2024年

セキュリティの現状

競争が激化するAIの活用

splunk>

私はセキュリティの専門家およびリーダーとしての20年以上にわたるキャリアの中で、この業界の進化を何度も目の当たりにしてきました。しかし今回はこれまでとは違います。生成AIの普及によって、サイバーセキュリティは可能性と危険に満ちた新境地に突入しています。Splunkの『2024年セキュリティの現状』の調査では、多くのCISOと現場担当者がひたすら前だけを見てその道を切り開いていることが明らかになりました。新しいコンプライアンス規制においてCISOの説明責任が拡大されるなど、この先に何が待ち受けているかは誰にもわかりません。

セキュリティチームには、今日のサイバー環境でレジリエンスを強化するために生成AIをどのように活用できるか模索することが期待されています。調査では93%の回答者が生成AIをすでに導入していると回答し、生成AIがイノベーションを新たなレベルに引き上げるという認識がすでに広がっています。その用途としては、サイバー攻撃に対する防御の強化、より多くの情報に基づく意思決定、深刻なスキル不足の解消など、多岐にわたります。一方で、約3分の1が、生成AIに関するポリシーが未整備だと回答しています。また、最も懸念する脅威として、AIを悪用した攻撃が1位になっています。

コンプライアンス関連では、米国証券取引委員会(SEC)とEUのNIS2の罰則付きのインシデント報告規則が強化され、CISOの説明責任が拡大しています。このことは、見方を変えれば、セキュリティチームに自らの役割と立場を再構築するきっかけを与えてくれます。CISOにとっては、役員会議での発言力を増すチャンスであり、現場担当者にとっては、IT運用チーム、エンジニアリングチーム、クラウド管理チームとのコラボレーションを強化して、可視性の向上、対応時間の短縮、レジリエンスの強化につなげるチャンスです。

セキュリティチームがこの新しい道を開拓し続ける中で、Splunkは、防御力としての生成AIの潜在能力に大いに期待するとともに、セキュリティの優先事項がビジネスの優先事項だという認識が急速に広まっている状況に勇気づけられています。

Jason Lee

Splunk最高情報セキュリティ責任者(CISO)

押し寄せるイノベーションの波

2024年のセキュリティの状況にはちょっとした矛盾があります。セキュリティチームの前に幾多の困難(コンプライアンス要件の強化、国際情勢の緊迫化、脅威の高度化など)が立ちはだかる一方で、業界全体では進歩を遂げています。

調査では、サイバーセキュリティへの対応が以前よりも楽になったと回答した組織も増えています。コラボレーションの強化や脅威検出の迅速化が順調に進んでいるほか、多くの組織が、現在直面している問題を解決するために必要な権限とリソースを確保していることがその理由でしょう。

しかし、完全な勝利ははるか先です。セキュリティチームはまだ、生成AIの活用競争で敵を追い越そうとしている段階です。長年悩まされてきた巧妙な攻撃に生成AIが加わったらどれだけ深刻な事態になるか、心配の種は尽きません。

それでも、セキュリティチームはこの状況に対応できるとSplunkは考えています。生成AIがサイバーセキュリティにもたらす影響の全体像は不透明ですが、ひとつ確かなのは、競争はすでに始まっているということです。

目次

サイバーセキュリティ対策の負担は軽くなっている

セキュリティチームが成功の味を知ることはめったにありません。常に「この対策はうまくいっているのか」と自問するばかりです。調査では、サイバーセキュリティ要件への対応に関して感じている難易度がほぼ半々に割れ、41%が以前よりも楽になったと回答する一方で、46%が難しくなったと回答しました。

