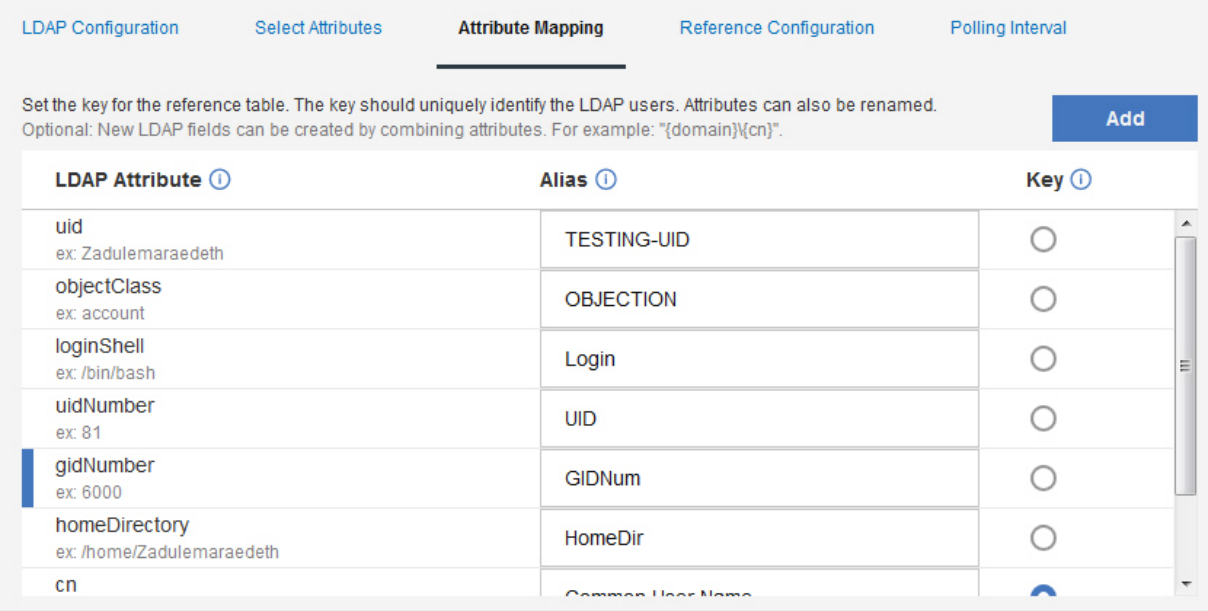
9. 「属性の選択 **(Select Attributes)**」タブで、LDAP サーバーから抽出する属性を選択します。以下のデフォルト値は Active Directory で機能します。
`userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`



10. オプション: 「属性マッピング」タブで、リファレンス・テーブルのキーを設定します。

ヒント: 新しい LDAP フィールドを作成するには、「追加」をクリックし、2 つの属性を結合します。例えば、次の構文を使用できます。`"Last: {ln}, First: {fn}"`

ヒント: LDAP データを複数のソースから同一のリファレンス・テーブルにマージする場合は、カスタム別名を使用して、ソースは異なるが同じ名前を持つ LDAP 属性を区別できます。



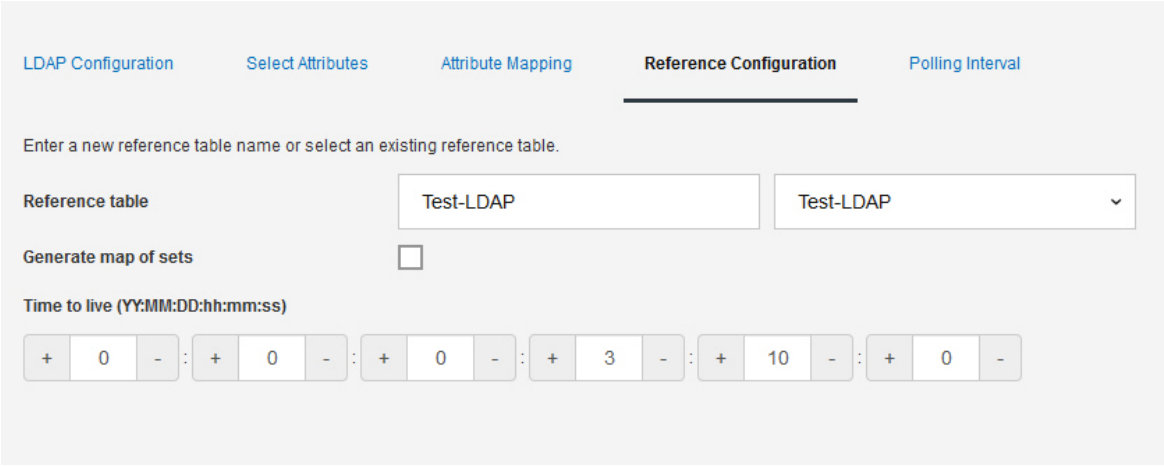
11. 「リファレンス構成」タブで、LDAP データを追加する新しいマップのリファレンス・マップを作成するか、既存のマップのリファレンス・マップを指定します。

    a. 「リファレンス・テーブル」フィールドに、新しいリファレンス・テーブルの名前を入力します。あるいは、LDAP データを追加する既存のリファレンス・テーブルの名前をリストから追加します。

    b. 「セットのマップの生成」チェック・ボックスは、デフォルトで無効にされています。このチェック・ボックスを有効にすると、データがリファレンス・セット・フォーマットで送信されるため、QRadar の検索が改善されますが、パフォーマンスに影響する可能性があります。

    c. 「存続時間」セクションに、マップのリファレンス・マップにデータを保持する時間を定義します。デフォルトでは、追加したデータに有効期限はありません。存続時間の期間を超えると、*ReferenceDataExpiry* イベントがトリガーされます。

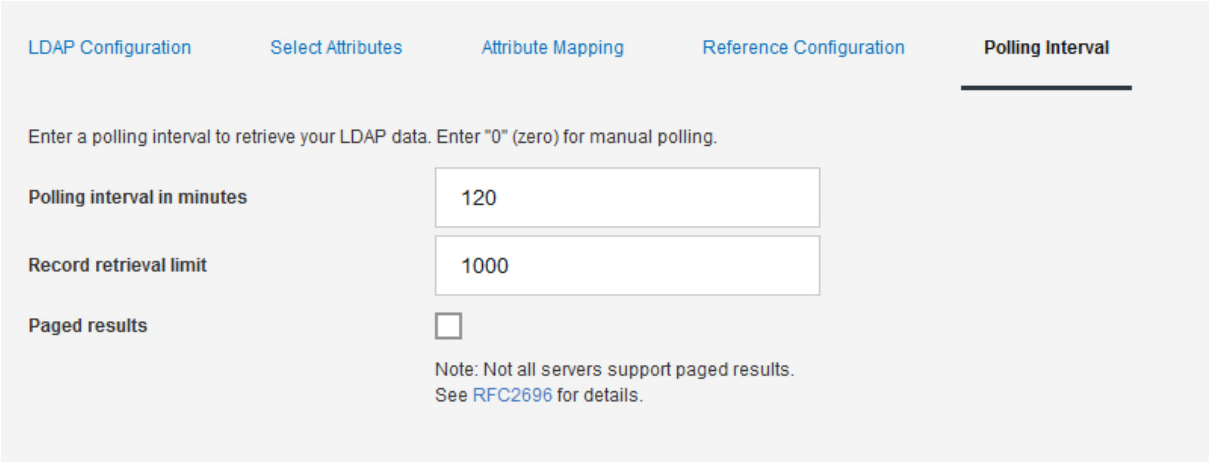
    注: 既存のマップのリファレンス・マップにデータを追加する場合、アプリケーションは元の存続時間パラメーターを使用します。これらのパラメーターは、「リファレンス構成」タブではオーバーライドできません。



12. 「ポーリング **(Polling)**」タブで、アプリケーションが LDAP サーバーに対してデータのポーリングを行う頻度を定義します。
    a. 「ポーリング間隔 **(分)**」フィールドに、アプリケーションが LDAP サーバーに対してデータのポーリングを行う間隔 (分) を定義します。

       注**:** ポーリング間隔の最小値は 120 です。ポーリング間隔としてゼロを入力することもできます。ポーリング間隔にゼロを入力した場合、フィードに表示されるポーリング・オプションを使用してアプリケーションを手動でポーリングする必要があります。
    b. 「レコード取得制限」フィールドに、ポーリングが返すレコード数の値を入力します。 デフォルトでは、100,000 レコードが返されます。返すことができる最大レコード数は 200,000 です。
    c. オプション: ポーリングごとに LDAP サーバーから返されるレコードの数が制限されないようにするために、「結果のページ分割」チェック・ボックスはデフォルトで選択されています。

       注**:** 結果のページ分割は一部の LDAP サーバーではサポートされていません。



13. 「保存」をクリックします。

UBA 設定の構成

IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、UBA アプリケーション設定を構成する必要があります。

QRadar 設定での許可トークンの構成

IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、「UBA の設定」で UBA 許可トークンを構成する必要があります。

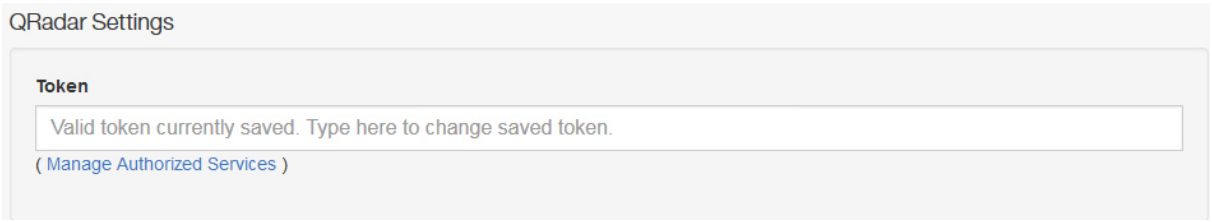
このタスクについて

重要**:** 管理者機能が制限されているため、QRadar on Cloud 管理者は QRadar アプリケーションの許可サービス・トークンを作成できません。QRadar on Cloud ユーザーの許可サービス・トークンの作成については、お客様サポートに依頼してください。

許可トークンを作成するには、以下のステップを実行する必要があります。すべての UBA 設定を構成するまで構成を保存しないでください。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「**UBA** の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
3. 「QRadar 設定」セクションで、「許可サービスの管理」 リンクをクリックします。



4. 「許可サービスの追加」をクリックします。
5. 「サービス名」フィールドに、UBA と入力します。
6. 「ユーザー・ロール」リストから「管理」ユーザー・ロールを選択します。
7. 「セキュリティー・プロファイル」リストで、この許可サービスに割り当てるセキュリティー・プロファイルを選択します。セキュリティー・プロファイルは、当該サービスが QRadar ユーザー・インターフェースでアクセスできるネットワークおよびログ・ソースを決定します。
8. 「有効期限日付」リストで、このサービスが期限切れになる日付を入力または選択します。有効期限日付が不要な場合は、「期限なし」を選択します。
9. 「サービスの作成」をクリックします。
10. 作成した UBA サービスを含む行をクリックし、メニュー・バーの「選択したトークン」フィールドからトークン・ストリングを選択してコピーします。
11. 「QRadar の設定」セクションに戻り、「トークン」フィールドに許可サービス・トークン・ストリングを貼り付けます。

次のタスク

『コンテンツ・パッケージ設定の構成』

コンテンツ・パッケージ設定の構成

IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、コンテンツ・パッケージ設定を構成する必要があります。

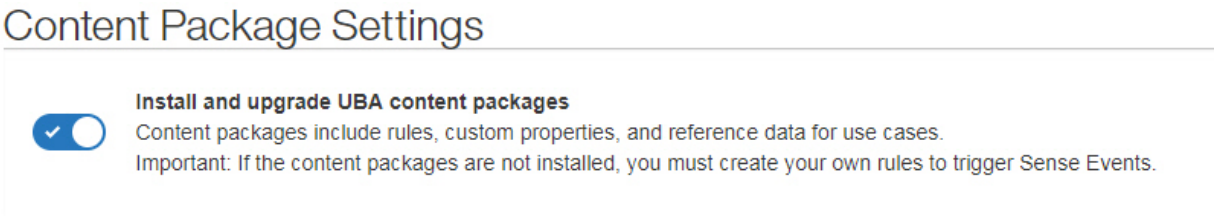
手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。

- IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。

2. 「**UBA** の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
3. 「コンテンツ・パッケージの設定」セクションの「**UBA** コンテンツ・パッケージのインストールおよびアップグレード」チェック・ボックスはデフォルトで有効になっています。UBA コンテンツ・パッケージをインストールしない場合は、チェック・ボックスをクリアして、構成を保存します。UBA コンテンツ・パッケージをインストールしない場合は、イベントを UBA に送信するセンス・イベントをトリガーするための独自のルールを作成する必要があります。

   注: 「**UBA** コンテンツ・パッケージのインストールおよびアップグレード」チェック・ボックスをクリアして構成を保存した後に、「UBA の設定」ページに戻ってチェック・ボックスを選択することに決めた場合、選択後に構成を保存すると、コンテンツがインストールおよびアップグレードされます。



次のタスク

『アプリケーション設定の構成』

アプリケーション設定の構成

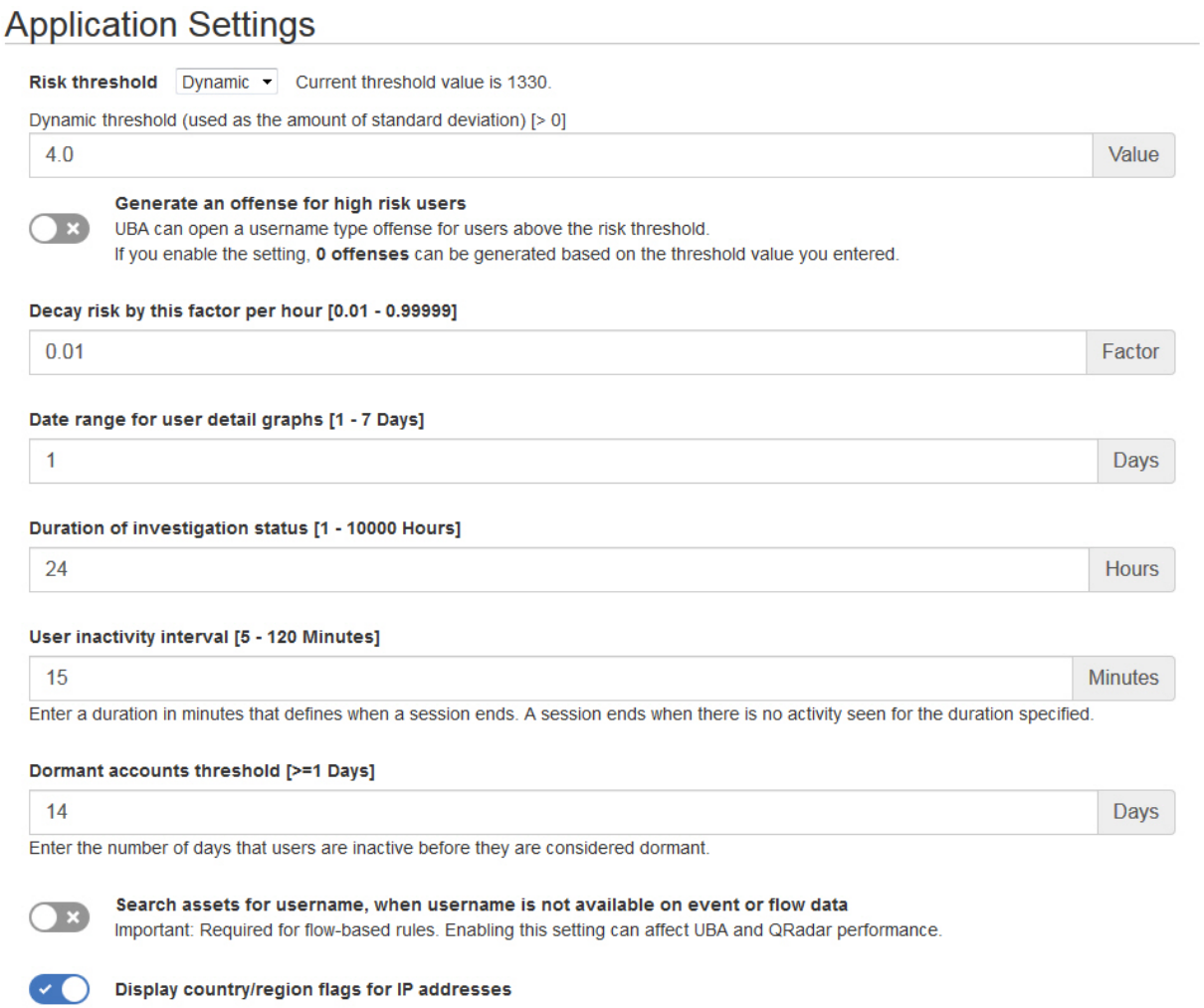
IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、UBA アプリケーション設定を構成する必要があります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「**UBA** の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
3. 「アプリケーション設定」セクションで、以下の設定を構成します。

オプション	説明
リスクしきい値	オフェンスのトリガー基準とするリスク・スコアの値を指定します。ユーザーのリスク・スコアがこの値に達するまで、そのユーザーに対してオフェンスはトリガーされません。リスク・スコア は、UBA ルールによって検出されるすべてのリスク・イベントの合計です。 以下のいずれかのオプションを選択します。 • 動的: デフォルト値は 4.0 です。この値を大きくすると、動的しきい値が大きくなり、結果的にオフェンス数が少なくなります。この設定を少なくとも 1 日間実行するまでは、「高リスク・ユーザーのオフェンスを生成」はオフにしておいてください。動的しきい値は、システム内のリスク・スコアの分布に基づいて 1 時間ごとに更新されます。この設定を有効にするかどうかは、トリガーされる可能性のあるオフェンスの数に基づいて決定できます。詳しくは『ヒント』を参照してください。 **注:** 得られたスコアに十分なばらつきがない場合、リスク・スコアはリスクの最も高いユーザーのスコアの +10 に設定されます。多数のオフェンスが不必要に生成されないように、こうした方法がとられます。 • 静的: デフォルト値は 100,000 です。環境が分析される前にオフェンスがトリガーされないようにするために、デフォルトでは大きな値に設定されています。「高リスク・ユーザーのオフェンスを生成」をオンにすると、リスクしきい値を超えたユーザーのユーザー名タイプのオフェンスをオープンできます。この設定を有効にするかどうかは、トリガーされる可能性のあるオフェンスの数に基づいて決定できます。 **ヒント:** UBA をセットアップし、デフォルト値はそのままにすることを検討してください。この設定を少なくとも 1 日間実行し、どのようなスコアが返されるかを調べます。数日後、ダッシュボードで結果を確認してパターンを判別します。それに基づいて、しきい値を調整できます。例えば、500 秒でこのスコアに達するユーザーが 1 人か 2 人いる一方で、ほとんどのユーザーは 100 秒でこのスコアに達するような場合は、しきい値を 200 か 300 に設定することを検討します。つまり、この環境での「標準」はおよそ 100 であり、これを上回るスコアには注意しなければならない可能性があります。
1 時間ごとのリスク減衰の係数	リスク減衰とは、毎時削減されるリスク・スコアの割合です。デフォルト値は 0.5 です。 **注:** この数値が高いほどリスク・スコアの減衰は速くなり、この数値が低いほどリスク・スコアの減衰は遅くなります。
ユーザーの詳細グラフの日付範囲 **(Date range for user detail graphs)**	「ユーザーの詳細」ページのユーザーの詳細グラフに表示される日付範囲。デフォルト値は 1 です。
調査状況の期間 **(Duration of investigation status)**	調査が完了するまでに割り当てられる時間数 (1 - 10,000)。
ユーザーの非アクティブ間隔	「ユーザーの詳細」ページには、セッションごとにグループ化されたアクティビティーを示すタイムラインが表示されます。「ユーザーの非アクティブ間隔」フィールドに入力された時間の間ユーザーが非アクティブである場合、セッションは終了します。デフォルト値は 15 分です。
休止アカウントのしきい値	ユーザーの非アクティブ期間の日数であり、この期間が過ぎるとそのユーザーは休止と見なされます。デフォルト値は 14 日です。詳しくは、 43 ページの『休止アカウント』を参照してください。(V3.2.0 以降で使用可能。)

オプション	説明
イベント・データまたはフロー・データにユーザー名がない場合、アセットでユーザー名を検索します	アセット・テーブル内でユーザー名を検索する場合は、このチェック・ボックスを選択します。イベント内にユーザーがリストされていない場合、UBA アプリはアセットを使用して IP アドレスに対するユーザーを検索します。 **重要:** この機能を使用すると、UBA アプリおよび QRadar システムでパフォーマンスに関する問題が発生するおそれがあります。 **ヒント:** 照会タイムアウトのしきい値を超えると、アプリからデータが返されなくなります。UBA ダッシュボードにエラー・メッセージが表示された場合は、このチェック・ボックスをクリアして「最新表示」をクリックしてください。
IP アドレスの国/地域フラグの表示 (Display country/region flags for IP addresses)	IP アドレスの国および地域フラグを表示しない場合は、チェック・ボックスをクリアします。



次のタスク

35 ページの『ユーザー・データのインポートおよびユーザー統合の構成』

ユーザー・データのインポートおよびユーザー統合の構成

IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するために、ユーザー・データをリファレンス・テーブルからインポートできます。

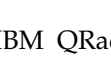
始める前に

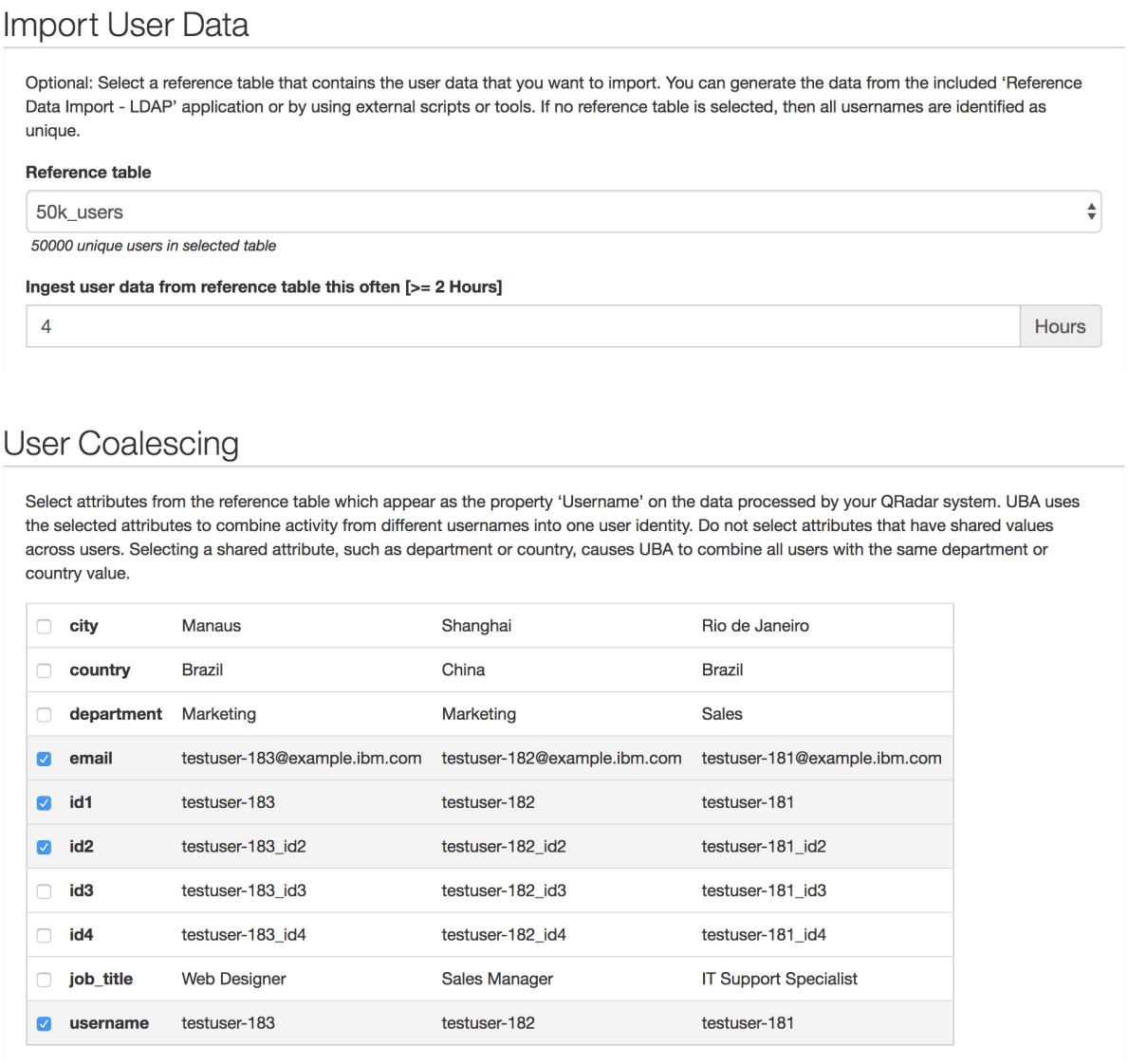
32 ページの『アプリケーション設定の構成』の手順を完了します。

このタスクについて

ユーザー・データのインポートおよびユーザー統合はオプションです。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「**UBA** の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
3. 「ユーザー・データのインポート」セクションで、「リファレンス・テーブル」を選択します。
4. リファレンス・テーブルにデータを取り込む間隔を時間数で入力します。
5. 「ユーザー統合」セクションで、選択したリファレンス・テーブルからプルする属性と、QRadar システムで「ユーザー名」として表示する属性を選択します。これらの ID のリスク・スコアは、プライマリー ID に加算され、プライマリー ID に関連付けられます。ユーザー間で値が共有されている属性は選択しないでください。例えば、同じ部門の複数のユーザーがいる場合、ユーザー名として「部門」は選択しないでください。「部門」や「国」などの共有属性を選択すると、UBA は同じ部門または国の値を持つすべてのユーザーを結合してしまいます。



次のタスク

『表示属性の構成』

表示属性の構成

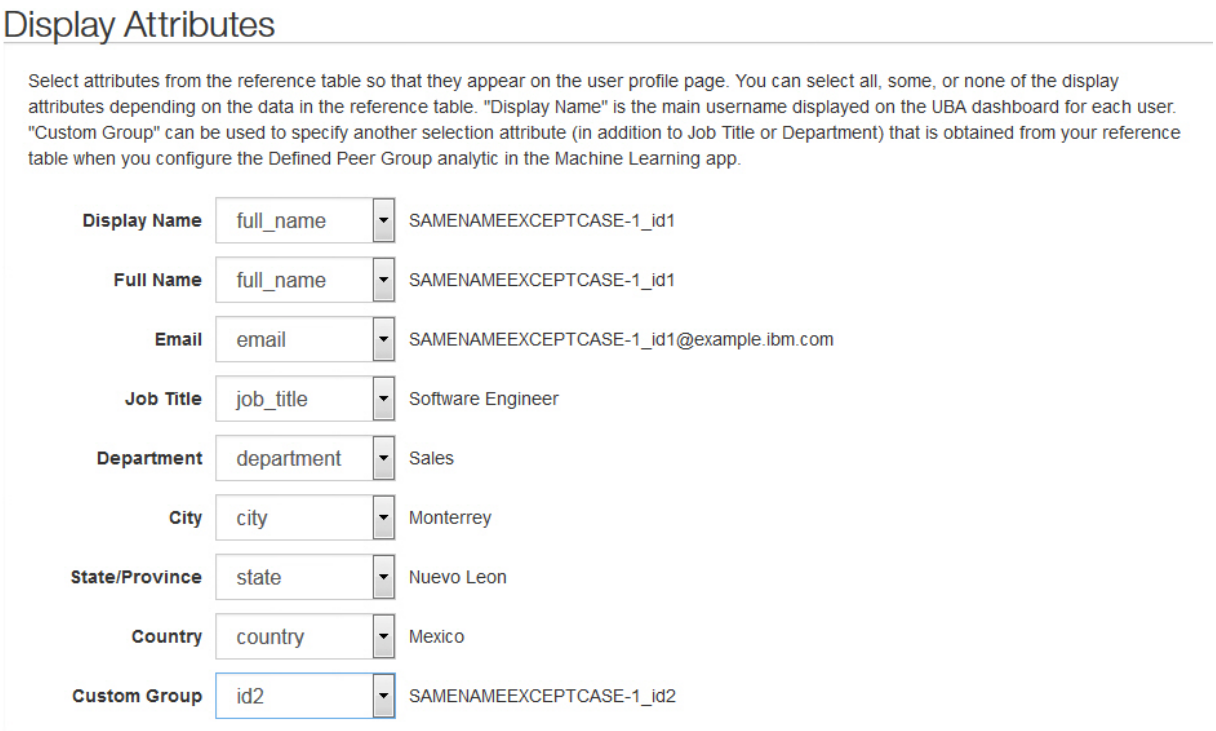
IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するために、「ユーザーの詳細」ページに表示する属性をリファレンス・テーブルから選択できます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「**UBA** の設定」アイコンをクリックします。

- QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。
- QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「**UBA** の設定」をクリックします。

3. 「表示属性」セクションで、「ユーザーの詳細」ページに表示する属性を選択します。



4. 「構成の保存」をクリックします。

5 管理

QRadar UBA アプリの権限の管理

管理者は、IBM QRadar の「ユーザー・ロール管理」機能を使用して、ユーザー・アカウントを構成および管理します。管理者は、QRadar UBA アプリの使用を許可されている各ユーザー・ロールに対して、「ユーザー分析」権限、「オフェンス」権限、および「ログ・アクティビティー」権限を有効にする必要があります。

このタスクについて

QRadar UBA アプリのインストール後、QRadar UBA アプリを使用するユーザーに割り当てられているユーザー・ロールに対して、「ユーザー分析」権限、「オフェンス」権限、および「ログ・アクティビティー」権限を有効にする必要があります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「システム構成」セクションの「ユーザー管理」をクリックし、「ユーザー・ロール」アイコンをクリックします。
3. 既存のユーザー・ロールを選択するか、新しいロールを作成します。
4. 以下のチェック・ボックスを選択してロールに権限を追加します。
   - ユーザー分析
   - オフェンス
   - ログ・アクティビティー
5. 「保存」をクリックします。

監視リストの作成

新規監視リストまたは既存の監視リストにユーザーを追加できます。

このタスクについて

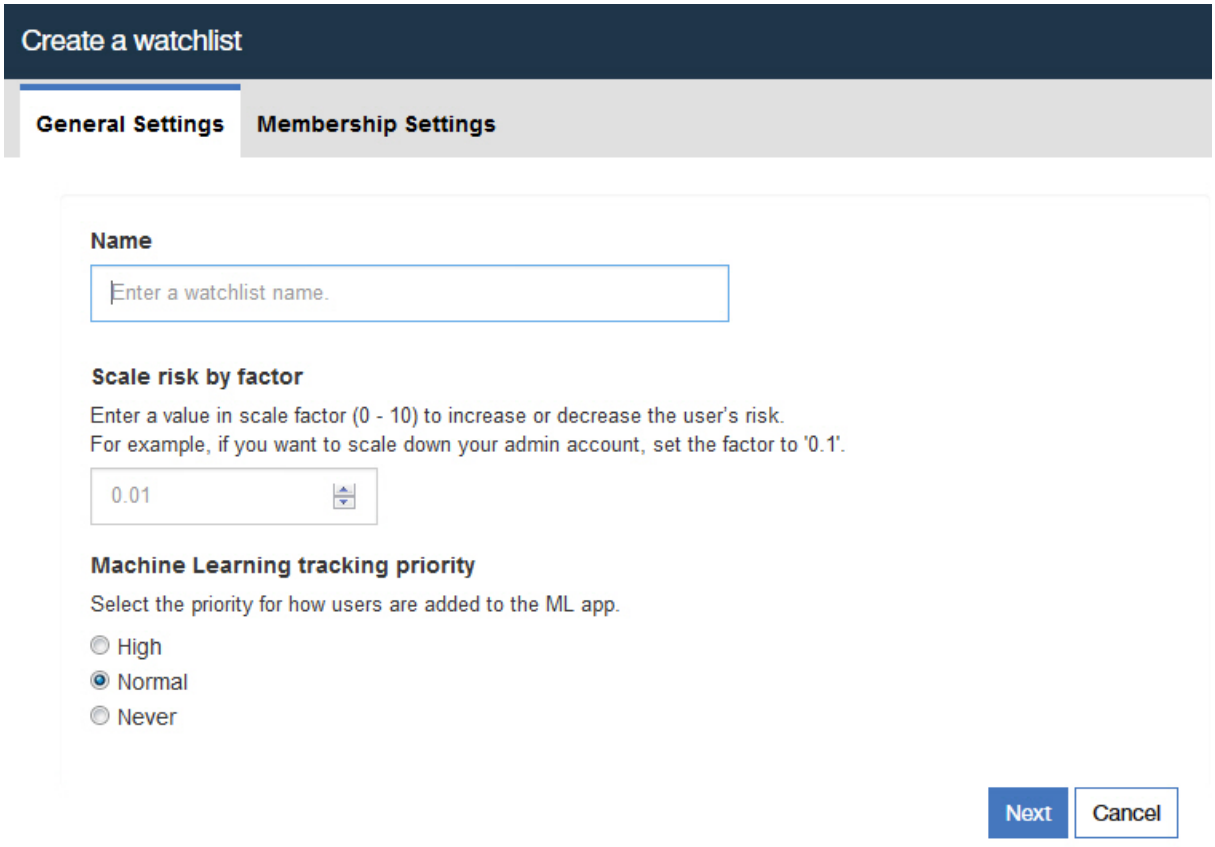
新規監視リストまたは既存の監視リストへのユーザーの追加は、「UBA ダッシュボード」、「ユーザーの詳細」ページ、または「検索結果」ページから実行できます。単一のユーザーを複数の監視リストのメンバーにすることができます。

手順

1. 「UBA ダッシュボード」または「ユーザーの詳細」ページから、「監視リスト」  アイコンをクリックします。

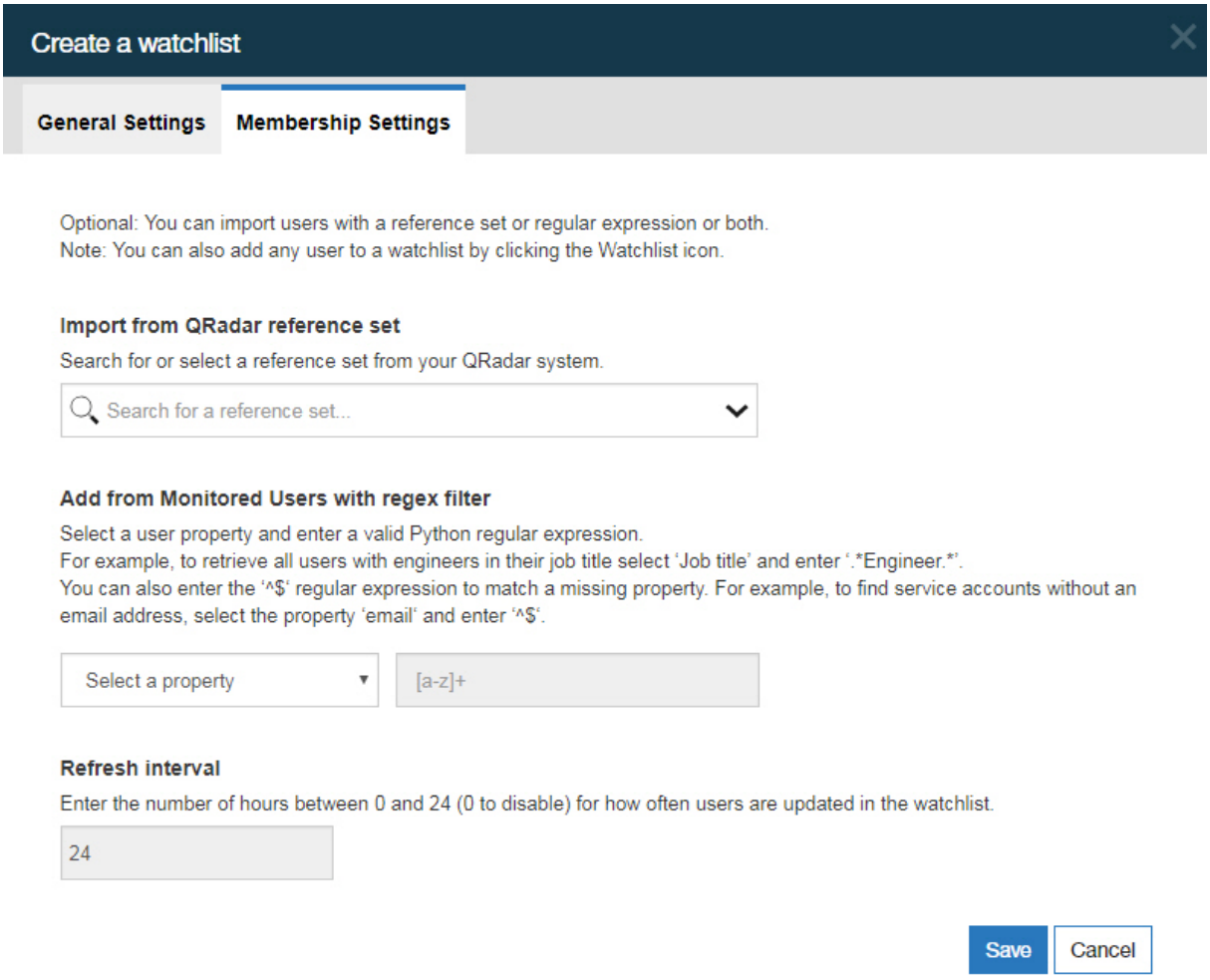
2. メニューから「新規監視リストの作成」を選択します。既存の監視リストにユーザーを追加するには、「追加先」をクリックして監視リストを指定します。
3. 「一般設定」タブで、監視リスト名を入力します。
4. 「リスクのスケール係数」フィールドの値を変更すると、ユーザーのリスク・スコアを人為的に増減させることができます。デフォルトの係数「1」の場合、リスク・スコアは変更されません。

