Secureworks®

ホワイトペーパー

サイバーセキュリティは常に時間勝負：大きな負担となる常時監視体制

24時間365日体制のサイバーセキュリティ業務における課題の軽減

残念なことに、サイバー攻撃は絶え間なく発生します。世界規模で組織化されている攻撃グループによる悪質なサイバー活動に対抗するには、サイバーセキュリティチームによる24時間365日体制の監視が不可欠です。

PsyberResilience Projectによると、「アメリカでサイバーセキュリティ業務に従事する70万人超の専門職らは昨今、デジタルファーストレスポンダー（企業や政府、地域社会全体を狙う執拗なサイバー攻撃の波に対峙し、サイバー防衛の最前線で立ち向かう部隊）と呼ばれる機会が増えている」とのことです[1]。

たとえ理想的なチーム体制と充分な時間があったとしても、リスクの高い状況を厳重に監視することは従業員にとって大きな負担になります。従業員はたちまち過労状態となり、脅威検知環境における人的ミスを誘発し、組織全体のセキュリティが脆弱化する恐れがあります。

同様に、業務量の増加が優秀な社員の離脱やセキュリティ部門のチームワーク崩壊を招き、結果としてサイバーセキュリティプログラムの有効性が低下し、実務能力に長けたセキュリティ担当者が現場から去ってしまう恐れもあります。Forrester社の調査によると、サイバーセキュリティ専門家の51%が「極度のストレスまたは過労」を経験しており、65%が「業務上のストレスが原因で、仕事を辞めようと思ったことがある」と回答しています[2]。さらに、ESG社の調査では、対象者の60%が「サイバーセキュリティ関連の仕事は、ワークライフバランスに悪影響を与える可能性がある」という質問に「そう思う」と答えており、38%が「業務によるストレスが度を超えている、と感じることがよくある」という質問に「そう思う」と答えています[3]。

本書では、セキュリティ実務を担う人材のひっ迫状況について掘り下げて解説します。さらに、チームメンバーの作業を自動化して軽減し、リスク緩和に向けた業務効率や対策の有効性を高めるための手段をいくつかご紹介します。

65% サイバーセキュリティ専門家の65%が「業務上のストレスが原因で、仕事を辞めようと思ったことがある」と答えています[2]。

38% サイバーセキュリティ専門家の38%が「業務によるストレスが度を超えている、と感じることがよくある」と答えています[3]。

出典：

[1] 10 Top Reasons for Cybersecurity Professional Burnout

[2] Forrester: Predictions 2022: Cybersecurity, Risk, and Privacy

[3] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V

サイバーセキュリティチームに課される様々な要求の中身

サイバーセキュリティチームの業務実態を紐解くための重要な第一歩は、無数の業務タスクをありのままに把握することです。サイバーセキュリティプログラムおよびチームの理想形は、「既存プラットフォームの事前チューニング・管理」と「インシデント対応や平常時のオペレーション」がバランス良く進められる体制です。

このようなサイバーセキュリティチームを実現するためには、以下の課題に対処する必要があります。

事前対応型（プロアクティブ）と事後対応型（リアクティブ）アプローチの使い分け

多くの実務者にとって、セキュリティの有効性は定点評価できるものではありません。新たな脅威が台頭し、新たな対応策が常に実装されている状況に身を置く実務者は、態勢整備およびリスク評価の観点で、プロアクティブな姿勢を維持する必要があります。一方、脅威緩和に関する新情報をもとに、自社環境を見直して侵害の有無を確認する回帰的なアプローチも必要です。セキュリティ業務の従事者は主に、このような形で業務のバランスを取っています。つまり、回帰分析やリスク緩和を考慮し、攻めと守りの微妙なバランスを見極める反復的な手法です。

インシデント対応

インシデントの監視や緩和だけでなく、事業資産を最大限保護しながらリスクを評価することもセキュリティチームの役割です。コンプライアンス担当部門など、他の事業部門からセキュリティチームに対し、監査や変更管理などの要請が来る可能性もあります。その場合、実際の侵害に対処しつつ、依頼された情報をすみやかに提供しなければなりません。一方で、法令・規則、各種要件などを文書化することもセキュリティチームの役割です。

