MICRO FOCUS

お客様事例
セキュリティ

Rabobank

国際金融機関のRabobankは、APT攻撃対策としてMicro Focus® ArcSight ESMを導入しています。ESMを利用することで、以前は検知できなかったサイバー脅威も検出できるようになりました。

概要

高度標的型攻撃 (Advanced Persistent Threat; 以下、APT攻撃) 増加し巧妙化が進む中、Rabobankはイベント相関と脅威検出の精度を向上させるため、自社のSIEM (セキュリティ情報およびイベント管理) ソリューションを使用して、より複雑なユースケースを構築する必要がありました。現在、Rabobankは、ArcSight Enterprise Security Manager (ESM) を導入することで、社内の数千のデータフィードから1日あたり百万件のセキュリティログの相関処理を行っています。Rabobankは、ESMを利用して数多くの高度なユースケースを構築し、ネットワーク上の異常な挙動や信頼できないデバイスを高い精度ですばやく検出しています。Rabobankは、以前には検知できなかった脅威を検出できるようになり、セキュリティ管理業務の生産性と有効性を改善すると同時に、セキュリティを強化しています。

「ESMにより、以前には検出できなかったセキュリティイベントを検出できるようになりました。ESMのおかげで、脅威をすばやく見つけ出し、ネットワークへの侵入や業務の中断を未然に防ぐことができます。ArcSightは、現代のサイバー攻撃が組織にもたらす被害に備えるための重要な保険です。」

Rabobank、
セキュリティオペレーションセンター長、
MARK BEERENDS氏

Rabobankは、世界最大規模の協同組合型金融機関の1つです。同社は19世紀に農業従事者グループによって設立され、オランダの農業金融をルーツとして発展してきました。現在では銀行業務、資産管理、リース、保険、不動産業を幅広く手がける国際的な金融サービス機関に成長しています。

Rabobankは、食品および農業分野での卓越した知識を活かすことで、世界の食糧問題を解消しながら、オランダ国内市場の発展にも寄与することを組織の使命としています。こうした大きな目標を達成するには、自社の情報ネットワークを最高レベルのセキュリティで保護する必要があります。

課題

他のすべての金融機関と同様に、Rabobankはあらゆる手段を使ったサイバー攻撃の脅威に常にさらされています。フィッシング詐欺やマルウェアは不正な迷惑行為ですが、最も厄介なのは、巧妙なサイバー犯罪者が密かに持続的なハッキング攻撃を仕掛けるAPT攻撃です。APT攻撃は一般に検出が難しく、見つかるまでに何か月もネットワーク内で活動していることがあ

Rabobank

概要

業界
銀行/金融サービス

所在地
オランダ

課題
高度なユースケースを構築してAPT攻撃を特定する精度を向上させ、迅速で的確な対応を行えるようにする。

製品とサービス
ArcSight Enterprise Security Manager

成果
+ イベント相関および脅威検出の精度向上によるネットワークセキュリティ管理の強化
+ セキュリティ管理業務の生産性と有効性の向上
+ よりハイレベルなセキュリティ体制の実現

ります。見つかったときにはすでに、データ喪失や業務中断などの被害が生じている可能性があります。

Rabobankは何年もの間、セキュリティアラートの分析にRSA enVisionを使用していました。セキュリティ管理の生産性と有効性を向上させるために、Rabobankはさらに高度なユースケースを構築して、セキュリティアラート全体からコンテキストに基づいた関連性を見つけ出す必要がありました。しかし、enVisionには必要な機能がなく、RSAによる新製品開発も進んでいませんでした。

ソリューション

増大するセキュリティ管理ニーズに対応するため、RabobankはArcSightやIBM QradarなどのRSAに代わる製品の検討を行いました。これらのツールを詳細に評価した結果、Rabobankは強固なSIEM機能を持つArcSight ESMを導入しました。

Rabobankのセキュリティオペレーションセンター長であるMark Beerends氏は、次のように説明しています。「ArcSight ESMが特に優れていたのは、非常に複雑なユースケースを構築できることでした。また、ITサービスアクティビティに関する大量のデータ収集を行うMicro Focus Service Managerなど、Micro Focusの他のソリューションと統合できることも大きな利点でした。」

高可用性セキュリティ監視

Rabobankでは、ArcSight ESMのインスタンスを3つ展開しています。高可用性およびディザスタリカバリ用にオランダ国内の2つのデータセンターにArcSight ESMを1つずつ展開し、テストおよび開発用にArcSight ESMを1つ展開しています。

同社のSIEMは日常業務に不可欠であるため、いずれかのサイトが失われた場合でも、本番環境のセキュリティ監視が1時間以上ダウンすることがないようにする必要がありました。テストおよび開発用のArcSight ESMにより、Rabobankのセキュリティ管理チームは、新しいユースケースを本番環境に導入する前に、ユースケースのテストを行って変更の影響を確認することができます。

