RSA NETWITNESS® ORCHESTRATOR

主な特長

- RSA NetWitness Platformとの統合
- 脅威インテリジェンス駆動型のインシデント管理
- セキュリティ侵害インジケーター（IOC）に基づく重要度の判定
- 強化されたプレイブック コントロールによるサービス品質の向上
- リアルタイムの実行
- 複数のチームおよびツール間の合理化されたコラボレーション
- 自動ドキュメント化
- 拡張性が高くセキュアなマルチテナント プラットフォーム
- 拡張可能な統合フレームワーク
- オンプレミスとクラウドへの柔軟な導入

主なメリット

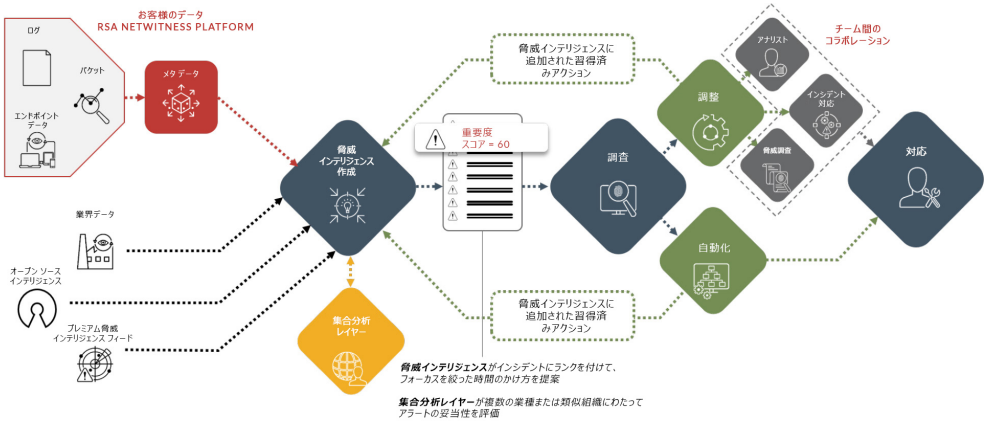
- 自動化：タスク指向の「人の作業」をソフトウェアに行わせて、脅威ハンティングを自動化
- オーケストレーション：意思決定の自動化または体系化
- ダッシュボードとレポート作成：脅威インテリジェンス駆動型メトリックの可視化
- インシデント管理とコラボレーション：エンドツーエンドのインシデント管理を提供
- 応答時間：レスポンス タイムを短縮してエラーを減らし、アナリストの生産性を向上させて、平均修復時間（MTTR）を最小化

最も重大な脅威にフォーカスする

攻撃対象領域が拡大し続ける時代に、コモディティ マルウェアから内部関係者による脅威、クライムウェア、国家主導によるエクスプロイトに至るまで、脅威アクターからデータや資産を保護することは、ますます複雑で時間のかかる作業になっています。すべての脅威が同じように発生するわけではなく、すべての脅威に注意を払う必要があるわけでもありません。しかし、予防、監視、調査の各テクノロジーがサイロ化され、互いに分離された状態では、誤検出をなくし、手動による反復的な作業を排除して、対応のフォーカスを絞ることはできません。セキュリティ チームには、セキュリティ オペレーション センター（SOC）がプロセスを効果的に自動化し、最も重大な脅威を検出して対応できるようになる包括的なソリューションが必要です。

RSA NetWitness® Orchestrator Built on ThreatConnect™は、完全なケース管理、インテリジェントなオートメーションとオーケストレーション、共同調査を組み合わせた包括的なセキュリティ オペレーション/オートメーション テクノロジーです。RSA NetWitness Orchestratorは、脅威の調査、ハンティング、対応に一貫性と効率性をもたらします。プレイブックと統合された脅威インテリジェンスを活用することで、アナリストのワークフロー、コラボレーション、対応を強化するだけでなく自動化も行います。RSA NetWitness Orchestratorは、RSA NetWitness Platformの結合組織としての役割を果たすと同時に、セキュリティ オペレーション チームのセキュリティ武器庫として機能します。