平常時

組織の安定状態を維持する上で、自社が直面するリスクレベル、利用可能な資金、コンプライアンスや法令・規則に関する潜在的な順守義務など、いくつかの課題があります。たとえば公共関連組織であれば、政府の基準およびコンプライアンス要件（HIPAAなど）を順守し、場合によっては違反リスクを評価する必要もあります。前述の例では、個人情報が流出した場合、違反リスクはきわめて深刻です。コストの多寡にかかわらず、このような事態を回避するための人材・ツール・プロセスには惜しみなく投資すべきです。

外的要因

2020年にリモートワークが急速に普及したことで、セキュリティチームの業務負荷が増大しました。リモートワーク対応における重点課題は、「従業員がスムーズに業務を継続できるよう、必要なツールを支給すること」および「生産性の維持に必要な各種ツールに従業員がアクセスできるよう、健全なインフラを整備すること」でした。

しかし情報の「可用性」だけでなく、「機密性」と「完全性」にも十分注意を払う必要があります。リモート勤務する従業員の大半は、機密保持を徹底できる環境に居住していません。さらに、特定の情報に応じたアクセス権の設定および、脆弱な状態で情報が露出しかねない外部デバイス（USB、プリンタなど）に関する全社的なポリシーが充分検討されてこなかった可能性もあります。

100%リモート体制を継続中の組織もあれば、ハイブリッド型の勤務体制を取り入れた組織もあります。リモート体制を継続する組織は、インフラ監視のリモート関連項目に何らかの変化が生じていないか分析を続ける必要があります。リモート勤務期間にセキュリティチームが監視不能だったシステム環境について詳細分析すべきかをチーム内で確認する必要があるため、業務量がさらに増えます。

チームへの負担

大多数のグローバル企業の監視体制に、「業務時間外」という言葉はありません。かつては、24時間365日監視を標榜していても実際の勤務体制には波がありました。しかし今や企業だけでなく攻撃グループもますますグローバル化し、昔とは状況が異なるため、セキュリティチームは年中無休・フルスピードで稼働しなければなりません。

絶え間なく押し寄せる脅威

「ニューノーマル」の到来によりアラート件数が肥大化し、チームの疲弊を招くこともあります。止むことのない攻撃の波に対処するチームは、休む暇さえありません。アラートの件数があまりにも増え、全体の30%をやむを得ず「無視する」ようになったという事例もあります[4]。

統合管理システムの欠如

さらに、事業や情報資産に対するリスクが最も高い「重篤な脅威」だけに集中したい、という顧客ニーズもあります。しかし、そのための統合管理システムがないため、セキュリティ担当者は各種ツールをいくつも組み合わせてリスクや深刻度の高低を評価するしかありません。担当者はこれらのツールやプロセスに経験則を融合して業務に当たるため、継続的な学習・能力開発が必要です。

プロセス

プロセスの保守管理もそれ自体がストレス要因となり、過労につながります。調査結果を文書化し、アクションを追跡管理するためのツールの種類にもよりますが、堅牢なチケット起票システムが存在しない場合、複雑で時間のかかる手順を踏まなければ適切なプロセスを徹底できないこともあります。

出典：

[4] IDC, "In Cybersecurity, Every Alert Matters" Thought Leadership White Paper, October 2021

相互依存関係

セキュリティオペレーションは真空状態で成立しているわけではありません。多くの企業では、インフラ管理と情報セキュリティの担当部署が異なっています。情報資産自体の維持・強化を担当する責任者が、セキュリティ担当責任者とは別の組織やグループに所属していることもあります。インシデント対応または平常状態の物理資産へのエージェント実装の可否を判断するのは、セキュリティ部門とは全く別の指揮命令系統や要件を有するIT部門やITサービス部門の担当者かもしれません。こうした状況ではセキュリティチームの権限が及ばないことがあるため、対応の遅れなどの問題につながる恐れがあります。

「DIY」型セキュリティ対策の重圧

さらに、予算や個人データ保護などの観点からセキュリティプログラムのすべてを自社／自組織内で維持しなければならないという大きなプレッシャーもあります。「深刻度の低いインシデントの中から深刻度の高い侵害に発展しそうなものを見極め、事業リスクに発展する重要項目に集中できるよう工数を調整する」という作業は、社内の実務担当者だけでは手に負えない可能性もあるでしょう。

業務支援に役立つテクノロジー

幸いなことに、サイバーセキュリティベンダーが提供する各種テクノロジーや関連サービスを利用すれば、セキュリティ実務担当者の業務を軽減することができます。以下はその一例です。

XDR

セキュリティ脅威の予防・検知・対応を実行するSaaSプラットフォームをベースとした製品であり、エンドポイント、ネットワーク、クラウドをはじめとする様々なセキュリティシステムのテクノロジーをXDRプラットフォーム上で統合します。それぞれのポイントソリューションが収集した監視データを一元化し、機械学習や厳選した脅威インテリジェンスを適用して悪質な活動を検知し、お客様組織のセキュリティ担当者にアラートを配信します。

MDR

該当分野のソリューションを最大限活用可能なスタッフ・ノウハウ・時間が足りない多くの組織にとって、単一のソフトウェア製品だけではニーズを満たせない場合があります。そこで、多くの組織に欠けている人的リソースを強化し、専門家による知見を提供する「マネージド・ディテクション＆レスポンス（通称MDR）」が登場しました。MDRは機械学習およびSaaSプラットフォームの高度なテクノロジーと、経験豊富で強固なセキュリティオペレーション専門チームの力に融合したサービスです。ベンダー側でアラートの調査、切り分け、エスカレーションを行うセキュリティアナリストに加え、深刻な問題が発生した場合はインシデント対応コンサルタントも出動します。また、お客様環境を監視する脅威ハンターが先手を打って脅威を除去します。

集合知としてのインテリジェンス

変化の激しい環境では、元々の状況（過去のトレンド）と最近の状況（新たなツールキット、ルートセットなど）の両方を考慮しなければなりません。幅広い顧客基盤および長年の経験を有する外部のサイバーセキュリティ専門家は、脅威のアクティビティ種別や解決策について比類ない視点を提供できます。外部専門家の叡智を活用することで、自社における脅威の全体像を第三者の視点で把握できます。この全体像に、類似案件にもとづく最適解に関する外部専門家の視点を重ね合わせることで、インテリジェンスを拡充できます。これにより業務量が軽減するとともに、社内スタッフだけでは見過ごされていたかもしれない詳細な知見も得られます。

攻撃が四六時中発生する現代において、24時間365日体制のサイバーセキュリティアプローチは不可欠です。莫大なプレッシャーにさらされるサイバーセキュリティ実務担当者らは、メンタルヘルスの悪化につながる「ストレスレベルの上昇」を訴えています[5]。しかも、世界規模でサイバーセキュリティ人材が不足していること（推定272万人）を考えると、この状況は当分続くでしょう[6]。

60% 調査対象者の60%が「サイバーセキュリティ関連の仕事は、ワークライフバランスに悪影響を与える可能性がある」と回答しています[5]。

272万人 世界で272万人のサイバーセキュリティ人材が不足しています[6]。

激務をこなすセキュリティチームにとっての朗報は、XDR、MDRおよびセキュリティ業界自体の叡智などを提供する外部ベンダーの力を借りれば業務負荷を軽減し、効率化を推進できることです。

外部の視点や支援を通じてセキュリティチームを補強することで、チームメンバーが新たな洞察と活力をもって仕事に取り組むことができます。これにより、バランスの良い職場環境が実現すると共に、事業リスクをより一層軽減できます。

出典：

[5] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V

[6] (ISC)² Cybersecurity Workforce Study, 2021

Secureworks®

Secureworks（セキュアワークス、NASDAQ: SCWX）は、Secureworks® Taegis™を通じてお客様のビジネス進捗を保護するサイバーセキュリティのグローバルリーダーです。Taegisはクラウドネイティブなセキュリティ分析プラットフォームであり、20年以上にわたる実業務を通して蓄積された脅威インテリジェンスとリサーチに基づき構築されています。お客様は、高度な脅威を効果的に検知し、合理的な調査と関係チーム間のコラボレーションを行い、そして適切な対応アクションを自動化することが可能となります。

コーポレート本部

米国
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

ヨーロッパおよび中東

フランス
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

ドイツ
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

英国
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

アラブ首長国連邦
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971 4
420 7000

アジア、太平洋地域

オーストラリア
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

日本
〒100-8159
東京都千代田区大手町一丁目2番1号
Otemachi Oneタワー17階
+81-3-4400-9373
www.secureworks.jp