お客様成功事例

セキュリティ

NPC Ukrenergo

Micro Focus ArcSightは、チーム間のコラボレーションとデータドリブンなセキュリティ分析により、高度な脅威検出と脅威対応を大幅に改善します。

NPC Ukrenergo について

NPC Ukrenergo はウクライナの電力会社です。同国のエネルギーシステムの運用と技術を管理しています。また、発電所から各地の電力供給会社の配電網への送電も担っています。8,000 人以上の従業員を擁し、各地の 8 つの電力システムを通じてウクライナ全土にサービスを提供しています。

サイバー攻撃による全国規模の停電

2015年12月、ウクライナの送電網に対して、「BlackEnergy」と呼ばれるサイバー攻撃が仕掛けられました。この攻撃は、送電網に対するサイバー攻撃として初の「成功例」として知られています。ハッカーが同国の 3 社の配電会社の情報システムに侵入し、1 ～ 6 時間にわたり、230,000 人の消費者への電力供給を一時的に停止させました。

主要なインフラストラクチャ企業である NPC Ukrenergo は、自社のセキュリティプロセスについて綿密な検査を実施しました。NPC Ukrenergo の Senior Information Security Analyst、Dmitriy Ryzhkov 氏は次のように話します。「当社のように、産業用制御システムを保護する組織には、特別なルールが必要です。可用性とビジネス継続性が最優先事項です。中断が発生すれば、国民全員に深刻な影響を及ぼすことになるためです。当社のシステムは、IT チームではなく、運用チームとインフラストラクチャチームが管理しています。包括的なセキュリティ管理のためには、チーム間のコラボレーションが不可欠です。チーム間のコラボレーションとセキュリティソリューションのサポートがなければ、当社のシステムは攻撃に対して無防備になるでしょう。」

「Micro Focus ArcSight により、真の脅威を迅速に検出できるだけでなく、ほぼリアルタイムでオーケストレーションされたインシデント対応を自動化することもできます。ArcSight の柔軟性により、将来に向けてインテリジェントにインシデント対応ができます」

DMITRIY RYZHKOV氏
Senior Information Security Analyst
NPC Ukrenergo

チーム間コラボレーションの基盤となる ArcSight データベース

同社は、セキュリティオペレーションセンター (SOC) が必要だとの判断に至りました。SOC とは、組織および技術レベルでセキュリティ問題を一元管理する組織です。将来の攻撃について学び、その攻撃から組織を保護し、SOC の構成に対する理解を深めるためのステップとしては、包括的なセキュリティ

UKRENERGO
National power company

概要

業界
エネルギー、公益

所在地
ウクライナ

課題
脅威データの可視化とチーム間コラボレーションの促進により、重要なインフラストラクチャをサイバー攻撃から保護

製品とサービス
Micro Focus ArcSight Enterprise Security Manager (ESM)
Micro Focus ArcSight Logger

主な成功要因
+ チーム間コラボレーションを改善
+ 可視性の向上により、アラートとインシデント対応を改善
+ スクリプティングや自動化などの高度な機能により、時間を短縮
+ 高度な脆弱性評価とリスク評価を実現

ArcSight ESM のデータは、当社の経営陣が奨励するチーム間コラボレーションのための最適な基盤となりました。脆弱性をピンポイントで突き止めることのできるダッシュボードを作成し、IT セキュリティ、保守、運用の各チームが協力して、対応することができました。

DMITRIY RYZHKOV氏
Senior Information Security Analyst
NPC Ukrenergo

お問い合わせ先：
www.microfocus.com

情報イベント (SIEM) ソリューションを知るのが最適です。Micro Focus ArcSight Enterprise Security Management (ESM) は、セキュリティ分析により強力で効率的な脅威検出と脅威対応を実現するソリューションとして市場で広く知られています。これは同社のチームが必要としていたソリューションでした。

そこで、NPC Ukrenergo はインフラストラクチャの評価に取り掛かりました。「効率的に SIEM を導入するためには、インフラストラクチャと IT のシステム運用を完全に理解しなければなりません。」と Ryzhkov 氏は言います。「どのようなデータログが保存されているか？どのタイプのユーザーが、どのレベルのアクセス権を持っているか？当社の環境に対して脆弱性スキャンを実行し、対策が必要なリスクのレベルを評価しました。そして、脆弱性スキャンの結果データを Arcsight ESM コンソールで分析しました。ArcSight ESM の機能を把握するのに時間が必要でした。しかし、把握してしまえば、このソリューションがもたらすチャンスと柔軟性は明白でした。ArcSight ESM のデータは、当社の経営陣が奨励するチーム間コラボレーションのための最適な基盤となりました。脆弱性をピンポイントで突き止めることのできるダッシュボードを作成し、IT セキュリティ、保守、運用の各チームが協力して、対応することができました。」

セキュリティオペレーターがサイバーセキュリティのトレンドや情報を互いに共有して、ベストプラクティスのフレームワークを開発し、そのフレームワークを通じてカスタムのユースケースを構築しました。イベントソースを SIEM に追加したことも、重要な成功要因の 1 つでした。各チームは、ArcSight Flex Connector を活用して多数のデータソースタイプを接続し、データを収集、集合、クレンジング、エンリッチ化し、そのデータでセキュリティ分析を実行しました。ESM でデータを構造化することにより、データの利便性とコスト効率が向上しました。また、ArcSight Logger に組み込まれたコンテンツ、ダッシュボード、レポートにより、コンプライアンス文書をより迅速に作成し、コンプライアンス関連の負担を軽減することにも成功しました。

リアルタイムの脅威管理のための多層 SOC

フレームワークが SOC 組織内に浸透していく中で、そこに脅威インテリジェンスとインシデント対応を追加しました。ダッシュボードにより、NPC Ukrenergo が採用する MITRE ATT&CK フレームワークにセキュリティイベントをマッピングします。このナレッジベースが、特定の脅威モデルや手法を開発するための基盤となります。多数のイベントソース、具体的なユーザー行動分析、および MITRE ATT&CK フレームワークに加え、より高度なユースケースを追加した結果、リスク評価の明確化、可視性の強化、アラートとインシデント対応の改善が実現しました。

NPC Ukrenergo は、MITRE 原則に沿って SOC の責任を複数の層に分割しました。Ryzhkov 氏は次のように説明します。「ArcSight ESM を使用して次のようなモデルを開発しました。まず、第 1 層がセキュリティイベント、脆弱性スキャン、緊急アラートのリアルタイムモニタリングとトリアージを担当します。次に、第 2 層がインシデントの分析 / 調整 / 対応、フォレンジックアーティファクトの処理、内部ユーザーによる脅威の対応サポートを担当します。第 3 層となるシステム管理責任者は、インフラストラクチャの運用 / 保守とツールのエンジニアリング / デプロイを担当します。最後の第 4 層は、大幅な時間短縮につながるスクリプティングや自動化などの高度な機能を活用します。各チームが緊密に連携し、インテリジェンスを共有しながら、互いを支援しています」

Ryzhkov 氏は次のように結論付けています。「最高水準のセキュリティ保護を実現している組織でさえも、セキュリティ侵害と無縁ではいられません。しかし、当社の強みは、真の脅威を迅速に検出して対応できる点です。脅威は、検出が遅れれば遅れるほど、深刻な被害をもたらします。Micro Focus ArcSight により、真の脅威を迅速に検出できるだけでなく、オーケストレーションされた対応を通じて、ほぼリアルタイムで自動的に対応できます。ArcSight の柔軟性により、将来に向けてインテリジェントに適応できます」

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

168-JA0706-001 | M | 09/20 |