opentext™ | Cybersecurity

お客様事例

Turkcell

ArcSight のモジュールと MITRE ATT&CK フレームワークを組み合わせることにより、高度なリアルタイムデータ相関付けとインシデント対応を実現します。

Turkcell の概要

Turkcell は、トルコで設立され、同国に本社を置く通信およびテクノロジーの統合サービスプロバイダーです。音声、データ、TV、デジタルセキュリティサービス、モバイルおよび固定ネットワークで付加価値の高いコンシューマーおよびエンタープライズサービスを顧客に提供しています。

数十億件のセキュリティイベントから意味のあるアラートを抽出

世界中に 5,000 万人以上の加入者がいる Turkcell において、データセキュリティとプライバシーは不可欠です。高度なサイバーセキュリティ脅威と KVKK (トルコ個人情報保護法令) およびトルコデータ保護法などのデータプライバシーに関する規制が、同社が先進的なサイバー防衛センター (CDC) を導入する契機となりました。セキュリティアナリストとデジタルフォレンジックのチームがインシデント対応チームおよびプランニングチームと連携して業務に当たっています。同社は、強力で効率的な脅威検出とセキュリティデータアナリティクスによる対応が可能な、OpenText の次世代のセキュリティ情報およびイベント管理 (SIEM) を構築するため、ArcSight Enterprise Security Manager (ESM) by OpenText を選択しました。Turkcell のサイバー防衛センター担当マネージャーである Cihan Yuceer 氏は次のように説明します。「当社は、マネージドサービスセキュリティプロバイダー (MSSP) として 20 社以上の企業のお客様にサービスを提供しています。CDC は、550 を超えるデータソースから 1 日に 60 億件のデータログを処理しています。このデータログはフィルターによって 30 億件まで絞り込まれ、その後 18 億件のログに集約されます。お客様の MSSP として 4 億件のログに高度なデータの相関分析を継続的に実行すると、対処が必要なアラートは 1 日 300 件以上になります。ArcSight ESM の強力なリアルタイム相関分析により、迅速に脅威を検出して対処できるようになりました」

> 「[OpenText™] Vertica Analytics Platform は ArcSight Intelligence に組み込まれているため、ArcSight Smart Connector のソースからセキュリティログデータを取得し、高度な相関分析とデータアナリティクスを高速で実行できるのです」
>
> **Cihan Yuceer 氏**
> サイバー防衛センター担当マネージャー
> Turkcell

Turkcell CDC のエンジニアは、データ漏洩、ブランド保護、脆弱性のモジュールからなる BOZOK 脅威インテリジェンスプラットフォームを統合運用センター (IOC) プラットフォームで開発しました。Turkcell は、ArcSight ESM と IOC プラットフォームを脅威インテリジェンスのユースケースに使用することを予定しています。

TURKCELL

概要

業種

電気通信

所在地

トルコ

課題

550 を超えるソースの 60 億件のデータログから、サイバー脅威を効率的かつ迅速に検出して対処

製品とサービス

ArcSight ESM
ArcSight Intelligence
ArcSight SOAR

成功ポイント

- 1 日 60 億件のデータログから 300 件の意味のあるアラートと 20 件のエスカレーションを抽出
- ArcSight の強力な相関分析と Turkcell の BOZOK 脅威インテリジェンスプラットフォームを組み合わせることにより脅威を検出して対処
- ArcSight SOAR の機能を使用した SLA および監査コンプライアンス
- MITRE ATT&CK コンプライアンスによるサイバーセキュリティの強化

「ArcSight ツールセットの統合機能が優れていることは実証済みです。当社では、MITRE ATT&CK コンプライアンスや ArcSight ESM の新しいデータソース、その他のユースケースと ArcSight SOAR によるレポート作成、ArcSight Intelligence によるセキュリティ全体の強化を利用した、エンドツーエンドの SIEM を構築できるようになりました」

Cihan Yuceer 氏
サイバー防衛センター担当マネージャー
Turkcell

お問い合わせ
www.opentext.com

ArcSight Intelligence の導入により、ArcSight ESM の機能が強化されました。ArcSight Intelligence は、未知の脅威を迅速に検出する脅威検出ソフトウェアによりセキュリティ運用をサポートします。Turkcell は、数十億件のイベントから優先度が設定された脅威のリストを抽出できるようになったため、アラート対応の労力が削減され、重要な脅威に集中できるようになりました。ArcSight ESM の年中無休セキュリティモニタリングと ArcSight Intelligence by OpenText の優先度設定プロセスを組み合わせたことにより、インシデント対応チームが 1 日に処理するエスカレーションケースは約 20 件になりました。

ArcSight を活用した KPI と SLA のトラッキング

ArcSight ESM は、MITRE ATT&CK フレームワークにアルタイム検出と機械学習の機能を提供します。このフレームワークは、世界中からアクセス可能な無料のサービスです。サイバーセキュリティ戦略の強化を目指す組織に最新の包括的なサイバー脅威情報を提供します。Turkcell は、高速データ処理機能も高く評価しています。Yuceer 氏は次のように述べます。「ArcSight Intelligence に [OpenText™] Vertica Analytics Platform が組み込まれているため、ArcSight Smart Connector のソースからセキュリティログデータを取得し、高度な相関分析とデータアナリティクスを高速で実行できるのです」

Turkcell CDC で収集されるアラートの数は日々増加しています。最優先事項は、損害が発生する前に脅威に対して適切な措置を講じる十分な時間を、セキュリティスタッフのために確保することです。ArcSight SOAR by OpenText では、すべてのインシデントごとに詳細なレポートが作成されるため、マネージャーはイベントの履歴を把握して将来の方向性をより適切に計画できます。すべてのレポートのログが ArcSight ESM に転送されて、監査を目的とする週次エグゼクティブレポートの作成、主要業績評価指標 (KPI) の追跡、サービスレベル契約 (SLA) の遵守の把握に使用されます。ArcSight SOAR のシームレスな自動化エンジンにより、Turkcell はエンジンの実行に必要な複雑なサイバー攻撃シナリオをいくつでも定義できるようになりました。すべての日常的なタスクや反復的なタスクを戦術的に自動化できるため、サイバー脅威が増加してもセキュリティチームが活動の規模を拡大できます。

ArcSight との統合によるエンドツーエンドの SIEM 構築

「ArcSight ツールセットの統合機能が優れていることは実証済みです。当社では、MITRE ATT&CK コンプライアンスや ArcSight ESM の新しいデータソース、その他のユースケースと ArcSight SOAR によるレポート作成、ArcSight Intelligence によるセキュリティ全体の強化を利用した、エンドツーエンドの SIEM を構築できました」と Yuceer 氏は述べています。

同氏はこのように締めくくっています。「当社は Micro Focus (現在は OpenText の傘下) とのパートナーシップに満足しています。製品管理および研究開発部門と直接協力して、Turkcell だけでなく他の ArcSight のユーザーにも役立つ新機能を開発してきました。優れたサポートが得られますし、セキュリティプロジェクトの協業では、Micro Focus (現在は OpenText の傘下) のプロフェッショナルサービスコンサルタントが当社の CDC チームメンバーに常に効果的にナレッジトランスファーをしてくれます」

opentext™ | Cybersecurity

OpenText Cybersecurityは、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurityのお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

768-JA0077-003 | O | 12/23 | © 2023 Open Text