データシート
セキュリティ

ArcSight Investigate

Micro Focus® ArcSight Investigateを利用すると、組織はセキュリティインシデントにプロアクティブに対処してインシデントの影響を軽減できます。

主な機能

- ホストプロファイラーダッシュボードを通じて、ホストの挙動を素早く分析し有益な情報を提供
- ガイド付きの提案を使って1日目からすぐにクエリの構築が可能
- セキュリティ調査向けに最適化された定義済みのビジュアライゼーションとカスタムチャートおよびダッシュボード機能
- Hadoopと容易に統合し、分析対象データの範囲を拡大

主なメリット

- 未知の脅威をすばやく見つけて対処
- アナリストの生産性を向上させることで人材不足に対応
- 応答時間を短縮してセキュリティインシデントの影響を軽減
- セキュリティイベントを網羅的に把握してリスクを低減

製品ハイライト

機械学習や高度な分析手法の登場にも関わらず、セキュリティ調査のあらゆる段階で、脅威を識別して適切な判断を行うために、セキュリティアナリストの能力や経験に大きく依存しています。スキルのある人材の需要は増加の一途をたどっており、米国 労働省労働統計局のレポートによると、2015年には米国だけで20万9,000件を超えるサイバーセキュリティの求人が埋まっておらず、求人の数は2010年から2015年の間に74パーセント増加しています。

こうしたスキルや人材不足が続く状況に対応するため、先進的な組織では従来のセキュリティツールの枠を越えた新しいテクノロジーを導入することで、セキュリティ運用のプロセス全体にわたる迅速化、簡素化、および分析力向上に取り組んでいます。

ArcSight Investigateは、変化し続けるセキュリティチームのニーズに対応する、最新の高度な分析プラットフォーム上に構築された次世代ハントおよび調査ソリューションです。ArcSight Investigateを利用すると、大量のデータをほぼ瞬時に処理することで、未知の脅威を見つけて対処できます。セキュリティアナリストは、この直感的で使いやすいソリューションを利用して優先度の高い脅威を高い精度ですばやく調査できます。さらに、ArcSight Investigateはデータレイクの活用にも対応しており、ビッグデータに基づいた分析を行うことで高い価値を実現します。

機能とメリット

脅威を即座に識別して迅速に対処

ArcSight Investigateは、ホストプロファイラーダッシュボードを通じてホストの挙動を詳細に分析することで、未知の脅威をこれまで以上にすばやく見つけ出すことができます。また、ユーザー識別機能を利用すると、クエリを作成

することなく、セキュリティイベントの影響を受けたユーザーを特定できます。

高性能分析プラットフォームであるVerticaを搭載しているため、調査プロセスでこれまでにない優れた分析能力を発揮します。Verticaの列型データベースは、従来の行指向データベースよりもはるかに速い速度でクエリに応答し、エクサバイト規模で分析を処理します。ArcSight Investigateには、こうした最新のテクノロジーが組み込まれており、他の調査ツールよりも最大10倍の速度で検索を実行して、数か月または数年分のデータでも数秒で結果を返すことができます。クエリを大規模に実行することが可能になるため、セキュリティアナリストは、検索の期間や結果のサイズの制約を受けることなく、自在にデータを探索できます。

