ネットワークとエンドポイントの脅威検出・対応のインテグレーションがもたらす防御力

環境全体の完全な可視化

攻撃者の戦術、技術、手順（TTP）を検出し、それに対応するには、その環境で起こっているすべてを完全に可視化することが役立ちます。ネットワークでは、攻撃対象領域となる非管理型 IoT デバイスや契約業者のデバイスと、多くの攻撃の最終標的である管理対象エンドポイントの情報が有用です。ネットワークとエンドポイントのセキュリティのインテグレーションにより、高度なサイバー脅威に対する効果的な防御が可能になります。

世界をリードする先進的なネットワーク脅威検出・対応プラットフォームである Arista NDR プラットフォームは、CrowdStrike Falcon Insight と完全かつ簡単に統合でき、これにより、非常に包括的な脅威検出、迅速で効果的な対応、封じ込め、フォレンジック分析機能を提供します。この組み合わせは、企業内の管理対象インフラストラクチャと管理対象外インフラストラクチャの両方において、強固なセキュリティ態勢を維持するために必要な可視化と信頼性を実現します。

インテグレーションがもたらすメリット

- 管理対象デバイスと管理対象外デバイスの可視化、検出、対応
- エンドポイントとネットワークのコンテキストでのキルチェーン調査が簡単に利用可能
- セキュリティ・オペレーションの統合で対応コストを削減
- 迅速で効果的な対応と封じ込めで修復までの時間を短縮

それぞれのプラットフォームの強み

ARISTA

Arista NDR プラットフォームは、管理対象エンドポイントに加え、50%以上の管理対象外インフラストラクチャの幅広いコンテキストを提供します。したがって、Arista NDR は、潜在的な攻撃対象領域とそこに含まれるビジネス資産を完全に可視化できます。

Arista NDR は、ネットワーク上のあらゆる動作を観測および分析し、ネットワーク上を移動する資産を追跡します。また、エンティティ間の関係と類似性を自律的に理解して提示します。このプラットフォームは異常または脅威を感知し、必要に応じて数秒以内に対応することができます。

CROWDSTRIKE

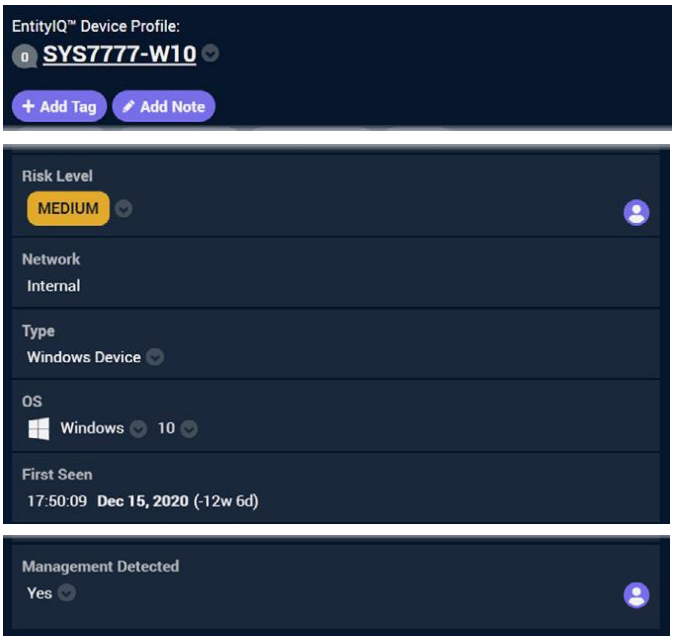
従来のエンドポイント・セキュリティ・ツールには盲点があり、高度な脅威を発見して阻止することができませんでした。CrowdStrike® Falcon Insight™は、組織全体のエンドポイントを完全に可視化することで、この問題を解決します。

Falcon Insight は、すべてのエンドポイント・アクティビティを継続的に監視し、リアルタイムでデータを分析して脅威のアクティビティを自動的に特定します。そのため、高度な脅威を発生時に検出および防止できます。また、すべてのエンドポイント・アクティビティは CrowdStrike Falcon®プラットフォームにストリーミングされるため、セキュリティ・チームはインシデントを迅速に調査し、アラートに対応し、新しい脅威を予防的に検出できます。

