

Kuwait Finance House

ArcSight のリアルタイム相関分析は、進化する脅威に対する高度な侵入防御と完全な規制準拠をサポートします



概要

Kuwait Finance House (KFH) は、イスラム金融（シャリーア・コンプライアント銀行）として知られる銀行ブームの先駆者です。1977年にクウェート国に設立された初のイスラム銀行で、今日世界で最も先進的なイスラム系金融機関の1つとされています。KFHは着実に事業を拡大し、イスラム金融業界をリードしながら金融先駆者としての地位を確立してきました。KFHのグループ銀行ネットワークは世界の複数の地域に展開され、504支店と1,263台のATM、約15,000人の従業員を擁しています。

「私たちは、ArcSight Marketplace と Activate フレームワークで、Micro Focus SOC の技術者と ArcSight コミュニティが開発したセキュリティルールセット、ダッシュボード、レポートを活用しています。これにより、セキュリティ対策と応答時間を大幅に改善することができました。」

MAJEED BEHZADI氏

Executive Manager, Group Information Security Management, IT Infrastructure Design
Kuwait Finance House

課題

他のあらゆる先進的金融機関と同じく、KFHも、増大するサイバー脅威に直面していました。グループ情報セキュリティ管理およびITIT インフラストラクチャデザイン担当のエグゼクティブマネージャーである Majeed Behzadi 氏は、包括的なセキュリティソリューションが必要となった理由を説明します。「基本的なセキュリティ監視ソリューションはあったのですが、脅威が増す環境において必要とされる相関分析機能がありませんでした。開発やサポートも不十分だったため、古いソリューションの利用をやめる前に新しいソリューションを見つけたいと考えました。ファイナンシャルサービス業界は PCI-DSS をはじめとする非常に厳しい規制に準拠しなければならず、24時間監視体制でセキュリティ情報イベント管理 (SIEM) 環境を管理できることが条件です。定期的に監査があるので、そのための包括的なレポート機能も必要です。」

ソリューション

徹底的な評価の末に、同氏のチームは、侵害防御とコンプライアンスの要件には ArcSight Enterprise Security Manager (ESM) と ArcSight Logger が最適な組み合わせであると判断しました。ArcSight ESM ではセキュリティイベントのリアルタイムの相関分析に関して有効な知見が得られます。ArcSight Logger は、あらゆるタイプのエンタープラ

بيت التمويل الكويتي
Kuwait Finance House



概要

■ 業界

ファイナンシャルサービス

■ 所在地

クウェート

■ 課題

組織全般のインフラストラクチャを可視化して、あらゆるサイバーセキュリティの脅威に迅速かつ効率的に対応する

■ 製品とサービス

Micro Focus ArcSight Enterprise Security Manager (ESM)
Micro Focus ArcSight Data Platform (ADP)
Micro Focus ArcSight Logger
Micro Focus ArcSight Activate Content Packages

■ 主な成功要因

- + インフラストラクチャ全体を監視して SIEM 環境の可視性を実現
- + 業界規制への完全準拠
- + 包括的なセキュリティレポート
- + あらゆる脅威に迅速かつ効率的に対応

「ESMの相関分析エンジンは業界最高水準です。 脅威の調査のためのデータ収集とイベントの相関分析が リアルタイムで行えるだけでなく、内部のプラットフォーム ルールに違反する脅威を優先的にエスカレートできるので、 とても役に立っています。」

MAJEED BEHZADI氏

Executive Manager, Group Information Security Management, IT Infrastructure Design
Kuwait Finance House

お問い合わせ先:
www.microfocus.com

イズマシデータの検索、レポート、アラート、分析が統合されたコスト効率に優れた汎用ログ管理ソリューションです。規制やセキュリティコンプライアンスの要件に応じたコンテンツが含まれているため、KFHセキュリティチームの負担が緩和されました。

