opentext™

成功事例

NPC Ukrenergo

ArcSight は、チーム間のコラボレーションとデータ駆動型のセキュリティ分析により、高度な脅威の検出と対応を大幅に改善しています。

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で初の「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、23 万人の消費者への電力供給を一時的に停止させました。

このため、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 の情報セキュリティ担当シニアアナリスト、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企業には、さまざま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、一般の人々に深刻な影響を及ぼすことになるためです。このシステムは、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、このシステムは攻撃に対して無防備になるでしょう」

「Micro Focus (現在は OpenText™ の傘下) 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対応を自動化できます。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」

DMITRIY RYZHKOV氏
情報セキュリティ担当シニアアナリスト
NPC Ukrenergo

チーム間コラボレーションのための 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、組織レベルおよび技術レベルでセキュリティ問題を一元管理する部門です。しかし、包括的なセキュリティ情報およびイベント管理 (SIEM) ソリューションは、企業が将来の攻撃について学び、その攻撃から組織を保護し、SOC の構成要素に対する理解

UKRENERGO
National power company

概要

- **業種**
  エネルギー、公益事業
- **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すること
- **製品とサービス**
  ArcSight Enterprise Security Manager (ESM)
  ArcSight Logger
- **成功ポイント**
  + チーム間コラボレーションを強化
  + 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、時間を節約
  + 高度な脆弱性評価とリスク評価を達成

「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プラットフォームになりました。当社の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ました。これにより、IT セキュリティ、保守、運用の各チームが協力して、脆弱性に対応することができます」

DMITRIY RYZHKOV 氏
情報セキュリティ担当シニアアナリスト
NPC Ukrenergo

お問い合わせ

を深めるための優れた中間ステップとなります。OpenText™ 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ことが市場で広く知られています。これは同社のチームがまず必要としていたソリューションでした。

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？どのようなユーザーが、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、その結果データを Arcsight ESM コンソールで活用しました。ArcSight ESM の機能を理解するのに時間がかかりましたが、理解してしまえば、その柔軟性と機会は明白でした。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プラットフォームになりました。当社の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ました。これにより、IT セキュリティ、保守、運用の各チームが協力して、脆弱性に対応することができます」

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と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 Connectors を活用して多数のデータソースタイプを接続し、データの収集、集約、クレンジング、エンリッチメントを行った後、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す。また、ArcSight Logger に組み込まれたコンテンツ、ダッシュボード、レポートで、コンプライアンス文書をより迅速に作成でき、NPC Ukrenergo のコンプライアンス関連の負担が軽減しました。

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 へと有機的に成長するに従って、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。NPC Ukrenergo が採用する MITRE ATT&CK フレームワークに、ダッシュボードでセキュリティイベントがマッピングされます。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っています。接続イベントソースの増加、具体的なユーザー行動分析、MITRE ATT&CK フレームワークとともに、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 では、MITRE 原則に沿って SOC の役割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、対応の他、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と保守、ツールのエンジニアリングと導入に注力します。最後の第 4 層には、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が含まれます。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すからです。Micro Focus (現在は OpenText™ の傘下) 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対応を自動化できます。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」

詳細はこちら：
www.opentext.com

opentext™