   注: ユーザーが複数の監視リストに含まれる場合は、最も高いスケール係数が適用されます。
5. 「**Machine Learning** 追跡の優先順位」セクションで、機械学習分析によるユーザーの追跡方法を指定する優先順位を選択します。
   - 「高」 - ユーザーは、機械学習分析ごとの最大ユーザー数まで常に追跡されます。
   - 「標準」 - ユーザーは、すべての上位ユーザーが追加された後に、最も高いリスクによって追跡されます。
   - なし - ユーザーは機械学習によって追跡されません。
6. 「次へ」をクリックします。



7. 「メンバーシップ設定」タブでは、リファレンス・セットまたは正規表現あるいはその両方から、ユーザーを自動的に監視リストに取り込むことができます。
8. オプション: 「**QRadar** リファレンス・セットからインポート」フィールドで、リファレンス・セットを検索するか、リストのリファレンス・セットをクリックして選択し、そのリファレンス・セットからすべての項目をインポートします。注: ユーザー名が含まれないリファレンス・セットもリストに表示される可能性があります。リファレンス・セットを選択したら、リンクをクリックして確認します。

9. オプション: 「正規表現フィルターを使用してモニター対象ユーザーから追加」フィールドで、ユーザー・プロパティーを選択し、有効な Python 正規表現を入力すると、UBA データベースで既に見つかっているユーザーを選択できます。
10. 「最新表示間隔」フィールドで、ユーザー・リストの更新頻度を示す時間数を入力します。 例えば、「10」と入力すると、ユーザー・リストが 10 時間ごとに更新されます。 「最新表示間隔」が値 0 (ゼロ) に設定されている場合は、「最新表示」をクリックして手動で監視リストを更新できます。
11. 「保存」をクリックします。



信頼できるユーザーのホワイトリストの参照

「リファレンス・セット管理」リストで、ホワイトリストに登録されている信頼できるユーザーのリストを確認できます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。

2. 「システム構成」セクションで、「リファレンス・セット管理」をクリックします。
3. 「リファレンス・セット管理」ウィンドウで、「**UBA : Trusted Usernames**」リファレンス・セットを選択します。
4. 「内容の表示」をクリックします。

ネットワーク・モニター・ツールの管理

IBM QRadar User Behavior Analytics (UBA) アプリのネットワーク・モニター・ツールを管理できます。

このタスクについて

ネットワーク・キャプチャー、モニター、または分析のプログラムの使用状況をモニターする場合、それらのプログラムが「UBA : Network Capture, Monitoring and Analysis Program Filenames」リファレンス・セットにリストされていることを確認します。次に、「**UBA : Network Capture, Monitoring and Analysis Program Filenames**」ルールを有効にする必要があります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「システム構成」セクションで、「リファレンス・セット管理」をクリックします。
3. 「リファレンス・セット管理」ウィンドウで、「**UBA : Network Capture, Monitoring and Analysis Program Filenames**」リファレンス・セットを選択します。
4. 「内容の表示」をクリックします。
5. 管理するアプリケーションを追加するには、「追加」をクリックし、ボックスに値を入力します。
6. アプリケーションを削除するには、アプリケーションを選択し、「削除」をクリックします。

次のタスク

「**UBA : Network Capture, Monitoring and Analysis Program Filenames**」ルールを有効にします。

制限付きプログラムの管理

IBM QRadar User Behavior Analytics (UBA) アプリの制限付きプログラムを管理できます。

このタスクについて

使用状況をモニターするアプリケーションがある場合、「UBA : Restricted Program Filenames」リファレンス・セットにアクセスして、モニターするアプリケーションを入力します。次に、「UBA : Restricted Program Filenames」ルールを有効にする必要があります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。

- IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。

2. 「システム構成」セクションで、「リファレンス・セット管理」をクリックします。
3. 「リファレンス・セット管理」ウィンドウで、「**UBA : Restricted Program Filenames**」リファレンス・セットを選択します。
4. 「内容の表示」をクリックします。
5. 管理するアプリケーションを追加するには、「追加」をクリックし、ボックスに値を入力します。
6. アプリケーションを削除するには、アプリケーションを選択し、「削除」をクリックします。

次のタスク

「**UBA : Restricted Program Filenames**」ルールを有効にします。

信頼できるログ・ソース・グループへのログ・ソースの追加

UBA アプリで特定のログ・ソースをモニターおよび報告しない場合、それらのログ・ソースを「**UBA : Trusted Log Source Group**」に追加できます。このグループにログ・ソースを追加すると、UBA アプリはそれらのログ・ソースのモニターを停止します。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. ログ・ソースの共通パラメーターを構成します。
5. ログ・ソースのプロトコル固有のパラメーターを構成します。
6. 「**UBA : Trusted Log Source Group**」チェック・ボックスを選択します。
7. 「保存」をクリックします。
8. 「管理」タブで「変更のデプロイ」をクリックします。

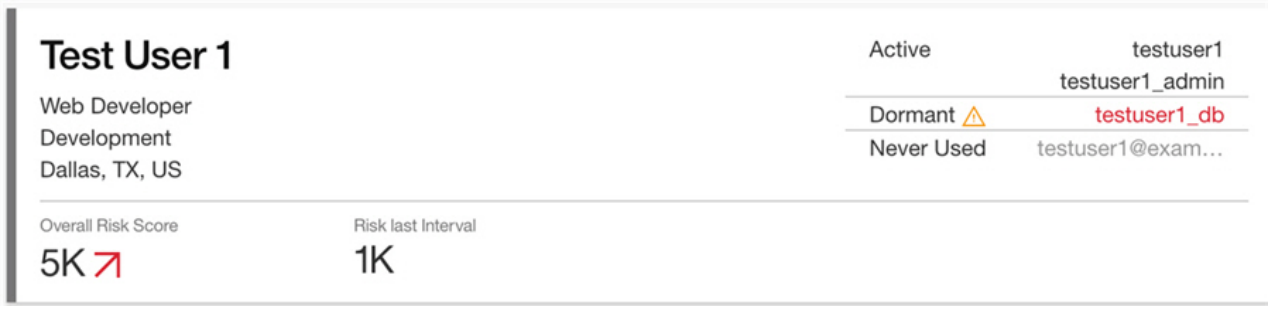
休止アカウント

休止アカウント、アクティブ・アカウント、またはまったく未使用のアカウントを持つ、システム内のユーザーを表示できます。

「ユーザーの詳細」ページでの休止アカウントの表示

V3.2.0 以降では、「ユーザーの詳細」ページで選択したユーザーに関連付けられたアカウントの状況を表示できます。

ユーザー・アカウントの状況	説明
アクティブ	構成済みの休止アカウントしきい値の期間内に、UBA によって QRadar ログ・ソースでイベントが確認されたアカウント。
休止 (Dormant)	UBA によって過去に少なくとも 1 つのイベントが確認されたが、休止アカウントしきい値の期間中に新たなイベントが確認されていないアカウント。
未使用 (Never Used)	UBA によって QRadar ログ・ソース内で該当するユーザー名に関するイベントが一切確認されていないアカウント。 アカウントが「未使用 (Never Used)」として特定される原因として、以下のアクティビティーが考えられます。 • 関連するユーザー名アカウントに対して QRadar ログ・ソースにこれまで記録が一切ないアカウントである。 • UBA V3.2.0 がインストールされる前にイベントが発生していた。注: UBA アプリケーションを初めてインストールすると、過去 1 時間に発生したイベントのみが分析され、アカウントが最後にアクセスされた時点が特定されます。初期分析後、UBA アプリケーションでは、アカウントの使用状況を監視するバックグラウンド・タスクの実行から次の実行までの間に発生したイベントが照会されます。 注: 「未使用 (Never Used)」というカテゴリーに入るアカウントは、LDAP アプリケーションからインポートされた可能性があります。



「休止アカウントを持つユーザー (Users with Dormant Accounts)」監視リスト

「休止アカウントを持つユーザー (Users with Dormant Accounts)」監視リストは、UBA アプリケーションによってユーザー・データがプルされると自動的に生成されます。「休止アカウントを持つユーザー (Users with Dormant Accounts)」監視リストは UBA ダッシュボードで確認できます。

この監視リストを削除すると、自動的には再作成されません。再作成する必要が生じた場合は、「監視リストの作成」画面の「メンバーシップ設定」タブで「**UBA : 休止アカウント (UBA : Dormant Accounts)**」リファレンス・セットを選択してください。

休止アカウントしきい値の構成

休止アカウントしきい値のデフォルト値は 14 日です。非アクティブ状態のユーザーが休止であると判断されるまでの日数を変更するには、「UBA の設定」ページの「アプリケーション設定」セクションを使用します (「管理設定 **(Admin Settings)**」 > 「ユーザー分析」 > 「**UBA** の設定」)。

休止のアカウントまたはユーザーへの応答

休止アカウントに対する応答は、用意されたルールから生成できます。アプリケーションからトリガーされるイベントを使用して、カスタム応答を作成することもできます。

休止だったアカウントが使用された、または使用が試みられたときにユーザーのスコアが増えるよう用意されたルールを使用するには、以下のルールが有効になっていることを確認します。

- 83 ページの『UBA : 休止アカウント使用の試み (UBA : Dormant Account Use Attempted)』
- 83 ページの『UBA : 休止アカウントが使用されました』

カスタム応答を作成するには、生成された以下のイベントをルールまたは照会で使用できます。

- 休止アカウントが見つかりました (QID 104000012)
- 休止アカウントが使用されました (QID 104000013)

関連概念:

10 ページの『UBA ダッシュボードとユーザーの詳細』
IBM QRadar User Behavior Analytics (UBA) アプリには、ネットワーク内のユーザーの全体的なリスク・データが表示されます。

関連タスク:

32 ページの『アプリケーション設定の構成』
IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、UBA アプリケーション設定を構成する必要があります。

39 ページの『監視リストの作成』
新規監視リストまたは既存の監視リストにユーザーを追加できます。

6 チューニング

パフォーマンス改善のための索引の有効化

IBM QRadar User Behavior Analytics (UBA) アプリのパフォーマンスを向上させるために、IBM QRadar で索引を有効にします。

このタスクについて

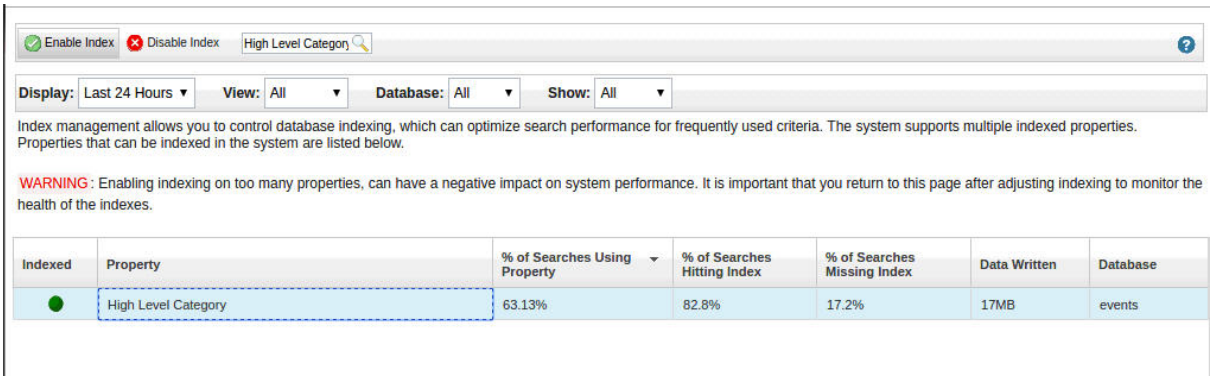
IBM QRadar および UBA アプリでの検索速度を上げるために、検索照会に以下の索引付きフィールドを追加してデータ全体の絞り込みを行います。

- 上位カテゴリー
- 下位カテゴリー
- senseValue
- senseOverallScore
- ユーザー名

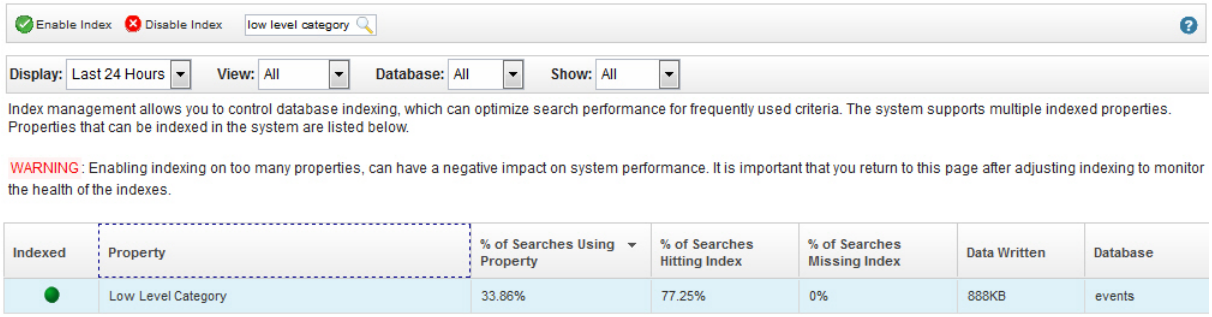
索引付けについて詳しくは、IBM Knowledge Center の以下のセクションを参照してください。https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_index_mgmt.html。

手順

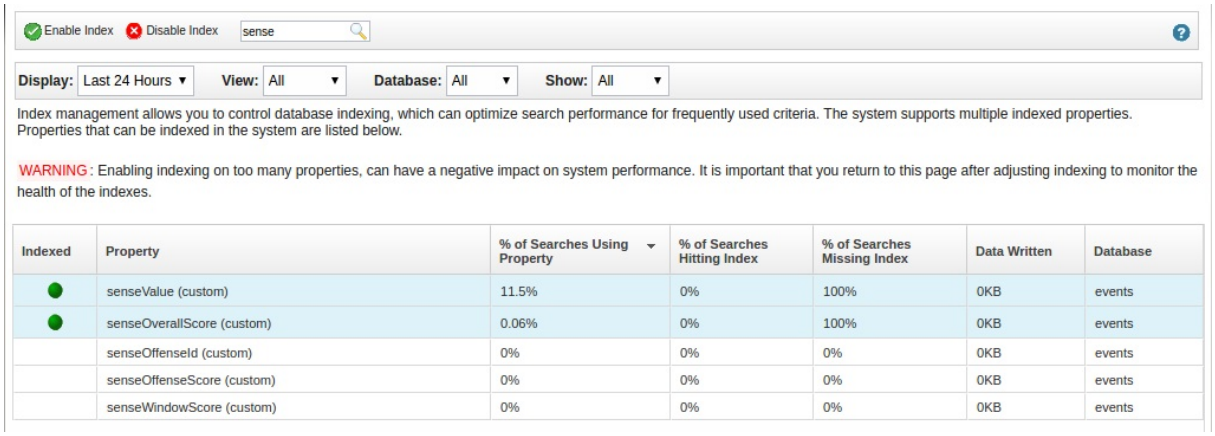
1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「システム構成」セクションの「索引管理」アイコンをクリックします。
3. 「索引管理」ページの検索ボックスに、**上位カテゴリー**と入力します。
4. 「上位カテゴリー」を選択し、「索引の有効化」をクリックします。



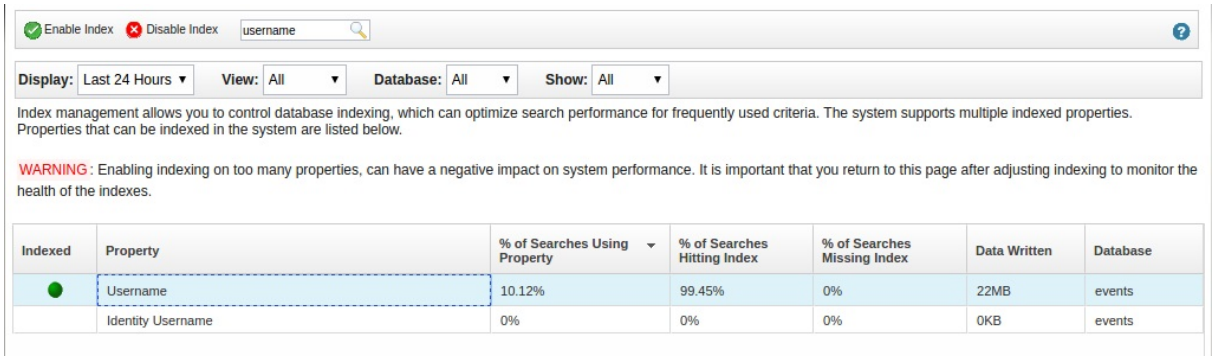
5. 「保存」をクリックします。
6. 「下位カテゴリー」を選択し、「索引の有効化」をクリックします。



7. 「保存」をクリックします。
8. 「索引管理」ページの検索ボックスに、sense と入力します。
9. 「**senseValue**」と「**senseOverallScore**」を選択し、「索引の有効化」をクリックします。



10. 「保存」をクリックします。
11. 「索引管理」ページの検索ボックスに、username と入力します。
12. 「ユーザー名」を選択し、「索引の有効化」をクリックします。



13. 「保存」をクリックします。

新規または既存の QRadar コンテンツと UBA アプリの統合

QRadar の「ルール・ウィザード」を使用して、既存またはカスタムの QRadar ルールを UBA アプリに統合します。

このタスクについて

固有のニーズを満たすために、既存の QRadar ルールを UBA アプリに統合して、QRadar に組み込まれている機能を使用することができます。

制約事項**:** UBA および機械学習リファレンス・セットを使用するためのルールのカスタマイズは行わないでください。カスタム・ルールでリファレンス・セットを使用しようとすると、UBA アプリ内で障害が発生することがあります。

手順

1. 既存のルールのコピーを作成します。これにより、基本ルールの更新によって、新しいルールで行った編集が影響されないようにします。
2. 「ルール・ウィザード」でルールを開き、「ルールの応答」セクションにナビゲートします。
3. 「新規イベントのディスパッチ」オプションを有効化または編集します。その際、「イベントの説明」のテキスト形式が `senseValue=#,senseDesc='sometext',usecase_id='rule UUID'` になるようにしてください。
4. 「上位カテゴリー」を「センス」に設定します。
5. 「終了」をクリックして変更を保存します。

   注**:** ルールがフロー・データに適用される場合は、「イベント・データまたはフロー・データにユーザー名がない場合、ユーザー名を探してアセットを検索します」オプションを有効にして、ユーザー名のないイベントでユーザー・マッピングのルックアップを試行できるようにする必要があります。

リファレンス・セット

User Behavior Analytics アプリと Machine Learning アプリでは、ユーザー情報を保管するためにリファレンス・セットが使用されます。一部のリファレンス・セットはアプリケーション専用に予約されており、それらを変更することも、カスタム・ルールの作成時に使用することもできません。

カスタマイズできるリファレンス・セット

リファレンス・セット	説明
UBA : 高リスク・ユーザー	「*UBA : 高リスク・ユーザー*」リファレンス・セットは「UBA の設定」ページの「オフェンスをトリガーするリスクしきい値」の値から作成されます。ユーザーの最大数は 10,000 であり、リファレンス・セットは 5 分ごとに再作成されます。
UBA : トラステッド・ユーザー名 (UBA : Trusted Usernames)	ユーザー名を「*UBA : トラステッド・ユーザー名 (UBA : Trusted Usernames)*」リファレンス・セットに追加できますが、ルールおよびレポートに使用しないでください。「*UBA : トラステッド・ユーザー名 (UBA : Trusted Usernames)*」リファレンス・セット内のユーザーについてはオフェンスが生成されません。
UBA : ML 常に追跡される監視リスト (UBA : ML Always Tracked Watchlist)	「*UBA : ML 常に追跡される監視リスト (UBA : ML Always Tracked Watchlist)*」リファレンス・セットは、「ユーザーの詳細」ページの「詳細設定」セクションの「**Machine Learning** で追跡」の対象として選択したユーザーから作成されます。ユーザー名を「*UBA : ML 常に追跡される監視リスト (UBA : ML Always Tracked Watchlist)*」リファレンス・セットに追加できますが、ルールおよびレポートに使用しないでください。

カスタマイズできないリファレンス・セット

制約事項: 以下のリファレンス・セットをカスタム・ルール作成のために変更および使用しないでください。

- UBA - 現行の ML 追跡ユーザー (UBA - Current ML Tracked Users)
- UBA - 以前の ML 追跡ユーザー (UBA - Previous ML Tracked Users)
- UBA - 現行の簡略 ML 追跡ユーザー (UBA - Current Abridged ML Tracked Users)
- UBA - 以前の簡略 ML 追跡ユーザー (UBA - Previous Abridged ML Tracked Users)
- UBA - 現行のピア・グループ ML 追跡ユーザー (Current Peer Group ML Tracked Users)
- UBA - 以前のピア・グループ ML 追跡ユーザー (Previous Peer Group ML Tracked Users)

7 UBA アプリのルールおよびチューニング

IBM QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

User Behavior Analytics (UBA) アプリには、カスタム・ルールに基づくユース・ケースが組み込まれています。これらのルールを使用して、UBA アプリ・ダッシュボード用のデータが生成されます。UBA アプリ V3.0.0 からは、UBA アプリ内でルールの表示、フィルタリング、およびチューニングを実行できます。V2.8.0 以前では、QRadar の「ルール・リスト」の「User Behavior Analytics グループ (User Behavior Analytics Group)」でルールを表示および変更できます。

注**:**

- デフォルトでは、UBA アプリの一部のルールが有効になっていません。
- 1 つ以上のログ・ソースで、特定の UBA ルール用の情報を提供する必要があります。ログ・ソースは特定の順序では優先順位付けされません。

制約事項**:** UBA および機械学習リファレンス・セットを使用するためのルールのカスタマイズは行わないでください。カスタム・ルールでリファレンス・セットを使用しようとすると、UBA アプリ内で障害が発生することがあります。詳しくは、 49 ページの『リファレンス・セット』を参照してください。

QRadar でのルールの処理方法について詳しくは、https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_rul_mgt.html を参照してください。

「ルールおよびチューニング」ページ

UBA アプリ V3.0.0 では、「ルールおよびチューニング」ページ (「管理設定 **(Admin Settings)**」 > 「ユーザー分析」 > 「ルールおよびチューニング」) が導入されています。

「ルールおよびチューニング」ページには、インストールされている UBA アプリのバージョンに付属するすべてのルールのリストが表示されます。現在の有効化状況と、対応するリファレンス・セットが表示されます。

「ルールおよびチューニング」ページでは、以下の操作を実行できます。

- ルールを有効化または無効化する
- QRadar ルール・ウィザードに素早くアクセスしてルールを確認または編集する
- リファレンス・セットに素早くアクセスしてその内容を確認または編集する
- ルール・テーブルを、カテゴリー、状況、デフォルトのリスク・スコア、必要なリファレンス・セット、およびコンテンツの依存関係に基づいてフィルタリングする
- ルール・テーブルを、ルール名、リファレンス・セット、または状況を基準としてソートする
- テーブル内の項目や、ルールの説明ツールチップ内で検出された単語を検索する
- 各ルールのヘルプ文書にアクセスする

UBA : ブルート・フォース認証の試行

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ブルート・フォース認証の試行

デフォルトで有効

True

デフォルトの senseValue

5

説明

認証障害ブルート・フォース・アタック (水平および垂直) を検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証の失敗 (BB:CategoryDefinition: Authentication Failures)
- BB:UBA : 認証ブルート・フォース試行の検出 (水平) (BB:UBA : Detecting Authentication Bruteforce Attempts (Horizontal))
- BB:UBA : 認証ブルート・フォース試行の検出 (垂直) (BB:UBA : Detecting Authentication Bruteforce Attempts (Vertical))

データ・ソース

3Com 8800 シリーズ・スイッチ、APC UPS、AhnLab Policy Center APC、Application Security DbProtect、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba ClearPass Policy Manager、Aruba モビリティー・コントローラー、Avaya VPN Gateway、Barracuda Web Application Firewall、Barracuda Web Filter、Bit9 Security Platform、Bluemix プラットフォーム、Box、Bridgewater Systems AAA サービス・コントローラー、Brocade FabricOS、CA ACF2、CA SiteMinder、CRE システム、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、Catalyst スイッチ用 Cisco CatOS、Cisco FireSIGHT Management Center、Cisco ファイアウォール・サービス・モジュール (FWSM)、Cisco IOS、Cisco Identity Services Engine、Cisco Intrusion Prevention System (IPS)、Cisco IronPort、Cisco NAC アプライアンス、Cisco Nexus、Cisco PIX Firewall、Cisco VPN 3000 シリーズ・コンセントレーター、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、Citrix Access Gateway、Citrix NetScaler、CloudPassage Halo、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、Cyber-Ark Vault、CyberGuard TSP Firewall/VPN、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、ESET Remote Administrator、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterasys XSR セキュリティー・ルーター、Enterprise-IT-Security.com SF-Sherlock、Epic SIEM、イベント CRE インジェクション、Extreme 800 シリーズ・スイッチ、Extreme Dragon Network IPS、Extreme HiPath、Extreme Matrix E1 スイッチ、Extreme Networks ExtremeWare オペレーティング・システム

(OS)、 Extreme スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper Junos WebApp Secure、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、McAfee ePolicy Orchestrator、Microsoft IAS Server、Microsoft IIS、Microsoft ISA、Microsoft Office 365、Microsoft SCOM、Microsoft SQL Server、Microsoft SharePoint、Microsoft Windows セキュリティー・イベント・ログ、Motorola SymbolAP、Netskope Active、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500、Nortel イーサネット・ルーティング・スイッチ 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 ソフトウェア、OpenBSD OS、Oracle Acme Packet SBC、Oracle Audit Vault、Oracle BEA WebLogic、Oracle Database リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : 非エグゼクティブ・ユーザーによってアクセスされたエグゼクティブ専用のアセット

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 非エグゼクティブ・ユーザーによってアクセスされたエグゼクティブ専用のアセット

デフォルトで有効

False

デフォルトの senseValue

15

説明

非エグゼクティブ・ユーザーがエグゼクティブ専用のアセットにログオンしたことを検出します。このルールと共に 2 個の空のリファレンス・セット「UBA : Executive Users」および「UBA : Executive Assets」がインポートされます。環境でフラグを立てるアカウントおよび IP アドレスを追加または削除するには、これらのリファレンス・セットを編集します。リファレンス・セットの構成後にこのルールを有効にしてください。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- BB:CategoryDefinition: ファイアウォールまたは ACL の受け入れ (BB:CategoryDefinition: Firewall or ACL Accept)

必須の構成

リファレンス・セット「UBA : エグゼクティブ・ユーザー (UBA : Executive Users)」および「UBA : エグゼクティブ・アセット (UBA : Executive Assets)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry

Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : 重要なアセットへの高リスク・ユーザー・アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 重要なアセットへの高リスク・ユーザー・アクセス

デフォルトで有効

False

デフォルトの senseValue

15

説明

インシデント (オフェンス) に関与するユーザーが重要なアセットにアクセスしたことを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)

必須の構成

リファレンス・セット「重要なアセット (Critical Assets)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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 : 単一 IP からの複数 VPN アカウントへのログイン失敗

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 単一 IP からの複数 VPN アカウントへのログイン失敗

デフォルトで有効

True

デフォルトの senseValue

5

説明

「UBA : 単一 IP からの複数 VPN アカウントへのログイン失敗」リファレンス・セットから VPN アカウントのログイン失敗を検出します。

サポート・ルール

- UBA : 単一 IP からの複数 VPN アカウントへのログイン失敗の取り込み
- BB:UBA : VPN ログイン失敗 (BB:UBA : VPN Login Failed)

必須の構成

ルール「UBA : 単一 IP からの複数 VPN アカウントへのログイン失敗の取り込み」を有効化します。

データ・ソース

Cisco Adaptive Security Appliance (ASA)

UBA : 単一 IP からの複数 VPN アカウントへのログイン

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 単一 IP からの複数 VPN アカウントへのログイン

デフォルトで有効

False

デフォルトの senseValue

5

説明

同じ IP アドレスからの複数の VPN ユーザーをマップした後、リスク・スコアを引き上げます。同じ IP アドレスからの複数の VPN ユーザーをこのルールが検出すると、その IP アドレスが「UBA : 単一 IP からの複数 VPN アカウントへのログイン」に追加されます。このルールを有効にする前に、必ずルール「UBA : 単一 IP からの複数 VPN アカウントへのログインの取り込み」を有効にして、「UBA : 単一 IP からの複数 VPN アカウントへのログイン」リファレンス・セットにデータを設定してください。

サポート・ルール

- UBA : 単一 IP からの複数 VPN アカウントへのログインの取り込み
- BB:UBA : VPN ログイン成功 (BB:UBA : VPN Login Successful)

必須の構成

ルール「UBA : 単一 IP からの複数 VPN アカウントへのログインの取り込み」を有効化します。

データ・ソース

Cisco Adaptive Security Appliance (ASA)

UBA : 無許可アクセスの繰り返し

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 無許可アクセスの繰り返し

デフォルトで有効

True

デフォルトの **senseValue**

10

説明

無許可アクセス・アクティビティーの繰り返しが検出されたことを意味します。

サポート・ルール

UBA : 無許可アクセス

必須の構成

ルール「UBA : 無許可アクセス」を有効化します。

データ・ソース

Akamai KONA、Amazon AWS CloudTrail、Application Security DbProtect、Arbor Networks Pravail、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba モビリティー・コントローラー、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 サービス・コントローラー、Brocade FabricOS、CA ACF2、CA SiteMinder、CRE システム、Carbon Black Protection、Centrify Server Suite、Check Point、Cilasoft QJRN/400、Cisco ACS、Cisco Adaptive Security Appliance (ASA)、Cisco CSA、Cisco Call Manager、Catalyst スイッチ用 Cisco CatOS、Cisco ファイアウォール・サービス・モジュール (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、構成可能なファイアウォール・フィルター、CorreLog Agent for IBM zOS、カスタム・ルール・エンジン、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterasys XSR セキュリティー・ルーター、Epic SIEM、イベント CRE インジェクション、Extreme Dragon Network IPS、Extreme スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP AFM、F5 ネットワークス BIG-IP ASM、Fidelis XPS、フロー分類エンジン、Forcepoint V シリーズ、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、H3C Comware Platform、HP Network Automation、HP Tandem、Honeycomb Lexicon File Integrity Monitor、Huawei S シリーズ・スイッチ、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 プラットフォーム、Juniper Networks ファイアウォールおよび 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 サーバー、Linux OS、Linux iptables ファイアウォール、Mac OS X、McAfee Firewall Enterprise、McAfee IntruShield ネットワーク

IPS アプライアンス、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 セキュリティー・イベント・ログ、NCC Group DDos Secure、Nortel Contivity VPN スイッチ、Nortel Multiprotocol Router、Nortel VPN Gateway、OS Services Qidmap、OSSEC、Okta、Open LDAP ソフトウェア、OpenBSD OS、Oracle Audit Vault、Oracle BEA WebLogic、Oracle Database リスナー、Palo Alto PA シリーズ、PostFix MailTransferAgent、ProFTPD サーバー、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 オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム DHCP ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Sophos Enterprise Console、Sophos Web Security Appliance、Squid Web プロキシー、Stonesoft Management Center、Sun ONE LDAP、Symantec Critical System Protection、Symantec Endpoint Protection、Symantec Gateway Security (SGS) アプライアンス、Symantec System Center、Symark Power Broker、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : 無許可アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 無許可アクセス

デフォルトで有効

True

デフォルトの senseValue

10

説明

無許可アクセス・アクティビティーが検出されたことを意味します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : アクセス拒否
- BB:UBA : アプリケーション拒否 (BB:UBA : Application Denies)

データ・ソース

Akamai KONA、Amazon AWS CloudTrail、Application Security DbProtect、Arbor Networks Pravail、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba モビリティー・コントローラー、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 サービス・コントローラー、Brocade FabricOS、CA ACF2、CA SiteMinder、CRE システム、Carbon Black Protection、Centrify Server

Suite、Check Point、Cilasoft QJRN/400、Cisco ACS、Cisco Adaptive Security Appliance (ASA)、Cisco CSA、Cisco Call Manager、Catalyst スイッチ用 Cisco CatOS、Cisco ファイアウォール・サービス・モジュール (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、構成可能なファイアウォール・フィルター、CorreLog Agent for IBM zOS、カスタム・ルール・エンジン、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterasys XSR セキュリティー・ルーター、Epic SIEM、イベント CRE インジェクション、Extreme Dragon Network IPS、Extreme スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP AFM、F5 ネットワークス BIG-IP ASM、Fidelis XPS、フロー分類エンジン、Forcepoint V シリーズ、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、H3C Comware Platform、HP Network Automation、HP Tandem、Honeycomb Lexicon File Integrity Monitor、Huawei S シリーズ・スイッチ、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 プラットフォーム、Juniper Networks ファイアウォールおよび 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 サーバー、Linux OS、Linux iptables ファイアウォール、Mac OS X、McAfee Firewall Enterprise、McAfee IntruShield ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、NCC Group DDos Secure、Nortel Contivity VPN スイッチ、Nortel Multiprotocol Router、Nortel VPN Gateway、OS Services Qidmap、OSSEC、Okta、Open LDAP ソフトウェア、OpenBSD OS、Oracle Audit Vault、Oracle BEA WebLogic、Oracle Database リスナー、Palo Alto PA シリーズ、PostFix MailTransferAgent、ProFTPD サーバー、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 オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム DHCP ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Sophos Enterprise Console、Sophos Web Security Appliance、Squid Web プロキシー、Stonesoft Management Center、Sun ONE LDAP、Symantec Critical System Protection、Symantec Endpoint Protection、Symantec Gateway Security (SGS) アプライアンス、Symantec System Center、Symark Power Broker、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : サービスまたはマシン・アカウントによる Unix/Linux システム・アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : サービスまたはマシン・アカウントによる Unix/Linux システム・アクセス

デフォルトで有効

True

デフォルトの senseValue

15

説明

UNIX サーバーおよび Linux サーバーのサービス・アカウントまたはマシン・アカウントにより開始された対話式セッション (GUI および CLI を使用、ローカル・ログインおよびリモート・ログインの両方) を検出します。アカウントおよび許可される対話式セッションは、「UBA : Service, Machine Account」および「UBA : Allowed Interaction Session」の各リファレンス・セットにリストされています。環境でフラグを立てる対話式セッションを追加または削除するには、これらのリファレンス・セットを編集します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: ファイアウォールまたは ACL の受け入れ (BB:CategoryDefinition: Firewall or ACL Accept)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)

必須の構成

リファレンス・セット「UBA : サービスおよびマシン・アカウント (UBA : Service, Machine Account)」および「UBA : 許可された対話式セッション (UBA : Allowed Interactive Session)」に適切な値を追加します。

