変革をすすめるCISOのためのSOARガイド

セキュリティチームがプロアクティブかつ
戦略的に行動するための時間を確保し
ビジネスのイノベーションと成長へ

splunk>

目次

ビジネスリーダーが求めているのは革新的なセキュリティチーム

変わりつつあるCISO(最高情報セキュリティ責任者)の役割

かつてのCIOやCTOと同様に、CISOの役割も責任範囲が限定された協力者の立場から、より一体的かつ戦略的にビジネストランスフォーメーションを支える推進者へと進化しつつあります。成功を収めている企業の多くは、デジタルおよびビジネスの真のトランスフォーメーションにはセキュリティの最新化が不可欠であることを認識しています。

PwCの調査によれば、エグゼクティブの40%が求めているCISOとは、部門横断型のアジャイルなチームを率いて、デジタルトランスフォーメーションの流れについていくだけでなく、多くの場面で進むべき道を示すことができるCISOです。[1]

Information Security Systems Associationの実施した調査によると、世界中のセキュリティ担当者が、CISOにとって最も重要な資質として、コミュニケーション能力とリーダーシップを挙げていることが明らかになりました。[2]

エグゼクティブが最も重要視する4つの資質

1. 戦略的思考
2. 賢明なリスクテイクの能力
3. リーダーシップスキル
4. イノベーションの機会を見極めて推進する能力

さらにISSAの調査によると、大部分のセキュリティアナリストはより戦略的な役割を担うことを望んでおり、リーダーシップ、コミュニケーション、ビジネスのスキルを磨くことで、成長と変革を率いる必要性を認識しています。

“情報セキュリティは、今や攻撃を防ぐためだけのものとは見なされていません。セキュリティはビジネスを支え、加速する手段なのです”

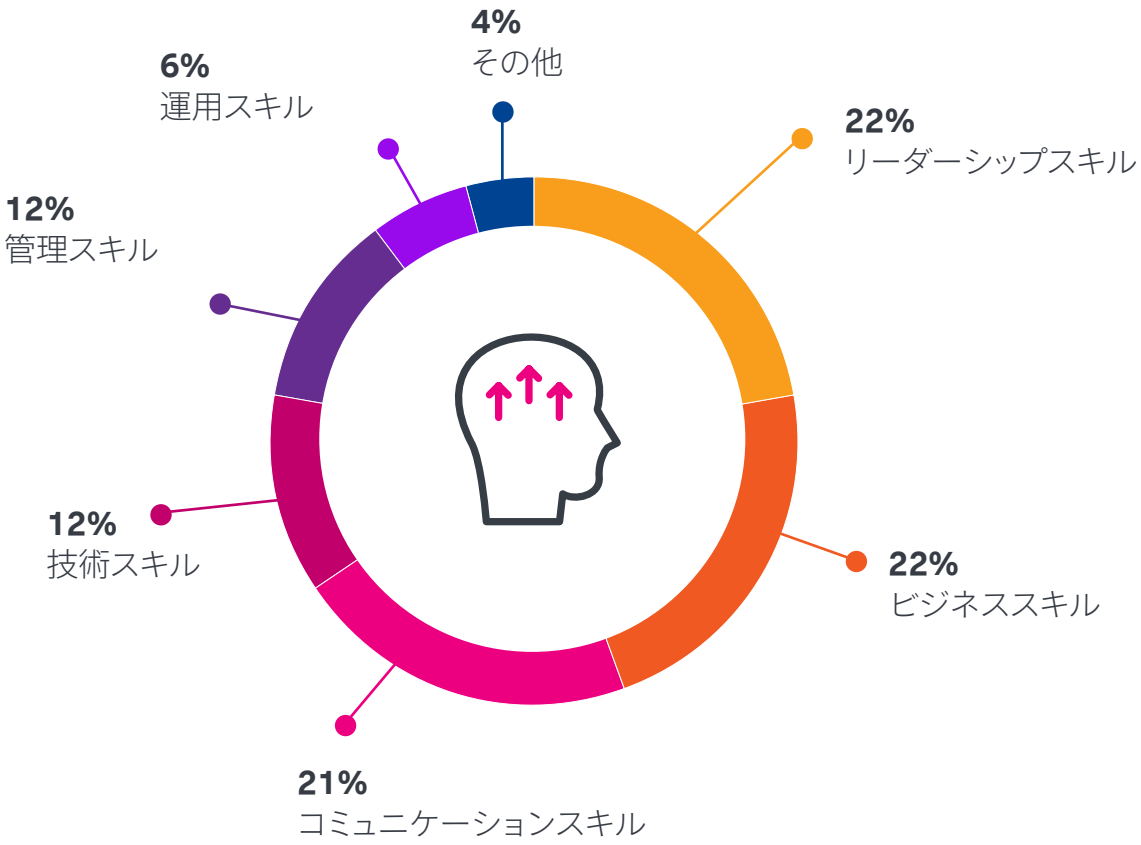
–Splunk CISO、Yassir Abousselham

[1]https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights/cyber-strategy.html
[2]https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