オーケストレーションとオートメーションの中心となる脅威インテリジェンス



RSA NETWITNESS ORCHESTRATORのシステム要件

物理インスタンス

- 物理サーバーの要件
  - アプリケーションサーバー（プレイブックなし）
    - メモリー： 16GB
    - CPUコア数：8（2GHz）
    - 推定ストレージ：50GB
  - アプリケーションサーバー（プレイブックあり）
    - メモリー：48GB
    - CPUコア数：8（2GHz）
    - 推定ストレージ：150GB
  - データベースサーバー（200万個未満のインジケーター）
    - メモリー：12GB
    - CPUコア数：6（2GHz）
    - ストレージ：20GB
  - データベースサーバー（200万～500万個のインジケーター）
    - メモリー： 16GB
    - CPUコア数：8（2GHz）
    - ストレージ：40GB
  - データベースサーバー（500万～1,000万個のインジケーター）
    - メモリー：32GB
    - CPUコア数：12（2GHz）
    - ストレージ：60GB
  - Elasticsearch®サーバー（200万個未満のインジケーター）
    - メモリー：12GB
    - CPU/vCPUコア数：6（2GHz）
    - ストレージ：20GB
  - Elasticsearchサーバー（200万～500万個のインジケーター）
    - メモリー： 16GB
    - CPU/vCPUコア数：8（2GHz）
    - ストレージ：40GB
  - Elasticsearchサーバー（500万～1,000万個のインジケーター）
    - メモリー：32GB
    - CPU/vCPUコア数：12（2GHz）
    - ストレージ：60GB

インシデント管理の新定義

RSA NetWitness Orchestratorを使用すると、セキュリティ オペレーション チームは、サイロ化されたアラートを組織のセキュリティ武器庫から収集して、相互に関連づけられたコンテキストリッチなインシデント（重要なデータを含む）に変換できます。このソリューションは、ユーザーの評判、システム、IP、ネットワーク、関連するインシデント、常習犯、脅威に関するインテリジェンスを利用して、アナリストが情報に基づいた意思決定を迅速に行えるようにします。また、インシデント管理プロセスを綿密に構造化し、一貫性をもたせて自動的にドキュメント化して、インシデント管理ライフサイクル全体を通じてセキュリティ アラートを統合、関連づけ、強化することで、セキュリティ オペレーション関連の決定の基盤としての役割を果たします。

既知の脅威への対処を自動化して、未知の脅威を検出

可視性は効果的な脅威検出の鍵です。RSA NetWitness Orchestratorは、500を超えるアプリケーションと統合でき、無数のセキュリティ対応を実現します。たとえば、インシデントあたりの解決時間を短縮できる、透明性の高い共同調査などが可能です。セキュリティ アナリストは、ログ、ネットワーク、エンドポイント、セキュリティ、非セキュリティの各ソリューションにわたる包括的なデータを使用して、企業全体の脅威の検出と対応を加速できます。事前設定済みの豊富なプレイブックを利用するか、プレイブックを独自にカスタマイズして、一貫性のある精密なインシデント対応を実現できます。RSA NetWitness Orchestratorを使用して、既知および低リスクの脅威への対処を自動化し、封じ込めと根絶を迅速化することによって、これらの作業から解放されたアナリストが高リスクの問題を調査できるようにします。

脅威インテリジェンスに基づくオーケストレーションとオートメーション

RSA NetWitness Orchestratorは、特定のワークフローをトリガーするためだけにインテリジェンスを使用するソリューションとは異なり、すべてのオーケストレーションおよびオートメーション機能にわたって脅威インテリジェンスを活用することによって、状況に順応する豊富なコンテキストとプレイブックを実現します。また、ワークフロー内のチーム間の調整をサポートすることで、あらゆるインテリジェンスの価値を最大限に引き出すことができます。

RSA NetWitness Orchestratorは、脅威インテリジェンス、オーケストレーション、オートメーション、対応を組み合わせて、システム全体の包括的なインサイトを提供し、セキュリティ オペレーション チームが以下を行うことが可能にします。

- **適切な脅威インテリジェンスに基づくアラート、ブロック、隔離。**アラートやブロックなどの下位レベルのタスクであっても、適切な脅威インテリジェンスを使用することは重要です。検出と防止は自動化できますが、適切な脅威についてアラートを受け取り、それらの脅威をブロックできるようにするには、複数ソースからの検証済みの脅威インテリジェンスが必要です。
- **正確性、信頼性、精度の向上。**状況認識と過去のコンテキストは、意思決定の鍵となります。脅威インテリジェンスから直接作業することで、対応を迅速化し、より多くの攻撃を未然に防ぐこといが可能になります。事前に自動化できるタスクが多いほど、プロアクティブに対応できるようになります。誤検出を排除し、検証済みのインテリジェンスを使用することで、より正確な対応が可能になり、スピードと精度が高まります。
- **コンテキストを把握して改善を重ねる。**脅威インテリジェンスのしきい値（指標評判スコアなど）に基づいてタスクを自動化し、そのすべての情報を記憶します。これにより、プロセスを戦略的に評価し、どのように改善すべきかを確認できるようになります。