データ・ソース

Linux OS

UBA : ユーザー・アクセス - 重要なアセットへのアクセスに失敗しました

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ユーザー・アクセス - 重要なアセットへのアクセスに失敗しました

デフォルトで有効

True

デフォルトの senseValue

5

説明

このルールにより、重要なアセットのリファレンス・セット内に存在するシステムの認証失敗が検出されます。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証の失敗 (BB:CategoryDefinition: Authentication Failures)

必須の構成

リファレンス・セット「重要なアセット (Critical Assets)」に適切な値を追加します。

データ・ソース

3Com 8800 シリーズ・スイッチ、APC UPS、AhnLab Policy Center APC、Application Security DbProtect、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba ClearPass Policy Manager、Aruba モビリティー・コントローラー、Avaya VPN Gateway、Barracuda Web Application Firewall、Barracuda Web Filter、Bit9 Security Platform、Bluemix プラットフォーム、Box、Bridgewater Systems AAA サービス・コントローラー、Brocade FabricOS、CA ACF2、CA SiteMinder、CRE システム、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、Catalyst スイッチ用 Cisco CatOS、Cisco FireSIGHT Management Center、Cisco ファイアウォール・サービス・モジュール (FWSM)、Cisco IOS、Cisco Identity Services Engine、Cisco Intrusion Prevention System (IPS)、Cisco IronPort、Cisco NAC アプライアンス、Cisco Nexus、Cisco PIX Firewall、Cisco VPN 3000 シリーズ・コンセントレーター、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、Citrix Access Gateway、Citrix NetScaler、CloudPassage Halo、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、Cyber-Ark Vault、CyberGuard TSP Firewall/VPN、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、ESET Remote Administrator、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterasys XSR セキュリティー・ルーター、Enterprise-IT-Security.com SF-Sherlock、Epic SIEM、イベント CRE インジェクション、Extreme 800 シリーズ・スイッチ、Extreme Dragon Network IPS、Extreme HiPath、Extreme Matrix E1 スイッチ、Extreme Networks ExtremeWare オペレーティング・システム (OS)、 Extreme スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper Junos WebApp Secure、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、McAfee ePolicy Orchestrator、Microsoft IAS Server、Microsoft IIS、Microsoft ISA、Microsoft Office 365、Microsoft SCOM、Microsoft SQL Server、Microsoft SharePoint、Microsoft Windows セキュリティー・イベン

ト・ログ、Motorola SymbolAP、Netskope Active、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500、Nortel イーサネット・ルーティング・スイッチ 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 ソフトウェア、OpenBSD OS、Oracle Acme Packet SBC、Oracle Audit Vault、Oracle BEA WebLogic、Oracle Database リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : ユーザー・アクセス - 重要なアセットへのアクセスに失敗しました

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

以下をサポートします。

- UBA : User Access First Access to Critical Assets
- UBA : Critical Systems Users Seen Update

デフォルトで有効

True

デフォルトの senseValue

10

説明

UBA : User Access First Access to Critical Assets: これが、ユーザーが重要なアセットにアクセスした初回であることを示します。「Critical Systems Users Seen」リファレンス・コレクションは、観測の存続時間を制御します。デフォルトでは、このルールは、直近 3 カ月間での最初のアクセスを検出します。

UBA : Critical Systems Users Seen Update: 「Critical Systems Users Seen」リファレンス・コレクションで、既に存在する宛先 IP/ユーザー名の一致で、最後に確認された値を更新します。

サポート・ルール

- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「重要なアセット (Critical Assets)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : 複数のホストからのユーザー・アクセス (UBA : User Access from Multiple Hosts)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 複数のホストからのユーザー・アクセス (UBA : User Access from Multiple Hosts)

デフォルトで有効

False

デフォルトの senseValue

5

説明

許可された数を超えるデバイスから単一ユーザーがログインしたときに検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System

(IPS)、TippingPoint X Series アプライアンス、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 : ジャンプ・サーバーからの内部サーバーへのユーザー・アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ジャンプ・サーバーからの内部サーバーへのユーザー・アクセス

デフォルトで有効

False

デフォルトの senseValue

10

説明

ユーザーがジャンプ・サーバーを使用して VPN サーバーまたは内部サーバーにアクセスしたことを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)

必須の構成

リファレンス・セット「UBA : ジャンプ・サーバー (UBA : Jump Servers)」および「UBA : 内部サーバー (UBA : Internal Servers)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : User Access Login Anomaly

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : User Access Login Anomaly

デフォルトで有効

True

デフォルトの senseValue

5

説明

ローカル・アセットに対する一連のログイン失敗を示します。このルールは、アカウント漏えいや側方移動アクティビティーも示す場合があります。「Multiple Login Failures for Single Username」ルールが有効であることを確認してください。応答性が適合するように、このルールの突き合わせパラメーターと時刻期間パラメーターを調整してください。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- 単一ユーザー名の複数のログイン失敗 (Multiple Login Failures for Single Username)

必須の構成

ルール「単一ユーザー名の複数のログイン失敗 (Multiple Login Failures for Single Username)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : 匿名のソースからのアカウントにユーザーがアクセスしています

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 匿名のソースからのアカウントにユーザーがアクセスしています

デフォルトで有効

True

デフォルトの senseValue

15

説明

ユーザーが TOR、VPN などの匿名ソースから内部リソースにアクセスしていることを示します。

サポート・ルール

- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : User Time, Access at Unusual Times

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : User Time, Access at Unusual Times

デフォルトで有効

True

デフォルトの senseValue

5

説明

「UBA : Unusual Times, %」ビルディング・ブロックに定義されている、ネットワークに対して通常ではない時刻に、ユーザーが正常に認証していることを示します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- BB:UBA : 通常とは異なる時刻、夕方 (BB:UBA : Unusual Times, Evening)
- BB:UBA : 通常とは異なる時刻、夜間 (BB:UBA : Unusual Times, Overnight)

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、

Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : サービスもしくはマシン・アカウントによる VPN アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : サービスもしくはマシン・アカウントによる VPN アクセス

デフォルトで有効

True

デフォルトの senseValue

10

説明

サービス・アカウントまたはマシン・アカウントが Cisco VPN にアクセスすると、それを検出します。アカウントは、「UBA : Service, Machine Account」リファレンス・セットにリストされています。環境でフラグを立てるアカウントを追加または削除するには、このリストを編集します。

サポート・ルール

BB:UBA : VPN マッピング (ロジック) (BB:UBA : VPN Mapping (logic))

必須の構成

リファレンス・セット「UBA : サービスおよびマシン・アカウント (UBA : Service, Machine Account)」に適切な値を追加します。

データ・ソース

Cisco Adaptive Security Appliance (ASA)

UBA : VPN 証明書の共有

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : VPN 証明書の共有

デフォルトで有効

True

注**:** UBA : 「VPN 証明書の共有」ルールを使用する予定の場合は、Cisco Firewall DSM を以下のものに更新する必要があります。

- V7.2.8 の場合: DSM-CiscoFirewallDevices-7.2-20170619124928.noarch.rpm
- V7.3.0 以降の場合: DSM-CiscoFirewallDevices-7.3-20170619132427.noarch.rpm

デフォルトの **senseValue**

15

説明

このルールは、VPN イベントのユーザー名が「VPNSubjectcn」と等しくないことを検出します。これは、VPN 証明書共有が発生していることを示す場合があります。証明書共有や他の認証トークン共有は、誰が何を行ったかを識別するのを難しくする可能性があります。これにより、危険にさらされた場合に次の段階に進むのが困難になる可能性があります。

サポート・ルール

- BB:UBA : VPN マッピング (ロジック) (BB:UBA : VPN Mapping (logic))
- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

これらのルールは、関連するリファレンス・セットを必要なデータで更新します。

必須の構成

以下のルールを有効化します。

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

データ・ソース

Cisco Adaptive Security Appliance (ASA)

UBA : サービスまたはマシン・アカウントによる Windows アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : サービスまたはマシン・アカウントによる Windows アクセス

デフォルトで有効

True

デフォルトの **senseValue**

15

説明

Windows Server でサービス・アカウントまたはマシン・アカウントにより開始された対話式セッション (RDP、ローカル・ログイン) を検出します。アカウントは、「UBA : Service, Machine Account」リファ

レンス・セットにリストされています。環境でフラグを立てるアカウントを追加または削除するには、このリストを編集します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : サービスおよびマシン・アカウント (UBA : Service, Machine Account)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4776)

アカウントおよび特権

UBA : アカウント、グループ、または特権の追加

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : アカウント、グループ、または特権の追加 (旧称「UBA : アカウント、グループ、または特権が追加または変更されました」)

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが実行し、次のいずれかのカテゴリーにあてはまるイベントを検出します。ルールは、ユーザーの元のリスク・スコアを増分するための IBM センス・イベントをディスパッチします。

- Authentication.Group Added
- Authentication.Group Changed
- Authentication.Group Member Added
- Authentication.Computer Account Added
- Authentication.Computer Account Changed
- Authentication.Policy Added
- Authentication.Policy Change
- Authentication.Trusted Domain Added
- Authentication.User Account Added
- Authentication.User Account Changed
- Authentication.User Right Assigned

注: ユーザーのリスク・スコア全体に対するこのルールの影響を調整するために、ビルディング・ブロック・ルール「CategoryDefinition: Authentication User or Group Added or Changed 」を変更して、組織が注目するイベント・カテゴリーを追加することを検討してください。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : 認証ユーザー、グループ、またはポリシーの追加 (BB:UBA : Authentication User or Group or Policy Added)

データ・ソース

Akamai KONA、Amazon AWS CloudTrail、Application Security DbProtect、Arbor Networks Pravail、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba モビリティー・コントローラー、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 サービス・コントローラー、Brocade FabricOS、CA ACF2、CA SiteMinder、CRE システム、Carbon Black Protection、Centrify Server Suite、Check Point、Cilasoft QJRN/400、Cisco ACS、Cisco Adaptive Security Appliance (ASA)、Cisco CSA、Cisco Call Manager、Catalyst スイッチ用 Cisco CatOS、Cisco ファイアウォール・サービス・モジュール (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、構成可能なファイアウォール・フィルター、CorreLog Agent for IBM zOS、カスタム・ルール・エンジン、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterasys XSR セキュリティー・ルーター、Epic SIEM、イベント CRE インジェクション、Extreme Dragon Network IPS、Extreme スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP AFM、F5 ネットワークス BIG-IP ASM、Fidelis XPS、フロー分類エンジン、Forcepoint V シリーズ、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、H3C Comware Platform、HP Network Automation、HP Tandem、Honeycomb Lexicon File Integrity Monitor、Huawei S シリーズ・スイッチ、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 プラットフォーム、Juniper Networks ファイアウォールおよび 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 サーバー、Linux OS、Linux iptables ファイアウォール、Mac OS X、McAfee Firewall Enterprise、McAfee IntruShield ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、NCC Group DDos Secure、Nortel Contivity VPN スイッチ、Nortel Multiprotocol Router、Nortel VPN Gateway、OS Services Qidmap、OSSEC、Okta、Open LDAP ソフトウェア、OpenBSD OS、Oracle Audit Vault、Oracle BEA WebLogic、Oracle Database リスナー、Palo Alto PA シリーズ、PostFix MailTransferAgent、ProFTPD サーバー、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 オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム DHCP ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Sophos Enterprise Console、Sophos Web Security Appliance、Squid Web プロキシー、Stonesoft Management Center、Sun ONE LDAP、Symantec Critical System Protection、Symantec Endpoint Protection、Symantec Gateway Security (SGS) アプライアンス、Symantec System Center、Symark Power Broker、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : アカウント、グループ、または特権の変更

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : アカウント、グループ、または特権の変更 (旧称「UBA : 変更されたユーザー・アカウント」)

デフォルトで有効

True

デフォルトの **senseValue**

10

説明

ユーザーの有効な特権を上方または下方に変更するアクションによってユーザー・アカウントが影響を受けるときに、そのことを示します。

フォールス・ポジティブの注意**:** このイベントは、アカウント名の変更を、その変更を行っているユーザーであると誤検出する場合があります。このフォールス・ポジティブの可能性を削減するために、テスト「and when Username equals AccountName」を追加できます。

フォールス・ネガティブの注意**:** このイベントは、ユーザーのアカウント変更の一部のケースを検出しない場合があります。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : 認証ユーザー、グループ、またはポリシーの変更 (BB:UBA : Authentication User or Group or Policy Changed)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID:
626、642、644、1300、1317、625、629、4672、4722、4725、4738、4765、4767、4781、4737、4755)

UBA : アカウント削除による DoS 攻撃 (UBA : DoS Attack by Account Deletion)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : アカウント削除による DoS 攻撃 (UBA : DoS Attack by Account Deletion)

デフォルトで有効

False

デフォルトの senseValue

10

説明

アカウント削除イベントの数を固定の時間幅内で固定のしきい値に照らしてチェックすることにより、DoS 攻撃を検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : ユーザー・アカウントの削除 (BB:UBA : User Account Deleted)

データ・ソース

Amazon AWS CloudTrail (イベント ID: DeleteUser)

Application Security DbProtect (イベント ID: Login revoked - Windows、Login dropped - standard、Database role - dropped、Database user revoked)

Aruba モビリティー・コントローラー (イベント ID: authmgr_user_del)

Box (イベント ID: DELETE_USER)

Brocade FabricOS (イベント ID: SEC-1181、SEC-3028)

CA ACF2 (イベント ID: ACF2-L)

Check Point (イベント ID: user_deleted、device_deleted、User Deleted)

Cilasoft QJRN/400 (イベント ID: C20020)

Cisco Adaptive Security Appliance (ASA) (イベント ID: %PIX|ASA-5-502102、%ASA-5-502102)

Cisco FireSIGHT Management Center (イベント ID: USER_REMOVED_CHANGE_EVENT)

Cisco ファイアウォール・サービス・モジュール (FWSM) (イベント ID: 502102)

Cisco Identity Services Engine (イベント ID: 86008、86028)

Cisco NAC Appliance (イベント ID: CCA-1453、CCA-1502)

Cisco Nexus (イベント ID: SECURITYD-6-DELETE_STALE_USER_ACCOUNT)

Cisco ワイヤレス LAN コントローラー (イベント ID: 1.3.6.1.4.1.9.9.515.0.1)

CloudPassage Halo (イベント ID: Halo user deleted、Local account deleted (Linux のみ))

CorreLog Agent for IBM zOS (イベント ID: RACF DELUSER: No Violations)

カスタム・ルール・エンジン (イベント ID: 3035、3043)

Cyber-Ark Vault (イベント ID: 276)

EMC VMWare (イベント ID: AccountRemovedEvent)

Extreme Dragon Network IPS (イベント ID: HOST:LINUX:USER-DELETED、HOST:WIN:ACCOUNT-DELETED)

Extreme Matrix K/N/S シリーズ・スイッチ (イベント ID: User Deleted Event、has been deleted)

Extreme NAC (イベント ID: Deleted registered user)

Extreme NetsightASM (イベント ID: UserRemove)

フロー分類エンジン (イベント ID: 3035、3043)

Forcepoint Sidewinder (イベント ID: passport deletion、all passports revoked)

HBGary Active Defense (イベント ID: DeleteUser)

HP Network Automation (イベント ID: User Deleted)

Huawei S シリーズ・スイッチ (イベント ID: SSH/6/DELUSER_SUCCESS)

IBM AIX 監査 (イベント ID: USER_Remove SUCCEEDED)

IBM AIX サーバー (イベント ID: USER_Remove)

IBM DB2 (イベント ID: DROP_USER SUCCESS)

IBM DataPower (イベント ID: 0x81000136)

IBM IMS (イベント ID: USER DELETED)

IBM Proventia Network Intrusion Prevention System (IPS) (イベント ID: Delete User)

IBM QRadar Packet Capture (イベント ID: UserDeleted)

IBM Resource Access Control Facility (RACF) (イベント ID: 80 17.2、DELUSER_SUCCESS、80 17.0)

IBM Security Access Manager for Enterprise Single Sign-On (イベント ID: REVOKE_IMS_ID、DELETE_IMS_ID)

IBM Security Directory Server (イベント ID: SDS Audit)

IBM Security Identity Governance (イベント ID: 50、43、70005)

IBM Security Identity Manager (イベント ID: Delete SUCCESS、Delete SUBMITTED、Delete Success)

IBM SmartCloud Orchestrator (イベント ID: user)

IBM Tivoli Access Manager for e-business (イベント ID: 13408 - Succeeded、13408 Command Succeeded)

IBM i (イベント ID:
GSL2502、M250100、DO_USRPRF、GSL2602、GSL2601、M260100、MC@0400、GSL2501)

IBM z/OS (イベント ID: 80 1.35)

Juniper Networks Network and Security Manager (イベント ID: adm24473)

Linux OS (イベント ID: userDel、Account Deleted、DEL_USER)

McAfee Application/Change Control (イベント ID: USER_ACCOUNT_DELETED)

McAfee ePolicy Orchestrator (イベント ID: 20793)

Microsoft ISA (イベント ID: user removed)

Microsoft Office 365 (イベント ID: Delete User-PartiallySucceeded、Delete user-success、Delete User-success、Delete user-PartiallySucceeded)

Microsoft SQL Server (イベント ID: 24129、DR - US、DR - SL、DR - LX、DR - AR、DR - SU、24076、24123、38)

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4743、630、1327、647、4726)

Netskope Active (イベント ID: Delete Admin、Deleted admin)

Nortel Application Switch (イベント ID: User Deleted)

Novell eDirectory (イベント ID: DELETE_ACCOUNT)

OS サービスの Qidmap (イベント ID: Account Deleted、User Deleted)

OSSEC (イベント ID: 18112)

Okta (イベント ID: core.user_group_member.user_remove、app.generic.import.details.delete_user)

Oracle Enterprise Manager (イベント ID: Computer Delete (successful)、User Delete (successful))

Oracle RDBMS 監査レコード (イベント ID: DROP USER-Standard:1、53:1、53:0、DROP USER-Standard:0、53)

PGP Universal Server (イベント ID: ADMIN_DELETED_USER)

Palo Alto Endpoint Security Manager (イベント ID: User Deleted)

Pulse Secure Pulse Connect Secure (イベント ID:
SYN24849、ADM20722、ADM24473、SYN24745、SYN24850)

RSA Authentication Manager (イベント ID: unknown、Deleted user、REMOVE_ORPHANED_PRINCIPALS、REMOTE_PRINCIPAL_DELETE、DELETE_PRINCIPAL)

SIM 監査 (イベント ID: Configuration-UserAccount-AccountDeleted)

STEALTHbits StealthINTERCEPT (イベント ID: Active DirectorycomputerObject DeletedTrueFalse、Active DirectoryuserObject DeletedTrueFalse、Console user/group deleted、Console user/group deleted)

SafeNet DataSecure/KeySecure (イベント ID: Removed user)

Skyhigh Networks Cloud Security Platform (イベント ID: 10017)

Solaris BSM (イベント ID: delete user)

SonicWALL SonicOS (イベント ID: 559、1157、1158)

Trend Micro Deep Security (イベント ID: 651)

ユニバーサル DSM (イベント ID: 削除されたコンピューター・アカウント、削除されたユーザー・アカウント)

VMware vCloud Director (イベント ID: com/vmware/vcloud/event/user/remove、com/vmware/vcloud/event/user/delete)

Vormetric Data Security (イベント ID: DAO0090I)

iT-CUBE agileSI (イベント ID: AU8、U0)

UBA : 短期間でのユーザー・アカウントの作成と削除

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 短期間でのユーザー・アカウントの作成と削除

デフォルトで有効

True

デフォルトの senseValue

15

説明

短期間にユーザー・アカウントが作成および削除されたことを検出します。

サポート・ルール

- BB:UBA : ユーザー・アカウントの作成 (BB:UBA : User Account Created)
- BB:UBA : ユーザー・アカウントの削除 (BB:UBA : User Account Deleted)
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

UBA : 休止アカウントが使用されました

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 休止アカウントが使用されました

デフォルトで有効

True

デフォルトの senseValue

10

説明

休止と判断されているアカウントからログインが正常に行われたことが検出されました。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証の失敗 (BB:CategoryDefinition: Authentication Failures)

データ・ソース

イベントにユーザー名が示されている任意のサポート対象ログ・ソース。

UBA : 休止アカウント使用の試み (UBA : Dormant Account Use Attempted)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 休止アカウント使用の試み (UBA : Dormant Account Use Attempted)

デフォルトで有効

True

デフォルトの senseValue

15

説明

休止と判断されているアカウントからログインが試行され、失敗したことが検出されました。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証の失敗 (BB:CategoryDefinition: Authentication Failures)

データ・ソース

3Com 8800 シリーズ・スイッチ、APC UPS、AhnLab Policy Center APC、Application Security DbProtect、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba ClearPass Policy Manager、Aruba モビリティー・コントローラー、Avaya VPN Gateway、Barracuda Web Application Firewall、Barracuda Web Filter、Bit9 Security Platform、Box、Bridgewater Systems AAA サービス・コントローラー、Brocade FabricOS、CA ACF2、CA SiteMinder、CRE システム、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、Catalyst スイッチ 用 Cisco CatOS、Cisco FireSIGHT Management Center、Cisco ファイアウォール・サービス・モジュール (FWSM)、Cisco IOS、Cisco Identity Services Engine、Cisco Intrusion Prevention System (IPS)、Cisco IronPort、Cisco NAC アプライアンス、Cisco Nexus、Cisco PIX Firewall、Cisco VPN 3000 シリーズ・コンセントレーター、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、Citrix Access Gateway、Citrix NetScaler、CloudPassage Halo、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、Cyber-Ark Vault、CyberGuard TSP Firewall/VPN、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、 ESET Remote Administrator、Enterprise-IT-Security.com SF-Sherlock、Epic SIEM、イベント CRE インジェクション、Extreme 800 シリーズ・スイッチ、Extreme Dragon Network IPS、Extreme HiPath、Extreme Matrix E1 スイッチ、Extreme Matrix K/N/S シリーズ・スイッチ、Extreme Networks ExtremeWare オペレーティング・システム (OS)、Extreme スタック可能スイッチおよびスタンドアロン・スイッチ、Extreme XSR セキュリティー・ルーター、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、Forcepoint Sidewinder、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、HyTrust CloudControl、IBM AIX Audit、IBM AIX サーバー、IBM Bluemix プラットフォーム、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper Junos WebApp Secure、Juniper Networks ファイアウォールおよび 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 セキュリティー・イベント・ログ、 Motorola SymbolAP、Netskope Active、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500、 Nortel イーサネット・ルーティング・スイッチ 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 ソフトウェア、Oracle Acme Packet SBC、Oracle Audit Vault、Oracle BEA WebLogic、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Palo Alto PA シリーズ、Pirean Access: One、PostFix MailTransferAgent、ProFTPD サーバ

ー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、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 シリーズ・アプライアンス、Top Layer IPS、Trend Micro Deep Discovery Email Inspector、Trend Micro Deep Discovery Inspector、Trend Micro Deep Security、Tripwire Enterprise、Tropos Control、ユニバーサル DSM、VMware vCloud Director、Venustech Venusense Security Platform、Vormetric Data Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : 期限切れアカウントの使用

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 期限切れアカウントの使用 (旧称「UBA : 孤立、取り消し、または中断状態のアカウントが使用されました」)

デフォルトで有効

True

デフォルトの senseValue

10

説明

ユーザーが無効なアカウントまたは期限切れのアカウントでローカル・システムにログインしようとしたことを示します。このルールは、アカウントが危険にさらされたことを示す場合もあります。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 期限切れアカウントに対する認証 (BB:CategoryDefinition: Authentication to Expired Account)

データ・ソース

Catalyst スイッチ用 Cisco CatOS、Cisco 侵入防御システム (IPS)、Extreme Dragon Network IPS、IBM Proventia Network Intrusion Prevention System (IPS)、Juniper Junos WebApp Secure、Microsoft IAS Server、Microsoft Windows セキュリティー・イベント・ログ

UBA : 初回の特権エスカレーション

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 初回の特権エスカレーション

デフォルトで有効

True

デフォルトの **senseValue**

10

説明

ユーザーが特権アクセスをはじめて行使したことを示します。この報告ルールは、ベースライン設定の目的でユーザー動作を追跡できるようにするために無効にできます。

サポート・ルール

BB:UBA : 特権ユーザー、初回の特権使用 (ロジック) (BB:UBA : Privileged User, First Time Privilege Use (logic))

データ・ソース

APC UPS、AhnLab Policy Center APC、Amazon AWS CloudTrail、Application Security DbProtect、Arbor Networks Pravail、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba ClearPass Policy Manager、Aruba モビリティー・コントローラー、Avaya VPN Gateway、Barracuda Web Application Firewall、Bit9 Security Platform、Bluemix プラットフォーム、Box、Bridgewater Systems AAA サービス・コントローラー、Brocade FabricOS、CA ACF2、CA Top Secret、CRE システム、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、Catalyst スイッチ用 Cisco CatOS、Cisco FireSIGHT Management Center、Cisco ファイアウォール・サービス・モジュール (FWSM)、Cisco IOS、Cisco Identity Services Engine、Cisco Intrusion Prevention System (IPS)、Cisco IronPort、Cisco NAC アプライアンス、Cisco Nexus、Cisco PIX Firewall、Cisco VPN 3000 シリーズ・コンセントレーター、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、Citrix Access Gateway、Citrix NetScaler、CloudPassage Halo、Cloudera Navigator、CorreLog Agent for IBM zOS、カスタム・ルール・エンジン、Cyber-Ark Vault、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterprise-IT-Security.com SF-Sherlock、Epic SIEM、イベント CRE インジェクション、Extreme 800 シリーズ・スイッチ、Extreme Dragon Network IPS、Extreme HiPath、Extreme NAC、Extreme NetsightASM、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP ASM、F5 ネットワークス BIG-IP LTM、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、H3C Comware Platform、HBGary Active Defense、HP Network Automation、Honeycomb Lexicon File Integrity Monitor、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500、Nortel イーサネット・ルーティング・スイッチ 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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean 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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Critical System Protection、Symantec Endpoint Protection、Symantec System Center、システム通知、ThreatGRID Malware Threat Intelligence Platform、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : 新しいアカウントの使用が検出されました

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 新しいアカウントの使用が検出されました

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーがはじめて正常にログインしたことを示す報告機能を提供します。この報告ルールは、ベースライン設定の目的で一時的に無効にできます。

サポート・ルール

BB:UBA : ユーザーの初回アクセス (ロジック) (BB:UBA : User First Time Access (logic))

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

UBA : 疑わしい特権アクティビティー (初回に観察された特権使用)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしい特権アクティビティー (初回に観察された特権使用)

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが、これまでに実行していなかった特権アクションを実行したことを示します。観測結果は、セットのマップ「UBA : Observed Activities by Low Level Category and Username」に保持されます。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : 特権アクティビティー (BB:UBA : Privileged Activity)

データ・ソース

APC UPS、AhnLab Policy Center APC、Amazon AWS CloudTrail、Application Security DbProtect、Arbor Networks Pravail、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba ClearPass Policy Manager、Aruba モビリティー・コントローラー、Avaya VPN Gateway、Barracuda Web Application Firewall、Bit9 Security Platform、Bluemix プラットフォーム、Box、Bridgewater Systems AAA サービス・コントローラー、Brocade FabricOS、CA ACF2、CA Top Secret、CRE システム、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、Catalyst スイッチ用 Cisco CatOS、Cisco FireSIGHT Management Center、Cisco ファイアウォール・サービス・モジュール (FWSM)、Cisco IOS、Cisco Identity Services Engine、Cisco Intrusion Prevention System (IPS)、Cisco IronPort、Cisco NAC アプライアンス、Cisco Nexus、Cisco PIX Firewall、Cisco VPN 3000 シリーズ・コンセントレーター、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、Citrix Access Gateway、Citrix NetScaler、CloudPassage Halo、Cloudera Navigator、CorreLog Agent for IBM zOS、カスタム・ルール・エンジン、Cyber-Ark Vault、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterprise-IT-Security.com SF-Sherlock、Epic SIEM、イベント CRE インジェクション、Extreme 800 シリーズ・スイッチ、Extreme Dragon Network IPS、Extreme HiPath、Extreme NAC、Extreme NetsightASM、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP ASM、F5 ネットワークス BIG-IP LTM、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、H3C Comware Platform、HBGary Active Defense、HP Network Automation、Honeycomb Lexicon File Integrity Monitor、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500、Nortel イーサネット・ルーティング・スイッチ 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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean 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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Critical System Protection、Symantec Endpoint Protection、Symantec System Center、システム通知、ThreatGRID Malware Threat Intelligence Platform、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : 疑わしい特権アクティビティー (めったに使用されない特権)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしい特権アクティビティー (めったに使用されない特権)

デフォルトで有効

True

デフォルトの senseValue

10

説明

ユーザーが、最近実行していなかった特権アクションを実行したことを示します。観測結果は、セットのマップ「UBA : Recent Activities by Low Level Category and Username」に保持されます。このイベントの機密性は、「UBA : Recent Activities by Low Level Category and Username」に対するセットのリファレンス・マップの TTL (存続時間) を変更することで変更できます。TTL を増やすと、機密性が低下します。TTL を減らすと、機密性が向上します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : 特権アクティビティー (BB:UBA : Privileged Activity)

データ・ソース

APC UPS、AhnLab Policy Center APC、Amazon AWS CloudTrail、Application Security DbProtect、Arbor Networks Pravail、Arpeggio SIFT-IT、Array Networks SSL VPN アクセス・ゲートウェイ、Aruba ClearPass Policy Manager、Aruba モビリティー・コントローラー、Avaya VPN Gateway、Barracuda Web Application Firewall、Bit9 Security Platform、Bluemix プラットフォーム、Box、Bridgewater Systems AAA サービス・コントローラー、Brocade FabricOS、CA ACF2、CA Top Secret、CRE システム、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、Catalyst スイッチ用 Cisco CatOS、Cisco FireSIGHT Management Center、Cisco ファイアウォール・サービス・モジュール (FWSM)、Cisco IOS、Cisco Identity Services Engine、Cisco Intrusion Prevention System (IPS)、Cisco IronPort、Cisco NAC アプライアンス、Cisco Nexus、Cisco PIX Firewall、Cisco VPN 3000 シリーズ・コンセントレーター、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、Citrix Access Gateway、Citrix NetScaler、CloudPassage Halo、Cloudera Navigator、CorreLog Agent for IBM zOS、カスタム・ルール・エンジン、Cyber-Ark Vault、DCN DCS/DCRS シリーズ、DG Technology MEAS、EMC VMWare、Enterasys Matrix K/N/S シリーズ・スイッチ、Enterprise-IT-Security.com SF-Sherlock、Epic SIEM、イベント CRE インジェクション、Extreme 800 シリーズ・スイッチ、Extreme Dragon Network IPS、Extreme HiPath、Extreme NAC、Extreme NetsightASM、F5 ネットワークス BIG-IP APM、F5 ネットワークス

BIG-IP ASM、F5 ネットワークス BIG-IP LTM、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、H3C Comware Platform、HBGary Active Defense、HP Network Automation、Honeycomb Lexicon File Integrity Monitor、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500、Nortel イーサネット・ルーティング・スイッチ 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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean 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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Critical System Protection、Symantec Endpoint Protection、Symantec System Center、システム通知、ThreatGRID Malware Threat Intelligence Platform、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X シリーズ・アプライアンス、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 : 中断状態のアカウントの使用のユーザー試行

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 中断状態のアカウントの使用のユーザー試行

デフォルトで有効

True

デフォルトの senseValue

10

説明

使用停止アカウントまたは無効なアカウントにユーザーがアクセスしようとしたことを検出します。

サポート・ルール

- CategoryDefinition: 無効化されたアカウントに対する認証 (BB:CategoryDefinition: Authentication to Disabled Account)
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Cisco 侵入防御システム (IPS)、Extreme Dragon Network IPS、IBM Proventia Network Intrusion Prevention System (IPS)、Microsoft ISA、Microsoft Windows セキュリティー・イベント・ログ

UBA : ユーザーが休止状態になりました (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注: このルールは現在サポートされていません。 休止アカウントの情報は、V3.2.0 以降の UBA ダッシュボードで表示できます。詳しくは、 43 ページの『休止アカウント』を参照してください。

UBA : User Has Gone Dormant (no activity anomaly rule)

UBA : 休止アカウントが見つかりました (特権)

デフォルトで有効

False

デフォルトの senseValue

10

説明

このルールをアクティブにするには、「UBA : User Has Gone Dormant (no activity anomaly rule)」が有効になっている必要があります。

このルールは、ユーザー名のアクティビティー数が 80% より大きく変更されたことを示します。「UBA : User Dormant Account Found (privileged)」と「UBA : User Has Gone Dormant (no activity anomaly rule)」は、ユーザーによるアクティビティーの生成が長期間停止していることを示すためのルールです。この状態は、ユーザー名に関連付けられているアクティビティーが長期間停止していることから、そのユーザーがアクセスする必要がなくなったことを示している場合があります。ユーザー名のアクティビティーが短期間 (デフォルトでは 14 日) のうちに減少してゼロに近付き、ゼロになる前に新しいベースラ

イン (デフォルトでは 28 日) が設定された場合は、誤ったアラームが生成される可能性があります。「UBA : User Dormant Account Found (privileged)」に対する応答頻度制限が、各ユーザー名に対する長い期間以上の期間に設定されている場合は、こうした誤ったアラームがユーザーのリスク・スコアに影響することはありません。

注**:** ユーザー名のアクティビティーが短期間 (デフォルトでは 14 日) に減少してゼロに近付き、ゼロになる前に新しいベースライン (デフォルトでは 28 日) が設定された場合、「UBA : User Has Gone Dormant (no activity anomaly rule)」については誤ったアラームである可能性があります。この誤ったアラームは、「UBA : User Dormant Account Found (privileged)」に対する応答頻度制限がユーザー名あたりの長い間隔以上の期間に設定されていても、ユーザーのリスク・スコアに影響しません。

サポート・ルール

UBA : 休止アカウントが見つかりました (特権)

必須の構成

ルール「UBA : 休止アカウントが見つかりました (特権)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

参照動作

UBA : ビジネス/サービスの Web サイトをブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ビジネス/サービスの Web サイトをブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にユーザーがアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : コミュニケーション Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : コミュニケーション Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : エンターテイメント Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : エンターテイメント Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : ギャンブル Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ギャンブル Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : 情報技術 Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 情報技術 Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : 求職 Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 求職 Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

15

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : ライフスタイルの Web サイトをブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ライフスタイルの Web サイトをブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にユーザーがアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : 悪意のある Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 悪意のある Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

15

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : 混合コンテンツ/アダルト・コンテンツを含む可能性がある Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 混合コンテンツ/アダルト・コンテンツを含む可能性がある Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

10

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : フィッシング Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : フィッシング Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

15

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : ポルノ Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ポルノ Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

10

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : 詐欺/疑わしい/違法な Web サイトのブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 詐欺/疑わしい/違法な Web サイトのブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

ユーザーが、セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : 未分類の Web サイトをブラウズ

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 未分類の Web サイトをブラウズ

デフォルトで有効

True

デフォルトの senseValue

5

説明

セキュリティー・リスクや法的リスクの上昇を示す可能性がある URL にユーザーがアクセスしました。

サポート・ルール

BB:UBA : URL カテゴリー・フィルター (BB:UBA : URL Category Filter)

データ・ソース

Blue Coat SG アプライアンス、Cisco IronPort、McAfee Web Gateway、Check Point、Squid Web プロキシー、Palo Alto PA シリーズ

UBA : リスクのある URL にアクセスしているユーザー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : リスクのある URL にアクセスしているユーザー (旧称「X-Force リスクのある URL (X-Force Risky URL)」)

デフォルトで有効

True

説明

このルールは、ローカル・ユーザーが疑わしいオンライン・コンテンツにアクセスしている場合にそれを検出します。

サポート・ルール

- X-Force Risky URL
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- 「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。
- ルール「X-Force リスクのある URL (X-Force Risky URL)」を有効化します。

データ・ソース

Juniper SRX シリーズ・サービス・ゲートウェイ、Microsoft ISA、Pulse Secure Pulse Connect Secure

クラウド

UBA : 無許可ユーザーによる AWS コンソールのアクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 無許可ユーザーによる AWS コンソールのアクセス