技術的スキルだけでは組織を率いることができないとセキュリティアナリスト自身が認識

Enterprise Strategy Groupは、CSOまたはCISOとなるためにどのようなスキルが必要となるかについてセキュリティアナリストに質問しました

ソース：Enterprise Strategy Group



しかし多くの場合、**大量のアラートと、それに対応する人員の不足**という日々の現実の中で、セキュリティ責任者やアナリストは戦略的役割を果たすことができていません。

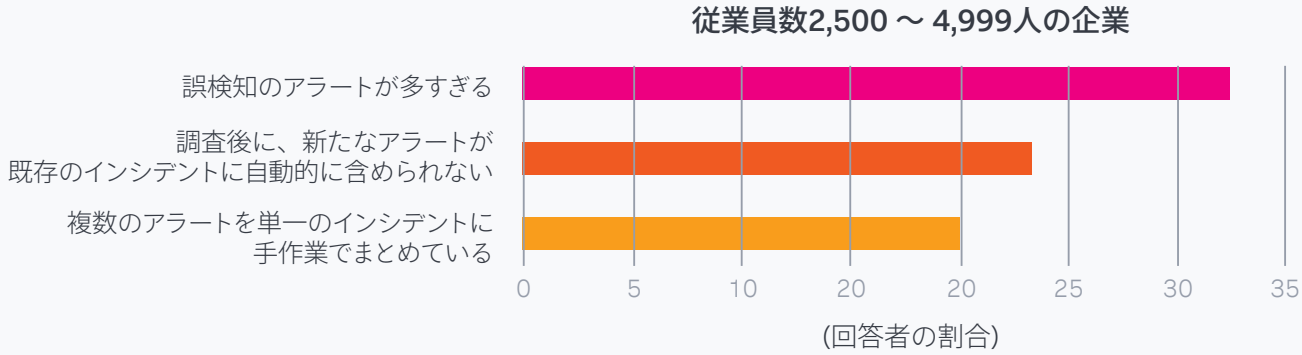
混乱から秩序へ

ISSAの調査によると、ほぼ3分の1のサイバーセキュリティ担当者が「膨大なワークロード」に対処することが仕事で最も負担が大きいと答えています。膨大なワークロードとは、1日に数百件、ときには数千件ものアラートであり、これに優先順位付け、調査し、対応しなければなりません。

アラートが調査されない上位3つの理由

毎日発生する疑わしいアラートのすべてに対して調査と対応を行うことができない理由は何ですか？

ソース：IDC



際限のないアラートに対応するという課題は、サイバーセキュリティ人材の不足によってさらに困難を極めています。スキルを備えたサイバーセキュリティ人材が世界中で不足しているために、SOCに必要な人員を適宜配置することができないのです。この繰り返し指摘されてきた人材不足の問題に、毎日発生する大量のアラートがさらに追い打ちをかけます。1日に生成されるセキュリティチケットの64%が処理されないままであるのはそのためです。[3] アナリストは毎日発生するアラートのすべてに対応することができず、企業は攻撃に対して脆弱な状態に陥っています。

64%

処理されない日々のセキュリティアラートの割合[4]

セキュリティチームがアラートの処理に手一杯であれば、CISOは戦略的指針を示すことはできず、アナリストは重要なエンジニアリングや最適化のタスク、自動化によるアラート対応、プロアクティブな脅威ハンティングといった作業を実施する時間的余裕はありません。

このような課題を解決するのがSOAR (セキュリティのオーケストレーションと自動化によるレスポンス)です。Splunk SOARのようなSOARプラットフォームは、セキュリティにおけるパワーバランスを変えます。日々の定型業務をアナリストの作業リストから取り除き、セキュリティツールのオーケストレーションを行うことによって、セキュリティチームは企業のセキュリティ体制の強化やビジネスの推進にもっと時間を割けるようになります。

[3]https://www.splunk.com/en_us/form/an-enterprise-management-associates-research-report.html

