MICRO FOCUS

お客様成功事例

セキュリティ

Dubai Electricity and Water Authority

ArcSight は、高度な SOC をサポートして、OT と IT の連携による優れたインテリジェントセキュリティを実現します。

概要

Dubai Electricity and Water Authority (DEWA) は、信頼性の高い電力供給および水道のサービスをドバイの市民と居住者に安定して提供しています。DEWA は、世界トップクラスの公益機関です。最高基準の品質、効率、可用性に基づいて、90 万人を超えるドバイの市民と居住者に世界トップクラスの電力と水道のサービスを提供しています。1 日あたりの DEWA の総生産能力は、電力は 11,413MW、水は 4 億 7000 万ガロンです。世界銀行の Doing Business 2019 レポートにおいて、アラブ首長国連邦代表の DEWA は、電力供給について 2 年連続で世界 1 位にランクされました。

課題

DEWA は国の重要なインフラストラクチャであるため、セキュリティ管理については独自の課題に直面します。サイバー攻撃によって都市機能全体が停止し、国の非常事態につながる可能性があるためです。重要なインフラストラクチャのプロバイダーにとって、公益事業ネットワークを管理するオペレーショナルテクノロジー (OT) は非常に重要です。公益事業ネットワークは、通常、外部との接続がない独立したシステムです。これまでは、この方法で安全が確保されると考えられてきましたが、この考えはもはや通用しなくなっています。DEWA の Specialist Cyber Security である Jacob Jacob 氏は次のように説明します。「私たちは、パブリック ISP ネットワークを通して何百万ものデバイスがインターネットに接続されている世界に住んでいます。モノのインターネット (IoT) は、スマートホームの太陽光発電機や自動車の充電ポイントなどで使用されるため、DEWA にも関係してきます。私たちがサイバーセキュリティの対策を開始したときに探していたのは、IT と OT を統合するソリューションでした。統合が実現すれば、システム間でデータを共有して、OT デバイスで脅威インテリジェンスを取得し、IT デバイスのモニタリングを強化することができます。」

「ArcSight により、セキュリティイベントのモニタリングとインシデントを管理するためのプラットフォームを実現できました。シームレスなデータ統合が可能になり、関連するセキュリティ基準と規制を遵守できるようになりました。資産の可視性が向上したため、99% の可用性を実現できました。

JACOB JACOB 氏
Specialist Cyber Security
Dubai Electricity and Water Authority

DEWA では、セキュリティ上重要な 3 つの優先事項に取り組んでいます。セキュリティイベントの影響の低減、セキュリティの脅威の検知と防止、ビジネスのダウンタイムおよびコンプライアンス違反の防止です。セキュリティデータの量が増え続ける中で、データ分析を強化したインテリジェンス主導型の防御が必要であることは DEWA にとって明らかでした。

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

概要

- **業界**
  エネルギーおよび公益事業
- **所在地**
  ドバイ、アラブ首長国連邦
- **課題**
  脅威インテリジェンスとデバイスのモニタリングを向上させるため、システム間でデータを共有できるよう、IT と OT を統合する。
- **製品とサービス**
  Micro Focus ArcSight Data Platform
  Micro Focus ArcSight Enterprise Security Manager
  Micro Focus ArcSight Investigate
- **成果**
  + セキュリティアラームが 30% 減少
  + リスク軽減率 98%
  + AI による検知でメーターの不正操作が軽減
  + 可視性の向上によるデバイス可用性 99%

「これまでと異なるアプローチを取って、リスクテーマを可視化し、ArcSight などの最新のビジネス強化テクノロジーを導入し、高度なセキュリティオペレーションセンター (SOC) を設立したことにより、アラームが 30% 削減されたため、効率的なリソース配分が可能になりました。」

JACOB JACOB 氏
Specialist Cyber Security
Dubai Electricity and Water Authority

お問い合わせ先:
www.microfocus.com

ソリューション

DEWA の研究により、データの混乱をセキュリティの知見に変えるオープンプラットフォームである、Micro Focus ArcSight などのエコシステムの構築が実現しました。Jacob 氏は、ArcSight の複数の機能に感銘を受けました。「ArcSight は、様々なソースからデータを取り込み、分析の基礎となるインテリジェントな相関関係を提供できます。DEWA は Elastic と協業しているため、ArcSight と Elastic のネイティブ統合ができたときは感激しました。これにより、分析機能が強化され、地理的背景に基づいた分析も可能になりました。モニタリングすべきデバイスが非常に多いため、さまざまなソースからデータを取得することが不可欠です。たとえば、バルブは適切に機能しているか、パイプラインのエリアがネットワークから切断されていないかなどを把握する必要があります。これらは、DEWA のサービス提供に重大な影響を与える可能性があるネットワークイベントです。」

ArcSight Data Platform (ADP)、ArcSight Enterprise Security Manager (ESM)、ArcSight Investigate は、既存の Hadoop、Spark、Elastic と連携できる高度なセキュリティエコシステムの一部です。ArcSight ポートフォリオと人工知能 (AI) を組み合わせることにより、データログ管理、データ分析、リアルタイムのアラートとモニタリング、セキュリティ分析、インテリジェントなセキュリティオペレーションが可能になります。

「DEWA にはメーターのデータを収集、相関、解析して不正操作を特定するビジネスユースケースがあるため、サイバーセキュリティの専門家として、メーターの不正操作を検知する必要があります。」と Jacob 氏は説明します。「ArcSight により、様々なデータソースを統合し、データストリームに AI を導入して、使用パターンを分析できるようになりました。現在では、データの改ざんが自動的に検出されて警告が出るようになっています。」

ArcSight による分析エコシステムは、次世代のセキュリティ運用モデルの構築に役立っています。アクティブなイベントのフィルタリングと優先度設定により、重要なアラームに集中できるようになりました。接続された 10 以上のソースからデータが収集するために 12 の最先端技術が統合されています。このインフラストラクチャは、DEWA が管理するデバイスとネットワークの 80% を網羅しています。セキュリティステータスをリアルタイムでビジュアル表示する 20 以上の運用ダッシュボードが自動的に生成されます。

また、OT もセキュリティエコシステムに統合されています。DEWA の 25 の拠点を網羅するインテリジェンス主導型の防御により、3,000 台近いデバイスが完全にモニタリングされ、リスク軽減率 98% を実現しています。

成果

砂漠に囲まれた都市では、水は、手に入りづらい貴重なコモディティです。DEWA は、適応型システムのエコシステムである ArcSight などのテクノロジーを活用し、AI ベースのイベントモニタリングで水道網の状態を予測できるようになりました。これにより、無駄を減らしたより正確な生産計画が実現しました。

Jacob 氏は次のように語ります。「ArcSight により、セキュリティイベントのモニタリングとインシデントを管理するためのプラットフォームを実現できました。シームレスなデータ統合が可能になり、関連するセキュリティ基準と規制を遵守できるようになりました。資産の可視性が向上したため、99% の可用性を実現できました。高度なデータ接続により、可視性を近い未来の目標である 100% まで高めることができると考えています。」

同氏は続けます。「これまでと異なるアプローチを取って、リスクテーマを可視化し、ArcSight などの最新のビジネス強化テクノロジーを導入し、高度なセキュリティオペレーションセンター (SOC) を設立したことにより、アラームが 30% 削減されたため、効率的なリソース配分が可能になりました。DEWA は、Micro Focus という戦略的パートナーを見つけました。今後も革新的なサイバーセキュリティ対策で協力できることを楽しみにしています。」

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