相互補完で実現されること

このインテグレーションにより、Arista NDR プラットフォームに Falcon Insight のエンドポイント・データが自動的に表示されます。

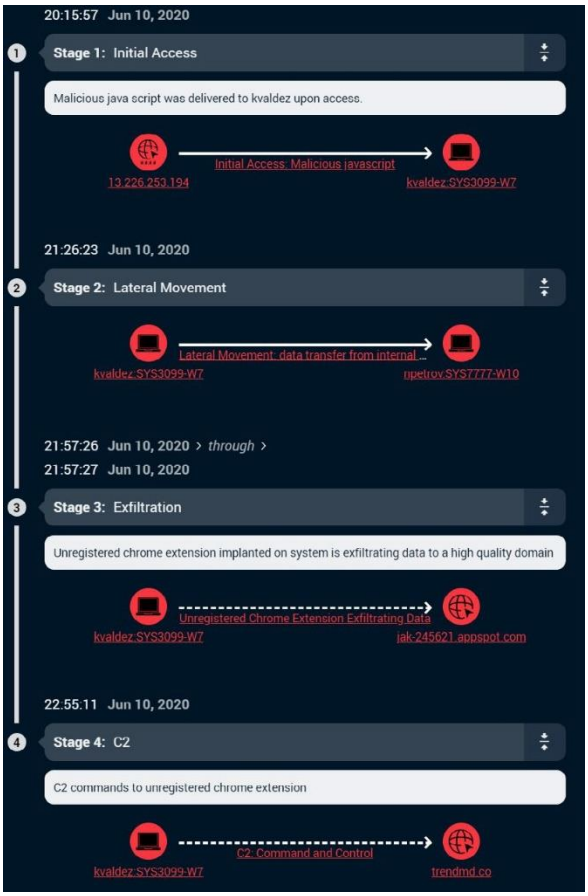
これにより、脅威を調査するセキュリティ・アナリストは、ネットワークとエンドポイントのコンテキストを利用して、効果的なリスク管理の判断を下すことができます。また、ワークフローの最適化と統合により、ヒューマン・エラーが減り、コンテキストを何度も切り替える運用オーバーヘッドも低減されます。Arista NDR のネットワーク可視化は、Falcon Insight で管理されないデバイス、ユーザー、アプリケーションを検出します。例えば、最近のある攻撃では、外部からアクセス可能になっている IoT デバイスを Arista NDR が発見しました。このデバイスは侵害された後、管理対象エンドポイント間のラテラル・ムーブメントに悪用されていました。この脅威は発見されて、迅速に封じ込められました。



可視化の詳細：インテグレーション事例

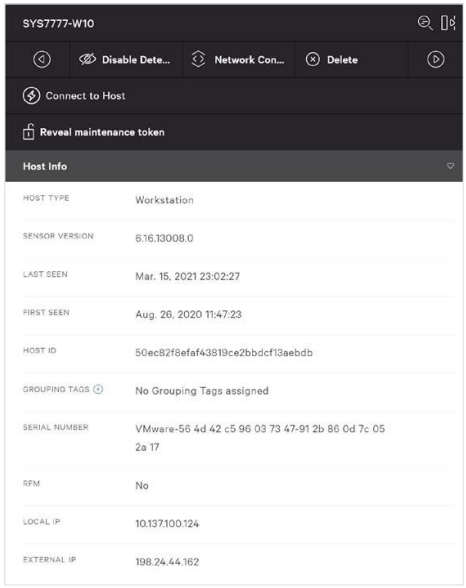
侵害のタイムラインの自動表示

Arista NDR は、疑わしいデバイスについてフラグが付けられたアクティビティを示すフォレンジック・タイムラインと、キルチェーン全体とともに調査に関連する他のデバイス、宛先、アクティビティを特定する広範な攻撃マップを自動的に作成します。



分離と修復

このインテグレーションにより、ワンクリックのエンドポイント修復でデバイスを隔離し、ラテラル・ムーブメント、コマンド・アンド・コントロール、データ流出を防ぐことができます。



ご利用案内 – インテグレーションをセットアップして環境を完全に可視化するには

このインテグレーションは、次の 2 つの簡単なステップでセットアップできます。

1 CrowdStrike プラットフォームを利用するための API キーと URL を取得してください。

2 Arista NDR のカスタマー・サクセスが、インテグレーションを有効化するための残りの作業を行います。

アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル 27F
Tel:03-3242-6401

西日本営業本部
〒530-0001 大阪市北区梅田 2-2 ヒルトンプラザウエストオフィスタワー 19F
Tel: 06-6133-5681

お問い合わせ先
Japan-sales@arista.com

www.arista.com/jp

2022 年 9 月 15 日