Check Point社：サイバーセキュリティソフトウェア企業がSplunkでインテリジェンスを強化

主な課題

Check Point社は、さまざまなデータセットからより有意義なインサイトを引き出して、脅威を緩和すると同時に運用と効率を改善したいと考えていました。

主な成果

Splunkを導入したCheck Point社は、ビジネス運用に関するインサイトをリアルタイムで得られるようになり、新型コロナウイルスの感染拡大を受けたリモートワークへの移行などの不測の事態にも先手で対応できるようになりました。

Check Point SOFTWARE TECHNOLOGIES LTD

業種：テクノロジー

ソリューション：セキュリティ

セキュリティソフトウェア企業が自社システムのセキュリティを確保する方法

Check Point社のサイバーセキュリティソリューションは、あらゆる規模の10万社以上の企業で利用されています。同社は、社内システムと5,400人の従業員のセキュリティについても最高レベルの基準を設けています。一方で、社内システムで日々収集されるテラバイト単位のデータからより有意義なインサイトを取得して、ビジネスの状況をより的確に把握し、運用全体のセキュリティを向上させたいと考えていました。

より迅速でスマートな調査と効果的な脅威対策

Check Point社は、組織のセキュリティに関するアカウンタビリティを向上させるためにSOC (セキュリティオペレーションセンター)を設立しました。そのプラットフォームとして選択したのがSplunk Enterprise Securityです。Splunkは、同社が扱うさまざまな形式のデータをすべて取り込み、すでに導入しているすべてのテクノロジーと連携できます。

「Check Pointはデータドリブン企業です」と、同社でグローバルCISO (最高情報セキュリティ責任者)を務めるJony Fischbein氏は言います。「当時の大きな課題は、収集した膨大な量のデータを統合して、有意義な情報に変換することでした」

以前使用していたSIEMツールからSplunkへの移行を開始してからわずか17日後に、Check Point社は、脅威検出率の向上やセキュリティ調査の迅速化など、導入効果を実感し始めました。

今日では、Splunkダッシュボードでシステムの現在の状態を可視化したり、自動アラートによって悪質なアクティビティやネットワークの脆弱性に関する通知を受け取っています。Fischbein氏はSplunkについて、開発者によるソースコードの社外持ち出しや、開発者が使用している製品の新しい脆弱性発見など、害をもたらす可能性のある問題をチームがすばやく効果的に調査して未然に防止できるようになったと評価します。

「今では、何を調査すべきで、問題が解決したかどうかを的確に把握できます。チームメンバーが直感でそう思うだけでなく、データがそれを裏付けてくれます」

データ活用の成果

5倍
セキュリティ調査のスピード

17日
Splunkへの移行にかかった日数

100%
在宅勤務をする従業員の新型コロナウイルスに対応した新しいセキュリティポリシーの準拠率

パンデミック下での安全とセキュリティの確保

データから有意義なインサイトを引き出すSplunkの能力は、新型コロナウイルスの感染拡大時に従業員の安全と生産性を確保するためにも役立ちました。

1人の従業員が新型コロナウイルス検査で陽性であることが判明したとき、Check Point社のITチームは、Splunkを使って全従業員のアクセスバッジを追跡し、感染の影響レベルを調査して、過去14日間にその従業員と接触した従業員を特定しました。そして、接触のあった従業員にただちにその旨を通知し、在宅勤務と自主隔離を指示しました。

「Splunkじゃなかったらできなかったでしょう」とFischbein氏は言います。

Splunkは、パンデミック下でのリモートワークのセキュリティ確保でも活躍しました。在宅勤務に関する組織の新しいセキュリティ対策が定められたとき、Fischbein氏はSplunkを使って従業員が対策を守っているかどうかを確認し、2週間以内に準拠率が100%に達したことをCEOに報告することができました。「この出来事で、Splunk導入の価値を経営陣に確実に証明できました。従業員の安全が守られ、在宅勤務でも生産性を維持できていることを、データで示したのです」

> Check Pointはデータドリブン企業です。当時の大きな課題は、収集した膨大な量のデータを統合して、有意義な情報に変換することでした”
>
> Check Point社グローバルCISO
> (最高情報セキュリティ責任者)、
> **Jony Fischbein氏**

従業員のリモートワークが続く中、Splunkを使って、開発者が個人所有のPCからダークウェブにアクセスしていないか、経理/会計担当者が会社支給のPCを他の従業員に使わせていないかなど、セキュリティリスクの検出と緩和にも取り組みました。こうした問題を発見したときは、上司からその従業員に、社内データや機密情報を保護するためのポリシーに従うよう指導してもらいました。

> 今では、何を調査すべきで、問題が解決したかどうかを的確に把握できます。チームメンバーが直感でそう思うだけでなく、データがそれを裏付けてくれます”
>
> Check Point社グローバルCISO
> (最高情報セキュリティ責任者)、
> **Jony Fischbein氏**

Splunkとともに成長する未来

Splunkの導入効果を実感したCheck Point社は、今後、ユースケースを拡大する計画です。

「今必要なことだけに役立つソリューションは欲しくありません。今は認識していない半年後、1年後の状況にも対応できるソリューションが欲しいのです」とFischbein氏は言います。「それがSplunkです。Splunkは組織とともに成長するソリューションです」

Check Point社は今後、脆弱な可能性のあるデバイスの隔離や従業員の個人情報管理の強化など、Splunkのタスク自動化機能を活用していく予定です。また、ヘルプデスク担当者自身で対応できるアラートを特定できるようにするなど、SOC以外のチームでのSplunkの活用方法も模索しています。

「Splunkがあれば、組織の隅々にまで目が届きます」とFischbein氏は言います。「また、何をするにもSplunkは大きな効果を発揮します」

Splunkの無料トライアルをダウンロードするか、Splunk Cloudの無料トライアルをお試しください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわりなく、お客様のニーズに最適な展開モデルでご利用いただけます。

splunk>

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp
splunkjp@splunk.com

© 2021 Splunk Inc. 無断複写・転載を禁じます。Splunk, Splunk>, Data-to-Everything, D2EおよびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

21-19735-Splunk-Tier2-Check Point-CS-A4-JA-202201