しかし、全体的には状況は改善しています。2022年のSplunkのセキュリティ調査レポート以降、サイバーセキュリティ対策の負担は軽減傾向にあります。

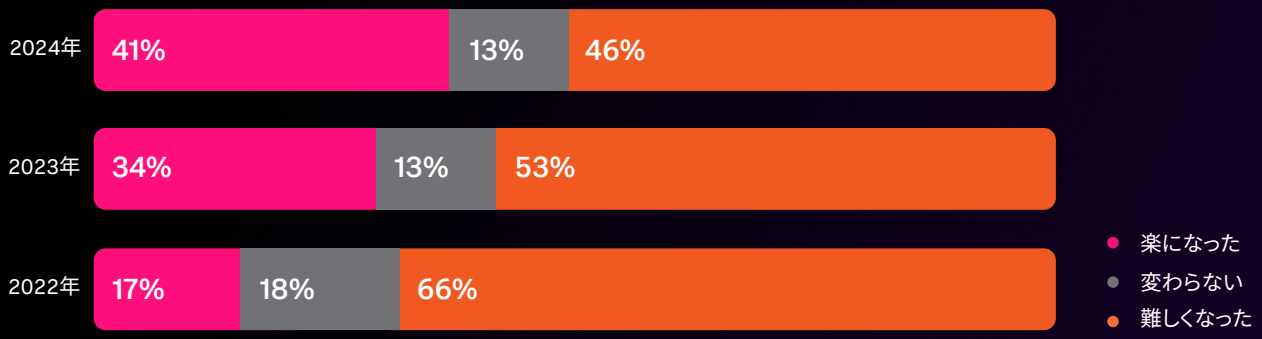
環境が複雑化し、攻撃が巧妙化していることを考えると、このことは意外に思えるかもしれません。組織の負担が軽くなった理由としては、セキュリティコントロールやプロセスが成熟し、実証済みの攻撃戦略に依存する攻撃者に先手を打てるようになったことが考えられます。

コラボレーションの強化も負担軽減の要因のひとつでしょう。調査では87%が、1年前よりも他のチームと緊密に連携するようになったと回答しています。また、4分の3 (75%)が、今年はIT運用チームとのコラボレーションを強化することを計画しています。

さらに、54%がソフトウェアエンジニアリングチームとのコラボレーションを強化することを計画しています。設計やコーディングといった開発初期の段階からセキュリティ対策を講じれば、脆弱性により効果的に対処できます。

脅威を検出するまでの時間も短くなっています。調査では、障害につながるインシデントのMTTD (平均検出時間)が概算で14日以内と回答した割合が55%にのぼりました。昨年の調査で同様に回答した割合が28%であったことを考えると、大きな改善です。ただし、攻撃者にとって14日間は、システムへの不正アクセスを成功させるのに十分な時間です。

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



それでも戦いは続く

サイバーセキュリティ要件への対応が難しくなっていると感じている回答者のうち38%が、その理由として脅威の巧妙化を挙げています。そこに、国家間の緊張やサイバー戦争の脅威の高まり、IoT、AI、マルチクラウド環境の普及によるデータの急増が追い打ちをかけています。この状況で、まだ基本的なサイバーセキュリティ対策に取り組んでいる段階の組織は、今後、新たな資産やエンドポイントのセキュリティ対策に苦労することになるでしょう。また、主な脅威ベクトルとして今年1位になった設定ミスなどの単純な人的ミスに対応する負荷も高くなりそうです。

コンプライアンス要件の厳格化も大きな壁です。特に、組織全体の違反に対して個人的に責任を負うことになるセキュリティ部門の幹部にとっては重大問題です。調査では、28%が規制コンプライアンスへの対応によって仕事の負担が増していると回答しています。それでも各国の政府は今後も義務化の圧力を強めていくでしょう。

緊急事態への対応に苦慮し、サーバーセキュリティの改善に多くの時間を取られていると回答した割合は27%で、例年から横ばいの状態が続いています。この結果は、長期的な戦略と投資が不十分であることを示唆しています。セキュリティアラートの量が多すぎて対応が追い付かない状況も相変わらずで、26%が大量のアラートを問題点として挙げています。

AIがクラウドを超える

今年の調査で特に注目すべき結果のひとつが、AIに対する大きな期待が現実のものになりつつあることです。回答者の半数近く(44%)が、2024年に重視する3つの取り組みのひとつとしてAIを挙げ、クラウドセキュリティを上回りました。

ただし、AIに多くのメリットを期待しているのはセキュリティチームだけではありません。法や規則に縛られない攻撃者たちもまた、大きな期待を寄せています。AIが攻撃側と防御側のどちらにより多くのメリットをもたらすかという質問については意見がほぼ半分に割れ、45%が攻撃側、43%が防御側により多くのメリットをもたらすと回答しました。

生成AIの急速な普及を受けて、人々は、**何ができるのか**について想像を膨らませると同時に、**何が起きるのか**という不安を抱いています。SOCでは何が起きるでしょうか。組織は安全で効果的な利用を促進するためのポリシーを導入するでしょうか。イノベーションを妨げることなくそのポリシーに対応するにはどうすればよいでしょうか。その答えが今、明らかになりつつあります。