デフォルトで有効

False

デフォルトの senseValue

10

説明

「AWS - 標準ユーザー」リファレンス・セット内の許可リスト外のユーザーによる Amazon Web Services (AWS) コンソールへの無許可アクセスを検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- IBM Security App Exchange からパッケージ IBM QRadar Content Extension for Monitoring Amazon AWS をインストールします。
- リファレンス・セット「UBA : ドメイン・コントローラー管理者 (UBA : Domain Controller Administrators)」に適切な値を追加します。ログ・ソース Amazon AWS Cloudtrail を構成します。

データ・ソース

Amazon AWS CloudTrail (イベント ID: ConsoleLogin)

UBA : 非標準ユーザーによる AWS リソースへのアクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 非標準ユーザーによる AWS リソースへのアクセス

デフォルトで有効

False

デフォルトの senseValue

10

説明

Amazon Web Services (AWS) リソースにアクセスしようとしている非標準ユーザーを検出します。

データ・ソース

Amazon Web Services 拡張

ドメイン・コントローラー

UBA : DPAPI バックアップのマスター鍵リカバリーの試行

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : DPAPI バックアップのマスター鍵リカバリーの試行

デフォルトで有効

True

デフォルトの senseValue

10

説明

DPAPI マスター鍵のリカバリーが試行されたことを検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4693)

UBA : Kerberos アカウント列挙の検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Kerberos アカウント列挙の検出

デフォルトで有効

True

デフォルトの senseValue

10

説明

同じ送信元 IP から Kerberos 要求を行うために大量のユーザー名が使用されていることを検出することにより、Kerberos アカウント列挙を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4768)

UBA : 同一ユーザーの Kerberos 認証の複数回失敗

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 同一ユーザーの Kerberos 認証の複数回失敗

デフォルトで有効

False

デフォルトの senseValue

15

説明

Kerberos 認証チケットの複数回の拒否または失敗を検出します。

サポート・ルール

- BB:UBA : 共通ログ・ソース・フィルター (BB:UBA : Common Log Source Filters)
- BB:UBA : Kerberos 認証の失敗 (BB:UBA : Kerberos Authentication Failures)

データ・ソース

Microsoft Windows Security Event Log

UBA : 非管理者によるドメイン・コントローラーへのアクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 非管理者によるドメイン・コントローラーへのアクセス

デフォルトで有効

False

デフォルトの senseValue

5

説明

非管理者アカウントによるドメイン・コントローラーへのアクセス試行を検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- BB:CategoryDefinition: 認証の失敗 (BB:CategoryDefinition: Authentication Failures)

必須の構成

リファレンス・セット「UBA : ドメイン・コントローラー (UBA : Domain Controllers)」および「UBA : ドメイン・コントローラー管理者 (UBA : Domain Controller Administrators)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Pass the Hash

デフォルトで有効

False

デフォルトの senseValue

15

説明

Pass the Hash エクスプロイトにより生成された可能性がある Windows ログオン・イベントを検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : 信頼されたドメイン (UBA : Trusted Domains)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4624)

UBA : ディレクトリー・サービス列挙の可能性 (UBA : Possible Directory Services Enumeration)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ディレクトリー・サービス列挙の可能性 (UBA : Possible Directory Services Enumeration)

デフォルトで有効

False

デフォルトの senseValue

5

説明

ディレクトリー・サービス列挙に対するスキャン行為の試行を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : ドメイン・コントローラー管理者 (UBA : Domain Controller Administrators)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4661)

UBA : ドメイン・コントローラーに対する SMB セッション列挙の可能性 (UBA : Possible SMB Session Enumeration on a Domain Controller)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ドメイン・コントローラーに対する SMB セッション列挙の可能性 (UBA : Possible SMB Session Enumeration on a Domain Controller)

デフォルトで有効

False

デフォルトの senseValue

10

説明

ドメイン・コントローラーに対する SMB 列挙の試行を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

以下のリファレンス・セットに適切な値を追加します。

- UBA : ドメイン・コントローラー
- UBA : ドメイン・コントローラー管理者

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 5140)

UBA : TGT 偽造の可能性

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : TGT 偽造の可能性

デフォルトで有効

False

デフォルトの senseValue

15

説明

ドメイン名の異常が含まれている Kerberos TGT を検出します。これは、Pass the Ticket エクスプロイトを使用して生成されたチケットを示している可能性があります。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : 信頼されたドメイン (UBA : Trusted Domains)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4768)

UBA : TGT PAC 偽造の可能性

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : TGT PAC 偽造の可能性

デフォルトで有効

False

デフォルトの senseValue

10

説明

Kerberos TGS からサービス・チケットを取得するために偽造 PAC 証明書が使用されたことを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : TCT PAC 偽造パッチ適用済みサーバー (BB:UBA : TCT PAC Forgery Patched Server)
- BB:UBA : TCT PAC 偽造パッチ未適用サーバー (BB:UBA : TCT PAC Forgery Unpatched Server)

必須の構成

リファレンス・セット「UBA : ドメイン・コントローラー管理者 (UBA : Domain Controller Administrators)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4672、4769)

UBA : 非ドメイン・コントローラーからの複製要求

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 非ドメイン・コントローラーからの複製要求

デフォルトで有効

True

デフォルトの senseValue

5

説明

不正なドメイン・コントローラーからの複製要求を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : ドメイン・コントローラー管理者 (UBA : Domain Controller Administrators)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4662)

UBA : 複数のホストによって使用される TGT チケット (UBA : TGT Ticket Used by Multiple Hosts)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 複数のホストによって使用される TGT チケット (UBA : TGT Ticket Used by Multiple Hosts)

デフォルトで有効

False

デフォルトの senseValue

15

説明

複数の異なるコンピューターでの Kerberos TGT チケットの使用を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

UBA : Kerberos アカウント・マッピング (UBA : Kerberos Account Mapping)

このルールは、関連するリファレンス・セットを必要なデータで更新します。

必須の構成

ルール「UBA : Kerberos アカウント・マッピング (UBA : Kerberos Account Mapping)」を有効化します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4768)

エンドポイント

UBA : 非セキュアまたは非標準プロトコルの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 非セキュアまたは非標準プロトコルの検出

デフォルトで有効

False

デフォルトの senseValue

5

説明

セキュアでないまたは標準外のプロトコルと見なされる無許可のプロトコルで通信しているユーザーを検出します。許可されるプロトコルは、「UBA : Ports of Authorized Protocols」リファレンス・セットにデフォルト値 0 (QRadar イベントのポート) でリストされています。このルールを有効にする前に、ご使用の環境から「UBA : Ports of Authorized Protocols」リファレンス・セットを編集してフラグを設定してください。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : 保護されていないポート (BB:UBA : Insecure Ports)
-

必須の構成

リファレンス・セット「UBA : 許可されたプロトコルのポート (UBA : Ports Of Authorized Protocols)」に適切な値を追加します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : 持続 SSH セッションの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 持続 SSH セッションの検出

デフォルトで有効

True

デフォルトの senseValue

10

説明

10 時間を超えてアクティブの状態が続いている SSH セッションを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : SSH セッションのクローズ (BB:UBA : SSH Session Closed)
- BB:UBA : SSH セッションのオープン (BB:UBA : SSH Session Opened)

必須の構成

このルールでは、検出を正確に行うために、「SSH オープン」イベントと「SSH クローズ」イベントの両方が発生することが求められます。使用されるログ・ソースに、この両方のイベントのイベント ID が含まれていない場合、不正確な結果を受け取る可能性があります。データ・ソースを調べて、使用されているログ・ソースのイベント ID を確認してください。

データ・ソース (SSH オープン)

Centrify Infrastructure Services (イベント ID: 27100、27104)

Cisco IOS (イベント ID: %SSH-5-SSH2_SESSION、%SSH-SW2-5-SSH2_SESSION)

カスタム・ルール・エンジン (イベント ID: 18037、3071)

Cyber-Ark Vault (イベント ID: 378)

Extreme XSR セキュリティー・ルーター (イベント ID: NEW_SSH_CONNECTION)

フロー分類エンジン (イベント ID: 3071、18037)

Huawei S シリーズ・スイッチ (イベント ID: SSH/4/SFTP_REQ_RECORD)

HyTrust CloudControl (イベント ID: AUN0120、unknown)

IBM AIX サーバー (イベント ID: sshd2 connection established、ssh-server connect、ssh-server session open)

IBM DataPower (イベント ID: 0x8100011e、0x810001e4、0x810001e5)

Juniper MX シリーズ、イーサネット・サービス・ルーター (イベント ID: SSH)

Juniper Networks AVT (イベント ID: SSH)

Mac OS X (イベント ID: OSX ssh session started)

OS サービスの Qidmap (イベント ID: Connection from、pam_open_session、pam_sm_open_session)

Solaris オペレーティング・システム認証メッセージ (イベント ID: ssh session opened)

ユニバーサル DSM (イベント ID: SSH オープン、SSH セッション開始)

データ・ソース (SSH クローズ)

Aruba モビリティー・コントローラー (イベント ID: sshd_disconnect)

Centrify Infrastructure Services (イベント ID: 27102)

Cisco IOS (イベント ID: %SSH-5-SSH_CLOSE、%SSH-SW2-5-SSH2_CLOSE、%SSH-5-SSH2_CLOSE)

カスタム・ルール・エンジン (イベント ID: 3072、18038、18040)

Cyber-Ark Vault (イベント ID: 380、381)

フロー分類エンジン (イベント ID: 3072、18038、18040)

Huawei S シリーズ・スイッチ (イベント ID: SSH/6/RECV_DISCONNECT)

IBM AIX サーバー (イベント ID: ssh-server disconnect、sshd2 connection lost、SSH Disconnect、sshd2 local disconnect、ssh-server session close)

OS サービスの Qidmap (イベント 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 (イベント ID: GWE24572)

ユニバーサル DSM (イベント ID: SSH 終了、SSH セッション終了、SSH クローズ)

UBA : インターネット設定の変更

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : インターネット設定の変更

デフォルトで有効

True

デフォルトの senseValue

15

説明

システムでのインターネット設定の変更を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4657)

UBA : マルウェア・アクティビティー - レジストリーの一括変更

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : マルウェア・アクティビティー - レジストリーの一括変更

デフォルトで有効

True

デフォルトの senseValue

15

説明

短い間隔で多数のレジストリー値を一括で変更する処理を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4657)

UBA : Netcat プロセス検出 (Linux)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Netcat プロセス検出 (Linux)

デフォルトで有効

True

デフォルトの senseValue

15

説明

Linux システムの netcat プロセスを検出します。

サポート・ルール

BB:UBA : 共通ログ・ソース・フィルター (BB:UBA : Common Log Source Filters)

データ・ソース

Linux OS (イベント ID: SYSCALL)

UBA : Netcat プロセス検出 (Windows)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Netcat プロセス検出 (Windows)

デフォルトで有効

True

デフォルトの senseValue

15

説明

Windows システム上の Netcat プロセスを検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4688)

UBA : ゴールド・ディスク・ホワイトリスト外のプロセス実行 (Linux)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ゴールド・ディスク・ホワイトリスト外のプロセス実行 (Linux)

デフォルトで有効

False

デフォルトの senseValue

15

説明

Linux システムで作成されたプロセスを検出し、そのプロセスがゴールド・ディスク・プロセス・ホワイトリストにない場合にアラートを出します。

注: このルールは、デフォルトでは無効になっています。このルールは、必ずリファレンス・セット「UBA : Gold Disk Process Whitelist - Linux」にホワイトリストとしてプロセス名を登録した後、または登録されているプロセス名を変更した後に有効にしてください。

必須の構成

リファレンス・セット「UBA : ゴールド・ディスク・プロセス・ホワイトリスト - Linux (UBA : Gold Disk Process Whitelist - Linux)」に適切な値を追加します。

サポート・ルール

BB:UBA : 共通ログ・ソース・フィルター (BB:UBA : Common Log Source Filters)

データ・ソース

Linux OS (イベント ID: SYSCALL)

UBA : ゴールド・ディスク・ホワイトリスト外のプロセス実行 (Windows)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ゴールド・ディスク・ホワイトリスト外のプロセス実行 (Windows)

デフォルトで有効

False

デフォルトの senseValue

15

説明

Windows システムで作成されたプロセスを検出し、そのプロセスがゴールド・ディスク・プロセス・ホワイトリストにない場合にアラートを出します。

注**:** このルールは、デフォルトでは無効になっています。このルールは、必ずリファレンス・セット「UBA : Gold Disk Process Whitelist - Windows」にホワイトリストとしてプロセス名を登録した後、または登録されているプロセス名を変更した後に有効にしてください。

必須の構成

リファレンス・セット「UBA : ゴールド・ディスク・プロセス・ホワイトリスト - Windows (UBA : Gold Disk Process Whitelist - Windows)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4688)

UBA : ランサムウェア動作の検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ランサムウェア動作の検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ランサムウェア感染中に一般的に見られる動作を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : Windows 共通プロセス (UBA : Windows Common Processes)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4663)

UBA : 制限付きプログラムの使用

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 制限付きプログラムの使用

デフォルトで有効

False

デフォルトの senseValue

5

説明

プロセスが作成され、そのプロセス名がリファレンス・セット「制限されたプログラムのファイル名 (UBA : Restricted Program Filenames)」にリストされているバイナリー名の 1 つと一致していることを示します。このリファレンス・セットは、デフォルトではブランクであるため、カスタマイズできます。リスク管理のためにモニターするファイル名をリファレンス・セットに設定できます。

モニター対象のプログラムの追加または削除について詳しくは、制限付きプログラムの管理を参照してください。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : 制限されたプログラムのファイル名 (UBA : Restricted Program Filenames)」に適切な値を追加します。

データ・ソース

Microsoft Windows Security Event Log

UBA : ユーザーによる疑わしいアプリケーションのインストール

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

以下のルールがサポートされます。

- UBA : ユーザーによる疑わしいアプリケーションのインストール
- UBA : Populate Authorized Applications

デフォルトで有効

False

デフォルトの senseValue

15

説明

アプリケーションのインストール・イベントを検出し、疑わしいアプリケーションが検出されたときに警告します。注: リファレンス・セット「UBA : Authorized Applications」には、組織で許可されているアプリケーション名を取り込みます。ルール「UBA : Populate Authorized Applications」を短期間有効にして、このリファレンス・セットにデータを取り込むことができます。

ルール「UBA : Populate Authorized Applications」により、このルールが有効な間にインストールされたアプリケーションの名前がリファレンス・セット「UBA : Authorized Applications」に取り込まれます。注: このルールはデフォルトでは無効になっています。ユーザーがアプリケーションをインストールしている間に名前を取り込むために、短期間有効にしてください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : ユーザーによる新規プロセスの実行

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

以下のルールがサポートされます。

- UBA : ユーザーによる新規プロセスの実行
- UBA : Populate Process Filenames

デフォルトで有効

False

デフォルトの senseValue

15

説明

ユーザーによって作成されたプロセスを検出し、ユーザーが新しいプロセスを実行したときに警告します。

ルール「UBA: Populate Process Filenames」により、「UBA : ユーザーによる新規プロセスの実行」のユーティリティー・ルールとして使用されるリファレンス・セット「UBA : Process Filenames」にデータが取り込まれます。注: このルールはデフォルトでは無効になっています。このルールを短期間有効にしてファイル名を取り込んでください。

サポート・ルール

「BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)」、「UBA : プロセスのファイル名の設定 (UBA : Populate Process Filenames)」

必須の構成

リファレンス・セット「UBA : プロセスのファイル名 (UBA : Process Filenames)」に適切な値を追加します。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4688)

UBA : ボリューム・シャドー・コピーの作成

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ボリューム・シャドー・コピーの作成

デフォルトで有効

True

デフォルトの **senseValue**

15

説明

vssadmin.exe または Windows Management Instrumentation のコマンド・ライン (WMIC) を使用して作成されたシャドー・コピーを検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 1 または 4688)

引き出し

UBA : Abnormal data volume to external domain (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注**:** このルールは、機械学習分析「外部ドメインへの異常ボリューム・データ」に置き換えられています。

- UBA : Abnormal data volume to external domain
- UBA : 外部ドメインへの異常なデータ・ボリュームの検出

注**:** ADE ルールを有効にすると、UBA アプリおよび ご使用の QRadar システムのパフォーマンスに影響を与える可能性があります。

デフォルトで有効

False

デフォルトの **senseValue**

15

説明

UBA : Abnormal data volume to external domain このルールは、アノマリ検出エンジンを使用して、ユーザーのトラフィック使用状況をモニターし、外部ドメインへの異常なデータ・ボリュームのトラフィックに対してアラートを発行します。

UBA : 外部ドメインへの異常なデータ・ボリュームの検出 これは、同一の個別 ADE ルール「UBA : Abnormal data volume to external domain」をサポートする CRE ルールです。このルールは、アノマリ検出エンジンを使用して、ユーザーのトラフィック使用状況をモニターし、外部ドメインへの異常なデータ・ボリュームのトラフィックに対してアラートを発行します。

データ・ソース

Juniper SRX シリーズ・サービス・ゲートウェイ、Microsoft ISA、Pulse Secure Pulse Connect Secure

UBA : Abnormal Outbound Transfer Attempts (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注**:** このルールは、機械学習分析「異常なアウトバウンド転送の試行」に置き換えられています。詳しくは、 196 ページの『「異常なアウトバウンド転送の試行」分析の構成』を参照してください。

UBA : Abnormal Outbound Transfer Attempts (V2.4.0 での名前: UBA : Abnormal Outbound Attempts)

UBA : Abnormal Outbound Transfer Attempts Found

注**:** ADE ルールを有効にすると、UBA アプリおよび ご使用の QRadar システムのパフォーマンスに影響を与える可能性があります。

デフォルトで有効

False

デフォルトの **senseValue**

15

説明

UBA : Abnormal Outbound Transfer Attempts (ADE rule) このルールは、アノマリ検出エンジンを使用してアウトバウンド・トラフィックの使用状況をモニターし、異常な試行回数に対してアラートを発行します。

UBA : Abnormal Outbound Transfer Attempts Found これは、同一の個別 ADE ルール「UBA : Abnormal Outbound Attempts」をサポートする CRE ルールです。このルールは、アノマリ検出エンジンを使用してアウトバウンド・トラフィックの使用状況をモニターし、異常な試行回数に対してアラートを発行します。

データ・ソース

すべてのサポート対象ログ・ソース。

UBA : 高リスク・ユーザーによる大量アウトバウンド転送

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 高リスク・ユーザーによる大量アウトバウンド転送

デフォルトで有効

False

デフォルトの senseValue

15

説明

高リスク・ユーザーによる 200,000 バイト以上のアウトバウンド転送を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

CEP 送信バイト数が定義されているログ・ソース。

UBA : 複数のファイル転送ブロック後のファイル転送

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 複数のファイル転送ブロック後のファイル転送

デフォルトで有効

True

デフォルトの senseValue

10

説明

最初はブロックされたが、その後 5 分以内にアップロードが成功しているファイル・アップロードをチェックすることにより、引き出しを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : ファイル転送のブロック (BB:UBA : Blocked File Transfer)
- BB:UBA : ファイル転送の成功 (BB:UBA : Successful File Transfer)

必須の構成

このルールでは、検出を正確に行うために、「ファイル転送のブロック (Blocked file transfers)」イベントと「ファイル転送の成功 (Successful file transfers)」イベントの両方が発生することが求められます。使用されるログ・ソースに、この両方のイベントのイベント ID が含まれていない場合、不正確な結果を受け取る可能性があります。データ・ソースを調べて、使用されているログ・ソースのイベント ID を確認してください。

データ・ソース (ファイル転送のブロック (Blocked file transfers))

Cilasoft QJRN/400 (イベント ID: C21020)

Cisco Call Manager (イベント ID: %UC_DRF-3-DRFSftpFailure)

Cisco IOS (イベント ID: %UPDATE-3-SFTP_TRANSFER_FAIL)

カスタム・ルール・エンジン (イベント ID: 18014、18071、18187、4032)

Extreme スタック可能スイッチおよびスタンドアロン・スイッチ (イベント ID: FFTP request failed)

フロー分類エンジン (イベント ID: 4032、18187、18014、18071)

Forcepoint Sidewinder (イベント ID: FTP Permits、denied ftp command)

IBM i (イベント ID: 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 侵入検知防御 (IDP) (イベント ID: TFTP:AUDIT:READ-FAILED)

Microsoft IIS (イベント ID: 530)

Microsoft Operations Manager (イベント ID: 22095)

OSSEC (イベント ID: 11504、11512)

ユニバーサル DSM (イベント ID: FTP アクション拒否、TFTP セッション拒否、FTP 拒否、ファイル転送拒否)

WatchGuard Fireware OS (イベント ID:
1CFF0002、1CFF0006、1CFF0007、1CFF0009、1CFF0001,1CFF0019、1CFF0000、1CFF0003)

データ・ソース (ファイル転送の成功 (Successful file transfers))

Cilasoft QJRN/400 (イベント ID: C21031)

Cisco FireSIGHT Management Center (イベント ID: FILE_EVENT、FILE_EVENT_0)

Cisco IOS (イベント ID: %FTPSERVER-6-NEWCONN)

Cisco IronPort (イベント ID: FTP_connection)

カスタム・ルール・エンジン (イベント ID: 18010、4031、18431、18183)

DG Technology MEAS (イベント ID: 119-003、119-070)

フロー分類エンジン (イベント ID: 18010、4031、18431、18183)

フロー・デバイス・タイプ (イベント ID: 21984、21879、51337、51336、35159、21910)

Huawei S シリーズ・スイッチ (イベント ID: FTPS/5/REQUEST)

IBM Proventia Network Intrusion Prevention System (IPS) (イベント ID: FTP、TFTP)

IBM i (イベント 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 シリーズ・イーサネット・サービス・ルーター (イベント ID: TFTP、FTP)

Juniper Networks AVT (イベント ID: TFTP、FTP)

Microsoft IIS (イベント ID: 150、125、225)

ProFTPD サーバー (イベント ID: FTP session opened)

Solaris オペレーティング・システム認証メッセージ (イベント ID: ftp connection)

SonicWALL SonicOS (イベント ID: 1112、1113)

Squid Web プロキシー (イベント ID: 3C0002_ALLOWED)

Trend InterScan VirusWall (イベント ID: Trend ftpconnect)

ユニバーサル DSM (イベント ID: ファイル転送、FTP オープン、FTP アクションの許可、TFTP セッションのオープン)

Verdasys Digital Guardian (イベント ID: Network Transfer Upload、Network Transfer Download)

WatchGuard Fireware OS (イベント ID: 2AFF0004、1CFF0019)

UBA : 疑わしいアクセスに続くデータ引き出し

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいアクセスに続くデータ引き出し

デフォルトで有効

False

デフォルトの senseValue

10

説明

異常な場所、制限された場所、または禁止された場所からのデータ・アクセスに続くデータ引き出しの試行を検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : データ引き出し (BB:UBA : Data Exfiltration)
- UBA : 制限された場所からのユーザー・アクセス
- UBA : 禁止された場所からのユーザー・アクセス
- UBA : User Geography, Access from Unusual Locations

必須の構成

以下のルールを有効化します。

- UBA : 制限された場所からのユーザー・アクセス
- UBA : 禁止された場所からのユーザー・アクセス
- UBA : User Geography, Access from Unusual Locations

データ・ソース

Cisco Stealthwatch (イベント ID: 45)

IBM Security Trusteer Apex Advanced Malware Protection (イベント 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 (イベント ID: 10003、10004)

UBA : ユーザー・ボリューム・アクティビティー異常 - 外部ドメインへのトラフィック (UBA : User Volume Activity Anomaly - Traffic to External Domains) (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注**:** このルールは現在サポートされていません。

- UBA : ユーザー・ボリューム・アクティビティー異常 - 外部ドメインへのトラフィック (UBA : User Volume Activity Anomaly - Traffic to External Domains)
- UBA : ユーザー・ボリューム・アクティビティー異常 - 外部ドメインへのトラフィック検出

デフォルトで有効

False

デフォルトの **senseValue**

10

説明

UBA : ユーザー・ボリューム・アクティビティー異常 **-** 外部ドメインへのトラフィック **(UBA : User Volume Activity Anomaly - Traffic to External Domains)** これは、同一の個別 ADE ルール「UBA : ユーザーのアクティビティー・ボリュームのアノマリ - トラフィック」をサポートする CRE ルールです。これは、アノマリ検出エンジンを使用して、ユーザーのトラフィックの使用状況をモニターし、通常ではない量のトラフィックについてアラートを発行します。

UBA : ユーザー・ボリューム・アクティビティー異常 **-** 外部ドメインへのトラフィック検出 これは、同一の個別ルール「UBA : ユーザー・ボリューム・アクティビティー異常 - 外部ドメインへのトラフィック (UBA : User Volume Activity Anomaly - Traffic to External Domains)」をサポートする CRE ルールです。このルールは、アノマリ検出エンジンを使用してアウトバウンド・トラフィックの使用状況をモニターし、異常な試行回数に対してアラートを発行します。

データ・ソース

Juniper SRX シリーズ・サービス・ゲートウェイ、Microsoft ISA、Pulse Secure Pulse Connect Secure

---

地域

UBA : 新規ロケーションからの異常なアカウント作成

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 新規ロケーションからの異常なアカウント作成

デフォルトで有効

True

デフォルトの **senseValue**

5

説明

新規ロケーションからの変則的なアカウント作成アクティビティーを検出します。

サポート・ルール

- BB:UBA : クラウド・エンドポイント (BB:UBA : Cloud Endpoints)
- BB:UBA : ユーザー・アカウントの作成 (BB:UBA : User Account Created)
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- UBA : ユーザー地域の変更

必須の構成

ルール「UBA : ユーザー地域の変更」を有効化します。

データ・ソース

AhnLab Policy Center APC (イベント ID: Administrator Account Add:Succeeded、ADD_ADMIN_ACCOUNT_SUCCESS)

Application Security DbProtect (イベント ID: Database user created、Login created - standard、Login added - Windows、Database role - created)

Aruba モビリティー・コントローラー (イベント ID: authmgr_user_add)

Bit9 Security Platform (イベント ID: User_group_created, User_group_modified, User_group_deleted, Console_user_created, Console_user_modified, Console_user_deleted)

Box (イベント ID: NEW_USER)

Brocade FabricOS (イベント ID: SEC-1180、SEC-3025、SEC-1182)

CA ACF2 (イベント ID: ACF2-L)

Check Point (イベント ID: User Added、device_added)

Cilasoft QJRN/400 (イベント: C20010、C20011)

Cisco Adaptive Security Appliance (ASA) (イベント ID: %PIX|ASA-5-502101、%ASA-5-502101)

Cisco ファイアウォール・サービス・モジュール (FWSM) (イベント ID: 502101、504001)

Cisco IOS (イベント ID: %APF-6-USER_NAME_CREATED)

Cisco Identity Services Engine (イベント ID: 86006)

Cisco NAC Appliance (イベント ID: CCA-1500)

Cisco PIX ファイアウォール (イベント 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 ファイアウォール (イベント ID: 502101)

Cisco ワイヤレス LAN コントローラー (イベント ID: %APF-6-USER_NAME_CREATED、1.3.6.1.4.1.9.9.515.0.2)

Cisco Wireless Services Module (WiSM) (イベント ID: %AAA-6-GUEST_ACCOUNT_CREATE、%APF-6-USER_NAME_CREATED)

CloudPassage Halo (イベント ID: Halo user added、Halo user re-added、Local account created (Linux のみ))

CorreLog Agent for IBM zOS (イベント ID: RACF ADDUSER: No Violations)

Cyber-Ark Vault (イベント ID: 180、2)

EMC VMWare (イベント ID: AccountCreatedEvent)

Extreme Dragon Network IPS (イベント ID: HOST:WIN:ACCOUNT-CREATED)

Extreme Matrix K/N/S シリーズ・スイッチ (イベント ID: created with、User Created Event)

Extreme NAC (イベント ID: Added registered user、Add Registered User)

フロー分類エンジン (イベント ID: 3031、3041)

Forcepoint Sidewinder (イベント ID: passport addition)

Fortinet FortiGate セキュリティー・ゲートウェイ (イベント ID: add、auth-logon)

Foundry Fastiron (イベント ID: SNMP_USER_ADDED)

HBGary Active Defense (イベント ID: CreateUser)

HP Network Automation (イベント ID: User Added)

IBM AIX 監査 (イベント ID: USER_Create SUCCEEDED)

IBM AIX サーバー (イベント ID: USER_Create)

IBM DB2 (イベント ID: ADD_USER SUCCESS)

IBM IMS (イベント ID: USER CREATED)

IBM QRadar Packet Capture (イベント ID: UserAdded)

IBM Resource Access Control Facility (RACF) (イベント ID: 80 10.0、80 10.2)

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

IBM Security Directory Server (イベント ID: SDS Audit)

IBM Security Identity Governance (イベント ID: 49、70004、42)

IBM Security Identity Manager (イベント ID: Add Success、Add SUBMITTED、Add SUCCESS)

IBM SmartCloud Orchestrator (イベント ID: user)

IBM Tivoli Access Manager for e-business (イベント ID: 13402 - Succeeded、13401 - Succeeded、13402 Command Succeeded、13401 Command Succeeded)

IBM i (イベント ID: GSL2401、MC@0300、GSL2402、M240100、CP_CRT)

Imperva SecureSphere (イベント ID: NEW_USERS_ACCOUNT、SOX_NEW_USERS、SOX - New users、New Users Account)

Itron スマート・メーター (イベント ID: CEUI-AUDIT-27、CEUI.AUDIT.26)

Juniper Networks Network and Security Manager (イベント ID: adm23303、aut20167、adm30407、aut20168、adm20716、adm20717)

Linux OS (イベント ID: ADD_USER)

McAfee Application/Change Control (イベント ID: USER_ACCOUNT_CREATED)

McAfee ePolicy Orchestrator (イベント ID: 20792)

Microsoft ISA (イベント ID: user added)

Microsoft SQL Server (イベント ID: CR - SU、CR - US、CR - SL、CR - LX、CR - AR、CR - WU、24127、24121、24075)

Microsoft SharePoint (イベント ID: 37)

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 624、645、1318、4720、4741)

NCC Group DDos Secure (イベント ID: 1003)

Netskope Active (イベント ID: Create Admin、Created new admin)

Novell eDirectory (イベント ID: CREATE_ACCOUNT)

OS サービスの Qidmap (イベント ID: User Account Added)

OSSEC (イベント ID: 5902、18110)

Okta (イベント 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 (イベント ID: add user)

Oracle Enterprise Manager (イベント ID: User Create (successful)、Computer Create (successful))

Oracle RDBMS 監査レコード (イベント ID: 51:1、51:0、CREATE USER-Standard:1、CREATE USER-Standard:0)

Oracle RDBMS OS 監査レコード (イベント ID: 51)

Pirean Access: One (イベント ID: IsimUserRegistration;*;1)

Pulse Secure Pulse Connect Secure (イベント ID: ADM23303、ADM20265、AUT20167、ADM30407、AUT20168)

RSA Authentication Manager (イベント ID: Added user、unknown、REMOTE_PRINCIPAL_CREATE、CREATE_PRINCIPAL、CREATE_AM_PRINCIPAL)

SIM 監査 (イベント ID: Configuration-UserAccount-AccountAdded)

STEALTHbits StealthINTERCEPT (イベント ID: Active DirectorycomputerObject AddedTrueFalse、Console ? user/group added、Console ■ user/group added、Active DirectoryuserObject AddedTrueFalse、Console - user/group added)

SafeNet DataSecure/KeySecure (イベント ID: Added user)

Salesforce Security Auditing (イベント ID: Created new Customer User、Created new user)

Skyhigh Networks Cloud Security Platform (イベント ID: 10016)

Solaris BSM (イベント ID: create user)

SonicWALL SonicOS (イベント ID: 558)

Symantec Encryption Management Server (イベント ID: ADMIN_IMPORTED_USER)

ThreatGRID Malware Threat Intelligence Platform (イベント ID: user-account-creation)

Trend Micro Deep Discovery Email Inspector (イベント ID: SYSTEM_EVENT_ACCOUNT_CREATED)

Trend Micro Deep Security (イベント ID: 650)

ユニバーサル DSM (イベント ID: 追加されたコンピューター・アカウント、追加されたユーザー・アカウント)

VMware vCloud Director (イベント ID: com/vmware/vcloud/event/user/create、com/vmware/vcloud/event/user/import)

Vormetric Data Security (イベント ID: DAO0089I)

iT-CUBE agileSI (イベント ID: U0、AU7)

UBA : 新規ロケーションからの異常なクラウド・アカウント作成

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 新規ロケーションからの異常なクラウド・アカウント作成

デフォルトで有効

True

デフォルトの senseValue

10

説明

新規ロケーションからのクラウド・アカウント作成アクティビティーを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:UBA : クラウド・エンドポイント (BB:UBA : Cloud Endpoints)
- BB:UBA : ユーザー・アカウントの作成 (BB:UBA : User Account Created)
- UBA : ユーザー地域の変更

必須の構成

ルール「UBA : ユーザー地域の変更」を有効化します。

データ・ソース

Amazon AWS CloudTrail (イベント ID: CreateUser)

Microsoft Office 365 (イベント ID: Add User-success、Add user-PartiallySucceded)

UBA : 複数の場所からのユーザー・アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 複数の場所からのユーザー・アクセス

デフォルトで有効

True

デフォルトの **senseValue**

5

説明

複数のロケーションまたはソースが同じユーザー・アカウントを同時に使用していることを示します。応答性が適合するように、突き合わせパラメーターと期間パラメーターを調整してください。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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 : 禁止された場所からのユーザー・アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 禁止された場所からのユーザー・アクセス

デフォルトで有効

False

デフォルトの senseValue

15

説明

「UBA : 許可される場所リスト (UBA : Allowed Location List)」にリストされていない場所からのユーザー・アクセスを検出します。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
-

必須の構成

リファレンス・セット「UBA : 許可される場所リスト (UBA : Allowed Location List)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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 : 制限された場所からのユーザー・アクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 制限された場所からのユーザー・アクセス

デフォルトで有効

False

デフォルトの **senseValue**

15

説明

「UBA : 制限される場所リスト (UBA : Restricted Location List)」にリストされている場所からのユーザー・アクセスを検出します。「地理的位置」から「UBA : 制限される場所リスト (UBA : Restricted Location List)」に国を追加できます。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
-

必須の構成

リファレンス・セット「UBA : 制限される場所リスト (UBA : Restricted Location List)」に適切な値を追加します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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 : ユーザー地域の変更

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ユーザー地域の変更

デフォルトで有効

True

デフォルトの senseValue

5

説明

一致は、ユーザーの最後のリモート・ログインとは異なる国からユーザーがリモートでログインしたことを示します。このルールは、特にルールとの一致が短時間の間に発生した場合、アカウント漏えいも示す場合があります。

サポート・ルール

- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- UBA : ユーザー地域マップ (UBA : User Geography Map)

必須の構成

ルール「UBA : ユーザー地域マップ (UBA : User Geography Map)」を有効化します。

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

サポート・ルール

User Geography Map

このルールは、関連するリファレンス・セットを必要なデータで更新します。

UBA : User Geography, Access from Unusual Locations

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : User Geography, Access from Unusual Locations

デフォルトで有効

True

デフォルトの **senseValue**

15

説明

ビルディング・ブロック・ルール「UBA : BB : Unusual Source Locations」に定義されている、ネットワークに対して通常ではない国で、ユーザーが認証できたことを示します。

サポート・ルール

- BB:UBA : 通常とは異なるソースの場所 (BB:UBA : Unusual Source Locations)
- BB:CategoryDefinition: 認証成功 (BB:CategoryDefinition: Authentication Success)
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

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 システム、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、構成可能な認証メッセージ・フィルター、CorreLog Agent for IBM zOS、CrowdStrike Falcon Host、カスタム・ルール・エンジン、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 スタック可能スイッチおよびスタンドアロン・スイッチ、F5 ネットワークス BIG-IP APM、F5 ネットワークス BIG-IP LTM、F5 ネットワークス FirePass、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、FreeRADIUS、H3C Comware Platform、HBGary Active Defense、HP Network Automation、HP Tandem、Huawei AR シリーズ・ルーター、Huawei S シリーズ・スイッチ、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 スマート・メーター、Juniper Junos OS プラットフォーム、Juniper MX シリーズ・イーサネット・サービス・ルーター、Juniper Networks ファイアウォールおよび 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 ネットワーク IPS アプライアンス、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 セキュリティー・イベント・ログ、Motorola SymbolAP、NCC Group DDos Secure、Netskope Active、Niara、Nortel Application Switch、Nortel Contivity VPN スイッチ、Nortel Contivity VPN スイッチ (廃止)、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 リスナー、Oracle Enterprise Manager、Oracle RDBMS 監査レコード、Oracle RDBMS OS 監査レコード、PGP Universal Server、Palo Alto Endpoint Security Manager、Palo Alto PA シリーズ、Pirean Access: One、ProFTPD サーバー、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 クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、Solaris BSM、Solaris オペレーティング・システム認証メッセージ、Solaris オペレーティング・システム Sendmail ログ、SonicWALL SonicOS、Sophos Astaro Security Gateway、Squid Web プロキシー、Starent Networks Home Agent (HA)、Stonesoft Management Center、Sybase ASE、Symantec Endpoint Protection、TippingPoint Intrusion Prevention System (IPS)、TippingPoint X Series アプライアンス、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、VormetricData Security、WatchGuard Fireware OS、genua genugate、iT-CUBE agileSI