[4]https://www.splunk.com/pdfs/analyst-reports/an-enterprise-management-associates-research-report.pdf

アナリストの1日の業務

SOARの活用前と活用後

1日あたり1万件の疑わしいインシデント

SOARなし

アナリストは、受け取った
アラートをすべて**手作業で**
選別、分析、管理

アナリスト

SOARあり

オーケストレーション
セキュリティインフラのオーケストレーションにより、
人材、プロセス、およびツールの価値を最大化

自動化
反復的なセキュリティタスクを自動化して、
より多くのアラートに対処

対応
自動化とコラボレーションを
活用して、よりスマートかつ
迅速に脅威に対応

日々発生する
すべての
アラートに
対処

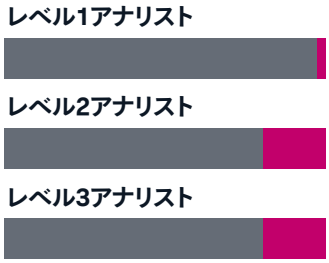
アナリスト

判断と行動

すべてのレベルのアナリストが、リアクティブな活動に大半の時間を費やしており、戦略的な活動に割り当てる時間がほとんどない。

リアクティブな
活動に費やす時間

戦略的な活動に
費やす時間



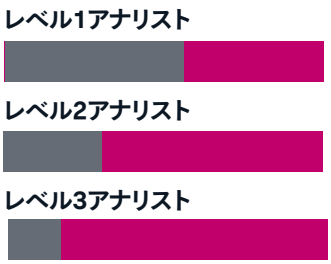
対応までの時間：
30分

判断と行動

SOARを活用することで、アナリストのワークフローがシンプルになり、コラボレーションでセキュリティインシデントに迅速に対応。

リアクティブな
活動に費やす時間

戦略的な活動に
費やす時間



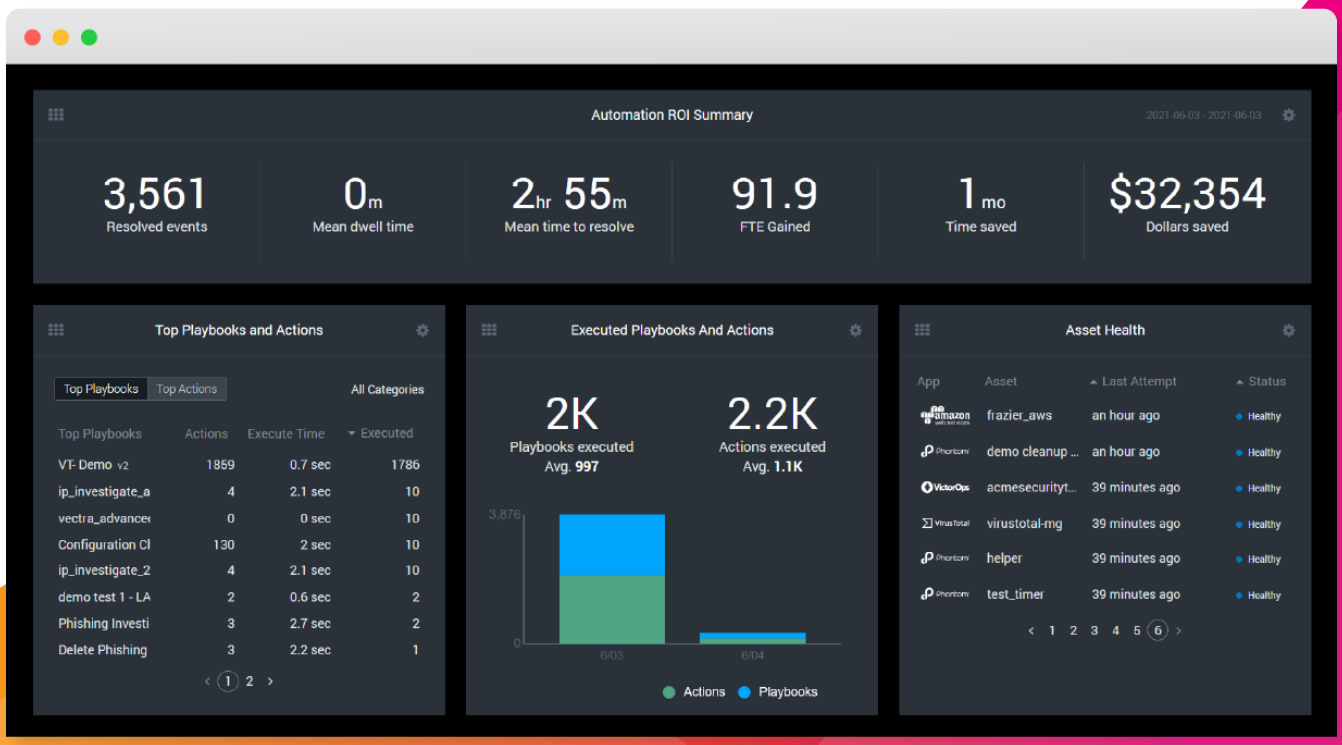
対応までの時間：
30秒

SOARのROI

ある試算によれば、フィッシング攻撃を防ぐための年間のコストは約70万ドルに上ります。また、ランサムウェアもコストがかかり、さらに長期にわたって企業の評判を損なうおそれがあります。SOARを利用すれば時間と費用を節約することができます。[5] 節約できる時間は、フルタイムの従業員1人分の手作業に匹敵します。たとえば、SOARプラットフォームを活用することで、3人のアナリストで編成されるSOCチームが、すべてを手作業で行う10 ～ 15人編成のチームと同等の成果を上げることができます。

> **“抱えている仕事の量に圧倒され、新たに人を雇うこともできないという臨界点が遅かれ早かれやって来ます。自動化はその唯一の解決策です”**
>