2024年にセキュリティについて重視する取り組み

AIゴールドラッシュへの突入

かつてカリフォルニアのゴールドラッシュでは、何十万人もの人々が一攫千金を夢見て西部に移住しました。今日の生成AIブームでも、無限の可能性が感じられる未開の地に、チャンスを求める多くの人々が危険を顧みず猛烈なスピードで飛び込んでいます。誰もが豊かな鉱脈を掘り当てて、先行者利益を獲得することを夢見ています。しかもその夢は、少し掘るだけで実現可能なのです。

生成AIの将来性と可能性

AIの中でも生成AIはすっかり主流となり、組織はビジネスを変革するためにAIを積極的に導入しています。eコマースでの顧客へのレコメンドのパーソナライズから、人間の脳のマッピング、レンブラントの筆使いの模倣まで、生成AIはほぼすべての業界で幅広く活用されています。

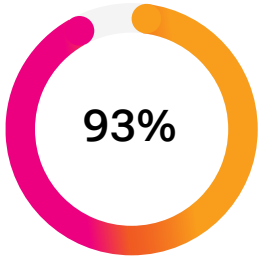
この流れは調査結果にも表れています。事業部門のエンドユーザーが公共の生成AIツールを業務に利用していると回答した割合は93%にのぼりました。ただし、この状況は、データの漏えいなど、生成AIに関連する脆弱性からビジネスを保護するセキュリティチームの負担が増えることを意味します。

それでも、生成AIに対する楽観的な考え方は、懐疑的であったセキュリティ関係者の間でも広まっています。セキュリティチームでの導入率は事業部門と大差なく、回答者の91%が公共の生成AIツールを利用していると回答しました。さらに、生成AIへの期待も大きく、46%が、生成AIはセキュリティチームにとって「ゲームチェンジャー」になると考えています。

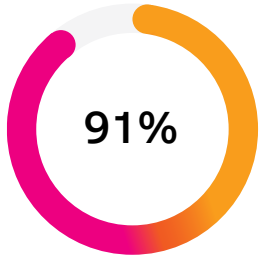
生成AIの活用競争は熾烈で、50%の回答者が、組織でサイバーセキュリティ対策として生成AIを利用するための正式な計画を策定中であるが、まだ完成していないか合意に至っていないと回答しています。

セキュリティとイノベーションは、適切に運用すれば両立可能です。ただし、経営幹部や取締役会からの圧力、または単に取り残されたくないというお馴染みの恐怖心がセキュリティチームでの生成AI導入の動機になっている場合は注意が必要です。

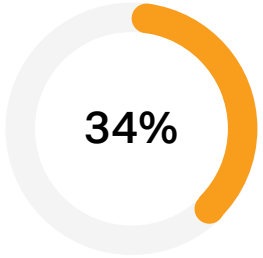
生成AIの導入に後れを取るポリシー策定



組織全体での導入率



セキュリティチーム内での導入率



生成AIに関する正式なポリシーが**未設定**

ほんの2年前には、公開されている生成AIツールを使用しているユーザーの人数を尋ねること自体が非常識と言える状況だったのに、今日では業務に生成AIを使用していないことの方が非常識になっています

— Splunk EMEA担当フィールドCTO兼戦略アドバイザー、Kirsty Paine

生成AIのポリシーは未知の領域

「すばやく行動し、破壊せよ」というモットーは、セキュリティの常識には反するかもしれませんが、スピーディーなイノベーションを求めるうえでは正しいかもしれません。セキュリティチームがポリシー作成を断ることはまずありませんが、生成AIの導入率がこれだけ高いにもかかわらず、34%の組織が生成AIの利用ポリシーを策定していません。

「生成AIの利用を厳しく制限しすぎると、競争に取り残されるだけでなく、生成AIを悪用する攻撃者の後手に回るリスクがあります」と、Splunk SURGeのプリンシパルセキュリティストラテジストであるShannon Davisは言います。