ネットワーク・トラフィックおよび攻撃

UBA : D/DoS 攻撃の検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : D/DoS 攻撃の検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ユーザーによるネットワーク・サービス妨害 (DoS) 攻撃を検出します。

注: このルールを使用するには、その前に、以下の手順に従う必要があります。

1. 「管理」タブから「**UBA** の設定」をクリックします。
2. アセット・テーブル内でユーザー名を検索する場合は、「イベント・データまたはフロー・データにユーザー名がない場合、ユーザー名を探してアセットを検索します」チェック・ボックスを選択します。イベント内にユーザーがリストされていない場合、UBA アプリはアセットを使用して IP アドレスに対するユーザーを検索します。
3. このイベント・ルールを使用するには「Snort Open Source IDS」ログ・ソースが機能している必要があります。

サポート・ルール

- BB:UBA : 共通ログ・ソース・フィルター (BB:UBA : Common Log Source Filters)
- BB:CategoryDefinition: DDoS 攻撃イベント (BB:CategoryDefinition: DDoS Attack Events)
- BB:CategoryDefinition: ネットワーク DoS 攻撃 (BB:CategoryDefinition: Network DoS Attack)
- BB:CategoryDefinition: サービス DoS (BB:CategoryDefinition: Service DoS)

データ・ソース

Akamai KONA、Application Security DbProtect、Aruba モビリティー・コントローラー、Barracuda Web Application Firewall、Brocade FabricOS、CRE システム、Check Point、Cisco Adaptive Security Appliance (ASA)、Cisco ファイアウォール・サービス・モジュール (FWSM) 、Cisco IOS、Cisco Intrusion Prevention System (IPS)、Cisco PIX Firewall、Cisco Stealthwatch、Cisco ワイヤレス LAN コントローラー、Cisco Wireless Services Module (WiSM)、カスタム・ルール・エンジン、CyberGuard TSP Firewall/VPN、Enterprise-IT-Security.com SF-Sherlock、イベント CRE インジェクション、Extreme Dragon Network IPS、Extreme HiPath、F5 ネットワークス BIG-IP AFM、F5 ネットワークス BIG-IP ASM、F5 ネットワークス BIG-IP LTM、Fair Warning、FireEye、フロー分類エンジン、ForeScout CounterACT、Fortinet FortiGate セキュリティー・ゲートウェイ、Foundry Fastiron、Huawei AR シリーズ・ルーター、IBM Proventia Network Intrusion Prevention System (IPS)、IBM Security Network IPS (GX)、Imperva Incapsula、Juniper Junos OS プラットフォーム、Juniper Junos WebApp Secure、Juniper Networks ファイアウォールおよび VPN、Juniper Networks Intrusion Detection and Prevention (IDP)、Juniper Networks Network and Security Manager、McAfee Firewall Enterprise、McAfee IntruShield ネットワーク IPS アプライアンス、McAfee ePolicy Orchestrator、Motorola SymbolAP、NCC Group DDos Secure、Niksun 2005 v3.5、Nortel Application Switch、OS Services Qidmap、OSSEC、Palo Alto PA シリーズ、Radware AppWall、Radware DefensePro、Riverbed SteelCentral NetProfiler、STEALTHbits StealthINTERCEPT、SafeNet DataSecure/KeySecure、Sentrigo Hedgehog、Skyhigh Networks クラウド・セキュリティー・プラットフォーム、Snort オープン・ソース IDS、SonicWALL SonicOS、Squid Web プロキシー、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 : ハニートークン・アクティビティー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ハニートークン・アクティビティー

デフォルトで有効

False

デフォルトの senseValue

10

説明

ハニートークン・アカウントを使用したアクティビティーを検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : ハニートークン・アカウント (UBA : Honeytoken Accounts)」に適切な値を追加します。

ログ・ソース・グループ「UBA : ハニートークン・アカウントを含むシステム (UBA : Systems with Honeytoken Accounts)」に適切なログ・ソースを追加します。

データ・ソース

「UBA : ハニートークン・アカウントを含むシステム (UBA : Systems with Honeytoken Accounts)」ログ・ソース・グループに追加されたすべてのログ・ソース。

UBA : ネットワーク・トラフィック: モニターおよび分析プログラムの使用状況のキャプチャー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ネットワーク・トラフィック: モニターおよび分析プログラムの使用状況のキャプチャー

デフォルトで有効

False

デフォルトの senseValue

15

説明

プロセスが作成され、そのプロセス名がリファレンス・セット「UBA : Network Capture, Monitoring and Analysis Program Filenames」にリストされているバイナリー名の 1 つと一致していることを示します。このリファレンス・セットは、ネットワーク・パケット・キャプチャー・ソフトウェアのバイナリー名をリストします。リファレンス・セットには、一般的なネットワーク・プロトコル分析ソフトウェアのファイル名がいくつか事前設定されています。

モニター用のプログラムの追加または削除について詳しくは、ネットワーク・モニター・ツールの管理を参照してください。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

リファレンス・セット「UBA : ネットワーク・キャプチャー、モニター、および分析プログラムのファイル名 (UBA : Network Capture, Monitoring and Analysis Program Filenames)」に適切な値を追加します。

データ・ソース

Microsoft Windows Security Event Log

UBA : User Behavior, Session Anomaly by Destination (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注**:** このルールは現在サポートされていません。

UBA : User Behavior, Session Anomaly by Destination

UBA : User Behavior, Session Anomaly by Destination Found

注**:** ADE ルールを有効にすると、UBA アプリおよび ご使用の QRadar システムのパフォーマンスに影響を与える可能性があります。

デフォルトで有効

False

デフォルトの **senseValue**

10

説明

UBA : User Behavior, Session Anomaly by Destination 過去にアクセスしたのとは大きく異なる宛先 IP アドレスにユーザーがアクセスしていることを示します。このイベントは、必ずしも危険にさらされていることを示すものではありません。動作の変更は、ユーザーの職務や処理習慣が大きく変わったことを示す場合があります。

UBA : User Behavior, Session Anomaly by Destination Found これは、同一の個別 ADE ルール UBA : User Behavior, Session Anomaly by Destination をサポートする CRE ルールです。これは、ユーザーが過去にアクセスしたものとは大きく異なる宛先 IP アドレスにユーザーがアクセスしていることを示します。このイベントは、必ずしも危険にさらされていることを示すものではありません。動作の変更は、ユーザーの職務や処理習慣が大きく変わったことを示す場合があります。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : ユーザー・イベントの頻度アノマリ - カテゴリー (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注: このルールは、機械学習分析「アクティビティー (カテゴリー別)」に置き換えられています。詳しくは、 198 ページの『「アクティビティー (カテゴリー別)」分析の構成』を参照してください。

UBA : ユーザー・イベントの頻度アノマリ - カテゴリー (ADE ルール)

UBA : User Event Frequency Anomaly - Categories Found

注: ADE ルールを有効にすると、UBA アプリおよび ご使用の QRadar システムのパフォーマンスに影響を与える可能性があります。

デフォルトで有効

False

デフォルトの senseValue

5

説明

UBA : ユーザー・イベントの頻度アノマリ **-** カテゴリー アノマリ検出エンジンを使用して、ユーザーのイベントのカテゴリー分布をモニターします。通常ではない頻度の変化についてアラートを発行します。

UBA : User Event Frequency Anomaly - Categories Found これは、同一の個別 ADE ルール UBA : User Event Frequency Anomaly - Categories をサポートする CRE ルールです。これは、アノマリ検出エンジンを使用して、ユーザー・イベントのカテゴリーの分布をモニターします。通常ではない頻度の変化についてアラートを発行します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : ユーザー・ボリューム・アクティビティー異常 - 内部ドメインへのトラフィック (User Volume Activity Anomaly - Traffic to Internal Domains) (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注: このルールは現在サポートされていません。

- UBA : ユーザー・ボリューム・アクティビティー異常 - 内部ドメインへのトラフィック (User Volume Activity Anomaly - Traffic to Internal Domains)
- UBA : ユーザー・ボリューム・アクティビティー異常 - 内部ドメインへのトラフィック検出

デフォルトで有効

False

デフォルトの senseValue

10

説明

これは、同一の個別ルール「UBA : ユーザーのアクティビティー・ボリュームのアノマリ - 内部ドメインへのトラフィック (UBA : User Volume of Activity Anomaly - Traffic to Internal Domains)」をサポートする CRE ルールです。これは、アノマリ検出エンジンを使用して、ユーザーのトラフィックの使用状況をモニターし、通常ではない量のトラフィックについてアラートを発行します。

データ・ソース

Juniper SRX シリーズ・サービス・ゲートウェイ、Microsoft ISA、Pulse Secure Pulse Connect Secure

---

QRadar DNS Analyzer

詳しくは、IBM QRadar DNS Analyzer を参照してください。

UBA : ブラックリスト・ドメインへのアクセスの可能性

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ブラックリスト・ドメインへのアクセスの可能性

デフォルトで有効

False

デフォルトの senseValue

5

説明

ユーザーがブラックリスト・ドメインにアクセスした可能性があることを示すイベントを検出します。IBM QRadar DNS Analyzer アプリが必要です。

必須の構成

このルールを有効にする前に、IBM QRadar DNS Analyzer アプリをインストールする必要があります。詳しくは、IBM QRadar DNS Analyzer を参照してください。

データ・ソース

IBM QRadar DNS Analyzer

UBA : DGA ドメインへのアクセスの可能性

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : DGA ドメインへのアクセスの可能性

デフォルトで有効

False

デフォルトの senseValue

5

説明

ユーザーがドメイン生成アルゴリズム (DGA) によって生成されたドメインにアクセスした可能性があることを示すイベントを検出します。IBM QRadar DNS Analyzer アプリが必要です。

必須の構成

このルールを有効にする前に、IBM QRadar DNS Analyzer アプリをインストールする必要があります。詳しくは、IBM QRadar DNS Analyzer を参照してください。

データ・ソース

IBM QRadar DNS Analyzer

UBA : スクワッティング・ドメインへのアクセスの可能性

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : スクワッティング・ドメインへのアクセスの可能性

デフォルトで有効

False

デフォルトの senseValue

5

説明

ユーザーがスクワッティング・ドメインにアクセスした可能性があることを示すイベントを検出します。IBM QRadar DNS Analyzer アプリが必要です。

必須の構成

このルールを有効にする前に、IBM QRadar DNS Analyzer アプリをインストールする必要があります。詳しくは、IBM QRadar DNS Analyzer を参照してください。

データ・ソース

IBM QRadar DNS Analyzer

UBA : トンネリング・ドメインへのアクセスの可能性 (UBA : Potential Access to Tunneling Domain)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : トンネリング・ドメインへのアクセスの可能性 (UBA : Potential Access to Tunneling Domain)

デフォルトで有効

False

デフォルトの senseValue

5

説明

ユーザーがトンネリング・ドメインにアクセスした可能性があることを示すイベントを検出します。IBM DNS Analyzer アプリが必要です。

必須の構成

このルールを有効にする前に、IBM QRadar DNS Analyzer アプリをインストールする必要があります。詳しくは、IBM QRadar DNS Analyzer を参照してください。

データ・ソース

IBM QRadar DNS Analyzer

QRadar Network Insights (QNI)

QRadar V7.2.8 での QNI ルールのインストールについて詳しくは、QRadar Network Insights Content v7.2.8 を参照してください。

QRadar V7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

UBA : QNI - Access to Improperly Secured Service - Certificate Expired

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Access to Improperly Secured Service - Certificate Expired

デフォルトで有効

False

デフォルトの senseValue

5

説明

QRadar Network Insights (QNI) により、期限切れの証明書を使用している SSL/TLS セッションが検出されました。Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を使用する通信をサーバーとクライアント間で確立する場合は、証明書が使用されます。証明書は、その証明書がどれくらいの期間有効であるかを示す有効期限日とともに発行されます。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Access to Improperly Secured Service - Certificate Invalid

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Access to Improperly Secured Service - Certificate Invalid

デフォルトで有効

False

デフォルトの senseValue

5

説明

QRadar Network Insights (QNI) により、無効な証明書を使用している SSL/TLS セッションが検出されました。Secure Sockets Layer (SSL) を使用する通信をサーバーとクライアント間で確立する場合は、X.509 証明書が使用されます。証明書は、その証明書の有効期間の開始日を示す発効日とともに発行されます。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length

デフォルトで有効

False

デフォルトの senseValue

5

説明

QRadar Network Insights (QNI) により、2048 未満の低い公開鍵ビット・カウントを持つ証明書を使用している SSL/TLS セッションが検出されました。強度の低い公開鍵証明書 (1024 ビット未満) を使用しているサーバーの場合、セキュリティーに関するリスクが発生するおそれがあります。NIST 資料 800-57 では、2011 年以降、2048 ビット以上の RSA キーを使用することが推奨されています。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate

デフォルトで有効

False

デフォルトの senseValue

5

説明

QRadar Network Insights (QNI) により、自己署名証明書を使用している SSL/TLS セッションが検出されました。公開アプリケーションまたは実動サーバー・アプリケーションで使用される自己署名証明書が原

因で、リモートの攻撃者が中間者攻撃を開始できる場合があります。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - 機密コンテンツの外国地域への転送

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - 機密コンテンツの外国地域への転送

デフォルトで有効

False

デフォルトの **senseValue**

5

説明

アクセスが制限された国および地域に機密コンテンツが転送されようとしていることを検出します。これらの国および地域は、「アクセスが制限された国/地域 (Countries/Regions with Restricted Access)」ビルディング・ブロックで定義されています。このルールを有効化する前に、このビルディング・ブロックがお客様のビジネス・ユース・ケースに従って設定されていることを確認してください。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Observed File Hash Associated with Malware Threat

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Observed File Hash Associated with Malware Threat

デフォルトで有効

False

デフォルトの senseValue

15

説明

フロー・コンテンツに含まれているファイル・ハッシュが、Threat Intelligence データ・フィードに含まれている既知の有害なファイル・ハッシュと一致する場合に、このルールがトリガーされます。これは、何者かがネットワーク経由でマルウェアを送信したことを示しています。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Observed File Hash Seen Across Multiple Hosts

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Observed File Hash Seen Across Multiple Hosts

デフォルトで有効

False

デフォルトの senseValue

15

説明

マルウェアに関連付けられている同じファイル・ハッシュが複数の宛先に転送されていることが検出された場合に、このルールがトリガーされます。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient

デフォルトで有効

False

デフォルトの senseValue

5

説明

存在しない受信者アドレスに送信された、拒否された E メール・イベントがシステム内で検出された場合に、このルールがトリガーされます。これは、スパムやフィッシング行為が行われようとした可能性があることを示しています。組織に関連する QID を含めるには、「BB:CategoryDefinition: Rejected Email Recipient」ビルディング・ブロックを構成します。このビルディング・ブロックには、Microsoft Exchange、Linux OS [running sendmail]、Solaris オペレーティング・システム sendmail ログ、および Barracuda Spam and Virus Firewall の各 QID が事前に取り込まれます。これらの QID は、モニタリングに適しています。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers

デフォルトで有効

False

デフォルトの senseValue

5

説明

特定の期間に、スパムまたはフィッシングが疑われる同じ件名の E メールが複数の送信サーバーで送信されている場合に、このルールがトリガーされます。

必須の構成

この QNI ルールを有効にする前に、QRadar Network Insights コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。 QRadar 7.2.8 の場合は、QRadar Network Insights Content v7.2.8 を参照してください。QRadar 7.3.0 以降の場合は、QRadar Network Insights Content v7.3.0+ を参照してください。

データ・ソース

QRadar Network Insights (QNI)

スキャン行為

詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : DHCP サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : DHCP サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、DHCP サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : データベース・サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : データベース・サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、データベース・サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : DNS サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : DNS サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、DNS サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : FTP サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : FTP サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、FTP サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : ゲーム・サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ゲーム・サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、ゲーム・サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : 汎用 ICMP の通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 汎用 ICMP の通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、ICMP プロトコルを使用するサーバー上での通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : 汎用 TCP の通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 汎用 TCP の通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、共通 TCP ポートを使用するサーバー上での通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : 汎用 UDP の通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 汎用 UDP の通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、共通 UDP ポートを使用するサーバー上での通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : IRC サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : IRC サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、IRC サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : LDAP サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : LDAP サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、LDAP サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : メール・サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : メール・サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、メール・サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : メッセージング・サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : メッセージング・サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、メッセージング・サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : P2P サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : P2P サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの **senseValue**

15

説明

ネットワーク内で、P2P サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : プロキシー・サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : プロキシー・サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの **senseValue**

15

説明

ネットワーク内で、プロキシー・サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : RPC サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : RPC サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、RPC サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : SNMP サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : SNMP サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、SNMP サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : SSH サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : SSH サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、SSH サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : Web サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Web サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、Web サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

UBA : Windows サーバーの通常ではないスキャンの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Windows サーバーの通常ではないスキャンの検出

デフォルトで有効

False

デフォルトの senseValue

15

説明

ネットワーク内で、Windows サーバーへの通常ではないスキャンを検出します。

必須の構成

このルールを有効にする前に、IBM Security Reconnaissance コンテンツ・パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM Security Reconnaissance Content を参照してください。

システム・モニター (Sysmon)

詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

UBA : 一般的なエクスプロイト・ツールの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 一般的なエクスプロイト・ツールの検出

デフォルトで有効

False

デフォルトの senseValue

10

説明

キーロガーや PsExec などの一般的に使用されるエクスプロイト・ツールの使用を検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 一般的なエクスプロイト・ツールの検出 (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 一般的なエクスプロイト・ツールの検出 (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

キーロガーや PsExec などの一般的に使用されるエクスプロイト・ツールの使用を検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 悪意のあるプロセスの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 悪意のあるプロセスの検出

デフォルトで有効

False

デフォルトの senseValue

10

説明

Windows ホストでの悪意のある動作を示すプロセスを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : ネットワーク共有へのアクセス

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ネットワーク共有へのアクセス

デフォルトで有効

False

デフォルトの senseValue

10

説明

ネットワーク共有に関する疑わしいアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Sysmon ルール

UBA : 疑わしいリモート・スレッドを作成するプロセスの検出 (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいリモート・スレッドを作成するプロセスの検出 (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

リモート・マシン上で疑わしいスレッドを作成しているプロセスを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 危険にさらされたホスト上での疑わしいアクティビティー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 危険にさらされたホスト上での疑わしいアクティビティー

デフォルトで有効

False

デフォルトの senseValue

10

説明

危険にさらされたホスト上で実行されるアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 危険にさらされたホスト上での疑わしいアクティビティー (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 危険にさらされたホスト上での疑わしいアクティビティー (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

危険にさらされたホスト上で実行されるアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしい管理アクティビティーの検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしい管理アクティビティーの検出

デフォルトで有効

False

デフォルトの senseValue

10

説明

まれにしか実行されない疑わしい管理アクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしいコマンド・プロンプト・アクティビティー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいコマンド・プロンプト・アクティビティー

デフォルトで有効

False

デフォルトの senseValue

10

説明

コマンド・プロンプト・スクリプトに関連したアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : システム・レジストリーでの疑わしい項目 (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : システム・レジストリーでの疑わしい項目 (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

Windows レジストリーの変更または更新に関連する疑わしいアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしいイメージ・ロードの検出 (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいイメージ・ロードの検出 (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

機密のロケーションにアップロードされる疑わしいイメージを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしいパイプ・アクティビティー (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいパイプ・アクティビティー (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

Windows ホスト上のプロセス・パイプに関連する疑わしいアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしい PowerShell アクティビティー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしい PowerShell アクティビティー

デフォルトで有効

False

デフォルトの senseValue

10

説明

Microsoft PowerShell スクリプトに関連したアクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしい PowerShell アクティビティー (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしい PowerShell アクティビティー (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

Microsoft PowerShell スクリプトに関連したアクティビティーを検出します。このルールを使用するには、「イベント・データまたはフロー・データにユーザー名がない場合、ユーザー名を探してアセットを検索します」機能を有効にする必要があります。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしいスケジュール済みタスク・アクティビティー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいスケジュール済みタスク・アクティビティー

デフォルトで有効

False

デフォルトの senseValue

10

説明

Windows ホスト上での疑わしいスケジュール済みタスクの作成を検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしいサービス・アクティビティー

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいサービス・アクティビティー

デフォルトで有効

False

デフォルトの senseValue

10

説明

Windows コンピューターでの疑わしいサービス・アクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : 疑わしいサービス・アクティビティー (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : 疑わしいサービス・アクティビティー (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

Windows コンピューターでの疑わしいサービス・アクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

UBA : ユーザー・アクセス制御バイパスの検出 (アセット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ユーザー・アクセス制御バイパスの検出 (アセット)

デフォルトで有効

False

デフォルトの senseValue

10

説明

ユーザー・アクセス制御 (UAC) バイパスを示すプロセス・アクティビティーを検出します。

必須の構成

このルールを有効にする前に、IBM QRadar Content Extension for Sysmon パックをインストールし、そのルール・コンテンツを有効にする必要があります。詳しくは、IBM QRadar Content Extension for Sysmon を参照してください。

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ

脅威インテリジェンス

UBA : リスクのあるリソースへの異常アクセス (UBA : Abnormal visits to Risky Resources) (ADE ルール)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注: このルールは現在サポートされていません。

- UBA : リスクのあるリソースへの異常アクセス (UBA : Abnormal visits to Risky Resources)
- UBA : リスクのあるリソースへの異常アクセスの検出

注: ADE ルールを有効にすると、UBA アプリおよび ご使用の QRadar システムのパフォーマンスに影響を与える可能性があります。

デフォルトで有効

False

デフォルトの senseValue

15

説明

UBA : リスクのあるリソースへの異常アクセス **(UBA : Abnormal visits to Risky Resources)** このルールは、アノマリ検出エンジンを使用して、ユーザーがリスクのあるリソース (疑わしい URL、匿名化、マルウェア・ホストなど) にアクセスした回数をモニターし、アクセス回数の異常な変化があったときにアラートを発行します。

UBA : リスクのあるリソースへの異常アクセスの検出 これは、同一の個別 ADE ルール「UBA : リスクのあるリソースへの異常アクセス (UBA : Abnormal visits to Risky Resources)」をサポートする CRE ルールです。このルールは、アノマリ検出エンジンを使用して、ユーザーがリスクのあるリソース (疑わしい URL、匿名化、マルウェア・ホストなど) にアクセスした回数をモニターし、アクセス回数に異常な変化があったときにアラートを発行します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : Locky による IOC の検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : Locky による IOC の検出

デフォルトで有効

False

デフォルトの senseValue

10

説明

X-Force キャンペーン・フィードから取り込まれる URL または IP を使用して、Locky による危殆化を示す痕跡 (IOC) があるユーザー・コンピューターを検出します。

サポート・ルール

- BB:UBA : 共通ログ・ソース・フィルター (BB:UBA : Common Log Source Filters)
- BB:UBA : IP を使用した Locky の検出 (BB:UBA : Detect Locky Using IP)
- BB:UBA : URL を使用した Locky の検出 (BB:UBA : Detect Locky Using URL)

必須の構成

- リファレンス・セット「UBA : IOC-Locky IP」および「UBA : IOC-Locky URL」に適切な値を追加します。
- 「管理設定 **(Admin Settings)**」 > 「**UBA** の設定」で「アセットからのユーザー検索 (User Lookup from Asset)」を有効にします。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : WannaCry による IOC の検出

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : WannaCry による IOC の検出

デフォルトで有効

False

デフォルトの senseValue

10

説明

X-Force キャンペーン・フィードから取り込まれる URL、IP、またはハッシュを使用して、WannaCry による危殆化を示す痕跡 (IOC) があるユーザー・コンピューターを検出します。

サポート・ルール

- BB:UBA : 共通ログ・ソース・フィルター (BB:UBA : Common Log Source Filters)
- BB:UBA : ハッシュを使用した WannaCry の検出 (BB:UBA : Detect WannaCry Using Hashes)
- BB:UBA : IP を使用した WannaCry の検出 (BB:UBA : Detect WannaCry Using IP)
- BB:UBA : URL を使用した WannaCry の検出 (BB:UBA : Detect WannaCry Using URL)

必須の構成

- リファレンス・セット「UBA : マルウェア・アクティビティー WannaCry - ハッシュ (UBA : Malware Activity WannaCry - Hash)」、「UBA : マルウェア・アクティビティー WannaCry - IP (UBA : Malware Activity WannaCry - IP)」、および「UBA : マルウェア・アクティビティー WannaCry - URL (UBA : Malware Activity WannaCry - URL)」に適切な値を追加します。
- 「管理設定 **(Admin Settings)**」 > 「**UBA** の設定」で「アセットからのユーザー検索 (User Lookup from Asset)」を有効にします。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : ランサムウェアによって変更された ShellBag

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : ランサムウェアによって変更された ShellBag

デフォルトで有効

True

デフォルトの senseValue

10

説明

標準的なマルウェアまたはランサムウェアの振る舞いを示す ShellBag レジストリーの変更を検出します。

サポート・ルール

BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

データ・ソース

Microsoft Windows セキュリティー・イベント・ログ (イベント ID: 4657)

UBA : リスクのあるリソースにユーザーがアクセスしています

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

注: このルールは現在サポートされていません。

「UBA : リスクのあるリソースにユーザーがアクセスしています」は、V2.3.0 以降ではデフォルトで無効にされています。現在、このルールは以下のタイプでリストされ、デフォルトで有効にされるようになっています。

- UBA : リスクのある IP にアクセスしているユーザー (匿名化)
- UBA : リスクのある IP にアクセスしているユーザー (ボットネット)
- UBA : リスクのある IP にアクセスしているユーザー (動的)

- UBA : リスクのある IP にアクセスしているユーザー (マルウェア)
- UBA : リスクのある IP にアクセスしているユーザー (スパム)

デフォルトで有効

False

デフォルトの senseValue

15

説明

不適切であるかリスクが高いと考えられる外部リソース、または感染の兆候がある外部リソースにユーザーがアクセスしたことを示します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : リスクのある IP にアクセスしているユーザー (匿名化)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : リスクのある IP にアクセスしているユーザー (匿名化) (旧称「X-Force リスクのある IP (匿名化) (X-Force Risky IP, Anonymization)」)

デフォルトで有効

True

説明

このルールは、ローカル・ユーザーまたはローカル・ホストが外部の匿名化サービスに接続している場合にそれを検出します。

サポート・ルール

- X-Force Risky IP, Anonymization
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- 「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。
- ルール「X-Force リスクのある IP (匿名化) (X-Force Risky IP, Anonymization)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : リスクのある IP にアクセスしているユーザー (ボットネット)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : リスクのある IP にアクセスしているユーザー (ボットネット) (旧称「X-Force リスクのある IP (ボットネット) (X-Force Risky IP, Botnet)」)

デフォルトで有効

True

説明

このルールは、ローカル・ユーザーまたはローカル・ホストがボットネット・コマンドと制御サーバーに接続している場合にそれを検出します。

サポート・ルール

- X-Force Risky IP, Botnet
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- 「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。
- ルール「X-Force リスクのある IP (ボットネット) (X-Force Risky IP, Botnet)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : リスクのある IP にアクセスしているユーザー (動的)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : リスクのある IP にアクセスしているユーザー (動的) (旧称「X-Force リスクのある IP (動的) (X-Force Risky IP, Dynamic)」)

デフォルトで有効

True

説明

このルールは、ローカル・ユーザーまたはローカル・ホストが動的に割り当てられた IP アドレスに接続している場合にそれを検出します。

サポート・ルール

- X-Force Risky IP, Dynamic
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- 「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。
- ルール「X-Force リスクのある IP (動的) (X-Force Risky IP, Dynamic)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : リスクのある IP にアクセスしているユーザー (マルウェア)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : リスクのある IP にアクセスしているユーザー (マルウェア) (旧称「X-Force リスクのある IP (マルウェア) (X-Force Risky IP, Malware)」)

デフォルトで有効

True

説明

このルールは、ローカル・ユーザーまたはローカル・ホストがマルウェア・ホストに接続している場合にそれを検出します。

サポート・ルール

- X-Force Risky IP, Malware
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- 「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。
- ルール「X-Force リスクのある IP (マルウェア) (X-Force Risky IP, Malware)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

UBA : リスクのある IP にアクセスしているユーザー (スパム)

QRadar User Behavior Analytics (UBA) アプリでは、特定の振る舞いの異常に対するルールに基づくユース・ケースがサポートされます。

UBA : リスクのある IP にアクセスしているユーザー (スパム) (旧称「X-Force リスクのある IP (スパム) (X-Force Risky IP, Spam)」)

デフォルトで有効

True

説明

このルールは、ローカル・ユーザーまたはローカル・ホストがスパムを送信するホストに接続している場合にそれを検出します。

サポート・ルール

- X-Force Risky IP, Spam
- BB:UBA : 共通のイベント・フィルター (BB:UBA : Common Event Filters)

必須の構成

- 「管理設定 **(Admin Settings)**」 > 「システム設定」で「X-Force Threat Intelligence フィードの有効化」を「はい」に設定します。
- ルール「X-Force リスクのある IP (スパム) (X-Force Risky IP, Spam)」を有効化します。

データ・ソース

すべてのサポート対象ログ・ソース

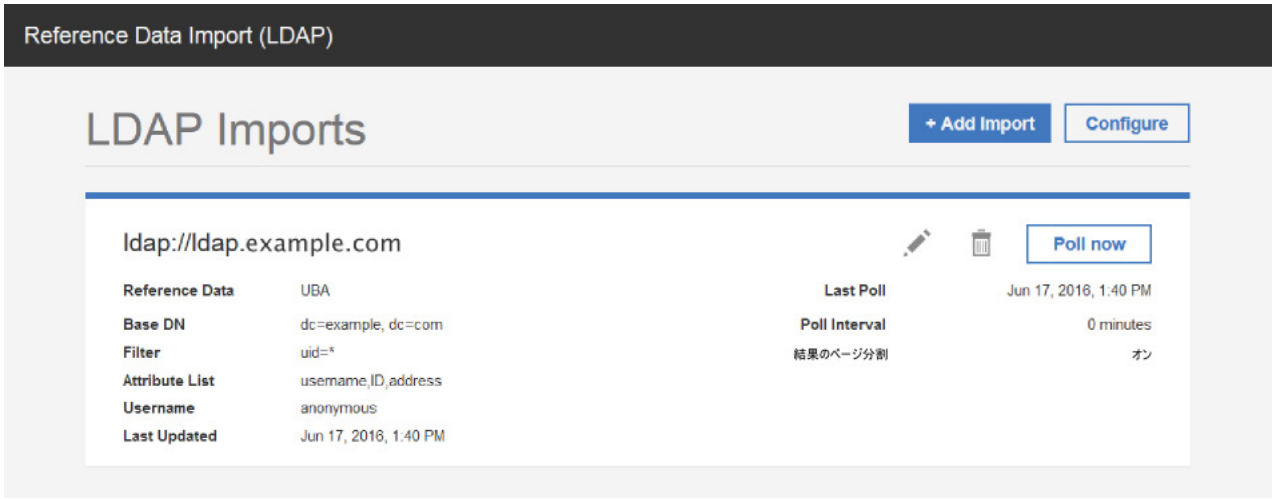
8 Reference Data Import - LDAP アプリケーション

Reference Data Import - LDAP アプリケーションを使用して、複数の LDAP ソースからのコンテキスト・アイデンティティー情報を QRadar コンソールに収集します。

重要: Reference Data Import - LDAP アプリケーションは QRadar on Cloud ではサポートされません。

IBM® QRadar® User Behavior Analytics (UBA) アプリケーションをインストールすると、Reference Data Import - LDAP アプリケーションもインストールされます。LDAP アプリケーションを使用すると、ユーザー・データを LDAP/AD サーバーまたは CSV ファイルから QRadar リファレンス・テーブルにインポートできます。インポートされたリファレンス・テーブルは、UBA アプリケーションで利用され、QRadar の検索やルールに使用されることもあります。

注: Reference Data Import - LDAP アプリケーションは QRadar V7.2.8 以降が必要です。



QRadar での LDAP データの使用

リファレンス・テーブルが更新されるたびに、`ReferenceDataUpdated` イベントがトリガーされます。リファレンス・テーブルに、LDAP データの存続時間値を設定できます。存続時間の期間を超えると、`ReferenceDataExpiry` イベントがトリガーされます。これらのイベントに応答するルールを作成したり、QRadar の「ログ・アクティビティー」タブでこれらのイベントのペイロードを照会するための検索を作成したりできます。

Reference Data Import - LDAP アプリケーションへのアクセス

QRadar Reference Data Import - LDAP アプリケーションにアクセスするには、「管理」設定で「**Reference Data Import LDAP**」アイコンをクリックします。

QRadar のリファレンス・データ収集について詳しくは、「*IBM QRadar SIEM* 管理ガイド」を参照してください。

LDAP アプリでサポートされるブラウザー

IBM Security QRadar 製品の機能が正しく動作するためには、サポート対象の Web ブラウザーを使用する必要があります。

以下の表に、サポートされる Web ブラウザーのバージョンをリストします。

表 1. *QRadar Reference Data Import LDAP* アプリでサポートされる *Web* ブラウザー

Web ブラウザー	サポートされるバージョン
Mozilla Firefox	45.2 延長サポート版
Google Chrome	最新版

CSV ファイルからのユーザー・データのインポート

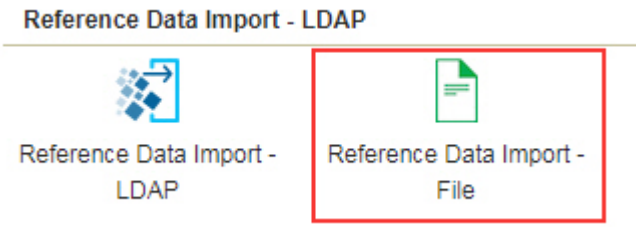
Reference Data Import - LDAP アプリケーションを使用して、ユーザー・データを含む CSV ファイルをアップロードできます。

このタスクについて

ユーザー・データが標準 CSV 形式である場合、そのデータを CSV ファイルから UBA アプリケーションにインポートできます。

手順

1. IBM QRadar V7.3.1 以降の場合、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. QRadar 7.3.1 以降の場合、「アプリケーション」 > 「参照データのインポート **- LDAP**」 > 「リファレンス・データのインポート **-** ファイル」をクリックします。



3. 「リファレンス・データのインポート (ファイル)」ウィンドウで、「構成」をクリックして許可サービス・トークンを作成します。
4. 「リファレンス・データのインポート (ファイル)」ウィンドウで、「インポート」をクリックします。
5. 「ユーザー・データの追加 (Add user data)」画面で、ユーザー・データを含む CSV ファイルを参照して指定します。

   注:

   ファイルは 5 MB 以下で、列名が設定されたヘッダー行があり、一意のデータを含む列が少なくとも 1 列ある必要があります。
6. 「次へ」をクリックし、既存のリファレンス・テーブルとデータをマージするか、リファレンス・テーブルを作成するかを選択します。

- 既存のリファレンス・テーブルにマージする場合は、「次へ」をクリックして既存のリファレンス・テーブルを選択します。
- リファレンス・テーブルを作成する場合は、「次へ」をクリックしてリファレンス・テーブルを作成します。

7. 「次へ」をクリックします。
8. 「属性マッピング」画面で、リファレンス・テーブルの属性名とキーを設定し、「インポート」をクリックします。

許可サービス・トークンの作成

リファレンス・テーブルにデータを追加するように LDAP サーバーを構成するには、その前に許可サービス・トークンを作成する必要があります。

始める前に

重要**:** 管理者機能が制限されているため、QRadar on Cloud 管理者は QRadar アプリケーションの許可サービス・トークンを作成できません。QRadar on Cloud ユーザーの許可サービス・トークンの作成については、お客様サポートに依頼してください。

このタスクについて

注**:** 許可サービス・トークンを送信した後、新しい許可サービス・トークンを反映するには変更をデプロイする必要があります。
IBM QRadar では、認証トークンを使用して、Reference Data Import - LDAP アプリケーションが行う API 呼び出しを認証する必要があります。「管理」設定の「許可サービスの管理」ウィンドウを使用して、許可サービス・トークンを作成します。

手順

1. 「Reference Data Import - LDAP」アプリケーション・ウィンドウで、「構成」をクリックします。
2. 「許可サービス・トークンの構成 (Configure Authorized Service Token)」ダイアログ・ボックスで、「許可サービスの管理」をクリックします。
3. 「許可サービスの管理」ウィンドウで「許可サービスの追加」をクリックします。
4. 以下のフィールドに関連情報を追加して「サービスの作成」をクリックします。
   a. 「サービス名」フィールドに、この許可サービスの名前を入力します。名前の長さは 255 文字までです。
   b. 「ユーザー・ロール」リストから「管理」を選択します。
   c. 「セキュリティー・プロファイル」リストで、この許可サービスに割り当てるセキュリティー・プロファイルを選択します。セキュリティー・プロファイルは、当該サービスが QRadar ユーザー・インターフェースでアクセスできるネットワークおよびログ・ソースを決定します。
   d. 「有効期限日付」リストで、このサービスが期限切れになる日付を入力または選択します。有効期限日付が不要な場合は、「期限なし」を選択します。
5. 作成したサービスを含む行をクリックし、メニュー・バーの「選択したトークン」フィールドでトークン・ストリングを選択しコピーして、「許可サービスの管理」ウィンドウを閉じます。
6. 「許可サービス・トークンの構成 (Configure Authorized Service Token)」ダイアログ・ボックスで、「トークン」フィールドにトークン・ストリングを貼り付け、「**OK**」をクリックします。
7. 新規許可サービス・トークンを反映するために変更をデプロイします。

次のタスク

『LDAP 構成の追加』

プライベート・ルート認証局の追加

プライベート・ルート認証局 (CA) バンドルを IBM QRadar にアップロードして LDAP アプリケーションで使用できます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「**Reference Data Import LDAP**」アイコンをクリックします。
3. 「Reference Data Import LDAP」 アプリケーションのメインウィンドウで、「構成」をクリックします。
4. 「ファイルの選択 **(Choose File)**」をクリックし、「アップロード」をクリックします。**.pem**ファイル・タイプのみがサポートされます。
5. 「**OK**」をクリックします。

LDAP 構成の追加

マップのリファレンス・マップにユーザー・データを挿入するために使用する LDAP サーバー情報を追加します。

始める前に

LDAP 構成を追加するには、その前に認証トークンを作成して、Reference Data Import - LDAP アプリケーションに追加する必要があります。

手順

1. 「Reference Data Import - LDAP」アプリケーション・ウィンドウで、「インポートの追加 **(Add Import)**」をクリックします。
2. 「**LDAP 構成 (LDAP Configuration)**」タブで、以下の情報を入力します。
   a. `ldap://` または `ldaps://` (TLS の場合) で始まる URL を「**LDAP URL**」フィールドに入力します。
   b. 「基本 **DN**」フィールドに、LDAP ディレクトリー・ツリー内で、サーバーがユーザーの検索を開始すべきポイントを入力します。

      例えば、LDAP サーバーがドメイン `example.com` にある場合は、以下を使用できます。
      `dc=example,dc=com`
   c. 「フィルター」フィールドに、リファレンス・テーブルにインポートされたデータをソートするために使用する 1 つまたは複数の属性を入力します。 例:

      ```
      cn=*; uid=*; sn=*
      ```

以下のデフォルト値は Active Directory で機能します: `(&(sAMAccountName=*)(samAccountType=805306368))`

d. 「属性リスト **(Attribute List)**」フィールドに、リファレンス・テーブルにインポートする属性を入力します。

以下のデフォルト値は Active Directory で機能します。
`userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`

e. 「ユーザー名」フィールドに、LDAP サーバーの認証に使用されるユーザー名を入力します。

f. 「パスワード」フィールドに、LDAP サーバーのパスワードを入力します。

3. 続行する前に、「接続のテスト」をクリックして、IBM QRadar が LDAP サーバーに接続できることを確認します。

接続試行が成功した場合は、LDAP サーバーからの情報が「**LDAP 構成 (LDAP Configuration)**」タブに表示されます。

4. 「次へ」をクリックします。

次のタスク

『属性の選択』.

