巧妙化するサイバー攻撃による被害拡大を最小限に抑える

ネットワークセキュリティ対策自動化ソリューション

サイバー攻撃の巧妙化とセキュリティ人財の不足にともない、初動対応の遅れに起因する内部拡散のリスクが増加しています。そこで日立グループは、SDN※1を利用して感染デバイスの切断や隔離などを自動化する「ネットワークセキュリティ対策自動化ソリューション」を開発。人手を介さないインシデント対応で運用コストを削減しつつ、サイバー攻撃による被害拡大を最小限に抑える環境の実現を可能にします。

※1 Software-Defined Networking

ネットワークセキュリティ対策を自動化

特定の企業や組織を狙い撃つ「標的型サイバー攻撃」の被害が拡大しています。さまざまなモノがインターネットでつながるIoT時代では、サイバー攻撃の被害は一企業にとどまらず、そのお客さま企業や社会全体にも多大な影響を与えるおそれがあります。その一方で企業の多くは、セキュリティ対策にあたる人財の不足に悩んでおり、マルウェア感染に対する初動体制の遅れが深刻な被害につながる事例も急増しています。

こうした課題に対処するためには、防御が難しい脅威に対しても通信遮断や隔離などのネットワーク制御を自動化することで、内部拡散を極小化しながら、セキュリティ担当者が新たな脅威への対応に集中できるよう支援する仕組みが必要です。そこで日立グループでは、新たに開発した「ネットワークセキュリティ対策自動化ソリューション」によって、お客さまのサイバー攻撃対策の強じん化・迅速化を力強く支援します。

業界標準のシステムに対応したSDKを提供

ネットワークセキュリティ対策自動化ソリューションは、株式会社 日立情報通信エンジニアリングのネットワークインテグレーション実績と、株式会社日立ソリューションズのセキュリティソリューション実績という両社の強みを生かして開発されたものです。具体的には、多くの企業で導入されているマシンデータ利活用基盤ソリューション「Splunk」※2のイベントログ収集・相関分析によって検知した脅威に対し、ネットワーク管理SDNシステム「Cisco Prime Infrastructure（以下、Cisco PI）」※3がネットワークを制御します。この両システムをつなぐ「インシデント レスポンス自動化SDK※4 for Prime Infrastructure（以下、インシデント対応SDK）」は日立情報通信エンジニアリングが開発したもので、SplunkとCisco PIをシームレスに連携することにより、従来は人手を介して実施していた初動対応（問題のある端末のネットワークからの遮断・隔離など）を自動化し、サイバー攻撃被害の最小化と運用管理コストの低減を可能にします。お客さまのネットワーク環境にCisco PIとインシデント対応SDKを追加するだけで利用可能なことが、大きな特長です。

※2 Splunk社（Splunk Services Japan合同会社）の製品で、日立ソリューションズが販売
※3 シスコ社（シスコシステムズ合同会社）の製品で、日立情報通信エンジニアリングが販売
※4 Software Development Kit

ネットワークセキュリティ対策自動化ソリューションの導入効果

■セキュリティ対策自動化による運用管理コストの削減

サイバー攻撃が検知された場合、あらかじめ設定されたネットワーク制御ポリシーのもと、自動でネットワークを制御するインシデントレスポンス機能を実装しており、問題のある端末の「切断」「隔離」「アクセス制御」を自動化します。また夜間・休日など情報システム管理者が不在の場合でも、人手を介さず初動対応を完了できるため、運用管理コストの低減にも貢献します。

■豊富な知見と導入実績に基づくノウハウを活用。膨大なログをリアルタイムに解析

Splunkは、サーバやPC、ネットワーク製品など多種多様な機器が出力する

膨大なイベントログの中から不審な動きをリアルタイムに検出します。日立ソリューションズの豊富な導入実績とそれに基づく知見から、不正があると疑われる機器やシステムのログを相関分析して、より高度なセキュリティ脅威の検知を行います。

■既存システムとの連携による投資コストの抑制

インシデント対応SDKは、さまざまなセキュリティ製品と柔軟に連携するユーザースクリプトを用意しています。お客さまがすでにお使いのセキュリティ製品をそのまま利用できるだけでなく、より高度なマルウェア対策システムへのアップグレードにも対応します。

巧妙化する脅威にも迅速に対応

日立グループは、ネットワークセキュリティ対策自動化ソリューションにおいて、「JP1/Integrated Management」や「McAfee ePolicy Orchestrator」などにも対応していくほか、今後さまざまな攻撃の内容やパターン、傾向を人工知能が機械学習することで、未知のマルウェアなどの脅威にも迅速に対応できるソリューションも提供していきます。

図「ネットワークセキュリティ対策自動化ソリューション」の概要

お問い合わせ先

(株)日立情報通信エンジニアリング 営業戦略統括本部
http://www.hitachi-ite.co.jp/inquiry/form/sdx.html
(株)日立ソリューションズ
https://www.hitachi-solutions.co.jp/inquiry/

■ 情報提供サイト
http://www.hitachi-ite.co.jp/products/nsa_sol/