データシート

セキュリティ

ArcSight Recon

Micro Focus ArcSight Recon は、SIEM ログ管理ツールおよびセキュリティ分析の包括的なソリューションです。コンプライアンスの負担を軽減し、フォレンジック調査の期間を短縮します。

製品概要

サイバーセキュリティの重要性はこれまでになく高まっています。オンラインでビジネスを行う企業の数、デジタルで保存される機密情報の量、リモートで処理される業務が大幅に増えているためです。犯罪者の侵入手段はより巧妙になり、コンプライアンスの規定は次第に厳格化されています。

セキュリティデータを組織が収集および保存するソースの数が膨大な数になったことで、データの監視と管理がより一層困難になっています。市販のソリューションの多くは、セキュリティのために構築されたものではありません。このため、SIEM、セキュリティのコンプライアンス、イベントのログ記録、フォレンジック調査に利用しようとすると却って効率が低下します。ログ記録とフォレンジック調査は、現在の SOC に不可欠です。現在のスタンダードであるというだけでなく、今後も引き続き利用できるソリューションが必要です。

ArcSight Recon は、ログの管理およびセキュリティ分析の包括的なソリューションです。コンプライアンスの負担を軽減し、フォレンジック調査の期間を短縮します。ログ管理におけるコンプライアンス、保存、レポート作成の要件を満たすとともに、ビッグデータを検索および分析する機能を備えています。Recon はセキュリティイベントのログ記録向けに設計されているため、セキュリティアナリストは直感的に使うことができます。運用に DBA は必要ありません。組織全体のデータログを統合し、膨大な量のイベントを処理して、すみやかに検索、ビジュアル表示、レポート作成に試用できるようにすることで、脅威の検知と対策を支援します。SOC のエンジニアは、Recon により

組織内のアラートの内容を詳細に把握できます。階層化された強力な分析を行うという ArcSight のミッションにおいて、Recon は重要な役割を担っています。

主な利点

ログの一元管理

ArcSight Recon は、多数のソース (ログ、クリックストリーム、センサー、ストリーミングネットワークトラフィック、セキュリティデバイス、Web サーバー、カスタムアプリケーション、SNS、クラウドサービスなど) から収集したテラバイト単位のマシンデータを保管します。データの保存、検索、監視、分析により、組織全体のセキュリティインテリジェンスを一元管理できます。Recon のイベント詳細パネルで個別のイベントおよびグループ化したイベントを調査できるため、迅速にデータを探すことができます。RAW Message ビューでは、加工される前のオリジナルのイベントログを調べることができます。シンプル、使い勝手、セキュリティを念頭に構築されています。運用に DBA は必要ありません。

主な特長

- イベント詳細パネル
- RAW Message ビュー
- 異常値検知
- ユーザーフレンドリーな検索バー
- コンテンツレポート作成パッケージ
- ArcSight 統合プラットフォーム
- シングル ID ログイン