関連タスク:

182 ページの『プライベート・ルート認証局の追加』
プライベート・ルート認証局 (CA) バンドルを IBM QRadar にアップロードして LDAP アプリケーションで使用できます。

181 ページの『許可サービス・トークンの作成』
リファレンス・テーブルにデータを追加するように LDAP サーバーを構成するには、その前に許可サービス・トークンを作成する必要があります。

『LDAP 属性マッピングの追加』
別名を追加して、リファレンス・テーブルのキーを設定できます。

属性の選択

LDAP サーバーから抽出する属性を選択します。

手順

1. 「属性の選択 **(Select Attributes)**」タブで、具体的な属性を検索し、LDAP サーバーから抽出する属性を選択します。
2. 「次へ」をクリックします。

次のタスク

LDAP 属性マッピングを追加します。

LDAP 属性マッピングの追加

別名を追加して、リファレンス・テーブルのキーを設定できます。

このタスクについて

LDAP データを複数のソースから同一のリファレンス・テーブルにマージする場合は、カスタム別名を使用して、ソースは異なるが同じ名前を持つ LDAP 属性を区別できます。

手順

1. 「属性マッピング」タブで、リファレンス・テーブルのキーを設定します。

   ヒント: 新しい LDAP 属性フィールドを作成するには、「追加」をクリックし、2 つの属性を結合します。例えば、次の構文を使用できます。`"Last: {ln}, First: {fn}"`

2. 「次へ」をクリックします。

次のタスク

LDAP データを保管するためのリファレンス・データ・テーブルを構成します。

関連タスク:

『リファレンス・データ構成の追加』
「リファレンス構成 (Reference Configuration)」タブを使用して、LDAP データを保管するためのリファレンス・データ・テーブルをセットアップします。

187 ページの『LDAP データの更新に応答するルールの作成』
QRadar のリファレンス・テーブルに LDAP サーバーからのデータを保管するように IBM QRadar Reference Data Import - LDAP アプリケーションを構成したら、そのデータを使用してイベント・ルールを作成できます。

リファレンス・データ構成の追加

「リファレンス構成 (Reference Configuration)」タブを使用して、LDAP データを保管するためのリファレンス・データ・テーブルをセットアップします。

始める前に

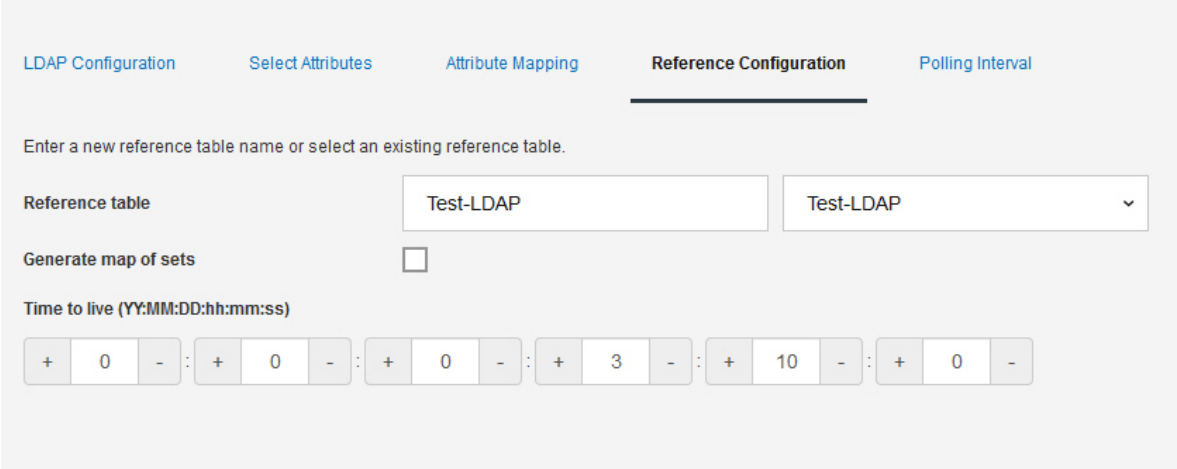
LDAP サーバー情報を構成した後、アプリケーションに渡される LDAP データを保管するためのリファレンス・テーブルをセットアップする必要があります。その後、保管されたデータを使用して、QRadar のルールを作成したり、検索とレポートを作成したりできます。

手順

1. 「リファレンス構成」タブを使用し、LDAP データの追加先として新規のリファレンス・テーブルを入力するか、既存のリファレンス・テーブルを指定します。
   a. 「リファレンス・データ」フィールドにリファレンス・データ収集の名前を入力するか、リストから既存のリファレンス・データ収集を選択します。
   b. 「セットのマップの生成」チェック・ボックスは、デフォルトで無効にされています。このチェック・ボックスを有効にすると、データがリファレンス・セット・フォーマットに送信されるため、QRadar の検索は向上されますが、パフォーマンスに影響する可能性があります。
   c. 「存続時間」フィールドを使用して、リファレンス・テーブルにデータを保持する時間を定義します。デフォルトでは、追加したデータに有効期限はありません。存続時間の期間を超えると、`ReferenceDataExpiry` イベントがトリガーされます。

      注: 既存のマップのリファレンス・マップにデータを追加する場合、アプリケーションは元の存続時間パラメーターを使用します。これらのパラメーターは、「リファレンス構成 **(Reference**

Configuration)」タブではオーバーライドできません。



2. 「次へ」をクリックします。

次のタスク

ポーリング間隔を設定します。

関連タスク:

『ポーリングの構成』

「ポーリング間隔 **(Polling Interval)**」タブを使用して、アプリケーションが LDAP サーバーに対して新規情報のポーリングを行う間隔を構成します。

ポーリングの構成

「ポーリング間隔 **(Polling Interval)**」タブを使用して、アプリケーションが LDAP サーバーに対して新規情報のポーリングを行う間隔を構成します。

始める前に

LDAP サーバー情報とリファレンス・データ収集を構成した後、アプリケーションが LDAP サーバーからデータを取得する間隔を構成します。

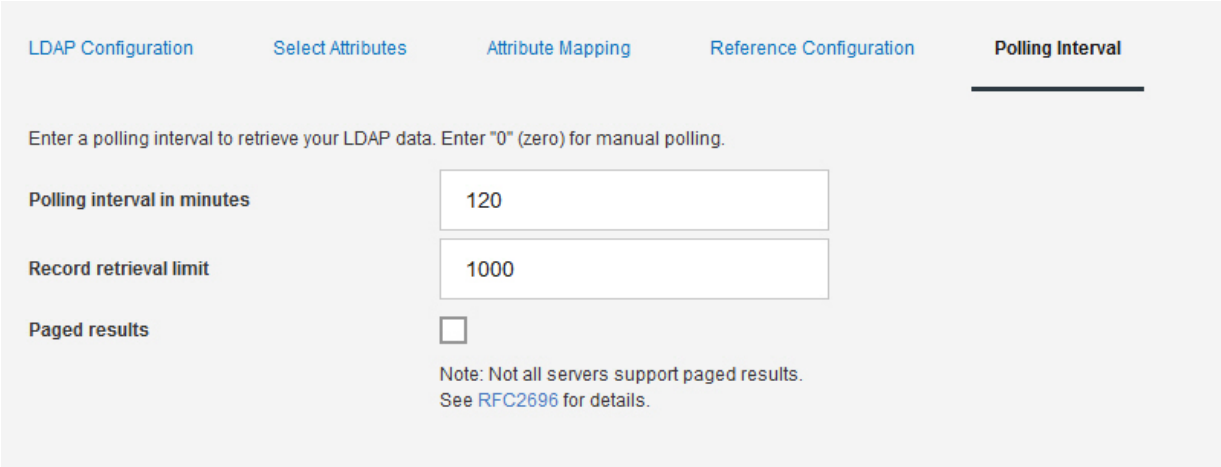
手順

1. 「ポーリング間隔 **(分) (Polling Interval in minutes)**」フィールドを使用して、アプリケーションが LDAP サーバーに対してデータのポーリングを行う間隔 (分) を定義します。

   ポーリング間隔の最小許容値は `120` です。
2. 「レコード取得の制限 **(Record retrieval limit)**」フィールドに、ポーリングが返すレコード数の値を入力します。

   デフォルトでは、100,000 レコードが返されます。返すことができる最大レコード数は 200,000 です。
3. ポーリングごとに LDAP サーバーから返されるレコードの数が制限されないようにするために、「結果のページ分割」チェック・ボックスはデフォルトで選択されています。

   注**:** 結果のページ分割は一部の LDAP サーバーではサポートされていません。
4. 「保存」をクリックします。



タスクの結果

LDAP サーバーからのデータが、構成した間隔で、選択したリファレンス・データ収集に追加されます。IBM QRadar コンソールの API ページを使用して、リファレンス・データ収集にデータが追加されたことを確認できます。

関連タスク:

『リファレンス・データ収集にデータが追加されたことの確認』

IBM QRadar の「API 資料 (API Documentation)」ページを使用して、作成済みのリファレンス・データ収集にデータが追加されたかどうかをテストできます。

リファレンス・データ収集にデータが追加されたことの確認

IBM QRadar の「API 資料 (API Documentation)」ページを使用して、作成済みのリファレンス・データ収集にデータが追加されたかどうかをテストできます。

このタスクについて

QRadar コンソールの「API 資料 (API Documentation)」ページには、Reference Data Import - LDAP アプリケーションで作成したリファレンス・テーブルに保管されているデータを表示できます。「API 資料 (API Documentation)」ページを使用して、アプリケーションによって LDAP 情報が更新されたことを確認できます。

手順

1. QRadar の「API 資料 (API Documentation)」ページにログインします。

   ```
   https://<Console_IP>/api_doc
   ```

2. ナビゲーション・ツリーで、最新の API を開きます。
3. 「**/reference_data**」 > 「**/table**」 > 「**/name**」 > 「**GET**」に進みます。
4. **Name** パラメーターの「値」フィールドに、LDAP 情報を保管するために作成したリファレンス・データ収集の名前を入力し、「試用」をクリックします。

   アプリケーションによって追加されたデータが「応答本体 **(Response Body)**」フィールドに返されます。

LDAP データの更新に応答するルールの作成

QRadar のリファレンス・テーブルに LDAP サーバーからのデータを保管するように IBM QRadar Reference Data Import - LDAP アプリケーションを構成したら、そのデータを使用してイベント・ルールを作成できます。

このタスクについて

LDAP サーバーに対してポーリングを行い、リファレンス・テーブルにデータが追加されると、`ReferenceDataUpdated` イベントがトリガーされます。「リファレンス構成 **(Reference Configuration)**」タブで構成した存続時間の期間を超えると、`ReferenceDataExpiry` イベントがトリガーされます。`ReferenceDataUpdated` イベント・ペイロードまたは `ReferenceDataExpiry` イベント・ペイロード内の内容に応答するルールを作成できます。

アプリケーションによってリファレンス・データ収集に保管された LDAP データは、QRadar 「ルール・ウィザード **(Rules Wizard)**」を使用することで構成できるルールで利用できます。「ルール・ウィザード **(Rules Wizard)**」には、「オフェンス」、「ログ・アクティビティー」、「ネットワーク・アクティビティー」の各タブからアクセスできます。

手順

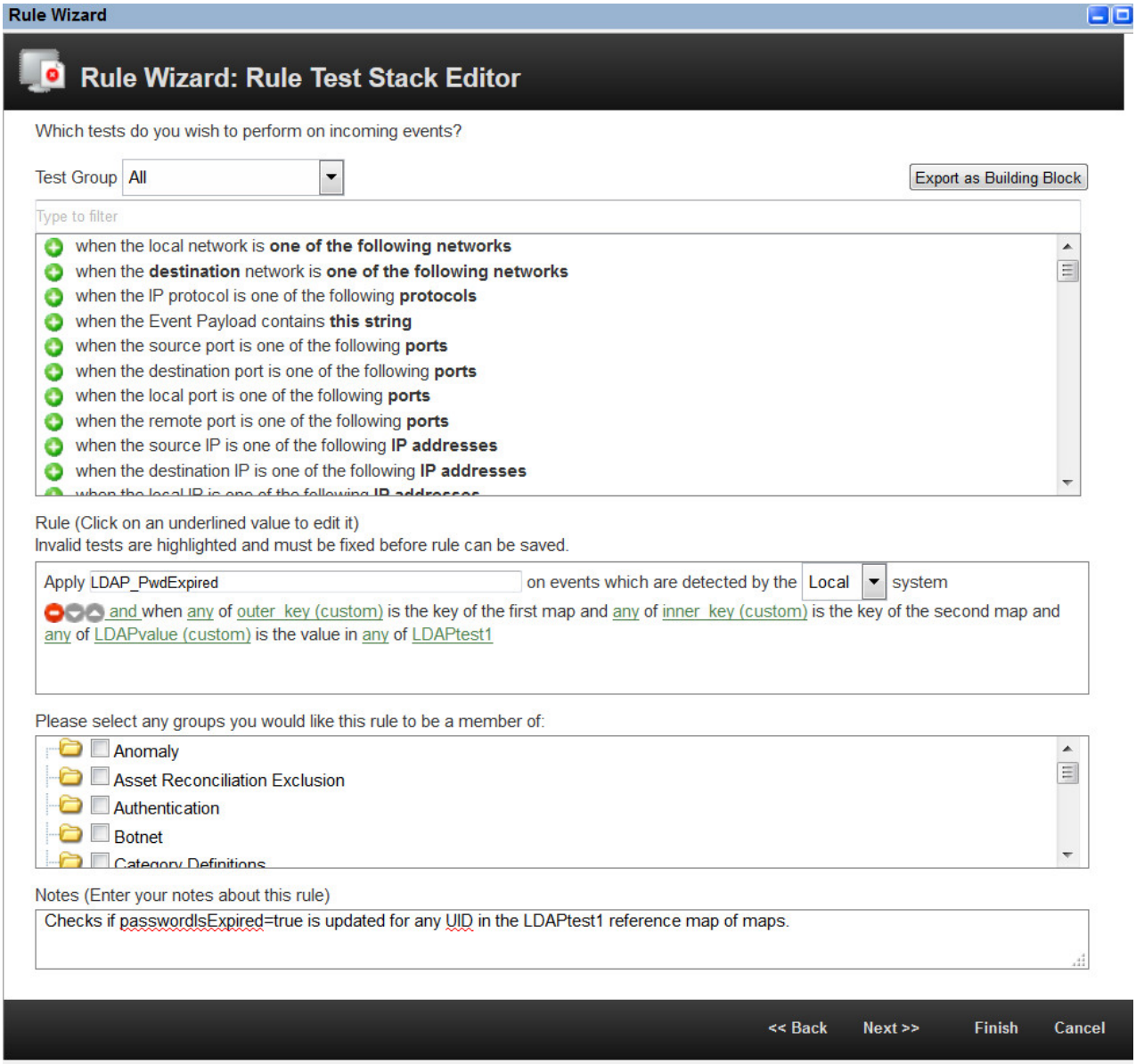
1. 「ログ・アクティビティー」 > 「ルール」 > 「アクション」 > 「新規イベント・ルール」をクリックします。
2. 「ルール・ウィザード」概要ページで、「次へ」をクリックします。
3. 「イベント」ラジオ・ボタンが選択されていることを確認し、「次へ」をクリックします。
4. ルールの名前を所定のフィールドに入力します。
5. 「テスト・グループ」リストからテストを選択し、使用するテストの横の「+」アイコンをクリックします。

   どのルール・テストを選択するかは、LDAP データを保持するリファレンス・データ収集から取得したい情報によって決まります。

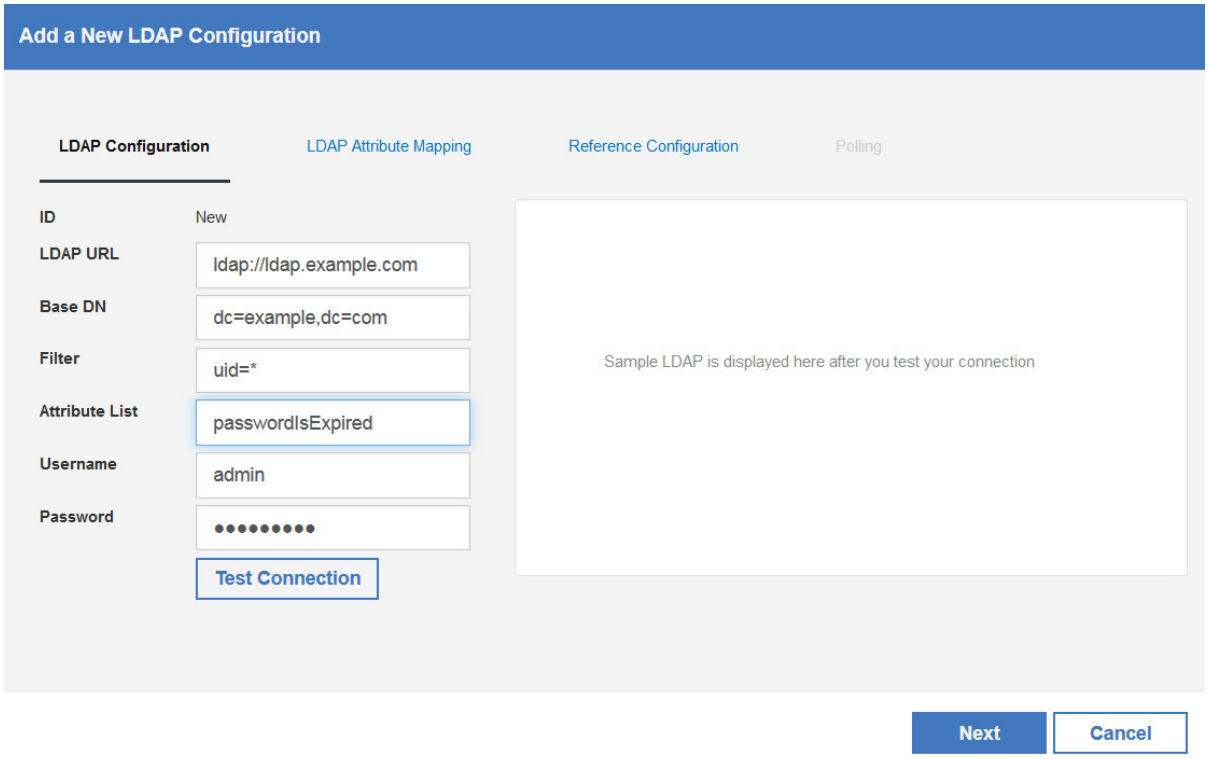
   以下のマップのリファレンス・マップのイベント・プロパティー・テストは、Reference Data Import - LDAP アプリケーションのリファレンス・テーブルが更新されるとトリガーされるイベントをテストすることを目的としています。

   ```
   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.
   ```

   LDAP 属性の **PasswordIsExpired** が **LDAPtest1** リファレンス・データ収集内のいずれかの UID に対して `true` に更新された場合に `ReferenceDataExpiry` イベント・ペイロードをテストするように、ルールが構成されます。



このイベント・プロパティー・テストを使用するには、「外部キー」 (最初のマップのキー)、「内部キー」 (2 番目のマップのキー)、および値のフィールドに対してカスタム・イベント・プロパティーを作成する必要があります。次の例では、Reference Data Import - LDAP アプリケーションが、パスワードの有効期限が切れたユーザーに関する情報を `example.com` の LDAP サーバーからインポートするように構成されています。



外部キー

このプロパティーには、アプリケーションの「LDAP 構成 (LDAP Configuration)」タブの「基本 **DN**」フィールドおよび「フィルター」フィールドで指定された LDAP フィールドに入力された値が含まれます。カスタム・イベント・プロパティーの正規表現は、次のようになります。

```
(uid=(.*?),dc=example,dc=com)
```

内部キー

このプロパティーには、アプリケーションの「LDAP 構成 (LDAP Configuration)」タブの「属性」フィールドで指定された LDAP フィールドに入力された値が含まれます。このフィールドには属性別名を使用できます。カスタム・イベント・プロパティーの正規表現は、次のようになります。

```
(passwordIsExpired)
```

値のフィールド

このプロパティーには、各ユーザーの **passwordIsExpired** LDAP 属性について取得されたデータが含まれます。カスタム・イベント・プロパティーの正規表現は、次のようになります。

```
(¥['true'¥])
```

カスタム・イベント・プロパティーについて詳しくは、「*IBM QRadar SIEM* ユーザーズ・ガイド」を参照してください。

6. 「次へ」をクリックします。
7. ルールに適用するルール・アクション、ルールの応答、およびルール・リミッターを選択し、「終了」をクリックします。

カスタム・イベント・ルールについて詳しくは、「*IBM QRadar SIEM* ユーザーズ・ガイド」を参照してください。

タスクの結果

次回、LDAP サーバーに対してポーリングを行い、作成済みのリファレンス・データ収集が更新されると、ルールがトリガーされます。

関連タスク:

183 ページの『LDAP 属性マッピングの追加』
別名を追加して、リファレンス・テーブルのキーを設定できます。

184 ページの『リファレンス・データ構成の追加』
「リファレンス構成 (Reference Configuration)」タブを使用して、LDAP データを保管するためのリファレンス・データ・テーブルをセットアップします。

9 Machine Learning Analytics アプリ

Machine Learning Analytics (ML) アプリを使用して機械学習分析用のユース・ケースを追加することにより、QRadar システムと QRadar User Behavior Analytics (UBA) アプリの機能が拡張されます。Machine Learning Analytics のユース・ケースを用いて予測モデリングを行うと、ユーザーの行動をさらに詳しく分析できます。ML アプリにより、ネットワーク内で予期されるユーザーの行動をシステムに学習させることができます。

重要: UBA アプリと ML アプリをインストールする前に、V7.2.8 以降の IBM QRadar をインストールする必要があります。

重要:

- UBA アプリを初めて構成してから 1 日経過した後に、Machine Learning Analytics 設定を有効にすることをお勧めします。この待機期間により、UBA アプリに、ユーザーのリスク・プロファイルを作成するための十分な時間が与えられます。
- モデルは 7 日ごとに更新されます。これは、Machine Learning Analytics アプリが最新のリスクの高いユーザーをモニターできるようにするためです。
- 各アプリで使用できるメモリー量は、QRadar コンソールによって制限されます。ML アプリのインストール・サイズ・オプションは、アプリケーションに対して QRadar が現在持っているメモリーの量に基づいています。
  - ML アプリをインストールするために必要な最小空きメモリーの量は、QRadar コンソールでは 2 GB、アプリケーション・ノードでは 5 GB です。
  - ML アプリによってモニターされるユーザーの数は、ML アプリのインストール・サイズおよび特定の「Machine Learning」分析によって異なります。「Machine Learning」分析によってモニターされるユーザーの最大数は、Machine Learning のインストール・サイズの 1 GB 当たり 500 ユーザーです。例えば、2 GB の場合は最大 1000 ユーザーになり、50 GB の場合は最大 25000 ユーザーになります。
- 使用可能なメモリーが不足していることが原因で、インストールが失敗することがあります。この事態は、他のアプリケーションがインストールされていることにより、アプリケーションに使用可能なメモリー量が減っている場合に発生する可能性があります。

Machine Learning Analytics の既知の問題

Machine Learning Analytics アプリには、インストールのための必須情報と既知の問題があります。

Machine Learning Analytics アプリには、以下に示す既知の問題があります。

- Machine Learning アプリの「機械学習の状況 (Status of Machine Learning)」セクションに警告メッセージが表示される場合があります。詳しくは、 222 ページの『ダッシュボードで Machine Learning アプリの状況が警告として示される』を参照してください。
- 使用可能なメモリーが不足していることが原因で、インストールが失敗することがあります。他の複数のアプリが既にインストールされていて、ML アプリで使用できるメモリー量が 10 GB 未満の場合、128 GB のコンソール上でインストールが失敗するおそれがあります。インストールが失敗した場合は、「失敗」というエラー・メッセージが表示されます。この状況を解決するには、他のアプリをいくつかアンインストールしてから、もう一度インストールを実行してください。

Machine Learning Analytics アプリのインストール前提条件

Machine Learning Analytics アプリをインストールする前に、ここで説明する前提条件が満たされていることを確認してください。

Machine Learning Analytics アプリをインストールするには、その前に以下のシステム要件が満たされていることを確認し、User Behavior Analytics (UBA) アプリの完全なインストールと構成を行う必要があります。

コンポーネント	最小要件
システム・メモリー	• コンソール: 64 GB • アプリケーション・ノード: 5 GB
IBM QRadar バージョン	V7.2.8 以降
Sense DSM	DSM RPM ファイルがインストールされている
UBA アプリ	• UBA V3.1.0 アプリがインストールされている • UBA の設定が構成されている • UBA ダッシュボードにユーザー・データが取り込まれている (「ユーザー分析」タブをクリックして確認)

IBM Sense DSM の手動インストール

UBA アプリおよび Machine Learning Analytics アプリは、以下の IBM Sense DSM ファイルを使用して、ユーザーのリスク・スコアとオフェンスを QRadar に追加します。

- V7.2.8 の場合: `DSM-IBMSense-7.2-20180814101121.noarch.rpm`
- QRadar V7.3.1 以降の場合: `DSM-IBMSense-7.3-20180814141146.noarch.rpm`

制約事項**:** デバイス・サポート・モジュール (DSM) のアンインストールは、QRadar ではサポートされていません。

1. DSM RPM ファイルを QRadar コンソールにコピーします。
2. SSH を使用して QRadar ホストに root ユーザーとしてログインします。
3. ダウンロードしたファイルが格納されているディレクトリーに移動します。
4. 以下のコマンドを入力します。

   ```
   rpm -Uvh <rpm_filename>
   ```
5. 「管理」設定から、「拡張」 > 「すべての構成のデプロイ」をクリックします。

注**:** UBA アプリのインストール手順および構成手順については、IBM Knowledge Center を参照してください。

関連タスク:

19 ページの『User Behavior Analytics アプリのインストール』
IBM QRadar 拡張の管理ツールを使用して、アプリケーション・アーカイブを直接 QRadar コンソールにアップロードおよびインストールします。

30 ページの『UBA 設定の構成』
IBM QRadar User Behavior Analytics (UBA) アプリで情報を表示するには、UBA アプリケーション設定を構成する必要があります。

Machine Learning Analytics アプリのインストール

Extension Manager から UBA アプリをインストールした後に、Machine Learning Analytics アプリをインストールします。

始める前に

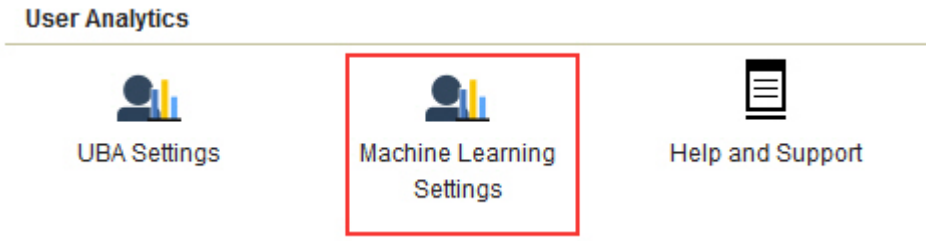
Machine Learning Analytics アプリのインストール前提条件がすべて満たされていることを確認してください。

このタスクについて

V2.1.0 以降の User Behavior Analytics (UBA) アプリをインストールした後、「機械学習の設定」ページから Machine Learning Analytics アプリをインストールできます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。



3. 「機械学習の設定」ページで、「**ML** アプリケーションのインストール」をクリックします。
4. プロンプトが表示されたら、「はい」をクリックして、アプリをインストールします。ML アプリのインストールには、数分かかります。

次のタスク

インストールが完了したら、ML ユース・ケースを有効にすることができます。次に「構成の保存」をクリックします。

Machine Learning Analytics アプリのアップグレード

「機械学習の設定」ページから Machine Learning Analytics アプリをアップグレードします。

始める前に

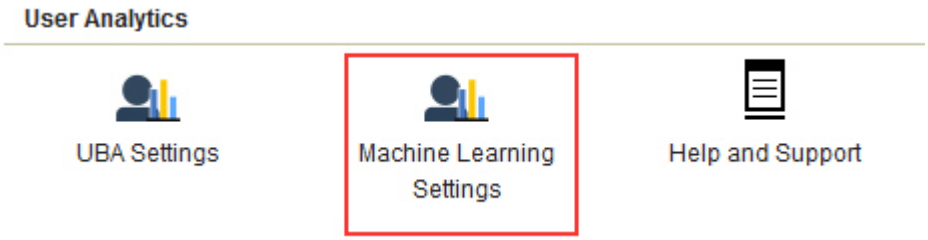
ML V2.2.0 以降を使用する UBA では、アップグレード手順はありません。Machine Learning アプリは、UBA アプリによって自動的にアップグレードされます。User Behavior Analytics (UBA) アプリをインストールまたはアップグレードした後、「機械学習の設定」ページから既存の Machine Learning Analytics アプリをアップグレードできます。

重要**:** Machine Learning Analytics (ML) アプリ V2.0.0 がインストール済みであり、UBA アプリの最新バージョンにアップグレードする場合は、QRadar Extension Manager から Machine Learning Analytics アプリをアンインストールしないでください。Extension Manager から Machine Learning Analytics アプリをアンインストールしようとすると、ML アプリのインストールで問題が発生することがあります。

注**:** Machine Learning Analytics アプリ V2.1.0 以下からアップグレードする場合、各ユーザー分析の「センス・イベントのリスク値」の値は、現行の Machine Learning デフォルト値に更新されます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。



3. 「機械学習の設定」ページで、「**ML** アプリケーションのアップグレード」をクリックします。
4. プロンプトが表示されたら、「はい」をクリックします。ML アプリのアップグレードには、数分かかります。
5. アップグレードの完了後、モデルの作成が再開されます。

次のタスク

Machine Learning Settings が正しく構成されたことを確認します。いずれかの設定を変更した場合は、必ず「構成の保存」をクリックしてください。

Machine Learning Analytics 設定の構成

Machine Learning Analytics アプリで情報を表示するには、Machine Learning Analytics アプリの設定を構成する必要があります。

「合計アクティビティー」分析の構成

「合計アクティビティー」機械学習分析を構成して、1 日のユーザー・アクティビティーの実際の量と予期される量 (学習済みの量) を UBA ダッシュボードに表示します。

このタスクについて

重要: 設定を構成または変更した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

重要: V2.2.0 以降、「センス・イベントのリスク値」のデフォルト値は変更されています。新しいデフォルト値は以前のデフォルト値も大幅に小さいため、新しいデフォルト値によって、既存のデフォルト値、または以前に変更した値が上書きされます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「合計アクティビティー」をクリックします。
4. 「有効」  をクリックして「合計アクティビティー」分析をオンにします。

   重要: 分析のモデルを生成するには、7 日分の有効なデータが必要です。
5. 「ユーザーの詳細ページにグラフを表示」トグルは、「ユーザーの詳細」ページに「合計アクティビティー」グラフを表示するようにデフォルトで有効になっています。「合計アクティビティー」グラフを「ユーザーの詳細」ページに表示しない場合は、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 5 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