KFHは現地の導入パートナーと協力し、2か月のうちにArcSightを利用したSIEM環境の運用を開始しました。データセンターベースのクラスター環境に導入し、別のサイトにセットアップすることで障害復旧に備えています。

Behzadi氏はArcSightによるKFHセキュリティオペレーションセンター(SOC)の日常業務のサポートについて、次のように述べています。「ESMの相関分析エンジンは業界最高水準です。脅威の調査のためのデータ収集とイベントの相関分析がリアルタイムで行えるだけでなく、内部のプラットフォームルールに違反する脅威を優先的にエスカレートできるので、とても役に立っています。さまざまなソースからのイベントをADPフィルターと集約機能で最適化し、毎秒およそ3,000件のイベントの管理が可能です。このため、付加価値の高い業務に組織のリソースを割り当てることができます。」

Behzadi氏は、コミュニティで得られるArcSight関連のコンテンツも評価しています。「私たちは、ArcSight MarketplaceとActivateフレームワークで、Micro Focus SOCの技術者とArcSightコミュニティが開発したセキュリティルールセット、ダッシュボード、レポートを活用しています。ArcSight Activateの数百のユースケースソリューションとESMパッケージを簡単にダウンロードしてESM環境に統合することが

できます。これにより、セキュリティ対策と応答時間を大幅に改善することができました。」

KFHはArcSight ESM/Loggerのレポートモジュールも活用しています。KFHのセキュリティチームが導入した包括的なダッシュボードレポートは、監査部だけでなく組織の多くの部署で使用されています。標準、カスタム、自動、アドホックの各レポートがすべてのセキュリティサービスをサポートします。

KFHではArcSightを多くの財務アプリケーションと統合しています。データの分断を解消して顧客データをリアルタイムの支払いに使用することで、電子決済機能をシームレスかつシンプルに活用できます。オンライン詐欺を減少させることができ、データの機密性が高まりました。

同社は、実績あるリアルタイムコアプロセッシングと金融市場専用の独自のクラウドプラットフォームであるFinastraのチャンネルソリューションを組み合わせた統合エンタープライズソフトウェアプラットフォームを構築しました。組織全体で整合性の取れた情報が利用できるように、顧客記録の追加と管理がシンプルに効率よく行えます。レポートと分析も同じデータベースからドラッグアンドドロップのレポート作成機能で簡単に実行できるため、コンプライアンスが向上します。

これらのユースケース向けにMicro Focusプロフェッショナルサービスで開発されたArcSight Flex ConnectorがArcSightマーケットプレイスで提供されています。KFHはこれらの高度なユースケースコンセプトを活

用して、IT/セキュリティログを財務データと相関付けて攻撃のクロス検証と脆弱性の特定に役立てています。

成果

KFHの主な目標は、規制への完全準拠とインフラストラクチャの可視性を実現して、あらゆる脅威イベントに迅速に対応する能力を向上させることでした。Behzadi氏は、この目標が達成されたと確信しています。「この分野の成功を評価するのは難しいことですが、全インフラストラクチャのすべての要素をArcSight-driven SIEMで100%監視できています。また、業界におけるIoTが重要性を増す中で、将来のデバイスやシステムの統合が容易に行えます。あらゆる業界規制に完全に準拠し、あらゆるセキュリティの脅威に迅速、生活に対応できる自信があります。」

KFHのセキュリティチームはSIEMにArcSight Data Platform (ADP)を追加することも検討しています。これにより、イベントデータを収集、正規化、拡張して、KFHの分析ツールなどの他のデータ処理ツールに容易に配布ができるようになります。

Behzadi氏は次のように締めくくります。「私たちは、SIEMを拡張して、銀行支店と銀行以外の子会社にもクウェートを中心としたグループレベルのセキュリティサービスを提供したいと考えています。私たちが導入したArcSightは、進化する脅威の中でもこの新しい課題に取り組むことができると思っています。ArcSightによって罰金や罰則が適用されるリスクを緩和し、あらゆるコンプライアンスの要件に対応することができます。今後もMicro Focusとの連携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