クラウドやIoTの導入から学んだのは、適切なプロセスと計画が欠如していると、最終的に痛い目を見るのはセキュリティチームであるということです。無計画にトレンドを追いかける姿勢は、これまで、従業員個人による勝手なクラウド契約や、セキュリティ対策が不十分なIoTデバイスの導入によるソフトウェア脆弱性の蔓延など、望ましくない結果を生んできました。セキュリティチームは、イノベーションのスピードを維持しつつ、慎重で持続可能なプロセスを確立する必要があります。

堅実なポリシーを作成するには、対象のテクノロジーがもたらす影響を理解する必要がありますが、65%の回答者が、生成AIに関する教育が不足していることを認めています。そもそも、生成AIの使い方に関する啓蒙活動をセキュリティチームだけで担うのには無理があります。

「AIの開発と利用を統制する部門横断的なガバナンスチームを設置して、責任あるAIの利用のための包括的なフレームワークを定めることが重要です」と、SplunkのAI担当VPであるHao Yangはアドバイスします。

生成AIの影響は広範囲に及ぶため、その統制には幅広い視点と専門知識が求められます。たとえばSplunkのAI委員会には、プロダクト/テクノロジー、法務、プライバシー、セキュリティ、人事、GTO (Go-To-Market)、マーケティングなど、さまざまな部門からメンバーが参加しています。

もちろん、堅実なセキュリティポリシーを定めたからといって必ずしも脅威を防げるわけではありません。それでも、データ漏えいなどの新たな脆弱性が入り込むリスクを最小限に抑えるためには非常に効果的です。

生成AIに法の手が伸びる

社内へのガバナンスと同様に、生成AIという新境地は比較的野放しの状態で、強制力のある法の力は及んでいません。しかしそれも今のうちです。AIに対するコンプライアンス規制の制定は着実に進んでいます。

たとえばEUのAI規制法では、リスクの度合いに応じた共通の規制フレームワークが導入される予定です。2023年、欧州議会は、初期の法案を修正して生成AIの規制を盛り込み、一定の透明性を確保することを義務付けました。その要件には、データベースへの基盤モデルの登録、技術文書の作成と保持などが含まれます。

米国では、バイデン政権が発表したAI権利章典において、ユーザーが自動化システムとやり取りする際は必ずその旨を通知し、ユーザーがそれを拒否した場合は人間とやり取りする代替手段を用意することが推奨されています。これらのガイドラインは、今後の行政措置に反映される可能性があります。