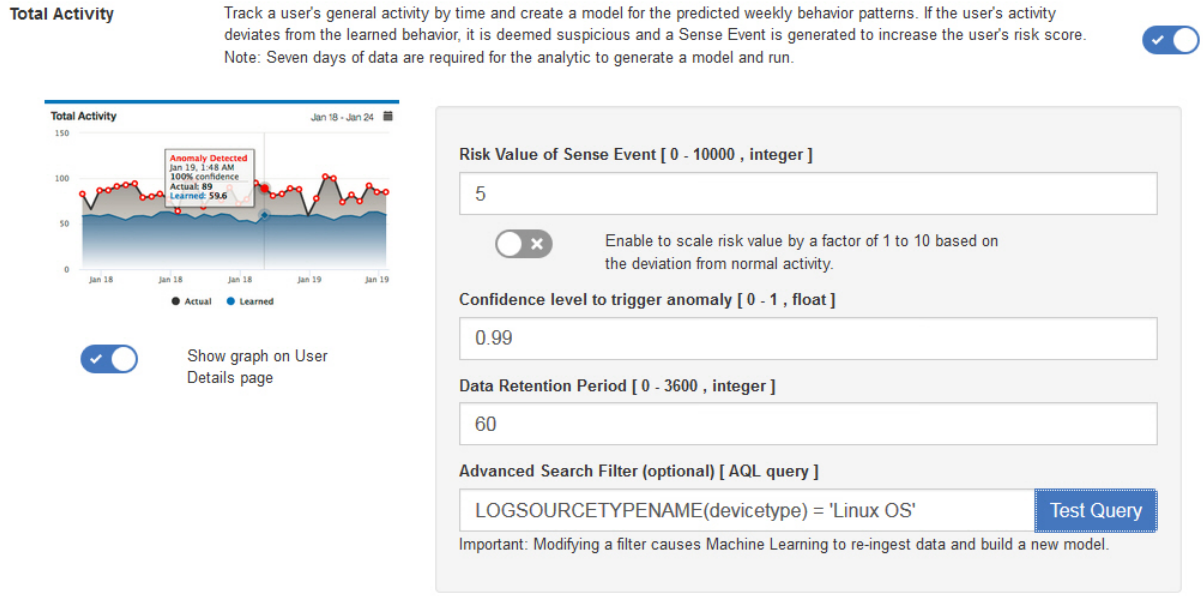
重要: AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。

- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

詳しくは、Ariel 照会言語を参照してください。

11. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「異常なアウトバウンド転送の試行」分析の構成

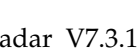
「異常なアウトバウンド転送の試行」機械学習分析を構成して、各ユーザーのアウトバウンド・トラフィック使用状況を「UBA ダッシュボード」に表示します。

このタスクについて

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

「異常なアウトバウンド転送の試行」機械学習分析は V2.8.0 以降で利用できます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー () をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「異常なアウトバウンド転送の試行」をクリックします。
4. 「有効」  をクリックして「異常なアウトバウンド転送の試行」分析をオンにします。

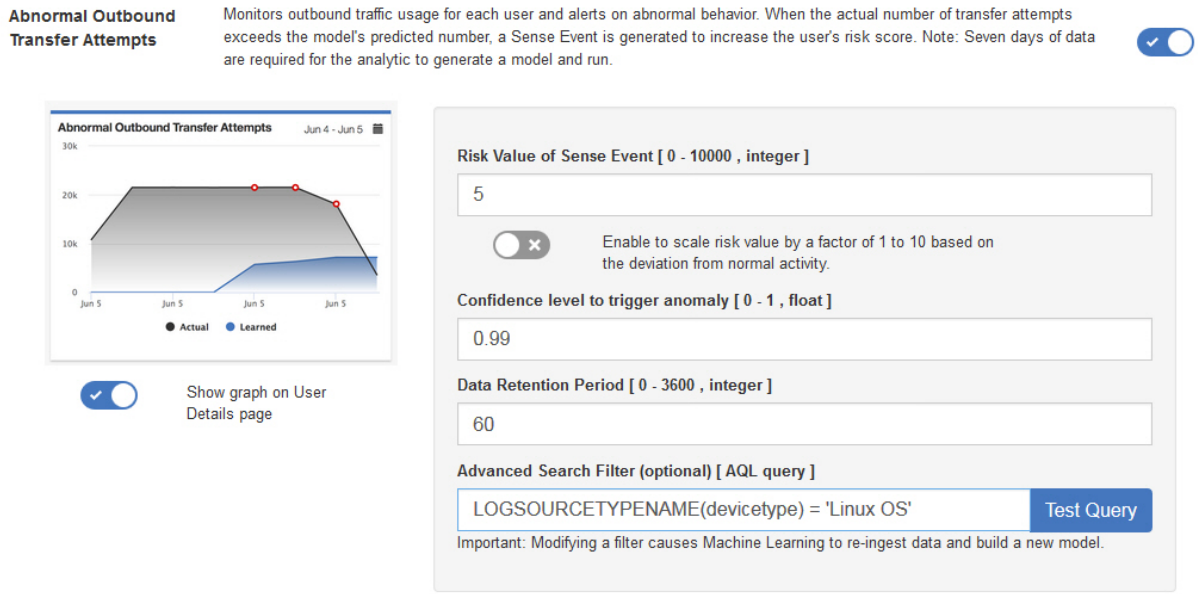
   重要: UBA コンテンツがシステムで有効になってから 7 日分のデータが必要です。
5. 「ユーザーの詳細ページにグラフを表示」トグルはデフォルトではオフになっています。「異常なアウトバウンド転送の試行」グラフを「ユーザーの詳細」ページに表示するには、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 5 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

    重要: AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。
    - **`REFERENCESETCONTAINS('Important People', username)`**
    - **`LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`**
    - **`INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`**

詳しくは、Ariel 照会言語を参照してください。

11. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「アクティビティー (カテゴリー別)」分析の構成

「アクティビティー (カテゴリー別)」機械学習分析を構成することで、ユーザー・アクティビティーの実際の行動パターンと予期される行動パターンを上位カテゴリーごとに UBA ダッシュボードに表示します。

このタスクについて

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

重要: V2.2.0 以降、「センス・イベントのリスク値」のデフォルト値は変更されています。新しいデフォルト値は以前のデフォルト値も大幅に小さいため、新しいデフォルト値によって、既存のデフォルト値、または以前に変更した値が上書きされます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。

- QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。

3. 「機械学習の設定」ページで、「アクティビティー **(**カテゴリー別**)**」をクリックします。

4. 「有効」  をクリックして「アクティビティー *(*カテゴリー別*)*」分析をオンにし、「ユーザーの詳細」ページで「アクティビティー *(*カテゴリー別*)*」グラフを表示します。

   重要**:** 分析の初期モデルを生成するには、7 日分の有効なデータが必要です。この QRadar システムで使用できるデータが 7 日分に満たない場合、7 日分のユーザー・データが累積されてから、初期モデルが生成されます。

5. 「ユーザーの詳細ページにグラフを表示」トグルは、「ユーザーの詳細」ページに「アクティビティー *(*カテゴリー別*)*」グラフを表示するようにデフォルトで有効になっています。「アクティビティー *(*カテゴリー別*)*」グラフを「ユーザーの詳細」ページに表示しない場合は、トグルをクリックします。

6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 1 です。

7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。

8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。

9. 「追跡するカテゴリー」セクションでは、上位イベント・カテゴリーがデフォルトで有効になっています。任意のカテゴリーをクリックすると、そのカテゴリーがモニター対象から除外されます。カテゴリーの詳細については、IBM Knowledge Center の上位イベント・カテゴリートピックを参照してください。

10. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。

11. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

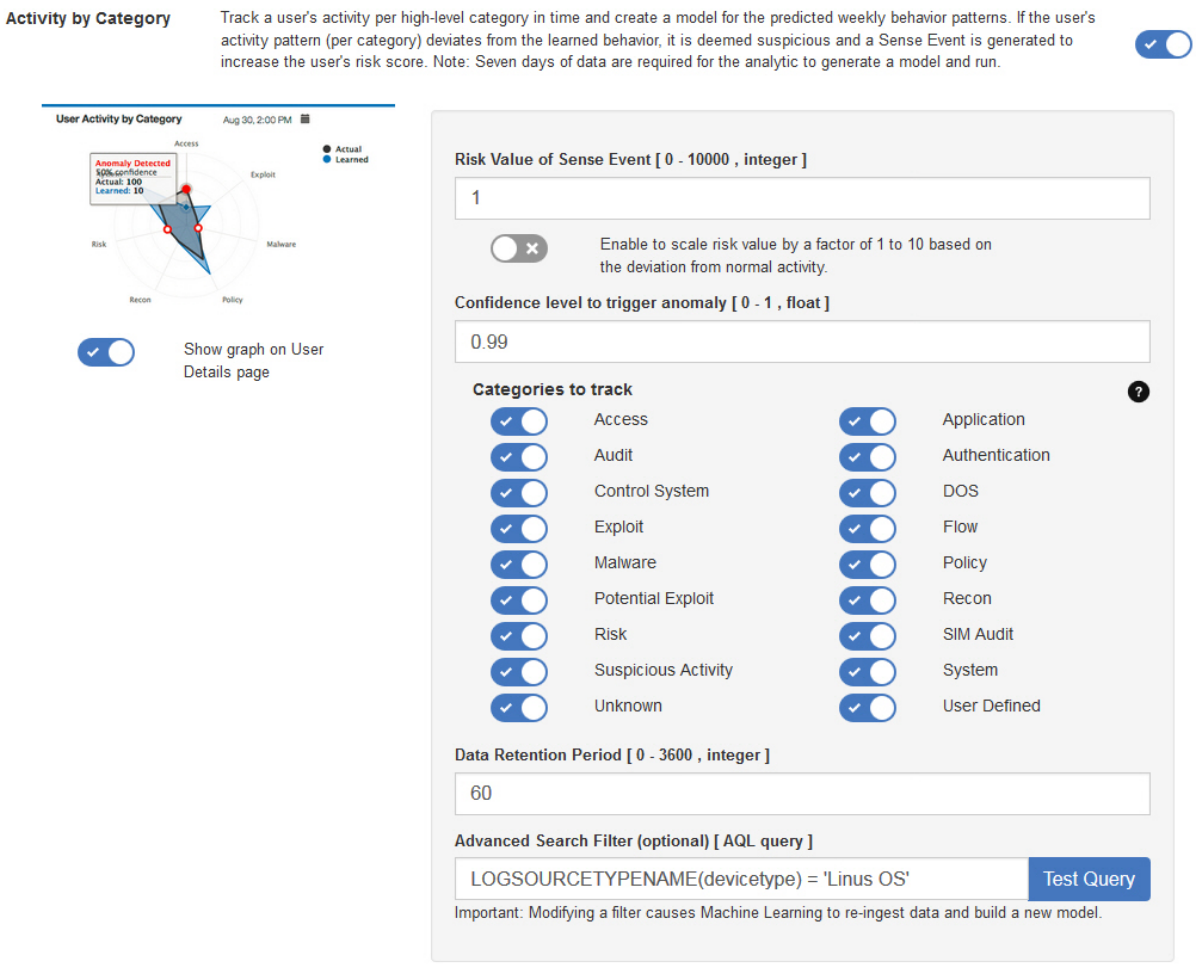
    重要**:** AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。

    - **`REFERENCESETCONTAINS('Important People', username)`**
    - **`LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`**
    - **`INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`**

    詳しくは、Ariel 照会言語を参照してください。

12. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「リスク状況」分析の構成

「リスク状況」機械学習分析を構成して、ユーザーのリスク・スコアの逸脱を UBA ダッシュボードに表示します。

このタスクについて

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

重要: V2.2.0 以降、「センス・イベントのリスク値」のデフォルト値は変更されています。新しいデフォルト値は以前のデフォルト値も大幅に小さいため、新しいデフォルト値によって、既存のデフォルト値、または以前に変更した値が上書きされます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。

- IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。

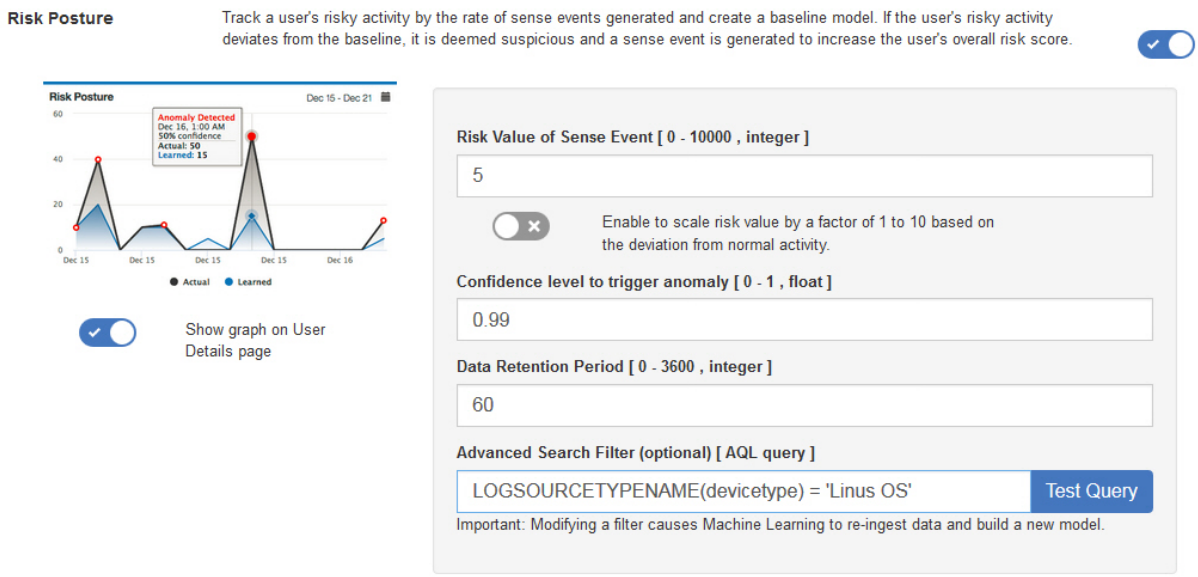
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「リスク状況」をクリックします。
4. 「有効」  をクリックして「リスク状況」分析をオンにします。

   重要**:** 分析のモデルを生成するには、7 日分の有効なデータが必要です。
5. 「ユーザーの詳細ページにグラフを表示」トグルは、「ユーザーの詳細」ページに「リスク状況」グラフを表示するようにデフォルトで有効になっています。「リスク状況」グラフを「ユーザーの詳細」ページに表示しない場合は、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 5 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

    重要**:** AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。
    - **`REFERENCESETCONTAINS('Important People', username)`**
    - **`LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`**
    - **`INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`**

    詳しくは、Ariel 照会言語を参照してください。
11. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「外部ドメインへの異常ボリューム・データ」分析の構成

「外部ドメインへの異常ボリューム・データ」機械学習分析を構成し、各ユーザーのローカルからリモートへのアップロード・ボリュームの実際の量と予期される (学習された) 量を UBA ダッシュボードに表示します。

このタスクについて

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

「外部ドメインへの異常ボリューム・データ」機械学習分析は V3.0.0 以降で利用できます。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「外部ドメインへの異常ボリューム・データ」をクリックします。

4. 「有効」  をクリックして、「外部ドメインへの異常ボリューム・データ」分析をオンにします。

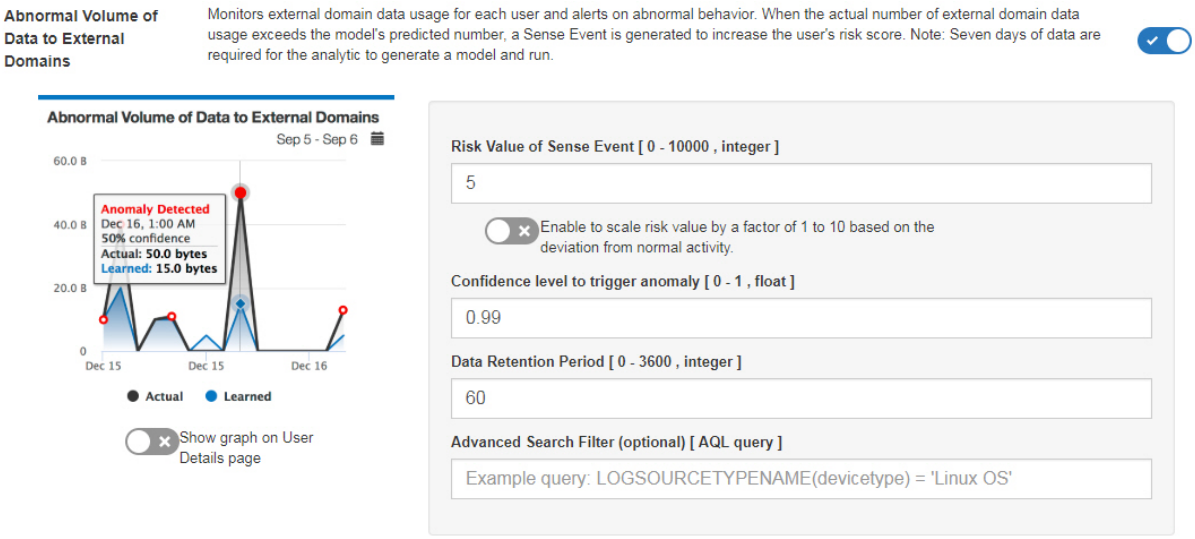
   重要: UBA コンテンツがシステムで有効になってから 7 日分のデータが必要です。
5. 「ユーザーの詳細ページにグラフを表示」トグルはデフォルトではオフになっています。「外部ドメインへの異常ボリューム・データ」グラフを「ユーザーの詳細」ページに表示するには、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 1 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

    重要: AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    詳しくは、Ariel 照会言語を参照してください。
11. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「アクティビティーの分布」分析の構成

「アクティビティーの分布」機械学習分析を構成することで、機械学習によってモニターされているすべてのユーザーの動的な振る舞いの集合体を UBA ダッシュボードに表示します。

このタスクについて

「アクティビティーの分布」機械学習分析は V2.2.0 以降で利用できます。

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「アクティビティーの分布」をクリックします。
4. 「有効」 をクリックして「アクティビティーの分布」分析をオンにし、「ユーザーの詳細」ページで「アクティビティーの分布」グラフを表示します。

重要: 分析のモデルを生成するには、7 日分の有効なデータが必要です。

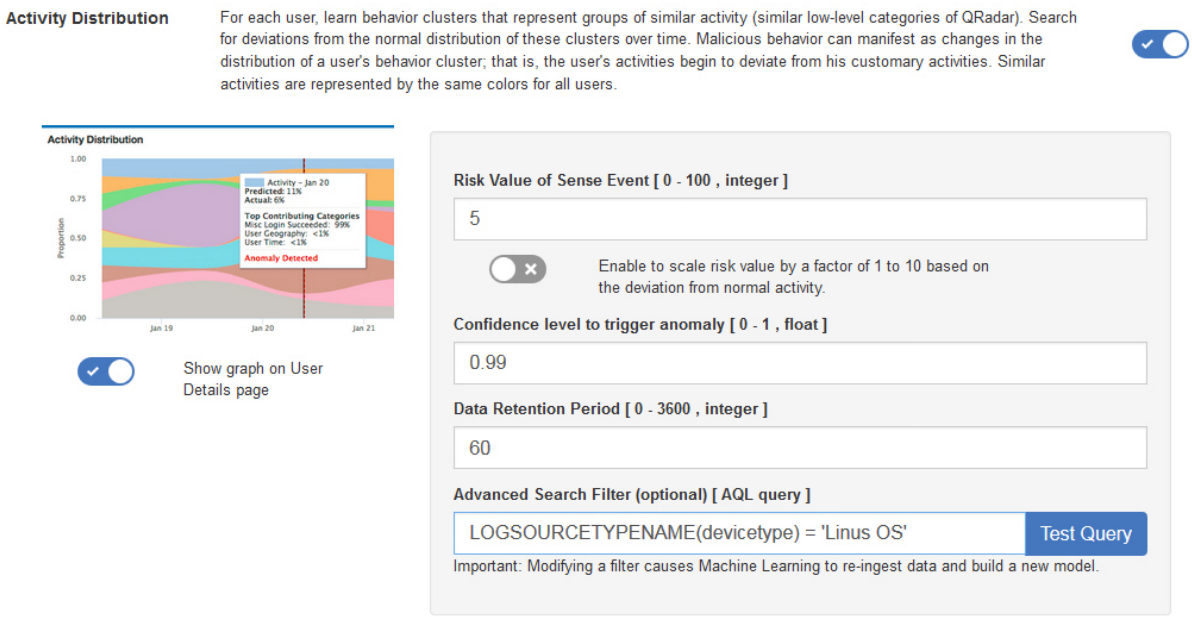
5. 「ユーザーの詳細ページにグラフを表示」トグルは、「ユーザーの詳細」ページに「アクティビティーの分布」グラフを表示するようにデフォルトで有効になっています。「アクティビティーの分布」グラフを「ユーザーの詳細」ページに表示しない場合は、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 5 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

    重要: AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。

    - `REFERENCESETCONTAINS('Important People', username)`
    - `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
    - `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

    詳しくは、Ariel 照会言語を参照してください。
11. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「定義済みピア・グループ」分析の構成

「定義済みピア・グループ」機械学習分析を構成して、ユーザーのイベント・アクティビティーが定義済みピア・グループのイベント・アクティビティーからどの程度逸脱しているかを UBA ダッシュボードに表示します。

始める前に

- 「定義済みピア・グループ」の分析を有効にするには、有効なユーザー・グループをリファレンス・テーブルに用意して、リファレンス・テーブルを使用するように「**UBA** の設定」 > 「表示属性」 > 「カスタム・グループ」を構成する必要があります。詳しくは、 218 ページの『定義済みピア・グループの分析のためのユーザー・グループ』を参照してください。
- 分析のモデルを生成するには、7 日分の有効なイベント・データが必要です。

このタスクについて

「定義済みピア・グループ」機械学習分析は V2.6.0 以降で利用できます。

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。

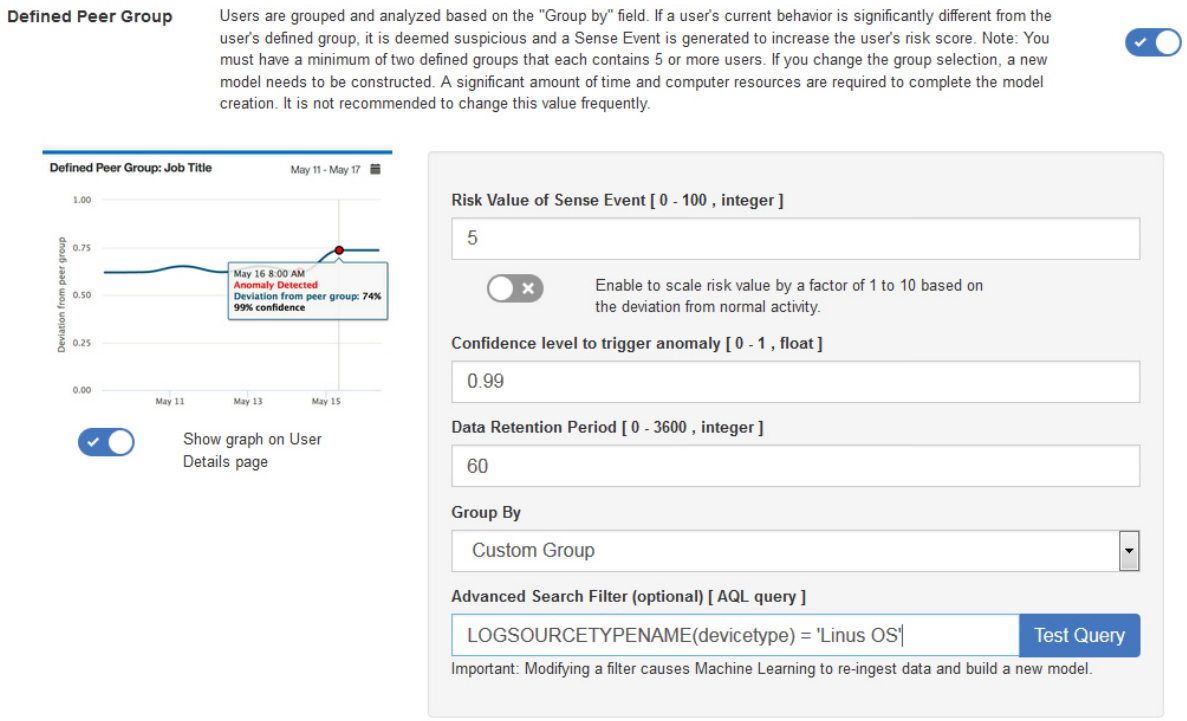
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「定義済みピア・グループ」をクリックします。
4. 「有効」  をクリックして「定義済みピア・グループ」分析をオンにします。

   重要: 分析のモデルを生成するには、7 日分の有効なデータが必要です。
5. 「ユーザーの詳細ページにグラフを表示」トグルは、「ユーザーの詳細」ページに「定義済みピア・グループ」グラフを表示するようにデフォルトで有効になっています。「定義済みピア・グループ」グラフを「ユーザーの詳細」ページに表示しない場合は、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 5 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. 「グループ化の基準」フィールドで、「定義済みピア・グループ」分析で使用するグループを選択します。
11. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

    重要: AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。
    - **REFERENCESETCONTAINS('Important People', username)**
    - **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
    - **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

    詳しくは、Ariel 照会言語を参照してください。
12. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

「学習ピア・グループ」分析の構成

「学習ピア・グループ」機械学習分析を構成して、分類されると見込まれた推定ピア・グループから、ユーザーがどれほど逸脱しているかを UBA ダッシュボードに表示します。

始める前に

- 「学習ピア・グループ」分析を有効にするには、アプリケーション・ノードをインストールする必要があります。詳しくは、https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_adm_appnode_intro.htmlを参照してください。
- 「学習ピア・グループ」分析のモデルを生成するには、7 日分の有効なイベント・データが必要です。

このタスクについて

「学習ピア・グループ」機械学習分析は V2.2.0 以降で利用できます。

重要: 設定を構成した後、データを取り込んで初期モデルを作成し、ユーザーの最初の結果が表示されるまでには、少なくとも 1 時間かかります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー (☰) をクリックしてから、「管理」をクリックして管理タブを開きます。

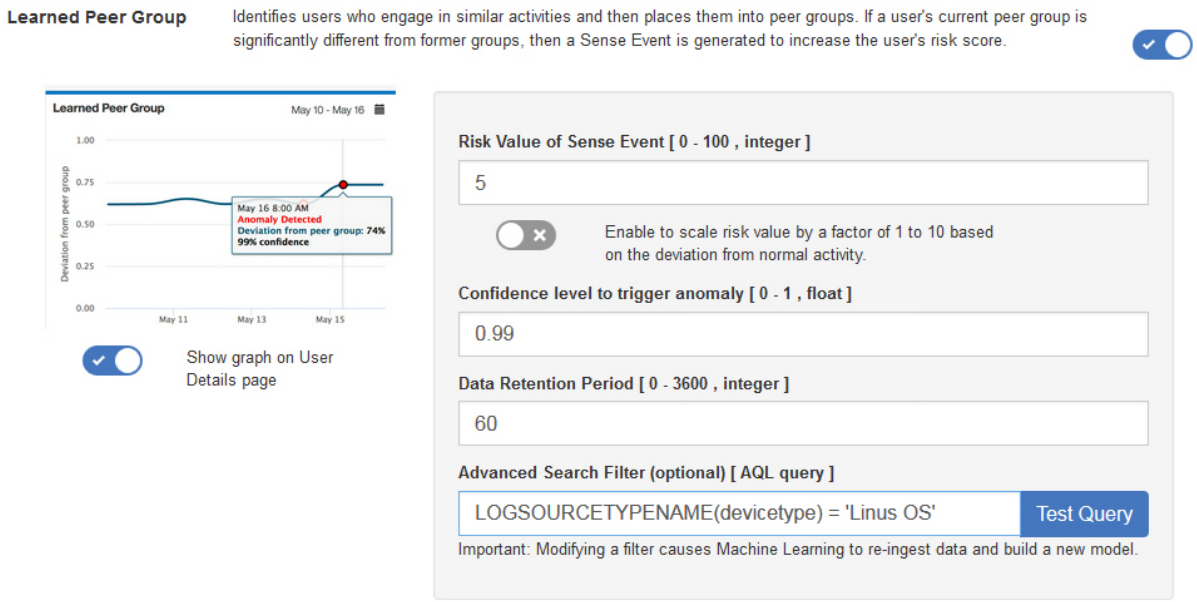
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
3. 「機械学習の設定」ページで、「学習ピア・グループ」をクリックします。
4. 「有効」  をクリックして「学習ピア・グループ」分析をオンにします。

   重要: 分析のモデルを生成するには、7 日分の有効なデータが必要です。
5. 「ユーザーの詳細ページにグラフを表示」トグルは、「ユーザーの詳細」ページに「学習ピア・グループ」グラフを表示するようにデフォルトで有効になっています。「学習ピア・グループ」グラフを「ユーザーの詳細」ページに表示しない場合は、トグルをクリックします。
6. 「センス・イベントのリスク値」フィールドで、センス・イベントがトリガーされる際にユーザーのリスク・スコアを増やすための値を入力します。デフォルト値は 5 です。
7. トグルを有効にしてリスク値をスケーリングします。有効にすると、基本リスク値が係数 (1 ～ 10 の範囲) で乗算されます。この係数は、ユーザーが期待される行動から逸脱しているというだけでなく、どれだけ逸脱しているかによって決まります。
8. 「アノマリをトリガーする信頼性間隔」フィールドで、異常なイベントをトリガーするまでの機械学習アルゴリズムの信頼性をパーセンテージで入力します。デフォルト値は 0.99 です。
9. 「データ保存期間」フィールドで、モデル・データを保存する日数を設定します。デフォルト値は 60 です。データの自動パージを無効にするには、この値を 0 (ゼロ) に設定します。
10. オプション: 「拡張検索フィルター」フィールドに AQL フィルターを追加して、QRadar 内の分析で照会するデータを絞り込むことができます。AQL 照会を使用してフィルタリングを行うことによって、分析するユーザーの数またはデータ・タイプを削減できます。構成を保存する前に、「照会のテスト」をクリックして QRadar で完全な AQL 照会を起動することで、照会を確認して結果を検証できます。

    重要: AQL フィルターを変更した場合、分析の既存のモデルに無効のマークが付けられ、モデルが再作成されます。再作成に必要な時間の長さは、変更されたフィルターによって返されるデータの量によって異なります。

    特定のログ・ソース、ネットワーク名、または特定のユーザーを含むリファレンス・セットにフィルターを適用できます。次の例を参照してください。
    - **`REFERENCESETCONTAINS('Important People', username)`**
    - **`LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`**
    - **`INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`**

    詳しくは、Ariel 照会言語を参照してください。
11. 「構成の保存」をクリックします。



タスクの結果

アプリがデータを取り込んで初期モデルを作成するまでに、少なくとも 1 時間かかります。

Machine Learning Analytics を使用した UBA ダッシュボード

Machine Learning Analytics を使用した IBM QRadar User Behavior Analytics (UBA) アプリには、Machine Learning Analytics の状況と、選択されたユーザーの追加の詳細情報が含まれます。

ダッシュボード

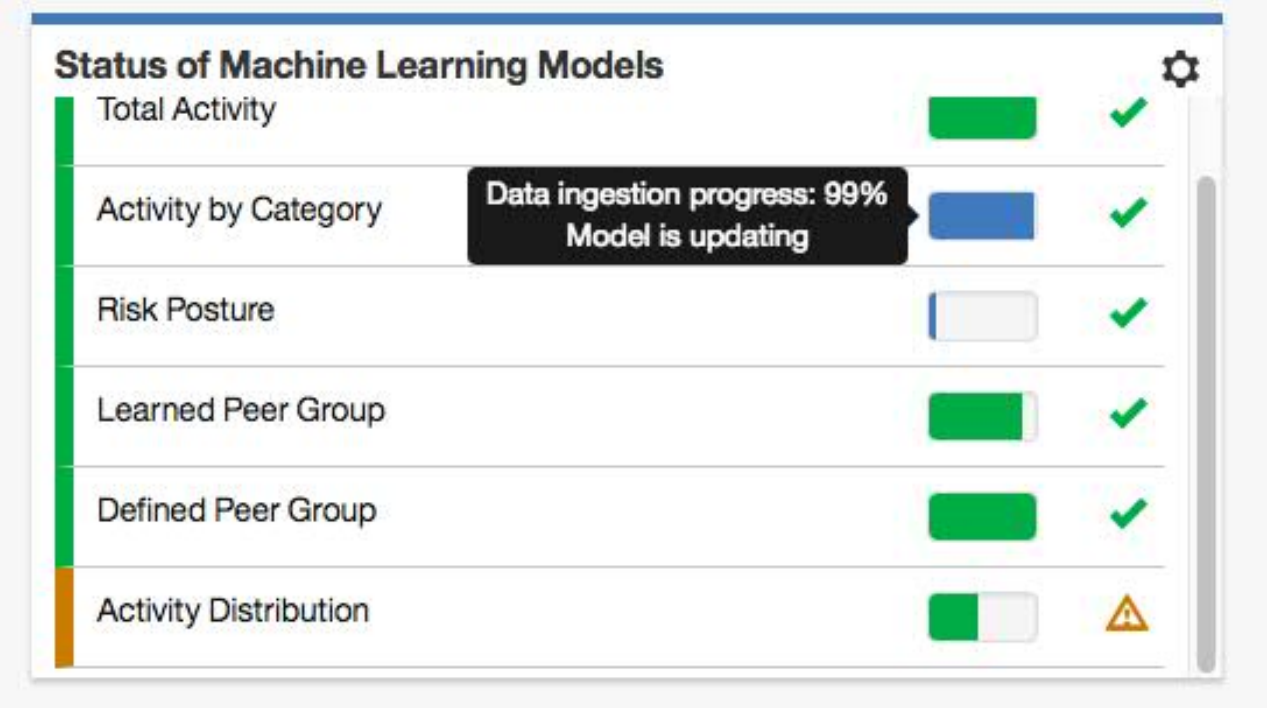
Machine Learning Analytics を有効にした後、「ユーザー分析」タブをクリックしてダッシュボードを開きます。

「機械学習モデルの状況」セクションに、有効にした分析ごとのモデルの取り込みとモデル作成の進行状況が表示されます。モデルは 7 日ごとに更新されることに注意してください。

- 青色の進行状況表示バーは、分析でデータを取り込み中であることを示しています。
- 緑色の進行状況表示バーは、分析でモデルを作成中であることを示しています。
- 緑色のチェック・マークは、分析が有効であることを示しています。
- 黄色の警告アイコンは、モデルの作成フェーズで問題が発生したことを示しています。 222 ページの『ダッシュボードで Machine Learning アプリの状況が警告として示される』を参照してください。

「**ML** の設定」アイコン  をクリックして「Machine Learning Analytics」ページを開き、Machine Learning Analytics のユース・ケースの構成を編集します。