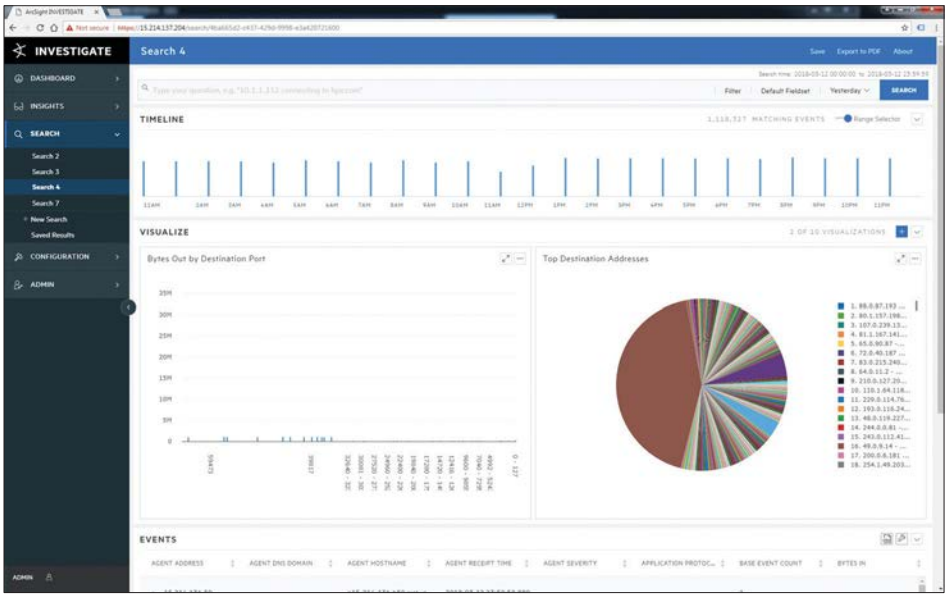

図1: ArcSight Investigateのダッシュボード

ガイド付き操作によるスマートな作業

ArcSight Investigateは、検索語句をセキュリティコンテキストで理解し、関連するクエリを動的に提案する直感的な検索インターフェイスを備えています。ユーザーは、提案された候補の中から選択するか、ドロップダウンメニューをクリックすることで、クエリの作成や修正を容易に行うことができます。ArcSight Investigateバージョン2.0には、定義済みのビジュアライゼーション機能が導入されているため、アナリストはこれをそのまま利用して包括的なビジュアル分析を行うことができます。このビジュアライゼーション機能は、必要に応じて編集または再構成することもできます。ArcSight Enterprise Security Manager (ESM) との直接統合により、ArcSight Investigateは ArcSight Enterprise Service Managerから自動クエリを読み込むことで、即座に調査を開始できます。経験の浅いセキュリティアナリストでも、複雑なクエリ言語や独自スキーマを学習することなく、すぐにクエリを作成できます。上級ユーザーは、スマート提案を使用することで、複雑なクエリを作成する時間を節約できます。

図2: ArcSight Investigateのホストプロファイラー

検索結果が得られても、その膨大な量のイベントを調べるのには時間と手間がかかります。ArcSight Investigateではデータを容易に操作できるため、ユーザーはクエリを実行したり他の分析ツールにデータをエクスポートしたりすることなく、データ間の移動、データの集計、およびビジュアル表示を行うことができます。定義済みのチャートタイプを使用すると、データを素早くビジュアル化して、パターン、異常、およびイベント間の関係を識別できます。チャートの保存またはビジュアルの追加を行い、カスタマイズしたダッシュボードを作成し、セキュリティアナリストが主要なメトリックを一目で確認できるようにして、進行中の調査を継続的に監視することができます。

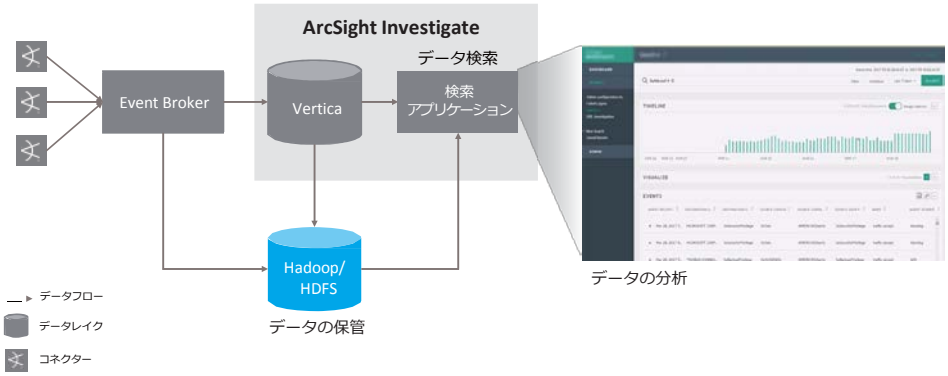

図3: Hadoop統合アーキテクチャー

対象を拡大し、未知の見えない脅威を明らかにする

構造化されていないばらばらなデータストレージは、調査の遅れにつながります。また、反復パターンや多段的な攻撃を十分に関連付けることができません。ArcSight Data Platformとの統合を通じて、さまざまなソースからのセキュリティデータの正規化とカテゴライズを行うことで、セキュリティチームはデータ探索用の構造化された単一のデータレイクを構築できます。ArcSight Investigateには、強力な分析機能が組み込まれているため、ビッグデータから意味のある情報を導き出して、見えない脅威を明らかにすることができます。

多くの組織では、Hadoopに保管された長期的なデータがセキュリティ調査にフルに利用されることはほとんどありません。これは、ユーザー操作に時間がかかるためです。ArcSight Investigateには、Hadoopに保管された過去のイベントにアクセスするユーザーインターフェイスが統合されているため、スムーズな操作が可能で、シームレスな表示を通じてあらゆる期間のデータを検索し分析できます。

セキュリティ運用の迅速化、簡素化、および有効性の向上

ArcSight Investigateでは、検索結果が瞬時に返されるため、セキュリティインシデントへの対応が迅速化されます。また、セキュリティアナリストは、さまざまな実験を行い直感に従って未知の脅威を探し出すことができます。構造化したすべてのデータを1つの場所にまとめて分析に利用できるようにすることで、調査を迅速化し、データから得られる情報の質を高めることができます。最も重要なのは、ArcSight Investigateの使いやすい検索インターフェイスと内蔵された分析機能により、手動タスクを効率化できることです。これにより、セキュリティアナリストに必要な専門知識やトレーニングの要件が軽減されます。また、重要度の高い作業を優先して行うことが可能になり、業務の効率化を実現することができます。

詳細情報

microfocus.com/investigate

www.microfocus.com

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

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