RSA NETWITNESS® PLATFORM

NetWitness Investigate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® Investigateとは？

NetWitness Platformは、ネットワーク上のすべてのトラフィックを調査および監視します。NetWitness Platformのサービスの1つであるDecoderは、ネットワーク内のパケット、ログ、エンドポイント データを収集、解析、保存します。Decoderに構成されたパーサとフィードは、収集したログおよびパケットをアナリストが調査できるよう、メタデータを作成します。別のタイプのサービスであるConcentratorは、メタデータのインデックスを作成し、保存します。NetWitness Investigateは、RSA NetWitness® Platformのデータ分析機能を提供します。アナリストはこの機能を使用して、パケット、ログ、エンドポイント データを分析し、セキュリティとITインフラストラクチャに対する内部または外部からの潜在的な脅威を特定することができます。

本書について

このガイドでは、SOCチームのすべてのメンバを対象に、NetWitness Investigateを構成し、ログおよびネットワーク イベントを調査するためのエンドツーエンドのガイドラインを提供します。NetWitness Investigateを使用してエンドポイントおよびユーザの行動を調査するためのエンドツーエンドのガイドラインについては、次のドキュメントを参照してください。

- *NetWitness Endpointクイック スタート ガイド*
- *NetWitness UEBAクイック スタート ガイド*

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。SOCチーム全体が対象のタスクです。

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する	*RSA NetWitness Platform 11.3リリース ノート*
NetWitness Investigateの仕組みを理解する	『*NetWitness Investigateユーザ ガイド*』の「NetWitness Investigateの仕組み」

セットアップ、インストール、またはアップグレード

NetWitness Investigateには、特別なセットアップ、インストール、またはアップグレード タスクは必要ありません。NetWitness Platformの一部に組み込まれています。ただし、次のタイプの分析を行う場合は、NetWitness Investigateと連携するコンポーネントをセットアップする必要があります。これらのタスクは管理者が行います。SOCマネージャがセットアップについて理解したい場合は参照してください。

説明	参考情報
	
Malware Analysisのインストールとセットアップ(スタンドアロンまたはサービス)	Malware Analysis構成ガイド
NetWitness Endpointのインストールとセットアップ(スタンドアロンまたはサービス)	NetWitness Endpointクイック スタート ガイド
NetWitness UEBAのインストールとセットアップ(スタンドアロンまたはサービス)	NetWitness UEBAクイック スタート ガイド

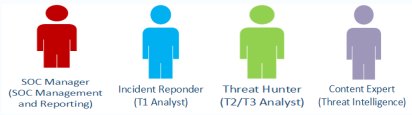
システムレベルの構成

管理者は、NetWitness Investigateのシステムレベルの環境設定を行います。次のタスクは、管理者が実行します。タスクは任意の順序で実行できます。SOCマネージャは、選択可能な構成オプションを理解する必要があります。

説明	参考情報
	
NetWitness Investigateを使用するアナリスト用に、RBAC(ロールベースのアクセス制御)を構成します。NetWitness Investigateに関連する権限を持つコンポーネントは次のとおりです:調査([ナビゲート]ビューおよび[イベント]ビュー)、Investigate-server([イベント分析]ビュー)、マルウェア([Malware Analysis]ビュー)、Endpoint-broker-server、Endpoint-server	『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*」
ユーザのロールによってアクセス可能なコンテンツを制限するようNetWitness Investigateを構成します(プレクエリ)。	『システム セキュリティとユーザ管理ガイド』の「*ロールごとのクエリおよびセッションの属性の検証*」
システム レベルでNetWitness Investigateのデフォルト設定と制限を構成します。	『システム構成ガイド』の「調査の設定の構成」

ユーザ環境設定の構成

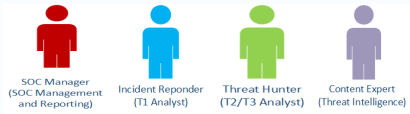
次のタスクは、脅威ハンター、コンテンツ エキスパート、インシデント対応者、SOCマネージャを対象としています。タスクは任意の順序で実行できます。

説明	参考情報
	
[ナビゲート]ビューおよび[イベント]ビューの環境設定を構成します。	『*NetWitness Investigateユーザ ガイド*』の「[ナビゲート]ビューおよび[イベント]ビューの構成」
[イベント分析]ビューの環境設定を構成します。	『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューの構成」
[Malware Analysis]ビューの環境設定を構成します。	『*Malware Analysisユーザ ガイド*』の「Malware Analysisの構成」

調査

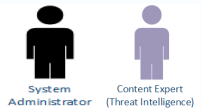
アナリストのスキル レベルと目的により、異なるタイプの調査を行うことができます。

- インシデント対応者(T1アナリスト)は、インシデントへの対応と改善のため、通常、NetWitness RespondからNetWitness Investigateに移行して、インシデントに関する詳細な情報を検索します。
- 脅威ハンター(T2/T3アナリスト)は通常、イベント、メタデータ、およびRAWコンテンツを詳細に調査することにより、改善が必要な問題を特定し、改善します。
- コンテンツ エキスパート(脅威インテリジェンス)は通常、イベント、メタデータ、RAWコンテンツ、ユーザ データ、ホスト データ、UEBAデータを詳細に調査することにより、新しい脅威インテリジェンスを調査したり、新しいフィードを評価および作成したり、セキュリティ侵害インジケータを警告する相関ルールを作成します。
- SOCマネージャは、ユース ケースを理解する必要があります。

説明	参考情報
	
実践的なユース ケースを学習する	『*NetWitness Investigateユーザ ガイド*』の「NetWitness Investigateの使用例」
ログとネットワークトラフィックのメタデータおよびRAWイベントを調査する	『*NetWitness Investigateユーザ ガイド*』の「調査の開始」
潜在的なマルウェアを調査する	Malware Analysisユーザ ガイド
エンドポイントを調査する	NetWitness Endpointユーザ ガイド
ユーザの行動分析を行う	NetWitness UEBAユーザ ガイド

メンテナンス

管理者は次のタスクを任意の順序で実行できます。

説明	参考情報
	
クエリのリストを管理し、NetWitness Platformシステムの様々なユーザのクエリ パターンを分析します。	『システム メンテナンス ガイド』の「URL統合を使用したクエリのメンテナンス」

説明	参考情報
システムレベルの構成を微調整して、パフォーマンスを向上させたり、データへのアクセスを制限します。	『システム セキュリティとユーザ管理ガイド』の*「ロールごとのクエリおよびセッションの属性の検証」* 『システム構成ガイド』の「調査の設定の構成」