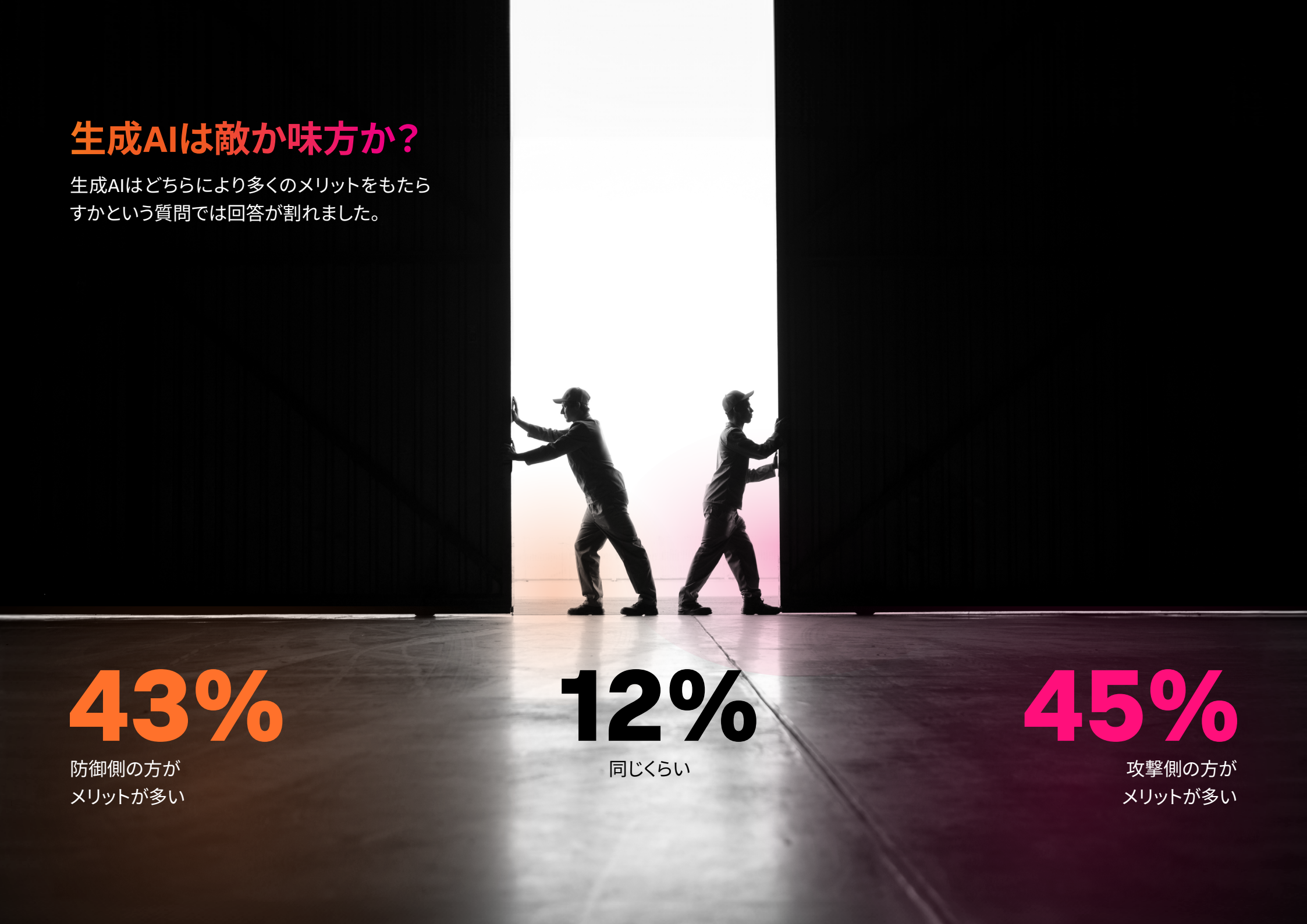
政府によるこうした規制が近い将来に続々と制定されることを意識しているのか、調査では45%の回答者が、優先して取り組むべき改善領域としてコンプライアンス要件への対応を挙げ、データ漏えい対策に次いで2位に入りました。この動きに先手を打つには、内部のコンプライアンス統制に改めて重点を置く必要があります。

AIの開発と利用を統制する部門横断的なガバナンスチームを設置して、責任あるAIの利用のための包括的なフレームワークを定めることが重要です

— Splunk AI担当バイスプレジデント、Hao Yang

生成AIは敵か味方か？

生成AIはどちらにより多くのメリットをもたらすかという質問では回答が割れました。



43%

防御側の方がメリットが多い

12%

同じくらい

45%

攻撃側の方がメリットが多い

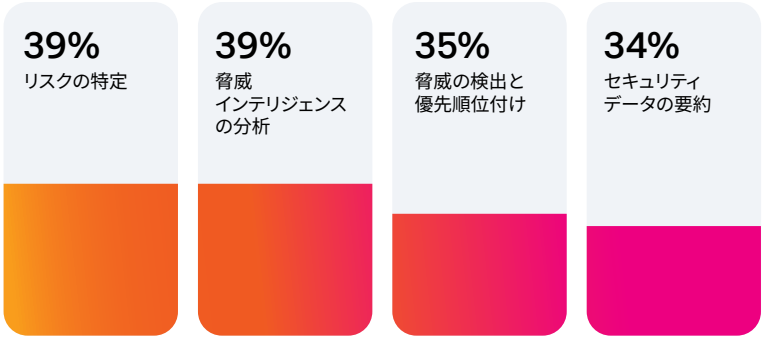
セキュリティチームの相棒としての生成AI

生成AIに対する見方は急激に好転しています。生成AIが防御側にメリットをもたらすと考える回答者の割合は、Splunkが『CISOレポート』のために行った8カ月前の調査では17%にとどまったのに対して、現在では約半数の43%に増加しています。

製品に生成AIを組み込むベンダーが増え、セキュリティワークフローでの有用性が実証されるにつれて、セキュリティチームは生成AIの可能性を見い出し始めています。生成AIを悪用した新たな攻撃やAIの学習データ汚染のリスクはあるものの、これらの脅威はまだ蔓延というレベルには至っていません。

セキュリティ関係者の間では楽観論が広がっているようで、脅威インテリジェンスの分析やリスクの特定をはじめとして、いくつかのサイバーセキュリティユースケースに生成AIが役立つと評価しています。