主な利点

- ログを一元管理
- 脅威をより迅速に検知して処理
- コンプライアンス用のレポート作成
- 大量のデータを保存
- 既存のセキュリティ環境との統合

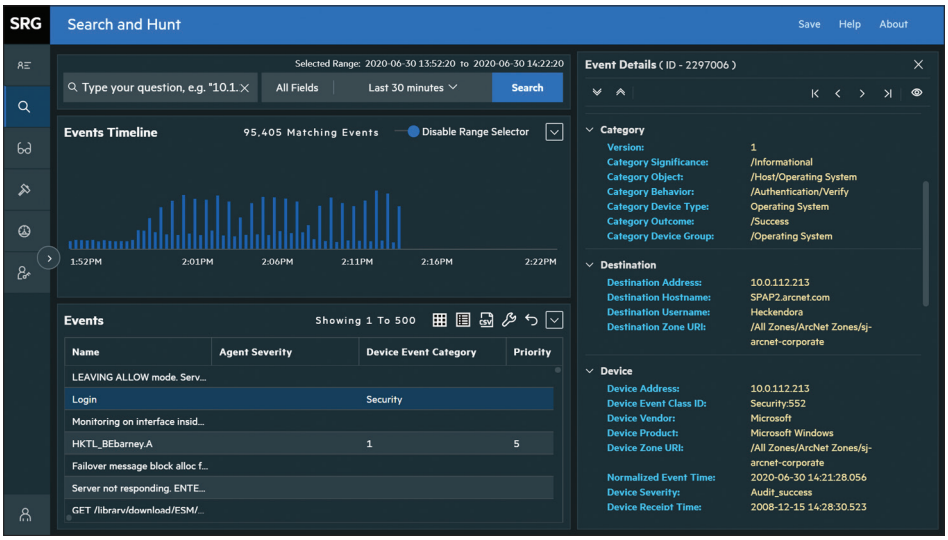

図 1 イベント詳細パネル

脅威をより迅速に検知して処理

Recon の動的クエリ提案機能により、強力なセキュリティ分析テクノロジーによって、膨大な数のログデータを最小限の労力で絞り込み、より短時間で結果を取得することができます。ArcSight Recon のカラム型データベースは、クエリーの回答を返す時間が一般的なデータベースよりも短いため、膨大な数のイベントを効率的に調べることができます。クリーンで構造化されたデータを一元管理することで、調査時間が短縮され、結果の品質が向上します。異常値検知機能による可視化により、ホストのふるまいのベースラインとなる指標からの逸脱を簡単に特定できます。Recon のユーザーフレンドリーな検索インターフェイスから、グリッドビュー、はメッセージビュー、および時間ベースのヒストグラムを表示できます。膨大な数のデータセットから容易に脅威を検知できるため、大規模なセキュリティ分析が可能になります。専門知識の要件とトレーニングは最小限で済みます。異常の優先度を設定することで、効率を向上できます。

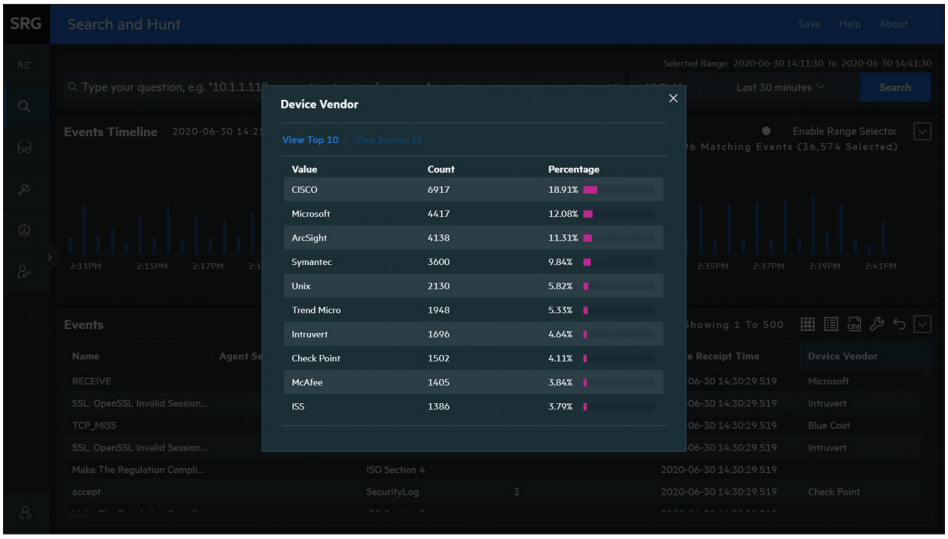

図 2 ベンダーデバイスの値を表すヒストグラム

コンプライアンス用のレポート作成

Recon のコンテンツレポート作成パッケージにより、短時間でコンプライアンスレポートを作成できます。レポート作成ウィザードを使用するか、テンプレートを選択して、クロス集計レポート、表、図表ベースのレポートを作成することができます。FIPS 140-2 コンプライアンス用のコンテンツが事前に用意されています。レポート作成テンプレートは今後のリリースで追加される予定です。Recon の MITRE ATT&CK コンテンツは、組織のコンプライアンスとセキュリティ対策の一貫性の確保に役立ちます。

大量のデータを保存

Recon のイベント集約およびログ圧縮の各機能により、より効率的にデータを保存できます。圧縮率が非常に高いため、セキュリティイベントのログデータの保存にかかるコストを抑えることができます。ArcSight SmartConnectors により、イベントを集約してフィルタリングできるため、ログの保存領域を節約できます。ArcSight Recon は、お客様の要件に合わせて拡張できるように構築されています。ノード 1 台に導入することも、複数のノードで導入することもできます。