注: 保存されている構成を編集すると新しいモデルが作成され、データ取り込みとモデル作成の待機時間がリセットされます。

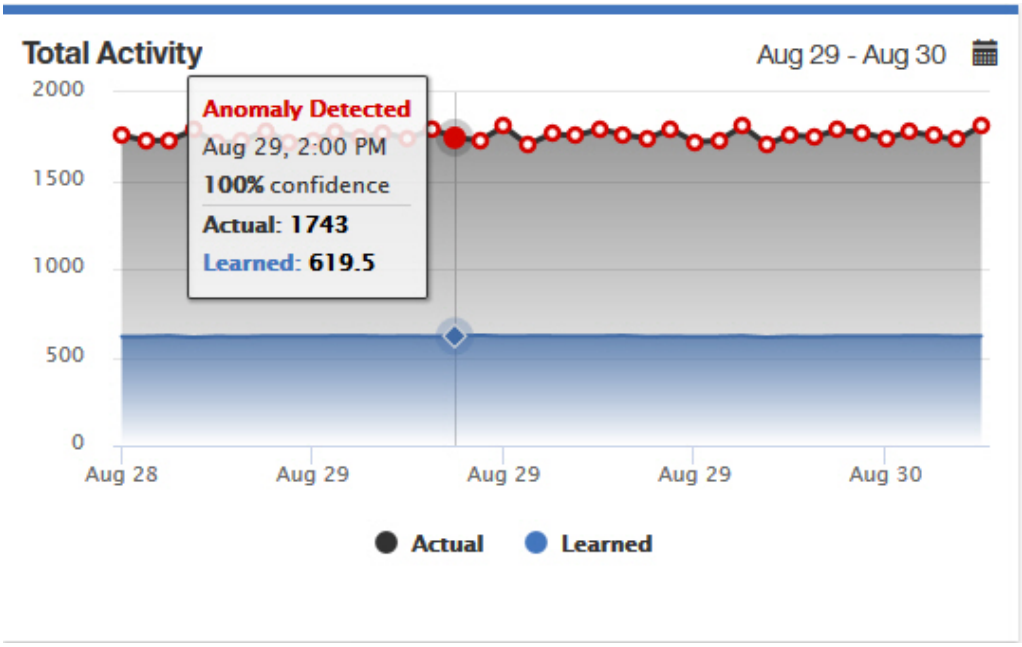


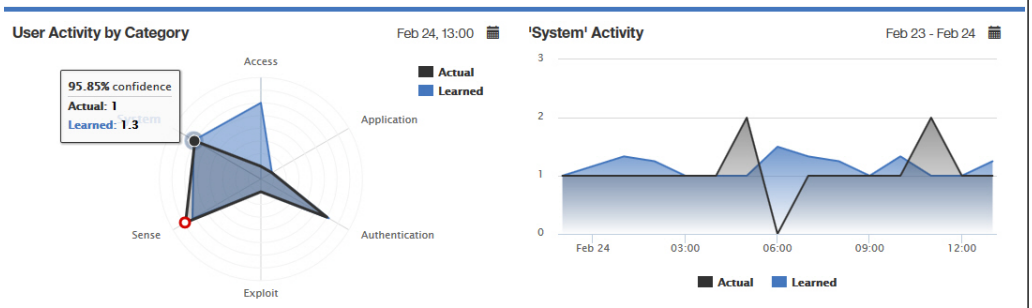
「ユーザーの詳細」ページ

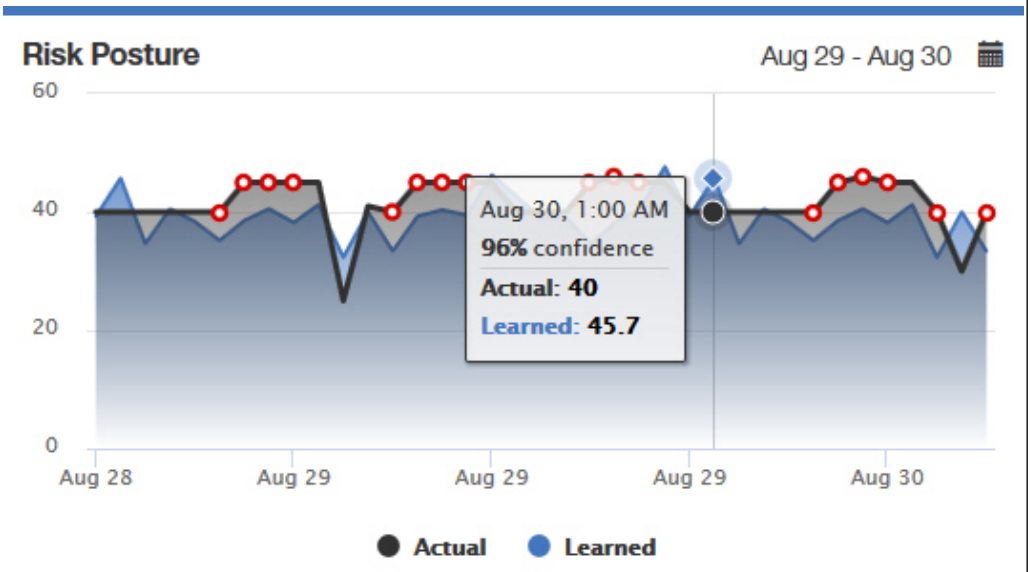
アプリ内の任意の場所からユーザー名をクリックして、選択したユーザーの詳細を表示できます。

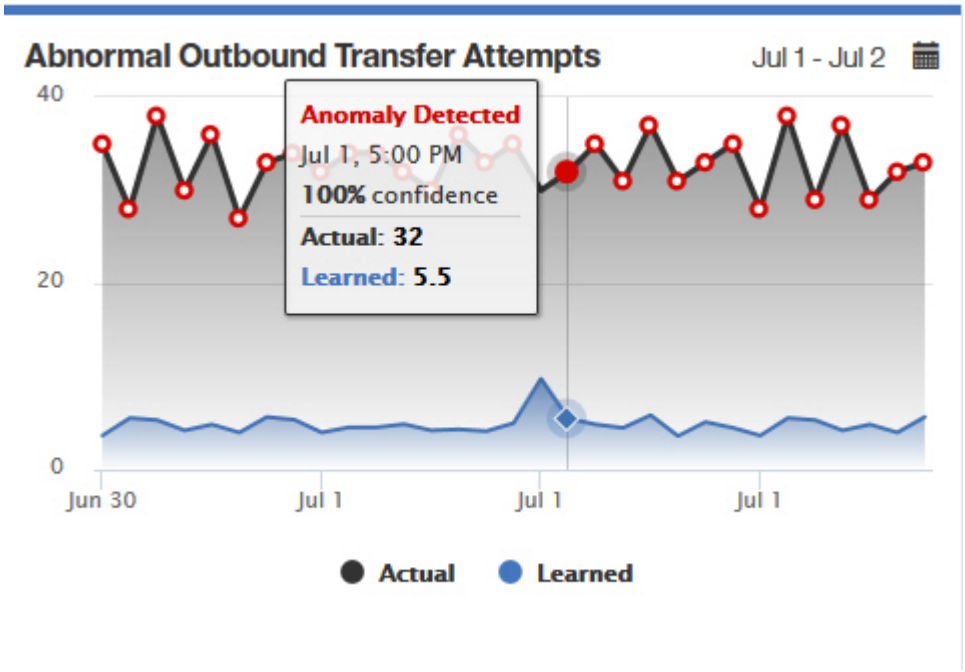
V2.5.0 以降、イベント・ビューアー・ペインでユーザーのアクティビティーをより詳細に確認できるようになりました。イベント・ビューアー・ペインには、選択したアクティビティーまたは選択した時点に関する情報が表示されます。イベント・ビューアー・ペイン内のイベントをクリックすると、Syslog イベントやペイロード情報などの詳細が表示されます。イベント・ビューアー・ペインは、「ユーザーの詳細」ページのすべてのドーナツ・グラフおよび折れ線グラフで使用できます。

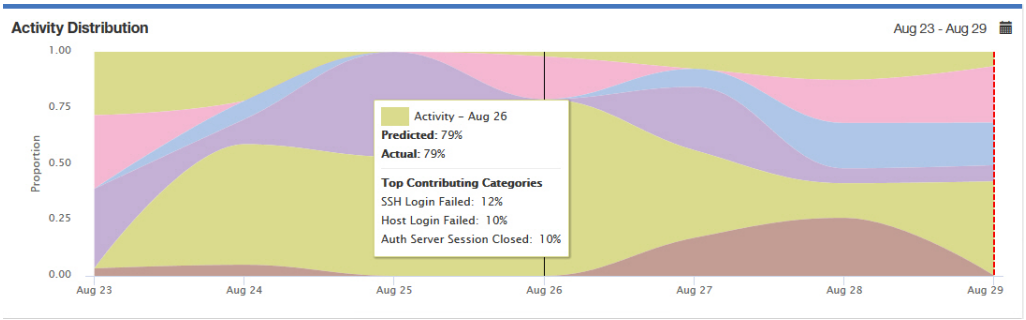
「ユーザーの詳細」ページで使用できる Machine Learning Analytics の各グラフについて、以下の表で説明します。

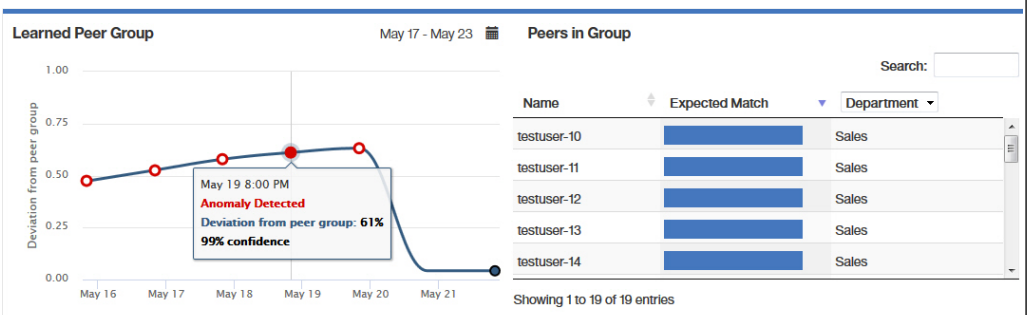
合計アクティビティー	ユーザー・アクティビティーの実際の量と予期される量 (学習済みの量) が終日にわたって表示されます。実際の値は、選択した期間中に当該ユーザーに関して発生したイベントの数です。予期される値は、選択した期間中に当該ユーザーに関して発生すると予測されたイベントの数です。赤い円は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。 「合計アクティビティー」グラフでは、以下の操作を行うことができます。 • データ・ノードをクリックすると、そのアノマリを構成しているイベントの照会リストが表示されます。 • カスタム日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 

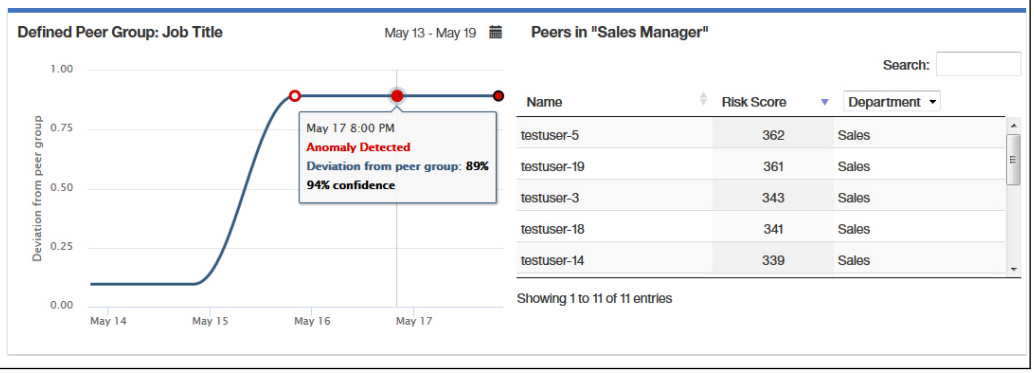
ユーザー・アクティビティー (カテゴリー別)	ユーザー・アクティビティーの実際の行動パターンと予期される行動パターンが上位カテゴリー別に表示されます。実際の値は、選択した期間中に当該ユーザーに関して発生した、上位カテゴリーごとのイベントの数です。予期される値は、選択した期間中に当該ユーザーに関して発生すると予測された、上位カテゴリーごとのイベントの数です。赤い円は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。 「ユーザー・アクティビティー (カテゴリー別)」グラフでは、以下の操作を行うことができます。 • 時刻と日付を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 • 任意のカテゴリーをクリックすると、そのカテゴリーのタイムライン・グラフが開きます。 選択したカテゴリーのタイムライン・グラフでは、以下の操作を行うことができます。 • データ・ノードをクリックすると、そのノードを表すイベントの照会リストが表示されます。 • カスタム日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 

リスク状況	ユーザーのリスク・スコアが予期されるリスク・スコア・パターンから逸脱している場合に表示されます。実際の値は、選択した期間中に当該ユーザーに関して発生したセンス・イベントのセンス値の合計です。予期される値は、選択した期間中に当該ユーザーに関して発生すると予測されたセンス・イベントのセンス値の合計です。赤い円は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。 「リスク状況」グラフでは、以下の操作を行うことができます。 • ノードをクリックすると、イベントの照会リストが表示されます。 • カスタム日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 

異常なアウトバウンド転送の試行	ユーザーのアウトバウンド・トラフィックの使用状況が、予想される動作から逸脱しているかどうかを示します。実際の値は、選択した期間中の当該ユーザーの転送試行回数です。学習される値はモデルの予測される転送試行回数です。赤い円は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。 「異常なアウトバウンド転送の試行」グラフでは、以下の操作を行うことができます。 • ノードをクリックすると、イベントの照会リストが表示されます。 • カスタム日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 

アクティビティーの分布 (V2.2.0 以降)	機械学習によってモニターされているすべてのユーザーの動的な振る舞いの集合体を表示します。これらの集合体は、機械学習によってモニターされているすべてのユーザーの下位アクティビティー・カテゴリーによって推定されます。実際の値は、その集合体との一致率です。予期される値は、その集合体との予測一致率です。このグラフでは、機械学習によってモニターされているすべてのユーザーの動的な振る舞いの集合体がそれぞれ色分けされて表示されます。特定のグループを表す色は、すべてのユーザーで同じです。赤い縦線は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。 「アクティビティーの分布」グラフでは、以下の操作を行うことができます。 • 各集合体の上にポインターを置くと、実際のアクティビティー・パーセンタイルと予測されたアクティビティーのパーセタイル、ならびに原因となっている下位カテゴリー上位 3 件が表示されます。 • 日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 

学習ピア・グループ (V2.2.0 以降)	分類されると見込まれた推定ピア・グループから、ユーザーがどれほど逸脱しているかを表示します。学習ピア・グループは、ユーザーの下位アクティビティー・カテゴリーによって推定されます。 赤い円は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。「ピア・グループからの逸脱」は、ユーザーが推定ピア・グループから逸脱している割合を意味します。「信頼性 **(Confidence)**」は、モデルをビルドしたときに基となった履歴データのコンテキストにおける逸脱のパーセンタイルです。逸脱および信頼性が両方ともしきい値を超えると、アラートがトリガーされます。 「学習ピア・グループ」グラフでは、以下の操作を行うことができます。 • データ・ポイントをクリックすると、「グループ内のピア」テーブルが表示されます。 • 日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 「グループ内のピア」テーブルには、そのグループに分類されることが見込まれるユーザーと実際にそのグループに含まれるユーザーのすべてが表示されます。以下の操作を行うことができます。 • ユーザー名をクリックすると、「ユーザーの詳細」ページが開きます。 • 「予期される一致」には、当該ユーザーがそのグループに分類されているという分析の信頼度が示されます。 • ドロップダウン・リストをクリックすると、表示するユーザー属性を選択できます。 • 検索によってユーザー名をフィルタリングできます。 

定義済みピア・グループ (V2.6.0 以降)	ユーザーのイベント・アクティビティーが定義済みピア・グループのアクティビティーからどの程度逸脱しているかを示します。この分析では、ユーザーによるイベントの低レベルのアクティビティー・カテゴリーを使用して、定義済みピア・グループからのユーザーの逸脱を判断します。 赤い円は、機械学習によりアノマリが検出されて、センス・イベントが生成されたことを意味します。「ピア・グループからの逸脱」は、ユーザーが定義済みピア・グループから逸脱している割合を意味します。「信頼性 **(Confidence)**」は、モデルをビルドしたときに基となった履歴データのコンテキストにおける逸脱のパーセンタイルです。逸脱および信頼性が両方ともしきい値を超えると、アラートがトリガーされます。 定義済みピア・グループの分析を表示するには、ユーザー・グループを定義する必要があります。詳しくは、『定義済みピア・グループの分析のためのユーザー・グループ』を参照してください。 「定義済みピア・グループ」グラフでは、以下の操作を行うことができます。 • データ・ポイントをクリックすると、「定義済みピア・グループ」テーブルのピアが表示されます。 • 日付範囲を指定するには、「カレンダー **(Calendar)**」アイコンをクリックします。 「定義済みピア・グループ」テーブルのピアは、現行ユーザー・グループで最もリスクの高いユーザーを示します。以下の操作を行うことができます。 • ユーザー名をクリックすると、「ユーザーの詳細」ページが開きます。 • ドロップダウン・リストをクリックすると、表示するユーザー属性を選択できます。 • 検索によってユーザー名をフィルタリングできます。 

定義済みピア・グループの分析のためのユーザー・グループ

「グループ化の基準」選択のいずれかを使用するユーザーが少なくとも 5 人いる 2 つ以上のグループ化を含むリファレンス・テーブルを使用するように UBA を構成している場合は、Machine Learning アプリケーションで、定義済みピア・グループの分析を有効にできます。

注**:** V2.6.0 以降では、UBA でユーザー・グループを抽出し、定義済みピア・グループの分析を有効にできます。

グループの選択は「役職」、「部門」、または「UBA の設定」ページの「表示属性」「カスタム・グループ」フィールドで定義したカスタム・プロパティーです。UBA が 3 つ以上の別個のグループを検出し、各グループに 5 人以上のユーザーがいる場合は、定義済みピア・グループの分析を有効にできます。有効なユーザー・グループを用意するために、ユーザーがユーザー・プロパティー (役職や部門などの LDAP

属性グループ) をリファレンス・テーブルとして抽出できるようにリファレンス・データのインポート LDAP アプリを構成できます。その上で、作成したリファレンス・テーブルを使用するように UBA を構成できます。

定義済みピア・グループの分析では、最大で 20 個のグループをモニターできます。構成された「グループ化の基準」フィールドのグループのうち、大きい順に 20 個のグループが選択されます。モニターするユーザーの数は、Machine Learning のインストール・サイズに応じたモニター対象ユーザーの制限を満たすように、各グループから比例配分によって減らされます。

要確認: リファレンス・テーブルのインポートには 2 時間の最小繰り返しスケジュールがあります。このスケジュールは「UBA の設定」ページで構成します。インポートを実行するようにスケジュールされた時刻に、新しいユーザー・グループ化属性がすべてインポートされます。

Machine Learning Analytics アプリのアンインストール

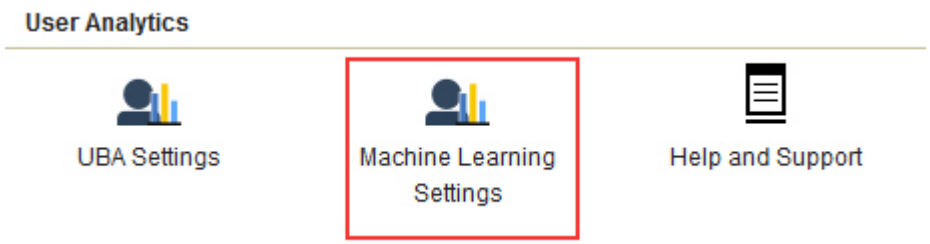
「機械学習の設定」ページから Machine Learning Analytics アプリをアンインストールします。

このタスクについて

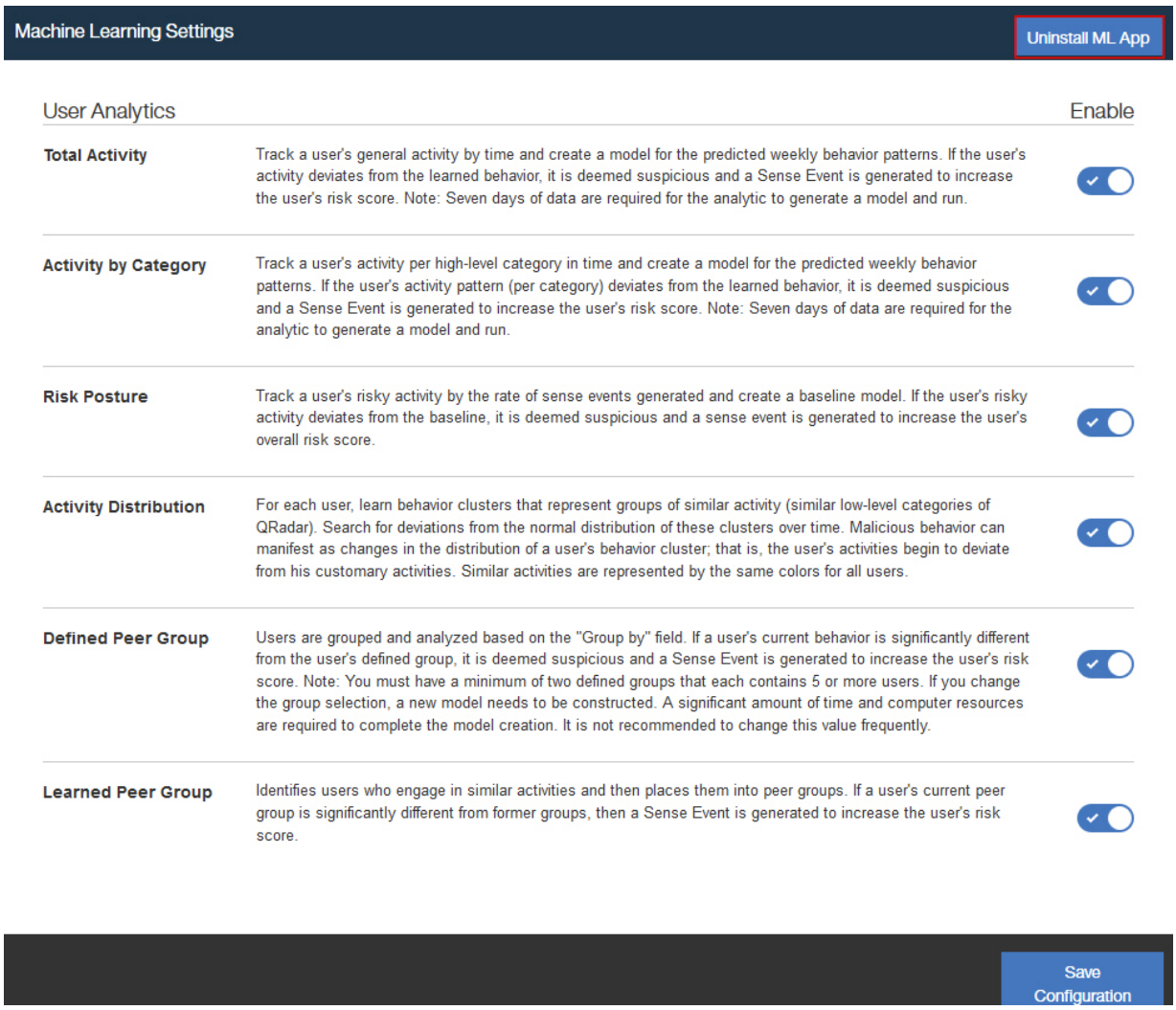
UBA アプリをアンインストールする前に、以下の手順に従って ML アプリをアンインストールする必要があります。UBA アプリをアンインストールする前に ML アプリをアンインストールしない場合、対話式 API 資料インターフェースから ML アプリを削除する必要があります。

手順

1. 「管理」設定を開きます。
   - IBM QRadar V7.3.0 以前で、「管理」タブをクリックします。
   - IBM QRadar V7.3.1 以降で、ナビゲーション・メニュー ( ) をクリックしてから、「管理」をクリックして管理タブを開きます。
2. 「機械学習の設定」アイコンをクリックします。
   - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。
   - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「機械学習の設定」をクリックします。



3. 「機械学習の設定」画面で、「**ML** アプリケーションのアンインストール」をクリックします。



4. アンインストールの確認を求めるプロンプトが表示されたら、「はい」をクリックします。

次のタスク

QRadar コンソールに再度ログインする前に、ブラウザー・キャッシュをクリアする必要があります。

10 トラブルシューティングとサポート

IBM 製品の問題を切り分けて解決するために、トラブルシューティングとサポートの情報を利用できます。

User Behavior Analytics アプリと Machine Learning Analytics アプリに関する一般的なサポートの質問に対する答えについては、https://developer.ibm.com/answers/topics/uba/ を参照してください。

UBA の「ヘルプおよびサポート」ページ

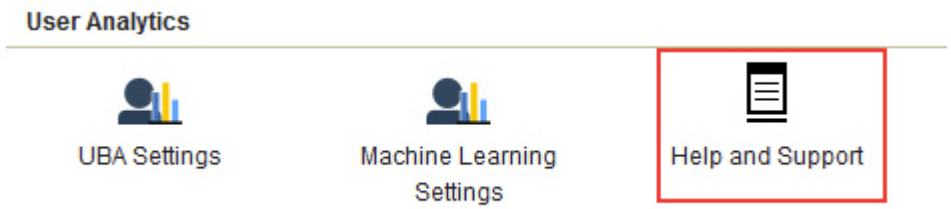
UBA アプリ (V2.5.0) には、UBA アプリ、LDAP アプリ、および Machine Learning Analytics アプリの使用に関する「ヘルプおよびサポート」セクションが用意されています。

UBA の「ヘルプおよびサポート」ページへのアクセス

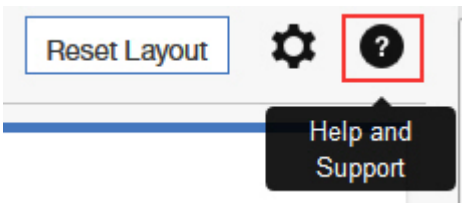
「ヘルプおよびサポート」ページには、資料、トラブルシューティングとサポート、ビデオ・チュートリアル、ログ・ファイル、および管理機能へのリンクが用意されています。「ヘルプおよびサポート」ページからログ・ファイルおよび完全な管理機能を表示するには、QRadar® 管理者特権が必要です。

UBA アプリをインストールした後、「ヘルプおよびサポート」ページに以下の場所からアクセスできます。

- 「管理」設定から:
  - QRadar V7.3.0 以前では、「プラグイン」 > 「ユーザー分析」 > 「ヘルプおよびサポート」をクリックします。
  - QRadar 7.3.1 以降では、「アプリケーション」 > 「ユーザー分析」 > 「ヘルプおよびサポート」をクリックします。



- 「ユーザー分析」タブで「ヘルプおよびサポート」アイコンをクリックします。



管理機能

ログ・ファイルおよび完全な管理機能を表示するには、QRadar® 管理者特権が必要です。

管理機能には、以下のアクションを実行する機能が含まれます。

- 「**UBA** データのクリア」をクリックして、すべての UBA ユーザー・データを削除しますが、現在の UBA 構成設定はすべて維持します。UBA データをクリアすると、UBA アプリを初めてインストールして「**UBA** の設定」を構成したときのように UBA アプリが動作します。Machine Learning アプリがインストールされている場合、「**UBA** データのクリア」ボタンにより ML アプリもリセットされます。
- Machine Learning アプリがインストールされている場合に、すべての Machine Learning 設定をリセットし、有効なすべての分析を無効にするには、「**ML** 設定のリセット」をクリックします。

サービス・リクエスト

サービス・リクエストは、問題管理レコード (PMR) とも呼ばれます。

IBM Software Technical Support に診断情報を送信するには、いくつかの方法があります。サービス・リクエストを開いたり、テクニカル・サポートと情報を交換したりするには、IBM ソフトウェア・サポートの技術サポートとの情報交換ページ (http://www.ibm.com/software/support/exchangeinfo.html) にアクセスしてください。また、サービス・リクエストはサービス・リクエスト (PMR) ツール (http://www.ibm.com/support/entry/portal/Open_service_request)を使用して直接送信することもできます。

ダッシュボードで Machine Learning アプリの状況が警告として示される

UBA ダッシュボード上の「機械学習モデルの状況」に警告メッセージが表示された場合、問題を解決するために以下の手順を確認してください。

「機械学習モデルの状況」で、分析に対して「モデルの作成に失敗しました **(Model failed to build)**」と示されている場合、この問題を解決するために推奨される以下の方法を試してください。

- ML アプリのエラー・ログを確認します。
- Machine Learning アプリを実行しているシステム上のディスク・スペースを確認します。
- UBA アプリにイベントが設定されたユーザーがあることを確認します。
- IBM お客様サポートに連絡します。

関連概念:

224 ページの『UBA および Machine Learning のログの抽出』
問題のトラブルシューティングには、UBA および Machine Learning のログ・ファイルを利用できます。

Machine Learning アプリの状況でデータ取り込みが進行しない

UBA ダッシュボード上の「機械学習モデルの状況」がデータ取り込みフェーズで進まなくなってしまった場合、問題を解決するために以下の手順を確認してください。

「機械学習モデルの状況」で、分析用のデータ取り込みが進行しなくなってしまった場合、この問題を解決するために推奨される以下の方法を試してください。

- Ariel サーバー・サービスを再始動します。

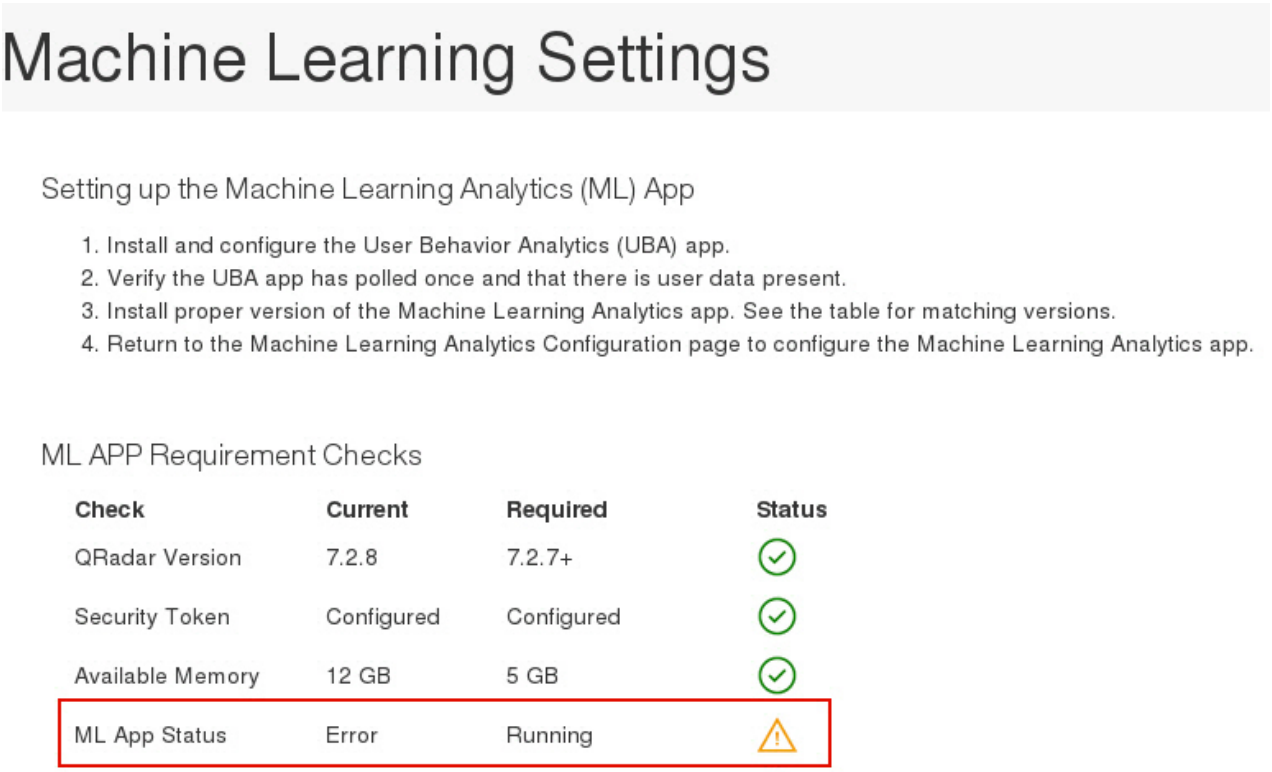
- Machine Learning アプリを実行しているシステム上のディスク・スペースを確認します。
- ML コンテナーの中を確認して、**UBAController** プロセスが実行中かどうかを調べます。
- IBM お客様サポートに連絡します。

ML アプリの状況がエラー状態にある

Machine Learning Analytics (ML) アプリのインストールが失敗して、「機械学習の設定」にエラー状況が表示された場合、**cURL** コマンド・ライン・ツールおよび API 資料の設定を使用して、ML アプリをアンインストールできます。

手順

「機械学習の設定」ページで「ML アプリケーションの状況」がエラーとして表示されている場合は、以下の手順に従って、インストールに失敗したアプリをアンインストールします。



注: 有効な認証トークンが必要です。構成済みの認証トークンのリストは、QRadar コンソールの「管理」設定にある「許可サービス」セクションで確認できます。

1. SSH を使用して、QRadar コンソールにログインします。
2. 以下のコマンドを実行します。

   # psql -U qradar -c 'select id,name,status from installed_application'

   出力例:

```
 id  |  name  |  status
-----+--------------------------------+---------
1356 | User Analytics | RUNNING
1358 | Machine Learning Analytics | ERROR
1357 | dataimport.ldap.applicationname | RUNNING
```

3. コマンドの出力で、Machine Learning Analytics の *id* 値を見つけて、記録します。
4. 次のコマンドを実行して、インストールに失敗した Machine Learning アプリをアンインストールします。*<valid token>* は有効な認証トークンで置き換え、*<id>* は記録した id 値で置き換えてください:
   # curl -X DELETE -k -H 'SEC:<valid token>' https://127.0.0.1/api/gui_app_framework/applications/<id>

Machine Learning アプリの削除

gui_app_framework API を使用して Machine Learning アプリを削除するには、以下の手順に従います。

1. QRadar コンソールを開き、API 資料ページ (https://*<host_address_port>*/api_doc) にナビゲートします。
2. バージョン番号が最も高い API のフォルダーを開きます (バージョン番号は QRadar のバージョンによって異なります。例えば、QR 7.2.8 では 7.0 です)。
3. `/gui_app_framework` フォルダーを開き、`/applications` を選択します。
4. この時点で、「**GET API (API** の取得**)**」がアクティブになっています。「試用」ボタンをクリックして、インストール済みアプリケーションのリストを表示します。
5. ステップ 4 で表示されたリストで、`Machine Learning Analytics` を検索し、`application_id` 属性値を確認します。
6. API 資料で `/applications` メニュー (ステップ 3 と同じ場所) を展開し、`/application_id` API を選択してから「削除」タブをクリックします。
7. ステップ 5 で確認したアプリケーション ID 値を入力し、「試用」ボタンをクリックしてアプリケーションを削除します。
8. API から、アプリケーションが正常に削除されたことを通知する HTTP 204 状況コードが返されるはずです。

UBA および Machine Learning のログの抽出

問題のトラブルシューティングには、UBA および Machine Learning のログ・ファイルを利用できます。

アプリケーション・ログ・ファイルのダウンロード

UBA アプリおよび Machine Learning アプリのログ・ファイルを 221 ページの『UBA の「ヘルプおよびサポート」ページ』から簡単にダウンロードできます。

UBA アプリのログ・ファイル

UBA アプリのログ・ファイルを Docker コンテナーから手動で抽出するには、以下の手順に従います。

1. UBA を実行中の QRadar ホストで、アプリのすべてのログ・ファイルを含めた zip ファイルを作成するのに十分なスペースがあるディレクトリーにナビゲートします。
2. 以下のコマンドを実行します。

   find /store/docker/v* -name uba.db
3. ディレクトリー・パスの `uba.db` までの部分をコピーします。

例えば、ディレクトリー・パスが以下のようになっているとします。
/store/docker/volumes/qapp-1001/uba.db
この場合、以下の部分をコピーします。
/store/docker/volumes/qapp-1001/

4. 以下のコマンドを実行します。ディレクトリー・パスは、ステップ 1 のディレクトリーで置き換えてください。

   zip -qr uba_logs.zip <your_path_here>log*

   例:
   zip -qr uba_logs.zip /store/docker/volumes/qapp-1001/log*

Machine Learning アプリのログ・ファイル

Machine Learning アプリのログ・ファイルを Docker コンテナーから手動で抽出するには、以下の手順に従います。

1. UBA を実行中の QRadar ホストで、アプリのすべてのログ・ファイルを含めた zip ファイルを作成するのに十分なスペースがあるディレクトリーにナビゲートします。
2. 以下のコマンドを実行します。

   find /store/docker/v* -name itproot
3. ディレクトリー・パスの `itproot` までの部分をコピーします。

   例えば、ディレクトリー・パスが以下のようになっているとします。
   /store/docker/volumes/qapp-1003/itproot
   この場合、以下の部分をコピーします。
   /store/docker/volumes/qapp-1003/
4. 以下のコマンドを実行します。ディレクトリー・パスは、ステップ 1 のディレクトリーで置き換えてください。

   zip -qr ml_logs.zip <your_path_here>log*

   例:
   zip -qr ml_logs.zip /store/docker/volumes/qapp-1003/log*

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。 IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項をご確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するに

あたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および「IBM Software Products and Software-as-a-Service Privacy Statement」(http://www.ibm.com/software/info/product-privacy) を参照してください。

一般データ保護規則

お客様自身が欧州連合の一般データ保護規則を含む各種法令を遵守するために必要な措置を講ずるのはお客様の責任です。お客様のビジネスに影響を及ぼす可能性のある関連法令の特定およびそれらの解釈、ならびにかかる関連法令を遵守するためにお客様が講ずるべき必要措置に関する助言は、お客様の責任により適格な弁護士から得るものとします。本書に記載の製品、サービス、および他の機能が、すべてのお客様の状況に適しているとは限らず、使用する際に制約を受ける場合があります。IBM は、法律、会計または監査に関する助言を提供することはしませんし、IBM のサービスまたは製品が、お客様のあらゆる法令遵守の裏付けとなる表明または保証もいたしません。

IBM 独自の GDPR 対応状況、GDPR の機能およびオファリングについて詳しくは、https://ibm.com/gdpr を参照してください。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21