生成AIが役立つサイバーセキュリティのユースケース



生成AIの実際の活用例

リスクの特定
生成AIによって、異なるデータセットをすばやく集約し、アラートに豊富なコンテキストを付加することで、リスクベースのアラートを強化できます。大規模言語モデル(LLM)の利用により、人間の能力をはるかに超えるスピードと効率でコンテキスト情報を収集できます。

脅威インテリジェンスの分析
LLMを利用することで、脅威インテリジェンスレポートで報告されている侵害の兆候(IoC)やMITRE ATT&CK技法をすばやく特定できます。これによって単調なインテリジェンス調査に費やす時間を節約し、詳細な分析にすばやく取り掛かることができます。

脅威の検出と優先順位付け
アラートの優先順位付けとトリアージは、アナリストの誤判断、疲労、ミスの影響を特に受けやすい作業です。生成AIを利用すれば、複数の脅威を同時に処理しながら高い精度で分類できます。

セキュリティデータの要約
生成AIを利用すれば、セキュリティデータをすばやく入念かつ正確に要約できます。これによってセキュリティチームは、バイデン政権が発行した国家のサイバーセキュリティ強化に関する大統領令をはじめ、最新の情報や動向を確認する時間を確保できます。

サイバーセキュリティのスキル不足を解消

どのSOCでも、高いスキルを持つ熟練の担当者は欠かせません。しかし今日では多くの組織が人材不足に悩んでいます。生成AIは、この喫緊の課題を軽減する救世主になるかもしれません。

調査では、86%の組織が生成AIでスキルを補うことを想定して初心者レベルのサイバーセキュリティ人材の採用を増やせると回答し、58%が初心者レベルの人材のオンボーディングにかかる時間を短縮できると考えています。さらに90%が、初心者レベルの人材が入社した後、SOCでのスキルアップに生成AIが役立つと回答しており、これにはPythonスクリプトの作成やテスト環境の準備などの基本的な作業が含まれます。

ベテランのセキュリティ担当者にとっても、生成AIは能力の強化に役立ちます。65%の回答者が、生成AIを利用することによって生産性が向上し、ベテランの担当者がより容易に最新情報を収集して、調査や検出などのエンジニアリングをすばやく行えるようになると期待しています。

一方でAIが人間の仕事を奪うという懸念がまったくないわけではなく、実際、約半数(49%)の回答者が、生成AIの導入によって一部のセキュリティ職がいずれなくなると考えています。しかしそれ以上に、新入社員のトレーニングや既存の従業員の負担軽減に役立つと期待されています。そもそも、生成AIを導入すると、プロンプトエンジニアリングなどの新しい職務が加わるため、サイバーセキュリティ人材の役割が変わるだけだと考えることもできます。

生成AIによるスキル不足の解消

86% 初心者レベルの人材の採用を増やせる

65% ベテランのセキュリティ担当者の生産性を向上させることができる

攻撃者を助ける生成AI

一方で当然のことながら、セキュリティチームは生成AIが攻撃者の武器として使われることを危惧しています。調査では45%の回答者が、生成AIはサイバー攻撃者により多くのメリットをもたらすと考えており、77%が懸念すべきレベルまで攻撃対象が拡大することを案じています。

テクノロジーが変わっても攻撃は変わらない

生成AIはどのような脅威を世界にまき散らすのでしょうか。可能性としては、未知の脅威が不意に襲ってくるよりも、セキュリティチームがすでに直面している脅威を生成AIが増幅させる方が高いでしょう。

調査では32%の回答者が、これまで以上に見破りにくいフィッシングメールの作成や悪質なスクリプトの巧妙化など、生成AIによる既存の攻撃の最適化を警戒しています。スキルの低い場当たり的な攻撃者が生成AIを悪用して、より巧妙なソーシャルエンジニアリング攻撃を仕掛けるようにもなるでしょう。また、28%の回答者が、生成AIによって既存の攻撃の量が増えることを懸念しています。

敵は内部にも

AIの脅威は常に外部からやって来るとは限りません。77%の回答者が、生成AIの利用拡大に伴ってデータ漏えいのリスクが高まると憂慮しています。一方で、データ漏えい対策を最優先事項としている組織は49%にとどまりました。その理由として、生成AIツールとの間でやり取りされるデータの流れを制御できるソリューションがまだあまり存在しないことが考えられます。

