お客様成功事例

セキュリティ

DNeX Technology S/B 社

ArcSight は、次世代 SOC のサポートにより、インシデントへのレスポンスタイムを短縮し、脅威検知を向上させます。

概要

DNeX(DNeX Technology S/B 社) は、マレーシアの貿易円滑化およびエネルギー業界の大手サービスプロバイダーです。同社の中核事業は幅広い専門企業と関わっており、各企業が、業界のエキスパートが設計し主導する、カスタマイズされたサービス、ソリューション、インフラストラクチャを提供しています。

課題

FORTRESS は、柔軟なセキュリティインフラストラクチャの導入により、変化し続ける IT セキュリティ環境の脅威に対応する、DNeX の中核サービスです。この一環として、同社のマネージドセキュリティサービス部門は、24 時間 365 日のモニタリングを実施するとともに、セキュリティ / 情報 / イベント管理 (SIEM)、セキュリティオペレーションセンター (SOC) の構築、セキュリティログ管理サービスを提供しています。これらは、マレーシアの金融サービス (FS) 機関が、24 時間 365 日リアルタイムでネットワークのトラフィックとトランザクションをモニタリングすることをすべての金融サービス機関に義務付けた、中央銀行の規制を順守するための鍵となるサービスです。これには、金融製品の全ブランド間のデータの相関も含まれます。

DNeX の CEO である Rodney Lee 氏は、この規制によって多くの銀行が直面している課題について、次のように説明します。「オンサイトの SOC と 24 時間 365 日のセキュリティモニタリングを導入すると、多くの組織に莫大なコストがかかります。そのようなリソースを持つ組織はありません。当社はスケールメリットを活用して、これをサポートします。当社とお客様との関係は信頼を基盤として築かれており、私自身は IT セキュリティのビジネスに 20 年間携わっています。当社は、中央銀行のモニタリング要件を把握しています。これが、新規のお客様の獲得における強みになっています。

同氏はさらに述べます。「Micro Focus® ArcSight には、リリース当初から注目していました。この製品は、私の考えでは今でも市場で No.1 の SIEM です。Gartner 社の Magic Quadrant で認められた信頼できるポジションも、これを裏付けています。」

「過去 20 年間に、多数の SIEM ソリューションが現れては消えるのを見てきました。しかしながら、ArcSight は現在でもトップの座にあります。ArcSight がなかったら、シフトあたり最小 2 名のスタッフで、すべてのお客様をサポートするミッションクリティカルな SOC を運営することはできないでしょう。」

RODNEY LEE 氏
CEO
DNeX

DNeX

概要

- **業界**
  ソフトウェアおよびテクノロジー
- **所在地**
  マレーシア
- **課題**
  コスト効率に優れた効率的なモデルにより、金融サービス機関と国家的重要インフラストラクチャ機関をサポートし、必須のセキュリティモニタリングを提供する
- **製品とサービス**
  ArcSight Enterprise Security Manager
- **成果**
  + オンサイト SOC と比較した場合のお客様コストの 50% 削減
  + 完全な可視化とレポーティングによる高度な脅威検知のサポート
  + 多様なソースの関連付けによるリソースの高リスク分野への割り当て
  + 高度なコネクタテクノロジーによる時間の節約

「22 件の FlexConnector/ パーサーの作成期間として、政府のお客様から提示された時間は 4 週間でした。ArcSight のおかげで、2 週間以内にプロジェクトを完了できました。」

RODNEY LEE 氏
CEO
DNeX

お問い合わせ先:
www.microfocus.com

ソリューション

ArcSight Enterprise Security Manager (ESM) は、高度なデータエンリッチメント機能を備えた、包括的なリアルタイムの脅威検知、分析、ワークフロー、およびコンプライアンス管理プラットフォームです。DNeX のデータセンターでホストされている ArcSight ESM は、通常 5 秒未満の遅延で、お客様のセキュリティログを処理し、分析します。

