RSA NETWITNESS® PLATFORM

NetWitness UEBAクイック スタート ガイド

RSA NetWitness® Platform 11.3

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、Dellが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Link の製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

この資料に記載される情報は、発行日時点で正確であるとみなされます。この情報は予告なく変更されることがあります。

6月 2019

NetWitness UEBAとは？

RSA NetWitness UEBA(User and Entity Behavior Analytics) は、ネットワーク環境のすべてのユーザとエンティティから危険な行動を検知し、調査、監視するための高度な分析ソリューションです。NetWitness UEBAは次の機能を提供します。

- 悪意のあるユーザや不正ユーザの検知
- リスクの高い行動の特定
- 攻撃の発見
- 新しいセキュリティ脅威の調査
- 潜在的な攻撃者のアクティビティの識別

本書について

このガイドでは、NetWitness Platform UEBAを構成し、UEBAの機能を使用するためのエンドツーエンドの手順を説明します。

RSA Link上のRSA NetWitness Platform 11.3のドキュメント

NetWitness Platformの製品ドキュメントは、機能ラインに沿って編成されています。特定のガイドまたはバージョンをお探しの場合は、「バージョン11.x マスター目次」を参照してください。

RSA NetWitness Platform 11.3のドキュメントは次のリンクからアクセスできます。同じドキュメントが2つの形式で提供されます。

- HTML形式のガイドは、現在サポート対象の11.xバージョンの最新情報を提供します: RSA NetWitness Platform 11.xドキュメント
- PDF形式のガイドは、特定のバージョンの情報を提供します: RSA NetWitness Platform 11.3 PDFドキュメント

ソフトウェアのバージョンに関係ないドキュメントは次のリンクからアクセスできます。

- ハードウェア セットアップ ガイド : https://community.rsa.com/community/products/netwitness/hardware-setup-guides
- フィード、パーサ、アプリケーション ルール、レポートなどのRSAコンテンツに関するドキュメント : https://community.rsa.com/community/products/netwitness/rsa-content

はじめに

次のタスクは、任意の順序で実行できます。

説明	参考情報
	
製品の更新、改善、既知の問題に関する情報を確認します。	リリース ノート
NetWitness UEBAを理解します。	*RSA NetWitness UEBAユーザ ガイド*

セットアップとインストール

スタンドアロン インストール

次のタスクは、ここに記載された順序で実行する必要があります。

説明	参考情報
	
サポート対象のハードウェアを確認します。	『*UEBAスタンドアロン インストール ガイド*』の「システム要件」トピック
UEBAの導入について理解します。	『*UEBAスタンドアロン インストール ガイド*』の「RSA NetWitness UEBAスタンドアロン インストール」トピック
ファイアウォールでポートを構成します。	『*UEBAスタンドアロン インストール ガイド*』の「RSA NetWitness UEBAスタンドアロン インストール」トピック
NetWitness Serverホストをインストールします。	『*UEBAスタンドアロン インストール ガイド*』の「インストール タスク」トピック
11.3 Log Hybridホストをインストールします。	『*UEBAスタンドアロン インストール ガイド*』の「インストール タスク」トピック
NetWitness UEBAをインストールして構成します。	『*UEBAスタンドアロン インストール ガイド*』の「インストール タスク」トピック
UEBA_AnalystsロールとAnalystsロールをUEBAユーザに割り当てます。	『システム セキュリティとユーザ管理ガイド 』の*「ロールの権限」*

新規インストール

次のタスクは、ここに記載された順序で実行する必要があります。

説明	参考情報
	
サポート対象のハードウェアを確認します。	『*物理ホスト インストール ガイド*』の「サポート対象のハードウェア」
UEBAのアーキテクチャを理解します。	『*導入ガイド*』の「NetWitness Platformネットワーク アーキテクチャ図」トピック
ファイアウォールでポートを構成します。	『*導入ガイド*』の「ネットワーク アーキテクチャとポート」トピック
NetWitness Serverホストおよびその他のコンポーネントをインストールします。	『*物理ホスト インストール ガイド*』の「タスク1: NetWitness Server(NW Server) ホストへの11.3のインストール」および「タスク2: その他のコンポーネント ホストへの11.3のインストール」 『*仮想ホスト インストール ガイド*』の「仮想環境でのNetWitness Platform仮想ホストのインストール」
UEBAをインストールします。	『*物理ホスト インストール ガイド*』の「RSA NetWitness® UEBA」
UEBA_AnalystsロールとAnalystsロールをUEBAユーザに割り当てます。	『*システム セキュリティとユーザ管理ガイド*』の「ロールの権限」

更新

次のタスクは、ここに記載された順序で実行する必要があります。

説明	参考情報
	
RSA LiveからEndpoint Packを導入します。これには UEBAとEndpointを統合するためのFile Category Lua Parserが含まれます。	導入時には、Endpoint Log Hybrid Log Decoderサービスを指定する必要があります。複数のEndpoint Serverがある場合は、すべてのEndpoint Log Hybrid Log Decoderサービスを選択します。
プロセスやレジストリなどのエンドポイント データ ソースを有効化して、UEBAでアラートを生成します。	「*更新ガイド*」の「エンドポイント データ ソースの有効化」
UEBAインジケータ フォワーダを有効化してUEBAインジケータをNetwitness Respond ServerとCorrelation Serverに転送し、インシデントを作成します。	「*更新ガイド*」の「UEBAインジケータ フォワーダの有効化」

説明	参考情報
NetWitness Platform 11.3に更新した後、BrokerまたはConcentratorのUUIDが変更されます。NetWitness Platformコア サービスを更新し、BrokerまたはConcentratorのUUIDを更新する必要があります。	「*更新ガイド*」の「BrokerまたはConcentratorのUUIDの更新」
Airflow構成を更新します。	「*更新ガイド*」の「Airflow構成の更新」
presidio_upgrade DAGが正常に完了したら、Airflowスケジューラ サービスを再起動します。	「*更新ガイド*」の「Airflowスケジューラ サービスの再起動」

調査

次のタスクは、任意の順序で実行できます。

説明	参考情報
	
高リスク ユーザを調査します。	『*RSA NetWitness UEBAユーザ ガイド*』の「高リスク ユーザの調査」トピック
上位アラートを調査します。	『*RSA NetWitness UEBAユーザ ガイド*』の「上位アラートの調査」トピック

監視

次のタスクは、任意の順序で実行できます。

説明	参考情報
	
ヘルス モニタでNetWitness UEBAのメトリックを確認します。	『RSA NetWitness UEBAユーザ ガイド』の「ヘルス モニタでのNetWitness UEBAメトリックの表示」トピック
UEBAの稼働状態を監視します。	『RSA NetWitness UEBAユーザ ガイド』の「ヘルス モニタでのUEBAの監視」トピック