本番環境では、Microsoft Windowsが稼動する3,000台のHPE ProLiantサーバーLinuxが稼動する1,000台のHPE ProLiantサーバー、および十数台のHPE Integrity NonStop BladeSystem NB54000cサーバーで生成されるデータストリームから、ArcSight ESMで1日あたりおよそ百万件のセキュリティログを収集しています。

また、Rabobankは、アプリケーションセキュリティテスト用に、他のArcSight ESMソフトウェア、Fortify on Demand、およびTippingPoint[1]も導入しています。Beerends氏は、次のように述べています。「ESMでセキュリティ上の脅威が見つかった場合は、TippingPointにフィルターを追加するだけでその脅威を容易にブロックできるため、ネットワーク上で問題が起きるのを未然に防ぐことができます。次はSIEMとIPS (侵入防御システム) の機能の統合に取り組む予定ですが、これには時間が必要です。」

成果

複雑なユースケースのサポートによる脅威検出精度の向上

ArcSight ESMの導入以来、Rabobankは30～40の複雑なユースケースを開発してきました。これにより、イベント相関およびセキュリティアラートの精度が大きく向上しました。これらのユースケースを通じて重要なコンテキスト情報が得られるため、セキュリティ管理チームは即座に対処が必要なアラートかどうかを判断することができます。

たとえば、パスワードの入力間違いは必ずしも問題でありませんが、通常と異なる時間帯や海外のIPアドレスからログインが行われているのであれば、重大な脅威を示唆している可能性があります。このような詳細な情報を得ることで、誤検知の数が減少し、Rabobankのネットワーク全体のセキュリティが強化されることになります。

Beerends氏は、次のように述べています。「ESMにより、いくつもの異なるデータフィードのイベントの相関付けを行うことが可能になります。相関付けが強化されることで、脅威を検出する精度が向上します。これは当社のセキュリティアナリストが、対処が必要な場所やタイミングを把握するのに役立っています。最も良い点は、必要なすべてのデータフィードをログ記録していることです。必要に応じて、新しいユースケースをいつでも実装することができます。」

たとえば、最近開発されたユースケースでは、Rabobankのネットワーク上にある不正なデバイスの識別を行っています。Rabobankは、オープンネットワークを運用しています。このオープンネットワークには、組織内の誰でも個人所有デバイスを使って接続することができます。しかし、サイバー犯罪者にオープンネットワークが利用され、ネットワーク内に侵入されてしまうおそれもあります。こうした行為を防ぐため、RabobankはESMを利用して、DHCPサーバー、Microsoft Active Directory、およびネットワーク環境からのデータを相関付けることで、デバイスが信頼できるものかどうかを判断しています。

ArcSight ESMとMicro Focus Service Managerの統合の重要性も実証されました。この統合を通じて、RabobankはITサービスのアクティビティを直接把握することができるため、いずれかのアプリケーションでレベル1アラートが発生した場合に、セキュリティ管理チームはSIEMに情報を手動で転送することなく、脅威の重大度を即座に判断することができます。

「ESMとの統合が進み、利用できる相関付けが増えたことで、当社のセキュリティ体制はさらに高度なものになっています」とBeerends氏は指摘しています。

セキュリティリスクの管理に加えて、RabobankではArcSight ESMのコンプライアンスレポート機能を利用して、法規制要件にも対応しています。たとえば、Rabobankは、システム管理者が適切な手順に従っていることを実証できる必要があります。ArcSight ESMでは、管理者のすべてのアクティビティに関するレポートが毎週作成されるため、Rabobankはコンプライアンス状況を容易に証明することができます。

1. 最初の公開 (2016年12月) 後、TippingPointはTrend Microに売却されました。

お問い合わせ先:
www.microfocus.com

サイバー攻撃の脅威に備える価値ある保険

リテールバンクであるRabobankは、サイバー犯罪者の格好の標的になっており、最新の検出が難しい攻撃が絶え間なく仕掛けられています。さらに、攻撃の件数は毎年確実に増加を続けています。しかし、RabobankはArcSight ESMを導入することで、強力なエンタープライズセキュリティ管理ソリューションを実現し、極めて巧妙化したAPT攻撃やその他のサイバー脅威にも対応し、自社のネットワークや重要な情報資産を保護できるようになりました。

Beerends氏は、次のように締めくくっています。「ESMにより、以前には検出できなかったセキュリティイベントを検出できるようになりました。ESMのおかげで、脅威をすばやく見つけ出し、ネットワークへの侵入や業務の中断を未然に防ぐことができます。ArcSightは、組織が現代のサイバー攻撃の被害に備えるための重要な保険です。」

詳細情報

www.microfocus.com/arcsightesm

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

www.microfocus.com

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