DNeX は、お客様のデータを完全に分離することで機密性を確保し、すべてのセキュリティログを包括的にバックアップしています。Lee 氏は、ArcSight がどのようにして DNeX のリーンなセキュリティ組織の運営を実現しているかについて、次のように説明します。「ArcSight はさまざまなソースのデータを処理し、高度なイベント相関機能を提供して、社内のプラットフォームルールに違反する脅威を正確にエスカレーションします。ユースケースの自動構築機能にも感謝しています。この機能により、インシデントが自動的に特定されるため、問題を見つけるためにセキュリティログを調べる必要がありません。こうした「レッドフラッグ機能」により、大幅に時間が節約されました。」

イベントソースが増えることにより、企業の可視性が向上するとともに、お客様の組織のセキュリティニーズに固有の、より複雑なユースケースを作成する能力も強化されます。非常に成熟した ArcSight の導入により、脅威情報の周知および関連付けが行われるとともに、受信イベントの 80% がノイズとして除外されるため、DNeX のチームはリスクの高い部分にリソースを集中させることができます。

Lee 氏とその部下は、ArcSight の SmartConnector と FlexConnector の使用に、大きなメリットを見い出しています。導入後すぐに使用可能な SmartConnector は、ネイティブの Windows イベントから API、データベースへの直接接続まで、あらゆる一般的なイベント形式をサポートしています。DNeX は、FlexConnector 開発ネットワークを活用して、ArcSight ESM と統合されたカスタムのコネクタ / パーサーを開発しました。これにより、インデックスを作成して相関エンジンで使用できるようになりました。

Lee 氏は次のように述べています。「最近、まったく未知のオープンソースのファイアウォールの事例に遭遇しました。これは主流のデータソースではありませんでしたが、30 分以内に FlexConnector を構築できたため、データを統合してこのお客様を完全に可視化できました。22 件の FlexConnector/ パーサーの作成期間として、政府のお客様から提示された時間は 4 週間でした。ArcSight のおかげで、2 週間以内にプロジェクトを完了できました。」

ArcSight のレポートおよびダッシュボード機能の有効性は、DNeX のお客様により実証されています。同社のお客様は、DNeX SIEM にログインし、ほぼリアルタイムのセキュリティステータスを提示するカスタムレポートを生成できます。DNeX は、お客様の「攻撃マップ」も作成しました。これらの機能は、セキュリティモニタリングの価値を視覚的に分かりやすく示すもので、お客様のオフィスに目立つように掲示できます。

DNeX は、トラフィックとネットワークのモニタリングが不可欠な、マレーシアの国家的に重要なインフラストラクチャもサポートします。重要なインフラストラクチャのプロバイダーは、通常、オペレーショナルテクノロジー (OT) ネットワークに大いに依存しており、そうしたネットワークの構成にはセキュリティが考慮されていないことがよくあります。しかし現在では、OT と IT の運用を統合するとともに、完全なセキュリティコンプライアンスの確立が必須です。DNeX は、ArcSight 主導の SIEM アーキテクチャによりこれをサポートします。同社はこれをマネージドサービスとしてだけでなく、柔軟なハイブリッドモデルでも提供しています。そのため、組織は、独自の SOC をホストして、営業時間外にはモニタリングサービスを DNeX に引き継ぐことができます。こうした柔軟なアプローチにより、お客様が 24 時間 365 日、独自のセキュリティオペレーションをホストするコストを半分に削減できます。

成果

10 年以上にわたって ArcSight に注力することにより、DNeX はお客様に高い付加価値を提供する、これまでにない企業へと成長しました。ArcSight への取り組みを継続している Lee 氏は、次のように述べています。「過去 20 年間に、多数の SIEM ソリューションが現れては消えるのを見てきました。しかしながら、ArcSight は現在でもトップの座にあります。ArcSight がなかったら、シフトあたり最小 2 名のスタッフで、すべてのお客様をサポートするミッションクリティカルな SOC を運営することはできないでしょう。」

同氏はこう締めくくります。「攻撃の状況は絶えず変化しており、日ごとに対応が困難なものになっていますが、ArcSight があることで対応に確信を持てます。」

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