既存のセキュリティ環境との統合

ストレージが統一されておらず、構造化されていない場合は、調査に時間がかかるうえ、パターンに結びつけることや複数ステージの攻撃を見つける際の制約になります。現在お使いのセキュリティオペレーションソリューションと統合することにより、セキュリティイベントを詳細に表示できます。ArcSight Recon は、Security Open Data Platform (SODP) アーキテクチャを採用しているため、480 種類を超えるソースからデータを収集、正規化、集約、拡充できます。ArcSight 2020.2 リリースでは、データの収集と保存が単一の統合ストレージプラットフォームに統合されました。Recon により、構造化されたデータレイクにデータを安全

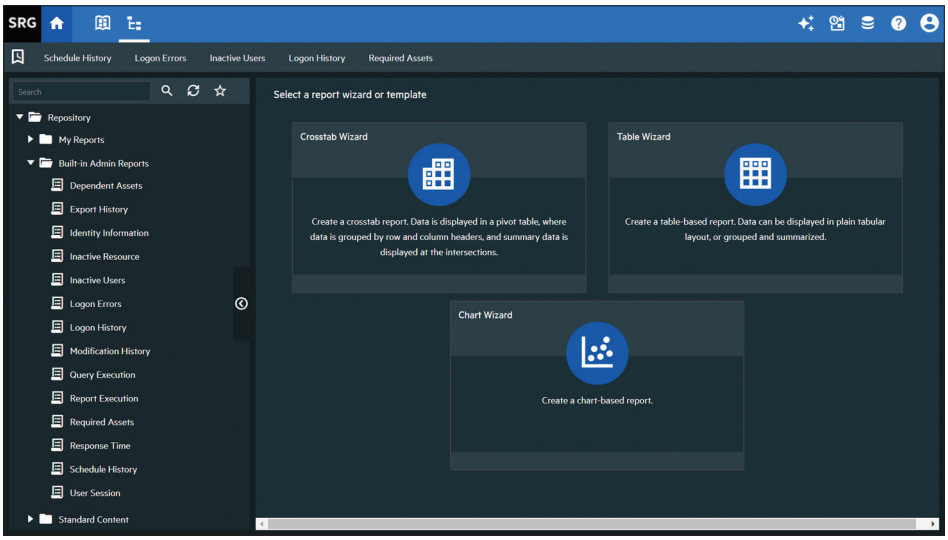

図 3 レポートの作成

に保存して、データを調査することができます。データを 1 度収集して保存するだけで、何度でも利用できます。今回の統合により、ボタンをクリックするだけで、ArcSight ESM、ArcSight Interset、ArcSight Recon を切り替えることができるようになりました。ArcSight のシングル ID ログイン (カスタマイズ可能) により、ArcSight ポートフォリオ製品の切り替えに要する時間を短縮できます。ソリューションを複数利用している場合は、主要なセキュリティツールと Recon を統合することができるため、調査にかかる時間が短縮され、ワークフローが効率化されて、応答時間を短縮することができます。

ArcSight を選ぶ理由

ArcSight の次世代 SIEM は、拡張性に優れた強力なプラットフォームです。セキュリティの専門家がセキュリティのプロフェッショナル向けに開発した統合ソリューションです。セキュリティ情報、ビッグデータの収集、ネットワーク、ユーザーおよびエンドポイントの監視、高度なセキュリティ分析テクノロジー (検知、調査、UEBA のソリューション) を独自に統合した包括的なアプローチにより、セキュリティインテリジェンスを提供します。リアルタイムでの脅威の検知と対応、コンプライアンスの自動化と保証、IT 運用に関するインテリジェンスを提供することにより、階層化された強力な分析アプローチによる企業の自己防衛を実現します。自社の SIEM ソリューションの強固さを主張するベンダーは数多くありますが、ArcSight のチームには、セキュリティに関する専門知識と経験があり、他のベンダーには真似できないリーダーシップがあります。Micro Focus は、次世代ソリューション、実証済みの手法、世界最大クラスの非常に複雑な SOC を扱ってきた 20 年の経験という他社にはない能力により、優れたセキュリティ対策と運用を支援します。

詳細情報はこちら：
www.microfocus.com/ja-jp/products/arcsight-recon/overview

お問い合わせ先:
www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp