2023年
セキュリティの現状

グローバル調査：先進組織に学ぶ
レジリエンス構築のための組織的な取り組み

splunk>

セキュリティ 2023：
セキュリティチームの現在地

組織のシステムがますます複雑化する中で、サイバー攻撃は増え続け、巧妙さも増しています。そして、セキュリティチームは相変わらずストレスを感じています。しかし、2023年のセキュリティ調査レポートでは、脅威への対応が追いつかないと回答した割合が減少するという驚きの結果が明らかになりました。

だからといって浮かれるのはまだ早いでしょう。セキュリティ要件を満たすのが2年前よりも難しくなっていると回答した割合は世界全体で53%にのぼり、厳しい状況が続いていることを物語っています。それでも2022年の66%から減少していることは確かです。明るい状況の中でも暗い兆しを見つけることが得意なSplunkのセキュリティエキスパートですら、2022年にはセキュリティチームを大混乱に陥れるほどの目新しい展開はほとんどなかったと口を揃えます。実際、SolarWinds攻撃やLog4jの脆弱性に匹敵する脅威はありませんでした。そのコメントを引用するならば「タイタニックを沈めるほどの氷山は現れなかった」のです。

このデータが示すのが明るい兆しなのか、単なる偶然の賜物なのかはまだわかりませんが、いずれにしても組織はこのチャンスを活かすべきでしょう。しかし、事はそう簡単ではありません。多くのセキュリティチームはリアクティブな対応に手一杯で、プロアクティブな対応に転換する余裕がありません。

調査では、詳しい分析のために、仕事がきつくなっていると答えた過半数の回答者にその理由を尋ねました。そこで挙げられた主な課題は以下のとおりです。

- 脅威が巧妙化している(38%、3年連続第1位)
- セキュリティスタックが複雑化している(30%)
- IaaSまたはSaaSの導入で監視や管理が難しくなっている(それぞれ29%、28%)
- 仕事量が多すぎて「リアクティブな対応」から抜け出せない(28%)

最後の課題は後続の一部の回答にも反映されています。たとえば、攻撃の件数または誤検知が多すぎて対応しきれない(それぞれ24%、25%)、十分なスキルを持つ人材を雇用したり定着させたりできない(それぞれ25%)などです。

これらの課題は国や地域によって差が見られます。たとえば、SaaSアプリケーションの監視やすべてのセキュリティデータの効果的な分析が難しくなっていると回答した組織の割合は、APAC地域では全世界の平均を5 ～ 7ポイント上回った一方、欧州ではその割合が低く、北米では世界平均とほぼ一致しました。

調査方法

今回の調査は、勤務時間の半分以上をセキュリティ業務に費やしているセキュリティ/ITリーダー 1,520人を対象に実施されました。

10カ国

北米、西ヨーロッパ、APAC地域にほぼ均等に分散：オーストラリア、カナダ、フランス、ドイツ、インド、日本、ニュージーランド、シンガポール、英国、米国

15の業界

航空宇宙・防衛、消費財、教育、エネルギー、金融サービス(銀行、証券、保険)、政府機関(連邦/中央、州、地方)、ヘルスケア、ライフサイエンス、製造、メディア、リテール(小売り)・卸売り、テクノロジー、通信、運輸・輸送・物流、公益

すべての業界と地域で共通していた点は、セキュリティリーダーと他部門のリーダーがレジリエンス(耐障害性および回復力)向上のためにコラボレーションする機会が増えていることです。従来のサイバーセキュリティではインシデントを未然に防ぐことに重点が置かれますが、レジリエンスはむしろ事後の対応を考える取り組みであり、インシデントが発生したときに何をするかに焦点が置かれます。

とはいえ、危機的な状況から効果的に回復するための対策は事前に立てておく必要があります。リスク評価、インシデント対応計画、テクノロジーやトレーニングへの重点的な投資には、サイバーセキュリティという枠を超えた戦略的思考が求められます。

今回の調査では、組織全体での連携で成果をあげ、連携しにくい「邪魔者」ではなく、成功に欠かせない重要な存在、重要なパートナー「イネーブラー」として存在感を高めるセキュリティチームが増えていることがわかりました。詳細は後述しますが、ビジネス部門のステークホルダーの79%がセキュリティチームを重要パートナーと考え、組織レベルの意思決定に参加させたり、セキュリティ予算を増やしたりしています。

また、セキュリティ予算を決めるビジネスリーダーは、レジリエンスに関する指標に注目し、MTTR (平均回復時間)を重視し始めています。実際、調査でもMTTRが重要指標のトップに挙げられました。

幅広い課題

今年のレポートで取り上げる注目すべき課題には以下のものが含まれます：

- **64%**のSOCが、セキュリティツールの数と種類が多すぎ、しかも互いにほとんど連携していないため、**インシデント対応が困難**になっていると回答しています。
- **88%**の回答者が、スキル不足または要員不足のいずれかを問わず**人材面での課題**を抱えています。
- 攻撃者が組織に侵入した後の**平均潜伏期間は2.24カ月**、約9週間に及びます。

一方で、さまざまな課題への取り組みも進んでいます。主な対策には以下のものが含まれます：

- **95%**の組織が**サードパーティリスク評価を強化**しています。
- **81%**の組織が**セキュリティ運用とIT運用の業務の統合**に取り組んでいます。
- **95%**の組織が今後2年間で**セキュリティ予算が増額**される予定だと回答し、56%が大幅な増額を見込んでいます。

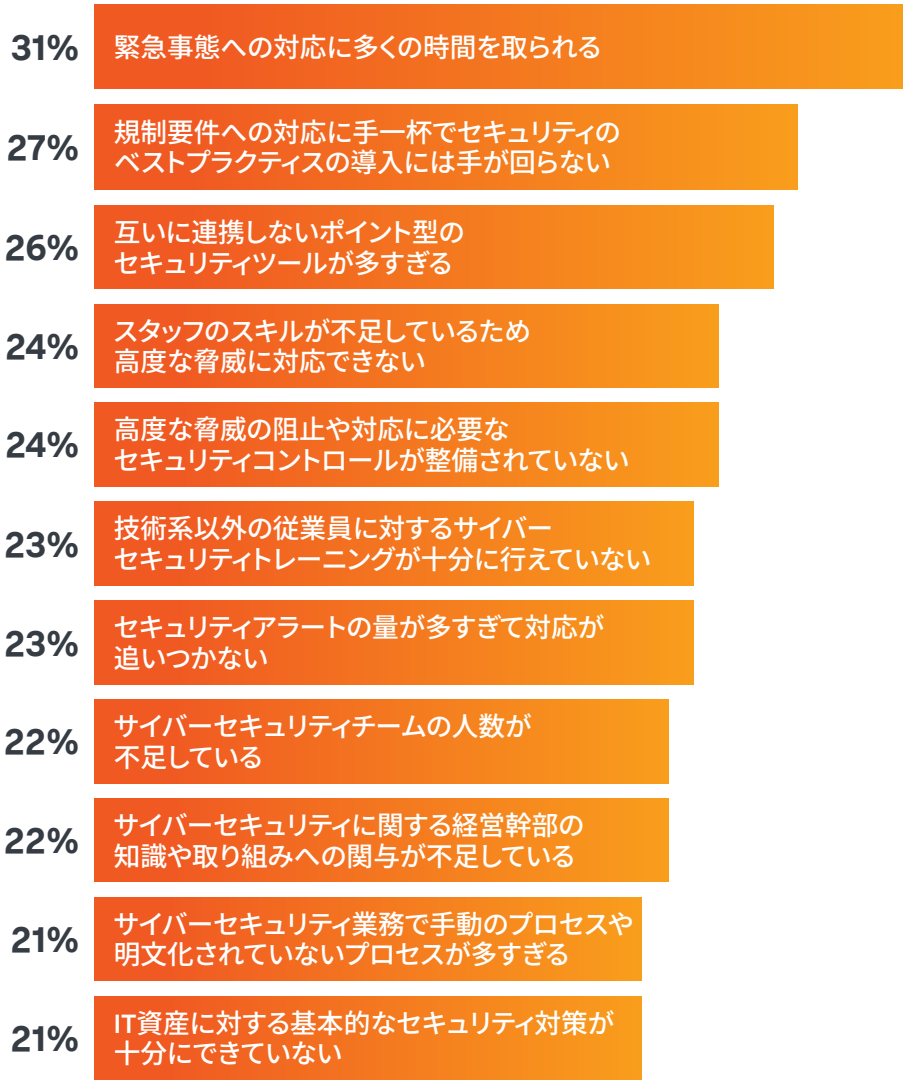
全体として、セキュリティチームがうまく対応できているかどうかに関係なく挙げられた課題は幅広く分散しました。突出した課題がない中で、緊急事態への対応に多くの時間を取られるという全般的な課題が1位に入ったのは妥当なところでしょう。

後れを取るような状況から抜け出せない原因はたくさんありますが、残念ながらその解決策はあまりありません。組織は何千ものサイバー攻撃を日常的に受けるため、対応が後手に回るのも無理はありません。優秀なセキュリティチームは最善を尽くして既知の攻撃ベクトルに先手を打ちますが、攻撃者は常に新しい手口を生み出すため、再び後手に回ってしまいます。

また、コンプライアンスの確保も年々難しくなっています。テクノロジーが進化し、データの活用法が広がると、攻撃手法も進化し、それが最終的に規制の強化につながるためです。

サイバーセキュリティの主な課題

組織内で特に大きな課題を3つ選択



SOCの状況

前述のとおり、セキュリティチームは追い込まれています。今日のSOC (セキュリティオペレーションセンター)は多くの仕事を抱える一方で、それを処理する人材が不足しています。

- **64%のSOCチームが、セキュリティツールや管理コンソールの数と種類が多すぎ、しかも互いにほとんど(またはまったく)連携していないため、包括的な調査や対応をタイムリーに行うことが難しいと回答しています。**
- **49%が、セキュリティイベントが増加しているにもかかわらず、トリアージ、調査、対応を手動で行っているため、人手が足りていないと回答しています。**

その結果、SOCの負担の増大がリスクを招いています。本来は調査すべきなのにSOCに余力がないために見過ごされているアラートは、回答者の推定で平均41%にのぼります。そして当然、調査していない中に真陽性のアラートがあれば、実際の攻撃につながる可能性があります。このことは、アラートを生成する高価なツールのROIが実際よりも低くなり、アナリストチームの効率と意欲が低下し、組織のセキュリティとレジリエンスが弱まるなど、あらゆる方面に悪影響を及ぼします。

景気の後退が続く中で、
人材不足の問題は深刻さを
増すと見込まれます。

55%の回答者が、景気後退を受けて人材の獲得と定着が難しくなると予想しています。

32%の回答者が、人材の獲得と定着は容易になると考えています。

人材不足の影響

長年の人材不足は今もなお深刻な状況です。88%の回答者がサイバーセキュリティ人材/スキルに課題があると答え、53%が概して十分な要員を確保できないこと(前年と同率)、59%が適切なスキルを持つ人材が見つからないこと(前年の58%から微増)を挙げています。

セキュリティリーダーは、勤務時間外の対応率の向上と、最優先の問題に24時間対応する負担の軽減を目的に、マネージドセキュリティサービスプロバイダー (MSSP)の利用を推進しています(42%が利用を増やしたと回答)。それにもかかわらず、過去12カ月間で人材不足を要因とするさまざまな問題が起きています。

- **81%の回答者が、チームメンバーが不慣れな業務を請け負わざるを得ない状況だと回答しています(前年の76%から増加)。**
- **81%が、チームの重要メンバーの1人以上が燃え尽き症候群により離職したと回答しています。**
- **78%が、セキュリティリーダーとしての仕事の負担が増え、別の職務への異動を検討していると回答しています(前年の70%から増加)。**
- **77%が、1つ以上のプロジェクト/イニシアチブが失敗したと回答しています(前年の68%から増加)。**

サイバーセキュリティの領域では人材不足が当たり前の状態です。しかし、この調査結果は、人材不足が慢性的な状況にあるだけでなく、深刻化していることを示しています。「いつもこんなものだ」と軽く見ていると、後で大きなツケを払うことになるかもしれません。

SOCの対応時間

人材不足の緩和策

セキュリティリーダーは人材不足の問題に手を打ち始めています。中でも前述のMSSPの利用は注目が高まっており、86%の組織がスキル不足を補うためにサービスプロバイダーを活用していると回答しています。さらに、56%の組織がセキュリティ運用業務の大半をサードパーティのサービスプロバイダーにアウトソースし、その多くが、セキュリティ運用の強化による昼夜を問わない対応と、サービスプロバイダーが提供する高度なツールの使用を目的にしています。利用範囲を今後拡大する予定だと回答した組織も42%にのぼります。

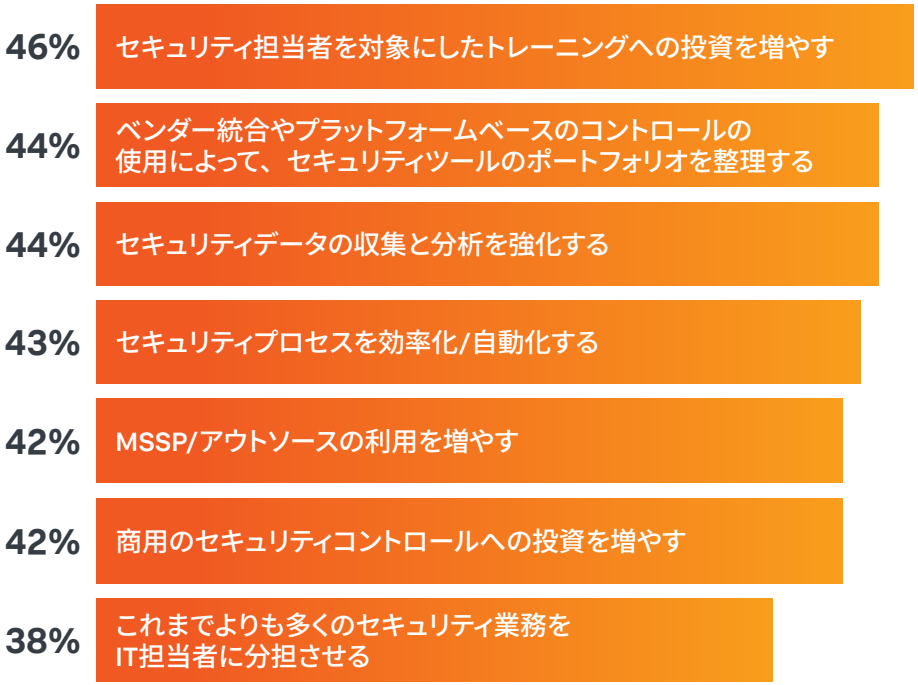
内部人材の活用も進んでいます。セキュリティチームの人材不足を補うために、86%の組織がセキュリティ以外の人材の再教育に取り組み、38%がこれまでよりも多くのセキュリティ業務をIT担当者に分担させる予定だと回答しています。

雇用による人材確保を除く人材不足対策では、どの地域でもトレーニングの増強が1位になりました。セキュリティチームがスキル向上の必要性を強く感じている領域の上位には、クラウドの運用とアーキテクチャ (41%)とセキュアなアプリケーション開発(42%)が入りました。

さらに、多くのチームが人材不足を補うために、自動化の導入、ツールの整理、データ活用を通じたチームの生産性向上に取り組んでいます(図を参照)。

人材不足を克服するために優先する対策

(人材補充を除く)



すべての地域で1位は「トレーニングへの投資を増やす」(45 ～ 47%)でしたが、APAC地域では「商用のセキュリティコントロールへの投資を増やす」(47%)が1位タイでした。

レジリエンスが重要指標に

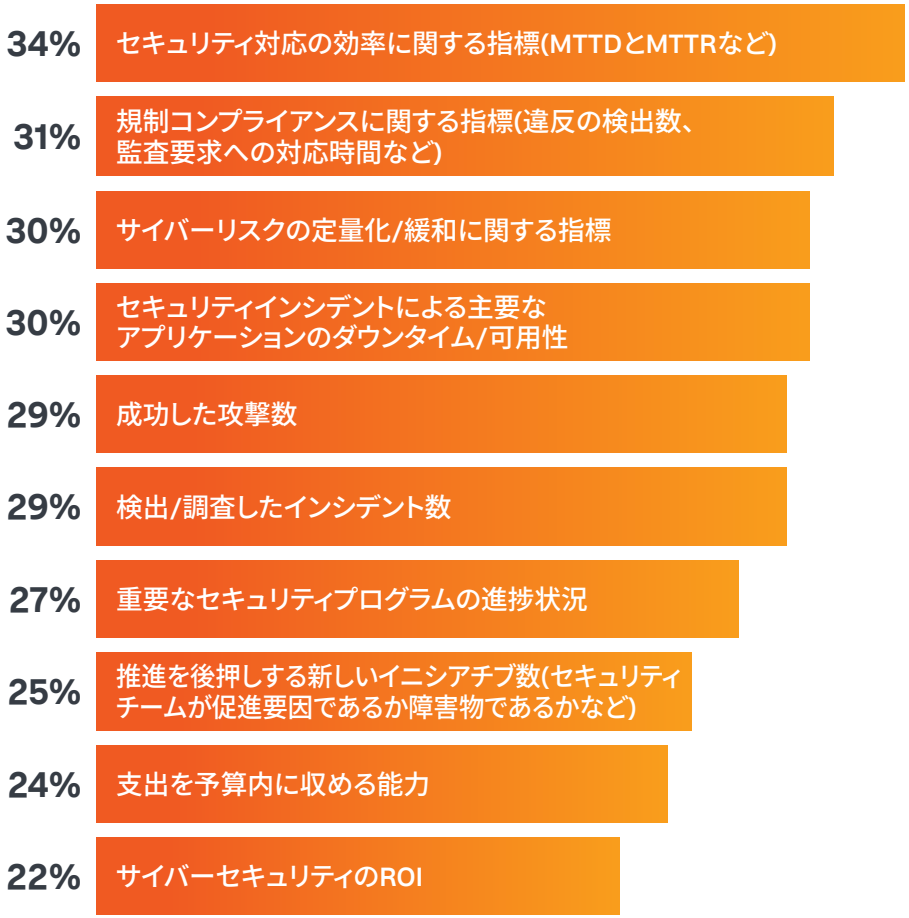
調査では、セキュリティ対策の効果を評価するためにビジネスリーダーが使用している主なパフォーマンス指標を3つ挙げてもらいました。その結果、レジリエンスに関する指標が重視されていることがわかりました。右の図に示した上位6つのうち4つ(コンプライアンスとリスク緩和以外)はレジリエンス戦略に直結する指標であり、MTTD (平均検出時間)とMTTR (平均復旧時間)が1位(34%)になったほか、攻撃やインシデントの発生件数よりもダウンタイム(30%)が上位に入りました。

受ける攻撃の数や巧妙さは組織が制御できるものではなく、次にどのような攻撃を受けるかも予測できませんが、MTTRは能動的に改善できます。また、サービス停止は完全には防げないことを踏まえれば、本当に重要なのは、そこからどれだけすばやく効果的に回復できるかです。

「MTTRは簡単に測定し、改善できます」と、Splunkの特別セキュリティストラテジストを務め、Splunkの脅威アドバイザリーチーム「SURGe」を率いるRyan Kovarは指摘します。「常に未知の脅威が登場するため、MTTDは確実に改善することはできません。SolarWinds攻撃はまったく想定外であったため、検出までに2年を要しました。しかし、MTTRは短縮できます。そしてそれは、レジリエンスの向上につながります」

ビジネスリーダーによるセキュリティ対策の評価指標

ビジネスリーダーがサイバーセキュリティの状況を把握するために最もよく使用する指標



セキュリティチームは以前から、自らがビジネスにとって価値のある存在であり、セキュリティの向上、そしてレジリエンスの強化は、新しいビジネスイニシアチブを否定するものではないことを理解しています。しかし、ビジネス部門がこの考え方を理解し、セキュリティチームがビジネスの成功に重要なパートナーであることを理解するまでには時間がかかりました。今回の調査では、多くの組織でビジネス部門がその点を理解し始めていることが明らかになりました。

実際、ビジネス部門のステークホルダーの79%が、セキュリティチームを信頼できる情報源(49%)または組織のミッションに欠かせないイネーブラー (30%)として評価しています。逆に、必要ではあるが邪魔な存在(12%)または完全な障害物(8%)と考えているステークホルダーは少数にとどまりました。

セキュリティチームに戦略的パートナーやイネーブラーとしての役割が与えられたことで、コラボレーションの範囲が広がり、レジリエンスが組織全体の問題として受け止められるようになっています。また、リーダーレベルでは、こうした尊重の姿勢と重要な意思決定への参加が具体的な成果として現れています。調査では、セキュリティリーダーがビジネス戦略に関わるようになったことで、46%がビジネス部門とのコラボレーションに関するセキュリティチームのスキルが向上したと回答し、42%がその結果としてセキュリティチームへの予算が増えたと回答しています。

79%のビジネスステークホルダーが、セキュリティチームは邪魔な存在ではなくパートナーだと考えています。

インシデント、アラート、脅威ベクトル

新しい戦略を取り入れ、部門横断的な連携が進む中でも、セキュリティチームは大きな課題に直面しています。攻撃者が手を緩める気配はありません。調査では、世界全体で、インシデントの件数が増え、脅威の潜伏時間が長くなり、ビジネスへの損害が大きくなっていることが明らかになりました。

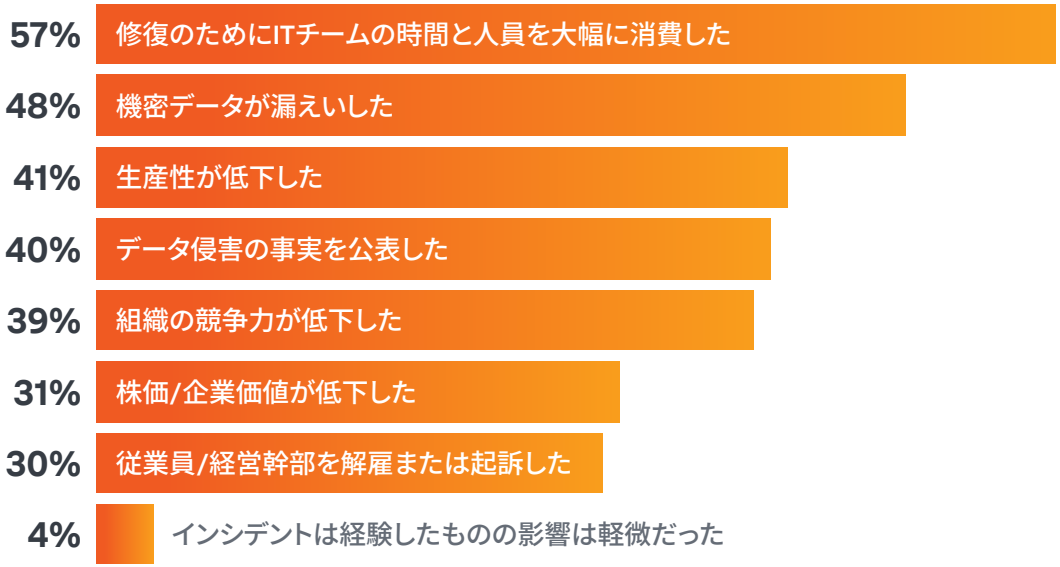
インシデントが及ぼす計り知れない影響

セキュリティインシデントは大きな悪影響をもたらします。対応と復旧に多くの時間とリソースを消費するだけではありません。調査では、インシデントによる損害として、組織の競争力の低下、株価の下落、信用の低下が多く挙げられました。一方で、インシデントは発生したが大きな被害はなかったと回答した組織はわずか4%にとどまりました。

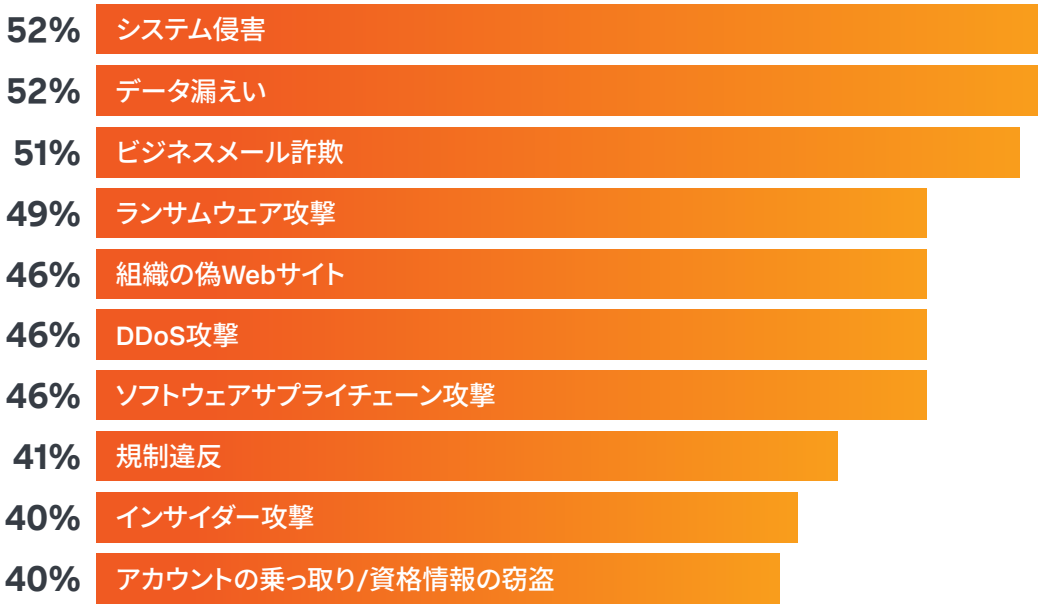
攻撃のタイプについては、今回の調査ではサプライチェーン攻撃を「サプライチェーンを通じて成功した実際の攻撃」と定義したため、その被害を受けた企業は世界全体で46%にとどまりましたが、もし「サードパーティのソフトウェアで悪用される前に発見して修正した脆弱性」を含めていたら、その割合は跳ね上がっていたでしょう。

侵入経路がどこでも、攻撃者にひとたび侵入されれば、攻撃に十分な時間を与えてしまいます。調査では、攻撃者がシステムに侵入してから内部関係者がそれに気づくまでの平均期間は2.24カ月、約9週間でした。これだけの時間があれば、攻撃者は余裕を持ってデータを盗み出したり壊したりできます。

過去2年間に経験したインシデントの影響



過去2年間に起きたインシデント



レジリエンスの欠如は喫緊の脅威

セキュリティチームはレジリエンス向上の重要性を理解しています。サイバーセキュリティインシデントによりビジネスクリティカルなアプリケーションで少なくとも月に1回はダウンタイムが発生すると回答した割合は62%にのぼります(前年の54%から増加)。こうしたダウンタイムの年間発生回数は平均で約22回でした(前年の19回から増加)。

セキュリティチームは、レジリエンス関連の指標の継続的な改善に取り組んでいます。調査では、目標削減率がMTTDで平均40%、MTTRで平均53%でした。実際、これらの指標は昨年よりも改善しており、サイバーセキュリティインシデントによって予定外のダウンタイムが発生したビジネスクリティカルなワークロードのMTTRは平均15.5時間で、前年の21.4時間から短縮しています。それでも、ダウンタイムのコストは年間収益の2.7%を占めます。

問題はコストの管理だけではありません。レジリエンス向上に取り組む理由として以下の点が挙げられています。

- **大規模なビジネス中断のリスクが高まっているため(83%)**
- **生産性の低下がイノベーションを阻害するリスクを生むため(79%)**
- **デジタルエクスペリエンスに対するダウンタイムが顧客離れにつながる可能性があるため(78%)**

この問題意識はリーダーレベルにも浸透しています。ほぼすべての組織(91%)が、サイバーレジリエンス戦略とその投資に関して、CISOがビジネス部門(財務、マーケティング、オペレーションなど)のリーダーと積極的にコラボレーションしていると回答しています。ただし、CISOにとってその道のりは容易ではないようです。

- **サイバーレジリエンスについて、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は31%にとどまりました。**
- **組織内で局所的にレジリエンス戦略を策定していると回答した割合も38%と低調でした。**
- **残りの31%は、レジリエンス戦略をまだ策定していないと回答しました。**

レジリエンスについて、**91%のCISO**がビジネス部門のリーダーとコラボレーションしている一方で、組織レベルで定められたアプローチがあると回答した割合は3分の1以下でした。

脅威のベクトルの分析

今回の調査で、多々ある脅威の中から特に懸念を抱いている脅威を3つ挙げてもらったところ、突出したものはなく、結果はほぼ均等に分散しました。ここでは、注目度の高い攻撃タイプとして、ソフトウェアサプライチェーンとランサムウェアの2つを深く掘り下げたいと思います。また、普及が進むパブリッククラウドが組織への攻撃の入り口になり得ることを考慮して、この脅威についても取り上げます。

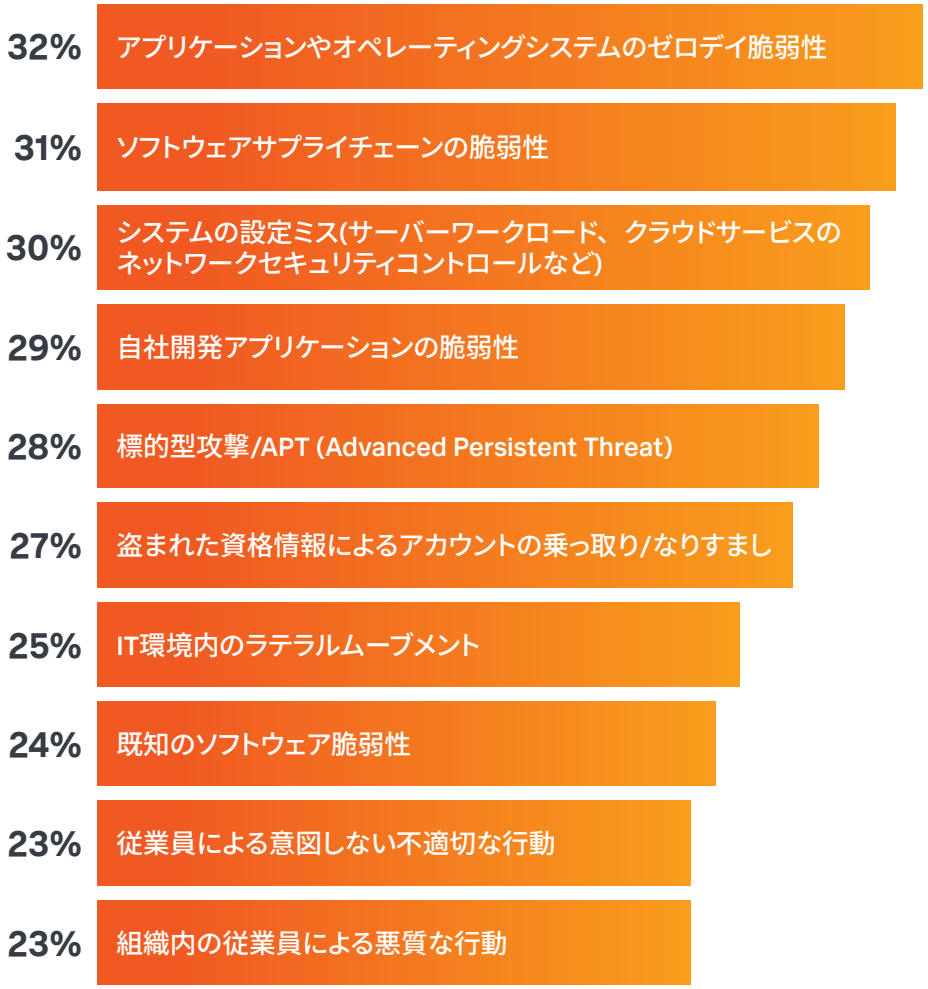
サプライチェーン：SolarWinds、Log4j、Kaseyaと、ソフトウェアの脆弱性を突く攻撃が続き、ソフトウェア-サプライチェーン攻撃が大きな注目を浴びました。実際、95%の組織がサードパーティリスク評価を強化していると回答し、前年の90%をさらに上回りました。

サプライチェーン攻撃に対するセキュリティ対策については、アプローチに大きなばらつきが見られます。17種類のサプライチェーン攻撃対策の中から導入済みのものを選択してもらったところ、次の3種類が26%で同率トップになりました。

- **セキュリティコントロールを評価して、サプライチェーン攻撃に有効な防止/検出方法を見極める**
- **認証システムを強化する**
- **セキュリティ対策の予算を増やす**

回答が分散し、多くの組織で導入される特定の対策がないことは、最近注目され始めたばかりの問題に対するアプローチがまだ定まっていないことを示しています。

特に懸念を抱いている脅威



ランサムウェア：ランサムウェアは新型コロナウイルスに似ています。まだ感染していない人もいますが、その数はどんどん減っているからです。2022年のセキュリティ調査レポートでの調査以来、ランサムウェア攻撃を受けたことがないと回答した組織は21%からわずか13%に減少しました。それに伴って、ランサムウェア攻撃によってデータやシステムにアクセスできなくなったと回答した組織は2022年の35%から今年は43%に増加しています。

攻撃を受けたときに身代金を支払う組織も増えています。組織または保険会社が身代金を支払ったと回答した割合は、昨年は66%でしたが、今年は75%に増加しました。状況の悪化はまだあります。要求された身代金の最大額が25万ドル以上と回答した組織は昨年の32%から今年は50%に増加し、実際に支払った身代金の最大額は平均で昨年の34万6,897ドルから43万978ドルと、1年で24%も増加しています。

この結果は意外でした。なぜなら、昨年の他の調査では身代金が減少傾向にあると考えられていたためです。今回のデータを調べ直すと、身代金額も支払い回数も増えていると回答したのは、実情をよく知っていると考えられるシニアレベルの回答者に多い(79%)ことがわかりました。

サプライチェーンのリスクと同様に、ランサムウェアでも導入している対策に大きなばらつきがありました。それでも、33%の組織が導入済みまたは導入を進めているとして比較的共通していた対策が、SIEMソリューションへの投資とメールセキュリティの強化です。このほか導入率が31%にのぼった4つの対策が、SOAR、高度な分析、多要素認証、エンドポイント設定強化ツールの活用です。

一方、隔離環境へのバックアップ/リストア機能への投資の割合が低調(21%)だったのは、組織が復旧よりも検出と対応を優先していることを示唆しています。

答えはデータにあり：検出データの収集と分析能力を向上させることがランサムウェア攻撃の被害を避けるために最も効果的だと回答した割合は91%にのぼりました。

クラウドセキュリティ：クラウドは今や組織にとってメインの環境です。SOCチームがパブリッククラウドでの問題の対応に大半の時間を費やしていると回答した割合は50%にのぼり、オンプレミスの13%を大きく上回りました。

IT環境のクラウド移行が進む中で、この傾向は続くでしょう。実際、ビジネスクリティカルなアプリケーションとワークロードの大半をクラウドで実行していると回答した組織は53%に達します。昨年の66%から低下しているのは興味深い点ですが、それでもかなりの数字です。また、パブリッククラウドについては、クラウドプロバイダーの防御をすり抜ける攻撃よりも、ユーザー側の設定ミスの方が脅威とみなされています。攻撃側も、手間をかけて突破口を開くよりも、ユーザーが招き入れてくれる機会を狙っています。

クラウドセキュリティについては、以下の課題が上位3つに挙げられました。

1. **データセンターとパブリッククラウド環境でセキュリティの一貫性を維持する(33%、3年連続1位であるものの前年の45%から減少)**
2. **アイデンティティ /アクセス管理(IAM)システムを正確かつ最新に保つ(32%、前年の3位から上昇)**
3. **複数のサイバーセキュリティコントロールを使用することによるコストと複雑さの増大(28%、前年の2位から低下)**

これらの課題の対策についても尋ねました。その結果、ここでも突出して多かった対策はなく、回答が分散しました。その中で多かったアプローチは以下のとおりです。

1. **コンプライアンス違反のある/業界のベストプラクティスに従っていないワークロード構成の特定(30%、3年連続1位であるものの前年の39%から減少)**
2. **セキュリティグループの設定(外部と接続するサーバーのワークロードをまとめるなど) (25%、前年の4位から上昇)**
3. **特権アカウントやサービスアカウントに関する監査証跡の強化(24%、昨年と同じく3位)**

クラウドアーキテクチャやハイブリッドアーキテクチャはまだ新しく、複雑で、絶え間なく変化しています。この領域では今後も難しい課題が生じることになるでしょう。

学ぶべきはクラウド：セキュリティチームがスキルを向上させなければならないという重圧を感じている領域として、41%の回答者がクラウドの運用とアーキテクチャを挙げました。

目標と戦略

サイバーレジリエンスと組織全体のビジネスレジリエンスの追求は、予算の増額から、コラボレーションの強化、クラウド、分析、自動化の導入促進まで、さまざまな面でセキュリティ戦略を後押しします。

レジリエンスを中心とした統合

新しい課題やなかなか解決しない課題に対処するため、組織はレジリエンスとアジリティに注目し始めています。調査では、51%の組織が今後12カ月間で、従来の事業継続/ディザスタリカバリー計画とサイバーレジリエンス向上の取り組みの融合に向けたソリューションの導入や投資を行う予定だと回答しています。さらに、48%がユーザー向けサービスの迅速復旧への投資、47%がセキュリティチームの迅速対応への投資を計画しています。

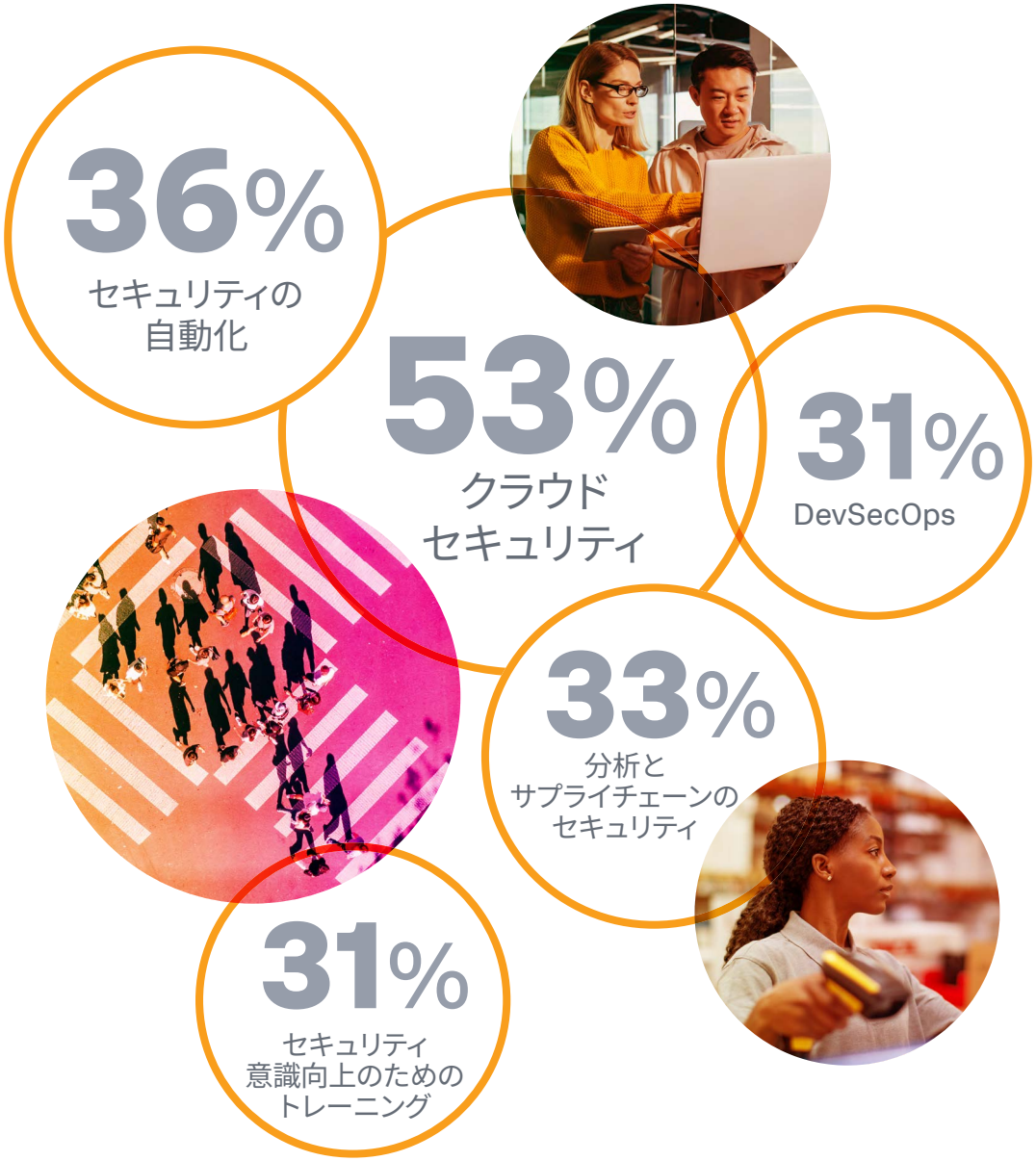
レジリエンスの確保とはチームスポーツのようなものです。多くの回答者は、セキュリティ運用と他の職務の統合(コラボレーションの強化、部門横断的なハイブリッドな役割の創設など)が今後重要になることを理解しています。

- **81%の組織が、セキュリティ運用とIT運用の業務の統合に取り組んでいます。**
- **69%の組織が、セキュリティ運用とデジタルエクスペリエンスの業務の統合に取り組んでいます。**
- **69%の組織が、セキュリティ運用とアプリケーション開発の業務の統合に取り組んでいます。**
- **61%の組織が、セキュリティ運用とオブザーバビリティの業務の統合に取り組んでいます。**

なぜでしょうか?それは、多くの回答者が、こうした統合は環境全体でリスクを可視化すること(58%)や、脅威の検出/対応プロセスでの連携を強化すること(55%)に役立つと考えているためです。

セキュリティについて重視する取り組み

特に優先する領域を3つ選択



予算の増額と優先事項の変化

セキュリティチームでは、コラボレーションの範囲が広がり、支出も増えています。調査では95%の回答者が今後2年間でセキュリティ予算が増額されると予測し、56%が大幅な増額を見込んでいます(前年の51%から増加)。

予算の使い道はツールとテクノロジーへの投資が大半ですが、そのアプローチは二分しており、50%が、あらかじめ統合機能を備えたプラットフォームベースのツールに注目し、残りの50%が、最適なソリューションを必要に応じてAPI経由で個々に統合するアプローチに関心を寄せています。

戦略の重点は昨年から変化し、今年のトップ4は以下のようになりました。

- **セキュリティ分析/運用ツールの総合的なソフトウェアアーキテクチャを開発および構築する(38%、前年は21%、3位タイから1位に上昇)**
- **セキュリティ運用プロセスの自動化とオーケストレーションを支援するセキュリティ運用ツールを導入する(35%、前年は22%)**
- **ツールとスタッフを組織レベルのSOCに統合する(35%、前年の15%から大幅増、トップ10圏外から急上昇)**
- **明文化されたセキュリティ運用プロセスを確立する(33%、前年の17%から増加、10位から上昇)**

これら上位4つの戦略は全体として、SOCの生産性、俊敏性、専門性の向上を目指しています。

95%の組織が今後2年間で
セキュリティ予算が増額される予定だと
回答し、56%が大幅な増額を見込んでいます。

分析と自動化

セキュリティ分析と運用の自動化およびオーケストレーションを支援するテクノロジーの導入状況は昨年とほぼ変わりません。今年は、これらのテクノロジーを導入している組織の割合が67%、幅広く導入している割合が37%で、それぞれ昨年の67%、36%と比べると実質的に同じと言えるでしょう。

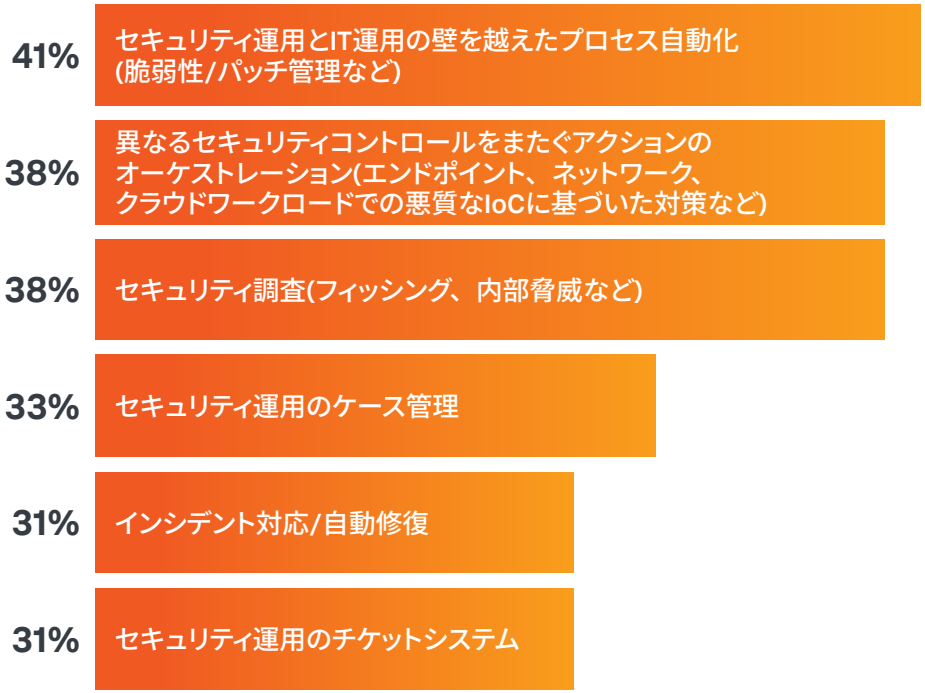
攻撃ライフサイクル全体を分析する目的としては、脅威検出の強化(37%)、サイバーリスクの特定のサポート(36%)、調査の迅速化(33%)、修復の自動化(35%)が多く挙げられました。

このほか、リアルタイムデータに基づくセキュリティプロセスの自動化(33%)と、調査の優先順位の判断材料(33%)も挙げられています。

タスクの自動化では以下の目標が上位に入りました。

- **IT運用システムへのセキュリティツールの統合(29%)**
- **外部の脅威インテリジェンスと内部のセキュリティデータの統合(27%)**
- **自動化とオーケストレーションによる基本的な修復タスク(エンドポイントセキュリティコントロールのアップデートなど)の自動化(27%)**

プロセス自動化で優先する目的



しかし、すべてが順調に進んでいるわけではありません。他の分析(IT運用、ビジネス、リスク管理など)を取り入れてセキュリティ分析を強化する取り組みは横ばい傾向です。これらのソースを高いレベルで統合していると回答した組織は、昨年は43%でしたが、今年は39%に減少しています(ほとんど統合していない組織は世界全体で35%)。高いレベルで統合している組織の割合は地域によって差が大きく、北米で45%だったのに対して、欧州は35%、アジア・パシフィック(以下APAC)は36%でした。

取り組みが後退した理由として最も有力なのは、データの複雑化と、異なるツールを統合することの難しさでしょう。

「分析を強化するには多くの複雑さを乗り越えなければなりません」とSURGeのリーダーを務めるRyan Kovarは指摘します。「パンデミックは多大な変化と膨大な数の新しいデータソースをもたらしました。このような分析の統合は、一度うまくいったとしても、新しいデータが追加されたらすべてを見直す必要があります」

そのため、ベンダー (弊社を含む)は、この複雑さをより少ない手間で解消して組織が問題を克服できるようにするための方法を常に模索しています。分析の統合を再び軌道に乗せるには、プロセスを最初からやり直すこと、つまり、統合の目標を定め、多くのセキュリティ分析ソリューション/ツールで提供される事前構築済みの検出機能を使ってデータを標準化し、チームとサイロの壁を越えてコラボレーションと信頼構築に取り組むことが必要です。

セキュリティ分析と他の分析データとの統合

IT運用、ビジネス、管理、その他の分析

セキュリティチームの地位向上

セキュリティチームは「面倒な存在」や「邪魔者」ではなく「重要パートナー」として受け入れられつつあることは前述のとおりです。その結果(またはその要因として)、すべてのレベルでコラボレーションが深まっています。

たとえば現場レベルでは、DevSecOpsが急速に広がっています。DevSecOpsのプラクティスを取り入れていない組織はわずか3%で、昨年の25%から大幅に減少しました。

リーダーレベルでは、91%のCISOがレジリエンス向上の取り組みで他のリーダーとコラボレーションをしていると回答しています。また、68%のCISOが取締役会と週1回(29%)または月1回(39%)ミーティングを行っており、四半期に1回以下と回答したのはわずか8%でした。こうしたミーティングの成果として多く挙げられたのは以下の点です。

- **ビジネス部門とのコラボレーション能力が向上した(46%)**
- **他部門のセキュリティ意識が高まった(44%)**
- **セキュリティ予算の優先順位が上がった(43%)**
- **セキュリティ予算が増額された(42%)**
- **サイバーセキュリティのイニシアチブが幅広い文化として浸透した(42%)**

全体として、コラボレーションの強化はセキュリティチームにとって、巧妙化する攻撃への有効な対抗手段になりつつあります。

63%の回答者が、DevSecOpsのメリットとして、運用効率の向上、クラウドセキュリティの強化、よりセキュアで信頼性の高いソフトウェアの開発、より強固でプロアクティブなセキュリティ態勢の確立をそれぞれ挙げています。

59%の回答者が、DevSecOpsを導入した結果、セキュリティインシデントが減ったと回答しています。

特に欧州の組織では、メリットがあったと回答した割合がすべての項目で世界平均を4 ～ 9ポイント上回りました。

推奨される取り組み

セキュリティチームが成功を収めるには、組織全体での連携が必要です。他の部門と連携し、パートナー関係を築いているセキュリティチームがレジリエンスの高い組織を構築するために実践している8つの取り組みをご紹介します。

組織のレジリエンスとは本質的に、脅威検出とインシデント対応を強化しようとするセキュリティチームの必死の努力だけでなく、包括的なコラボレーションによって成立します。実際、Splunkのお客様の多くは、ソフトウェア開発やインフラ監視から事業継続計画まであらゆる領域でセキュリティリーダーがIT部門やビジネス部門のリーダーと同じテーブルにつき、組織の保護対策について話し合うコラボレーション重視のアプローチを取り入れて、強力なレジリエンスを築いています。

今年の調査の結果を概観すると、信頼に基づくパートナーシップというテーマが浮かび上がります。こうしたパートナーシップを築いている組織がどのようにミッションを遂行しているかを分析することで、いくつかの推奨される取り組みが明らかになりました。最初の4つの取り組みは、部門横断的なパートナーシップの価値に直接関係するものです。

1.データと分析を活用して脅威検出と対応を最適化する

連携すべき重要な存在「イネーブラー」として認められているセキュリティチームの多くが分析を活用して、サイバーリスクの特定(38%、障害物と思われているチームでは26%)、脅威検出の強化(40%、同25%)、調査の迅速化(35%、同27%)、修復の自動化(38%、同22%)を実現しています。こうしたデータドリブンの姿勢で検出、調査、対応を効率化して、セキュリティ運用全体で成果をあげることは、組織全体でのセキュリティチームの地位向上にもつながります。

2.レジリエンス向上のための計画を立てる

セキュリティチームがビジネスイネーブラーとして認められている組織では、サイバーレジリエンスについて組織レベルで定められた正式なアプローチがあると回答した割合が32%と、セキュリティチームが障害物と思われている組織よりも高い数値でした。これは意味のある結果です。イネーブラーになるには、チーム内の努力だけではなく、組織レベルでレジリエンスの強化に取り組むことが必要であることを示しています。

3.レジリエンス向上に投資する

イネーブラーとして認められているセキュリティチームは、レジリエンス向上のために以下のソリューションへの投資計画を立てています。

- テクノロジー環境全体の可視化(48%、障害物と思われているチームでは38%)
- インシデントの対応と修復の迅速化(53%、同39%)
- 顧客/ユーザー向けサービスの復旧の迅速化(50%、同40%)
- 従来の事業継続/ディザスタリカバリー計画とサイバーレジリエンス向上の取り組みの融合(54%、同39%)

4.部門横断的なコラボレーションを促進する

イネーブラーとして認められているセキュリティチームは、直接関係する「すべて」の領域(IT運用、アプリケーション開発、オブザーバビリティ、デジタルエクスペリエンス)の担当部門とコラボレーションしていると回答した割合が32%で、障害物と思われているチーム(13%)の2.5倍にのぼりました。

セキュリティの観点では、レジリエンスは脅威ライフサイクルに対する包括的なアプローチとして注目されています。データ管理/分析ツールは異常の検出に役立ち、適切なプレイブックによる効果的な自動化は対応の迅速化に有効です。さらにセキュリティ運用に対する統合的なアプローチを確立することによって、ツールやデータのサイロ化の問題を解消できます(これこそまさにSplunkが常に目指していることです)。

推奨される取り組みとして次に紹介するのも、イネーブラーとして認められているセキュリティチームがよく実践している取り組みですが、必ずしも効果的なコラボレーションとは直接関係ありません。それでも、チーム間のパートナーシップを築いている組織がセキュリティ態勢の強化、レジリエンスの幅広い浸透、予算の増額のために実践しているベストプラクティスです。

5.基本対策を徹底する

イネーブラーとして認められているセキュリティチームは基本対策もしっかり行っています。連携しにくい、邪魔者と思われているチームでは、セキュリティインシデント防止の主な課題として、IT資産に対する基本的なセキュリティ対策ができていないことを挙げた割合が28%で、イネーブラーとして認められているチームの19%を大きく上回りました。これは興味深い結果でもあります。障害物と思われるのは基本に忠実すぎて融通が利かないからだと多くの人が考えるでしょう。しかし実際には、コラボレーションを推進するチームの方が基本対策を徹底しているのです。

6.クラウドのセキュリティを重視する

イネーブラーとして認められているセキュリティチームでは、クラウドワークロードの設定ミスや、CISなどのベストプラクティスのフレームワークとの不一致の特定を重視すると回答した割合が31%で、障害物と思われているチームの20%を大きく上回りました。クラウドワークロードを綿密にハードニングすることで組織のクラウドトランスフォーメーションプロジェクトの推進を後押しする姿勢が、高い評価を受ける一因と考えられます。「すぐに『No』と言うチームよりも『Yes』と言うチームの方が好かれるのは当然です」とSURGeのRyan Kovarは言います。

7.ランサムウェアリスク対策に投資する

イネーブラーとして認められているセキュリティチームでは、ランサムウェアリスクの緩和を明確な目的とした投資を増やしていると回答した割合がその他の組織を大きく上回りました。ランサムウェアの防御自体も大切ですが、こうしたチームは、この高度な脅威を防ぐための先手の対策に取り組んでいます。その点が、ビジネスリーダーに評価され、有効な関係を築ける理由の1つでしょう。具体的な投資対象は以下のとおりです。

- アノマリ検出のための高度な分析(35%、障害物と思われているチームでは18%)
- SOARソリューション(35%、同21%)
- EDR (エンドポイント検出/対応) (34%、同17%)
- 特権アカウントの監視(30%、同20%)

8.サプライチェーンの脅威に対してプロアクティブな対策を立てる

ランサムウェアと同様に、イネーブラーとして認められているセキュリティチームはサプライチェーンのリスクにも先手で取り組んでいます。この場合も、セキュリティやレジリエンスの向上だけでなく、信頼とパートナーシップを築いて組織内でのセキュリティチームの地位が向上するというメリットがあります。サプライチェーン攻撃では以下の対策が特に重視されています。

- CISOと経営陣/取締役会とのミーティング機会を増やす(26%、障害物と思われているチームでは15%)
- 脅威ハンティングやフォレンジック調査などのインシデント対応アクティビティを実践する(25%、同13%)
- 現在のセキュリティコントロールでサプライチェーン攻撃を防止/検出できるかどうかを評価する(30%、同15%)
- ログ調査を強化する(26%、同16%)

攻撃を完全に防ぐ対策、手順、特定の慣例がないことは誰もが知っています。しかし、セキュリティチームが他の部門と戦略的パートナーシップを築いている組織の戦略や戦術は、リスクを最小化しながら、レジリエンスを向上させて危機的状況を乗り切るための優れた方法です。

付録

前年(と前々年)との比較

世界平均の変化が大きかった項目

2022年はセキュリティ要件に対応するのが非常に困難な年でした。以前よりも対応が「やや」または「かなり」難しくなったと回答した割合は、2021年の49%から2022年には66%に跳ね上がり、2023年は53%に落ち着きました。

過去2年間のサイバーセキュリティ要件への対応の難易度：

	2021年	2022年	2023年
かなり難しくなった：	13%	28%	23%
やや難しくなった：	36%	38%	30%
変わらない：	20%	18%	13%
やや楽になった：	22%	10%	22%
かなり楽になった：	9%	7%	12%

セキュリティ要件への対応が難しくなったと答えた回答者がその原因として最も強く感じた変化は「脅威の状況の悪化」でした。この点を挙げた回答者は2021年が48%で、2022年と2023年には38%に減少しました(2021年に高くなっているのは、新型コロナウイルスの世界的な感染拡大からまだ1年も経たない時期に調査が行われたためだと思われます)。

過去2年間で受けた攻撃のタイプについても尋ねました。その結果、いずれのタイプでも2021年から2022年にかけて大幅に増え、2022年から2023年にかけては微増または横ばいの傾向が見られました。以下にその一部を挙げます。

- **データ漏えい：**39% (2021年)、49% (2022年)、52% (2023年)
- **ランサムウェア：**31% (2021年)、45% (2022年)、49% (2023年)
- **ビジネスメール詐欺:**42% (2021年)、51% (2022年)、51% (2023年)
- **インサイダー攻撃:**27% (2021年)、39% (2022年)、40% (2023年)

ダウンタイムも増加しています。セキュリティインシデントによるダウンタイムの発生頻度別の割合は2022年から2023年にかけて以下のように推移しています。

- **週1回以上：**21% (2022年)から24% (2023年)に増加
- **2 ～ 3週間に1回：**19% (2022年)から22% (2023年)に増加
- **1カ月に1回：**14% (2022年)から16% (2023年)に増加
- **2 ～ 3カ月に1回：**16% (2022年)から15% (2023年)に減少
- **数四半期に1回：**11% (2022年)から10% (2023年)に減少
- **1年に1回以下：**19% (2022年)から12% (2023年)に大幅に減少

MTTR (平均復旧時間)は2022年から改善しています。

- **数分以内：**10% (2022年)、17% (2023年)
- **数時間：**31% (2022年)、29% (2023年)
- **1日以内：**32% (2022年)、34% (2023年)
- **数日：**16% (2022年)、15% (2023年)
- **1週間以上：**10% (2022年)、6% (2023年)

戦略的優先事項も年とともに変化しています。以下4つの戦略は2023年に重要度が上がっています。

- **セキュリティ分析/運用ツールの総合的なソフトウェアアーキテクチャを積極的に開発および構築する：**38% (2022年 の21%、2021年の18%から増加)
- **ツールとスタッフを組織レベルのSOCに統合する：**35% (2022年の15%、2021年の14%から増加)
- **セキュリティ運用プロセスの自動化とオーケストレーションを支援するツールを導入する：**35% (2022年と2021年の22%から増加)
- **明文化されたセキュリティ運用プロセスを確立する：**33% (2022年の17%、2021年の15%から増加)

国別の特徴

セキュリティへの取り組みに関する国別の状況

オーストラリアおよびニュージーランド

オーストラリアおよびニュージーランド(ANZ)では、ランサムウェアはそれほど重大視されていません。今後1年間の最重要領域にランサムウェアを挙げた回答者はわずか19%で、APAC地域の他国の平均29%を大きく下回りました。その理由として、ANZ地域ではランサムウェア対策としてサイバー保険を利用する組織が多く、システムがロックされても被害は業務の中断程度で済む場合が多いことが考えられます。そのため、保険で対処できるランサムウェアよりも、ゼロトラストを重視する傾向があります。

ランサムウェア攻撃の被害に遭った組織の38%が、身代金を保険会社が支払うことが多いと回答しています(他国の平均は21%)。ANZ地域では、他の国と比べて身代金額が全体的に低く、保険料が比較的安いのかもしれません。ただし、その傾向が今後も続くという保証はありません。

その他の注目すべき結果は以下のとおりです。

- CISOがビジネス部門のリーダーとミーティングする頻度が低く、セキュリティ態勢について週1回話し合うと回答したCISOはわずか14%と、他国の平均30%の半分以下でした。
- DevSecOpsが非常に重要な領域だと回答した割合は平均をやや上回る一方で、その取り組みが成功していると回答した割合はあまり高くありません。DevSecOpsがインシデント削減につながったと回答した割合は49%にとどまり(他国の平均は60%)、コンプライアンス向上に役立ったと回答した割合も48%でした(同63%)。

カナダ

カナダでは、増加する脅威と厳しさを増すセキュリティ要件に不安を抱く組織が多く、過去2年間でセキュリティ要件に対応することがより困難になったと回答した割合が76%にのぼりました(他国の平均は51%)。

悲観的になるのも無理はないかもしれません。カナダでは、近年セキュリティインシデントが発生したと回答した割合が高く、システム侵害が62%、データ漏えいが65%で、いずれも他国の平均(どちらも51%)を上回っています。また、重要なワークロードのアップタイムと可用性の維持にも苦心しており、セキュリティインシデントによりビジネスクリティカルなアプリケーションで週1回以上ダウンタイムが発生していると回答した割合が33%と、米国の19%を大きく上回りました。

明るい面に目を向けると、MTTDとMTTRがいずれも平均を上回っています。

- MTTD：2週間以下と回答した割合が39% (米国では26%)
- MTTR：数分以内と回答した割合が24% (同14%)

つまり、カナダの組織はインシデントとダウンタイムの増加に苦しむ一方で、その対応は比較的迅速にできていると言えます。

さらに、DevSecOpsの導入によってセキュリティチームと開発チーム間のコラボレーションが促進されたと回答した割合が73%、コンプライアンスが向上したと回答した割合が71%で、いずれも米国のそれぞれ63%、59%を上回っています。

SOCの強化方法としてAIの能力を高く評価している点も特徴的で、不正行為の検出能力でAIテクノロジーは人間のアナリストを上回ると回答した割合が61%と、米国の40%を大きく上回りました。

フランス

フランスの組織はセキュリティ運用にかなり自信があるようです。セキュリティ要件への対応に困難を感じていると回答した割合はわずか14%で、欧州の他国の平均29%、世界の他国の平均24%を大幅に下回りました。考えられる理由は2つあります。

1. 適切なスキルを持つ人材の確保を課題に挙げた組織はわずか10%でした(欧州の他国の平均は23%、世界の他国の平均は26%)。
2. 誤検知/コンテキスト不明のアラートが大量に発生して処理が追いつかないと回答した組織はわずか12%でした(欧州の他国の平均は25%、世界の他国の平均は26%)。

不安を感じている組織が比較的少ない他の国と同様に(ドイツの項を参照)、インシデントも少ない傾向が見られます。

- 過去2年間でデータ漏えいの被害に遭った：29% (欧州の他国の平均は61%)
- コンプライアンス違反が発生した：23% (同54%)
- インサイダー攻撃が発生した：26% (同53%)
- アカウントの乗っ取りの被害に遭った：27% (同52%)

セキュリティインシデントによるビジネスクリティカルなアプリケーションのダウンタイムも少なく、週1回発生すると回答した割合が6%、年1回程度が22%で、欧州の他国の平均それぞれ40%、6%と大きな差が出ました。

レジリエンス強化の取り組みも比較的進んでいますが、気になる点もあります。今後1年間のレジリエンス投資でインシデント対応と修復の迅速化に重点を置くと回答した割合が61%で、欧州の他国の平均40%を上回った一方、データを既知の正常な状態に戻すことに重点を置くと回答した割合は31%で、欧州の他国の平均42%を下回りました。

その他の特徴として、ツールの複雑化が課題になっています。

- 全体的なセキュリティの課題として、連携しないポイント型のセキュリティツールが増えすぎて管理が難しくなっていると回答した割合が29%で、欧州の他国の平均19%を上回りました。
- クラウド固有の課題として、複数のサイバーセキュリティコントロールを使用することによるコストと複雑さの増加を挙げた割合が37%で、欧州の他国の平均24%をやはり上回りました。

どちらの結果も、フランスの組織はポイント型ツールの整理、統合を行う必要があることを示唆しています。もちろん、それによってセキュリティ運用の効率が下がることは避けなければなりません。

ドイツ

ドイツでは、過去2年間で脅威やセキュリティ要件への対応が困難になっていると回答した割合が38%にとどまり、欧州の他国の平均61%、世界の他国の平均54%の両方を大きく下回りました。

ドイツの組織が困難を感じていない理由は、レジリエンスの取り組みが進んでいるためと考えられます。サイバーレジリエンスについて組織レベルで定められた正式なアプローチがあると回答した割合は27%で、欧州の他国の平均18%を上回っています(世界平均とはほぼ同水準)。

インシデントの発生件数も比較的少なく、過去2年間にデータ漏えいの被害に遭った組織は40%にとどまり、欧州の他国の平均57%、世界の他国の平均53%と大きな差がありました。さらに、コンプライアンス違反(25%、欧州の他国の平均は52%)、インサイダー攻撃(32%、同50%)、ビジネスメール詐欺(36%、同63%)も少ない傾向にあります。

マイナス材料は、インシデント発生時の対応の遅さです。インシデント対応に関する分析では、攻撃者の侵入に気づくまでに約3カ月かかり、欧州の他国の平均である2カ月以内を大きく上回っています。MTTRにも同じような差が見られます。

ほかにも、適切なスキルを持つセキュリティ人材の獲得を課題に挙げた割合が33%で、欧州の他国の平均18%をかなり上回りました。また、AIに対して懐疑的で、アノマリ検出でAIは人間のアナリストを上回ると回答した割合は30%にとどまりました(欧州の他国の平均は53%)。セキュリティ運用の自動化とオーケストレーションも進んでおらず、広範囲で導入していると回答した割合が29%で、欧州の他国の平均40%を下回りました。人材不足とAIや自動化への投資不足はいずれ、セキュリティチームによる脅威やセキュリティ要件への対応が困難になるという形で影響が現れるかもしれません。

インド

調査結果を見ると、インドの組織もセキュリティ対応に手を焼いているようです。インドの組織は人材が豊富で、SOCにフルタイム勤務のメンバーが25人以上いると回答した割合が66%と、世界の他国の平均36%を大きく上回りました。一方で、セキュリティ要件への対応にはかなり苦戦しています。

- 攻撃件数が多すぎて対応が追いつかないと回答した割合は42%にのぼりました(世界の他国の平均は23%)。
- 大量の誤検知が負担になっていると回答した割合も44%と高い結果でした(同24%)。

問題の一因は、ツールのエコシステムの複雑さにあると考えられます。セキュリティスタックが複雑すぎると回答した割合は48%にのぼり、世界の他国の平均28%を大きく上回りました。

そのため、当然のことながら、過去2年間でデータ漏えいの被害に遭ったと回答した割合が59% (APAC地域の他国の平均は45%)、インシデントの影響でビジネス成果が大きく低下した(企業価値の低下など)と回答した割合が42% (同25%)と、いずれも高い結果になりました。

明るい材料は、CISOが課題解決のために立ち上がっていることです。セキュリティ態勢についてビジネス部門のリーダーと週1回話し合うと回答したCISOは33%にのぼりました(APAC地域の他国の平均は16%)。さらに、その取り組みの直接的な成果としてセキュリティ投資の優先順位が大幅に上がったと回答した割合も57%に達しています(同42%)。

もう1つの明るい材料は、セキュリティ運用と他の関連業務との統合が進んでいる点です。調査で挙げられた他のすべての領域(オブザーバビリティ、デジタルエクスペリエンス、IT運用、アプリケーション開発)とセキュリティ運用の業務を統合していると回答した割合が

42%にのぼり、APAC地域の他国の平均25%よりも高い数値となりました。この積極的な姿勢は、統合のメリットに大きな魅力を感じているためと考えられます。その目的として、74%がリスクの可視化(APAC地域の他国の平均は53%)、64%が問題の迅速な検出(同51%)、70%がセキュリティ運用と他の業務の統合による部門間コラボレーションの促進(同53%)を挙げています。

日本

日本では、ランサムウェア対策を重視する組織が多く、35%が今後1年間に重視する取り組みのトップ3に挙げています(APAC地域の他国の平均は23%)。その効果は出ているようで、過去2年間でランサムウェア攻撃の被害に遭ったと回答した割合は40%と、世界の他国の平均50%を下回りました。

その他の特徴としては以下の点が挙げられます。

- サイバーレジリエンスについて、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合は23%と低い結果でした(APAC地域の他国の平均は34%)。
- レジリエンスに関連するテクノロジーに投資する目的として可視性の向上を挙げた組織が37% (同46%)、ダウンストリームへのインシデントの影響の把握を挙げた組織が40% (同50%)と、いずれも低水準にとどまっています。

日本の組織はソフトウェアサプライチェーン攻撃に対する危機感が他国より低く、最近の世界的なインシデントを受けてCISOがビジネス部門のリーダーと話し合う機会が増えたと回答した割合が15% (APAC地域の他国の平均は29%)、ベンダーリスク管理のポリシーを見直したと回答した割合が16% (同26%)にとどまりました。

シンガポール

シンガポールでは、懸念事項が他の国とかなり異なる傾向が見られました。

まず、サプライチェーンについては、今後1年間に重視する領域としてソフトウェアサプライチェーンのセキュリティを挙げた割合が23%で、世界の他国の平均33%を下回りました。実際、最近の世界的なソフトウェアサプライチェーン攻撃後にその対策の優先順位が大幅に上がったと回答した割合が38%で、世界の他国の平均70%よりもかなり低い水準です。ソフトウェアサプライチェーンリスクの緩和策にもあまり積極的ではありません。

- サードパーティのサービスプロバイダーにリスク評価を依頼した：15% (世界の他国の平均は26%)
- ソフトウェアサプライチェーンに関するセキュリティポリシーを強化した：15% (同23%)
- 侵入テストやレッドチーム演習を行った：15% (同25%)

また、ランサムウェアについては、ランサムウェア対策となる主要なコントロールを導入した、またはそのための投資を増やしたと回答した割合が低調でした。

- EDR (エンドポイント検出/対応)：17% (世界の他国の平均は30%)
- ランサムウェア検出ルールを導入するためのソリューション：17% (同26%)
- アノマリ検出のための高度な分析：22% (同32%)

さらに、セキュリティ投資への意欲も低く、今後12 〜 24カ月間でセキュリティ投資を大幅に増やすと回答した組織は27%にとどまりました(世界の他国の平均は59%)。

現時点では、ランサムウェア攻撃やサプライチェーン攻撃の発生率は低いようですが、対策不足や投資不足は将来に向けてリスクになります。

英国

英国のセキュリティを取り巻く状況は厳しい様相を呈しています。データ漏えいの被害に遭った割合は68%で、欧州の他国の平均34%の2倍、規制違反が起きた割合は64%で、同24%の2倍以上という結果でした。さらに、これらのインシデントが企業価値の低下などの大きな被害につながったと回答した割合も37%で、欧州の他国の平均25%を大きく上回っています。

そのため、セキュリティ要件や脅威への対応に不安を抱くのは当然でしょう。過去2年間で対応がかなり困難になっていると回答した割合は35%で、欧州の他国の平均12%よりも高い数値を示しています。

その主な要因は2つ考えられます。1つは、誤検知/コンテキスト不明のアラートが大量に発生して処理が追いつかないと回答した割合が26% (欧州の他国の平均は15%)にのぼったこと、もう1つは、サイバーセキュリティ態勢の構築で規制要件への対応に手一杯でセキュリティのベストプラクティスの導入には手が回らないと回答した割合が30% (同20%)に達していることです。

レジリエンス向上の取り組みも進んでいません。正式なレジリエンス戦略をまだ策定していない組織の割合が25%で、世界の他国の平均の5倍でした。また、サイバーレジリエンスについて組織レベルで定められた正式なアプローチがあると回答した割合もわずか16%で、世界の他国の平均35%を大きく下回っています。

ただ、英国の組織は、やるべきことはわかっているようです。

- MTTDとMTTRの目標削減率は高く、それぞれ48%と67%でした(欧州の他国の平均はそれぞれ41%と48%)。
- レジリエンスの価値は理解しており、レジリエンスが向上しないことは、顧客を失うリスクにつながると強く思う割合が59%(同35%)、サービス停止や生産性低下に伴うイノベーションの遅れにつながると強く思う割合が57% (同28%)と高い結果になりました。
- 最近の世界的なソフトウェアサプライチェーン攻撃後にサードパーティによるリスク評価を大幅に強化した割合も79%で、欧州の他国の平均64%を上回っています。

米国

米国では、セキュリティ要件や増加する脅威への対応に不安を抱く組織が少ない傾向にあり、過去2年間で対応が困難になったと回答した割合は44%にとどまり、北米の他国の平均76%、世界の他国の平均56%をいずれも下回りました。負担を感じていない要因はいくつか考えられますが、重要な点を2つ挙げます。

1. 人材不足の課題はさほど深刻ではないようで、主な課題としてセキュリティチームの人員不足を挙げた組織は20%にとどまりました(北米の他国の平均は30%、世界の他国の平均は23%)。また、セキュリティチームの強化を目的としたマネージドサービスの利用率が高く、SOC業務の大半をパートナーに任せている組織が54%にのぼっています(同41%、56%)。
2. セキュリティ対策としてレジリエンスを非常に重視しており、サイバーレジリエンスについて、重要なすべてのシステムを対象に組織レベルで定められた正式なアプローチがあると回答した割合が45%に達しています(世界の他国の平均は25%)。

これらの強みから、米国の組織はセキュリティインシデントの被害が少なく、過去2年間に発生したインシデントは、データ漏えいが51% (北米の他国の平均は65%)、ビジネスメール詐欺が42% (同58%)、DDoS攻撃が39% (同53%)、システム侵害が46% (同62%)という結果でした。このため、ビジネスクリティカルなワークロードのダウンタイム発生頻度も低く、年間の平均発生回数は19件(同25件)でした。

今後1年間に戦略面で重視する領域では、DevSecOpsが37% (世界の他国の平均は28%)、セキュリティの自動化が41% (同35%)にのぼった一方、ランサムウェア対策を挙げた組織は19% (同30%)にとどまり、今後、ランサムウェア攻撃に遭う組織が増える可能性があります。

業界別の特徴

世界共通の4つの業界の特徴的なデータポイント

通信・メディア

通信・メディア業界では、調査結果のデータから2つの注目すべき傾向が読み取れます。

1. セキュリティツールの複雑さが大きな問題になっているようです。SOC業務に関する質問では、セキュリティツールや管理コンソールの数と種類が多すぎ、しかも互いにほとんど(またはまったく)連携していないため、包括的な調査や対応をタイムリーに行うことが難しいと回答した割合が47%で、他の全業界の平均37%を上回りました。

   以下の点がその要因と考えられます。

   - 既存のセキュリティツールでクラウド環境がサポートされていないと回答した割合が27%と、他の全業界の平均19%よりも高く、クラウド環境に対応したソリューションを個別に導入する必要があると感じていることがうかがえます。
   - IT運用とセキュリティ運用の業務を統合していると回答した割合が75%で、他の全業界の平均82%を下回っています。
   - 今後の重点領域としてプラットフォームベースのセキュリティツールの導入を挙げた割合が57%と、他の全業界の平均49%より高いことから、チームや環境の分断が複雑さを招いている可能性があります。

2. CISOがビジネス部門のリーダーと話し合う頻度が低く、全体的なセキュリティ態勢や重要指標についてCISOがビジネス部門のリーダーと週1回話し合うと回答した割合が17%にとどまりました(他の全業界の平均は30%)。

   CISOがビジネス部門のリーダーと頻繁に話し合う主なメリットの1つは、セキュリティ予算の増額を期待できることです。話し合いの頻度が低いことを考えると、今後24カ月間でセキュリティ予算が大幅に増えると回答した割合が45%にとどまったのも無理はないでしょう(他の全業界の平均は57%)。

金融サービス

金融サービス業界では、他の業界と比べて特徴的な点が3つありました。

1. ランサムウェアに関するリスクの緩和策が効果をあげています。ランサムウェア攻撃によってデータやシステムにアクセスできなくなったと回答した割合が32%と、他の全業界の平均45%と比べ低い数値となりました。一方で、ランサムウェアの検出、防止、対応の支援を目的とした以下の4つの領域への投資や追加投資を行っている割合は高くなりました。
   - メールセキュリティの強化：41% (他の全業界の平均は31%)
   - 具体的なランサムウェア検出ルールの作成/導入：32% (同24%)
   - アノマリ検出のための高度な分析ソリューションの導入：36% (同30%)
   - SIEM (セキュリティ情報/イベント管理)ソリューションの導入：39% (同32%)

2. サプライチェーン攻撃の防止策も効果をあげています。サプライチェーン攻撃の被害に遭ったと回答した割合が40%と、他の全業界の平均48%よりも低い数値でした。さらに、以下の対策も積極的に行っています。
   - ベンダーリスク管理ポリシーの再評価/変更：27% (他の全業界の平均は21%)
   - サプライチェーン攻撃を防御または検出できるかどうかに関する現行のセキュリティコントロールの評価：31% (同25%)
   - ソフトウェアサプライチェーンベンダーに対するアンケートや監査の強化：30% (同22%)

3. DevSecOps導入の取り組みには遅れが見られます。DevSecOpsの導入によって以下のメリットを実現したと回答した割合が全体的に低くなりました。
   - ソフトウェア開発プロジェクトの再現性の向上：56% (他の全業界の平均は63%)
   - プロアクティブなサイバーセキュリティ対策の実現：57% (同65%)
   - サイバーセキュリティチーム、開発チーム、運用チーム間のコラボレーションの促進：67% (同59%)
   - 監査への対応力の向上：55% (同62%)
   - クラウドに保存する機密データの保護：65% (同55%)

金融サービス企業はこの弱点を認識しているようで、今後1年間の重点領域としてDevSecOpsを挙げた割合が40%と、他の全業界の平均28%を大きく上回りました。

製造

製造業では、人材とスキル不足の問題が深刻化しています。たとえば、人材不足のため、増え続けるセキュリティイベントに対応できないと回答した割合は56%で、他の全業界の平均47%を上回っています。また、業務を円滑に進めるために、適切なスキルセットを備えた人材を十分に確保できていないと回答した割合も31%で、他の全業界の平均22%と比べ高い結果となりました。

そのため、過去12カ月間に人材不足に関連するさまざまな問題が起きています。

- 現在の仕事の負担が増えたため別の職務への異動を検討している：51% (他の全業界の平均は39%)
- チームメンバーが経験不足のままプロジェクトを率いることを求められる：60% (同40%)
- プロジェクトが失敗した：52% (同36%)

SOCが24時間365日の対応を実現している割合が17%にとどまり、他の全業界の平均27%を下回りました。逆に、営業時間内のみ対応している割合は30%で、他の全業界の平均13%を大きく上回っています。

スキル不足の解消策として自動化とAIに期待する組織が多いのも特徴で、セキュリティ分析のために機械学習テクノロジーを広範囲に活用していると回答した割合が43% (他の全業界の平均は32%)、セキュリティと運用の自動化およびオーケストレーションを支援するテクノロジーを広範囲に導入していると回答した割合が44% (同35%)にのぼりました。ただし、セキュリティインシデントによるビジネスクリティカルなシステムの停止が週1回発生すると回答した割合が44%で、他の全業界の平均19%を大幅に上回っていることから、これらの緩和策では人材不足を十分に補えていないと言えるでしょう。

行政・公共機関

行政・公共機関に共通する課題は、リスク対応が追いつかないことです。サイバーセキュリティ要件(コントロールの導入と調整、ネットワークアクティビティの監視、脅威インテリジェンスの追跡など)への対応が2年前と比べて難しくなったと回答した割合が3分の2以上(68%)にのぼり、他の全業界の平均52%を大きく上回りました。

特に大量のアラートが問題と思われ、最大のセキュリティ課題としてセキュリティアラートへの対応を挙げた割合が34%と、他の全業界の平均23%よりも高くなっています。

要因として考えられるのは、ツールの複雑化と人材不足の2つです。行政・公共機関では民間組織よりもこれらの問題が深刻で、両方を課題に挙げた組織が37%と、他の全業界の平均26%を上回りました。

また、セキュリティチームの負担軽減策としてのAI導入には一貫して懐疑的です。以下の領域でAIの能力が人間のアナリストを上回ると考える行政・公共機関は少ないようです。

- 脅威ハンティング：24% (他の全業界の平均は46%)
- イベントのトリアージと優先順位付け：43% (同28%)
- ユーザーの異常な行動の検出：30% (同47%)

インテリジェントな自動化はリスク対応の改善に効果的で、最終的に復旧時間の短縮につながります。行政・公共機関のMTTRは22.3時間と、他の全業界の平均15.1時間と比べて開きがあります。この点を踏まえて、自動化の導入を積極的に検討すべきでしょう。

Splunkのセキュリティとオブザーバビリティの統合プラットフォームで、組織のレジリエンスを向上させましょう。大規模な環境でもすばやく包括的に可視化して効果的なアクションにつなげることができます。あらゆるデジタルリスクに動じない安定した組織運用を支援するSplunkのソリューションをぜひご確認ください。

詳細はこちら

23-119356-Splunk-State of Security-EB-JA-202303

splunk>