> —McGraw Hill社シニアクラウドサイバーセキュリティアーキテクト、Jason Mihalow氏
>
> 導入事例を見る

Splunk SOARのメインダッシュボードで、セキュリティチームはSOCアクティビティの概要、重要なイベント、プレイブックを確認することができます。また、アクションの自動化によるROIのサマリーも表示されます。[Automation ROI Summary]には、SOCが利用している自動化の効果が、節約された時間やコスト、得られたFTE (フルタイム当量)、平均滞留時間などの形でリアルタイムで表示されます。



[5]https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

導入事例

Norlys社：SOARによる成功事例

Norlys社はデンマーク最大の公共サービスおよび電気通信企業であり、150万人の顧客を抱えています。独自のログ分析およびインシデント対応システムを構築して以来、同社のセキュリティチームは、反復的な作業、多すぎるツール、Web UIの遅さ、面倒なプロセスなどに悩まされていました。同社はSplunkを導入して、反復的な作業を自動化し、調査を一元化しました。

導入事例を見る

成果：

- 1週間に35時間の仕事量を節約
- 以前は30分かかっていたプロセスを30秒で完了
- チケット発行までの時間を98%短縮

Norlys社が自動化した上位5つの単純作業

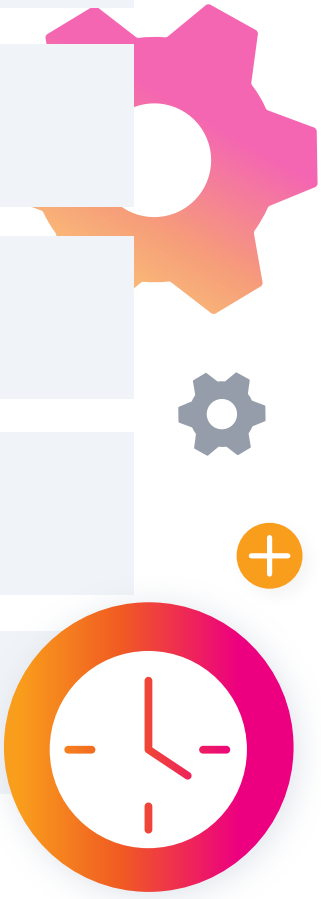
1 Splunk ESからSplunk SOARへ重要なイベントを転送
3分から**2秒**に短縮

2 AVアラート発生時の調査を自動化
40分から**10分**に短縮

3 脅威フィードからのIOC検出時の調査を自動化
15分から**10秒**に短縮

4 ブラウザ履歴の取得プロセスを自動化
30分から**20秒**に短縮

5 外部システムへのチケットオープンを自動化
10分から**10秒**に短縮



セキュリティモダナイゼーションでビジネスを変革

CISOがビジネスリーダーの求める戦略的パートナーとなり、セキュリティアナリストが専門能力を発揮する機会を見いだすためには、オーケストレーションと自動化が不可欠です。Splunk SOARを活用することで、セキュリティチームは、セキュリティツールとセキュリティ人材に対する投資の効果を最大限に引き出すことができます。

Splunk SOARを今すぐお試しください

splunk>