RSA NETWITNESS ORCHESTRATORのシステム要件

- オペレーティング システム：Red Hat® Linuxバリアント：Red Hat Enterprise Linux（RHEL）またはCommunity Operating System（CentOS）6または7
- Oracle® Java® Development Kit（JDK）：Oracle Java 8またはOpenJDK（JDKバージョン1.8）のローカル インストールへのアクセス
- Java Cryptography Extension：バージョン8
- Elasticsearch：Elasticsearchサーバー6.3.0
- Python®：Python 3.6.xのみのインストール：CPythonを指します
- Python SDK：TCEXバージョン1.0+
- Redis：Redis 4.0.10のインストール
- データベース（次のいずれかを選択）：
  - MySQL®：MySQL 5.7.x CommunityまたはEnterprise Editionのインストール
  - SAP S/4HANA®：SAP S/4HANA 2.0 SPS 02のインストール
  - PostgreSQL：PostgreSQL v11のインストール

注意：作業用データベースとして1つだけインストールしてください。

- **確信に基づく調整。**ネイティブのセンスメイキング分析を外部の脅威インテリジェンスに適用することで、誤検出を減らし、アラート、ブロック、隔離の正確さを高めることができます。残念ながら、大量の脅威情報フィードを取得することや、共有IOCをアクションに使用することはできません。順応性のあるスコアリングとコンテキスト化によってアクションを決定し、規模に応じたセンスメイキングを行って、アクションが必要かどうかを確認する必要があります。
- **セキュリティ オペレーションと対応から有機的なインテリジェンスを構築。**人材とデータは、究極の情報源です。オペレーションと対応の取り組みからインサイト、アーティファクト、目撃情報を収集したら、すぐにそれらを新しいIOC、敵対的な戦術と手法、セキュリティ ギャップに関する知識の形でインテリジェンスに変換できることが必要です。
- **情報とコンテキストの変化に応じて、プロセスを自動的に調整。**オーケストレーション機能を変化する脅威インテリジェンスに適合させ、インジケーター分類と脅威評価スコアに応じて内部プロセスを自動的に調整できることが必要です。これらのプロセスとワークフローを動的に更新して、チームの取り組みの妥当性と有効性を高めることができます。

柔軟で拡張性に優れた導入

RSA NetWitness Orchestratorは、マルチテナント、シングルテナント、および真のオンプレミス環境での導入をサポートするようにゼロから設計されています。導入形態に関係なく、データは安全に分離され、垂直方向と水平方向の両方の拡張を簡単に行えます。RSAは、一元管理された複数のネットワーク環境にわたるオーケストレーションをサポートします。

典型的なセキュリティ オーケストレーションとオートメーションのテクノロジーは、SOCのオートメーションとエンリッチメントを最大化するために必要なワークロードの量と範囲に対応できるだけの拡張性を備えていません。そのため、セキュリティ チームは少数のユースケースしか自動化できず、多くの手動ワークフローが残ったままとなります。RSA NetWitness Orchestratorは、オーケストレーションとオートメーションのワークロードをSOCとともに拡張できる、真にスケーラブルなアーキテクチャを提供します。セキュリティ チームは、実行の優先順位付け、特定のプレイブック専用のリソースの割り当て、ワークロードの需要の増加に応じたプレイブックサーバーの追加を行うことができます。

RSA NETWITNESS PLATFORM

30年以上のセキュリティ専門知識を持つRSAは、最大規模のグローバル組織が抱えているセキュリティ オペレーションの課題に対処できる、革新的なソリューションで市場をリードし続けています。新しいRSA NetWitness Orchestratorは、ログ、ネットワーク、およびエンドポイント全体にわたる広範な可視性を活用して、RSA NetWitness Platformとその全方位型SIEMと脅威防御製品を拡張します。

RSAについて

RSAはBusiness-Driven Securityソリューションを提供し、さまざまな組織が、統合的な可視性、自動化されたインサイト、および組織的なアクションを使用してデジタル リスク管理のための統合的なアプローチを採用できるようサポートしています。RSAのソリューションは、高度な攻撃の効果的な検出と対応、ユーザー アクセス制御の管理、さらにビジネス リスク、不正行為、サイバー犯罪の削減を目的として設計されています。RSAは、世界中の数百万人のユーザーを保護し、Fortune 500の企業の90%以上が成功し、革新的な変化に継続的に適応できるように支援しています。詳細はrsa.com/ja-jpをご覧ください。