さらに、生成AIに関する教育不足がこうした懸念を増長させています。セキュリティ部門の幹部の65%が生成AIを十分に理解していないと認めていることを考えれば、セキュリティ以外のチームで混乱が生じるのは必然と言えるでしょう。適切な教育を受けていないエンドユーザーは、組織の機密データをLLMに渡してしまうなどのミスを犯しやすくなり、最終的にセキュリティチームが苦境に立たされることになります。

想定される生成AIの悪用方法

それはまるで『馬ぐらい大きい1羽のアヒルと戦うのと、アヒルくらいの大きさの100頭の馬と戦うのと、どっちがいい?』と聞くようなものです。ひとつの大きな脅威と戦う方が対処しやすいかもしれませんが、生成AIは既存の攻撃の戦力を増やすという、むしろ避けたい方のシナリオを実現するでしょう

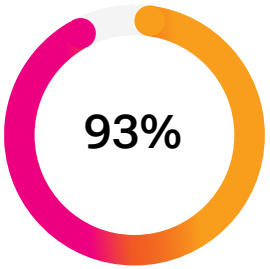
— Splunk EMEA担当フィールドCTO兼戦略アドバイザー、Kirsty Paine

生成AIの今後の展望

生成AIはこの先どこに向かうのでしょうか。誰も正確に予測することはできませんが、セキュリティチームはすでに機械学習という形でAIを利用しており、調査では93%が、その経験が生成AIの今後のアプローチに影響を与えると回答しています。

多くの組織が機械学習ツールの導入によって生産性が向上したと実感しており、92%がすでに大きな効果が出ていると評価しています。ただし、このテクノロジーは完璧ではないため特別なメンテナンスが必要です。調査では73%が従来のAIと機械学習機能で誤検知を経験し、91%がチューニングが必要だと回答しています。同様に、生成AIでもその価値を損なうハルシネーション(幻覚)を検出、防止するための対策が必要です。

従来のAIと機械学習ですでに堅固な基盤を築いている先進的な組織ほど、生成AIの価値を早期に引き出せる可能性が高いでしょう。



機械学習の利用経験が生成AIの今後のアプローチに影響を与えると考えている回答者の割合

先進的な組織の特徴

脅威に先手を打つことが急務となる中、一部の組織は、センターオブエクセレンス(CoE)モデルを取り入れて、成熟度の高いサイバーセキュリティ運用を確立しています。2024年には47%の回答者が、自社のセキュリティプログラムを「非常に先進的」と評価しています。このセクションでは、このグループを「取り組みが先進的な組織」と呼び、自社のセキュリティプログラムを「取り組みがまだ途上」と評価したグループと特徴や調査結果を比較します。

第一に、先進的な組織は、脅威への対応能力に自信を持っています。サイバーセキュリティ要件への対応が楽になったと回答した割合は、取り組み途上の組織で29%にとどまったのに対して、先進的な組織では49%にのぼりました。先進的な組織は他のいくつかの能力でも取り組みが途上の組織を上回り、究極のプラクティスと言える体制を確立しています。

適切なリソースと権限を確保している

組織の先進性は、最初からあるものではなく、作り上げるものです。成功の秘訣は、取締役会や事業部門のステークホルダーとの緊密な連携、部門横断的なコラボレーション、着実な投資にあります。先進的な組織では、先を見据えてセキュリティチームに予算を割り当てています。調査では、今後1 ～ 2年でサイバーセキュリティ予算が大幅に増額されると回答した割合が、取り組みが途上の組織で28%にとどまったのに対して、先進的な組織では67%にのぼりました。

ビジネスとの密接なつながりも先進的な組織の強みで、実に95%が、課題に対処するために必要なリソースと権限を確保していると回答しています。この点は、Splunkの『CISOレポート』で明らかになった、47%のCISOが現在CEOの直属になっているという結果とつながります。

コラボレーションが進みレジリエンスに対する意識が高い

ビジネスとのつながりを強化するには、CEOに声を届けるだけでなく、他のさまざまな部門と連携することが重要です。先進的な組織は、以下の技術部門と積極的にコラボレーションしています。

コラボレーションする相手	取り組みが先進的な組織	取り組みが途上の組織
ソフトウェアエンジニアリング	56%	46%
エンジニアリング運用	51%	31%
IT運用	76%	67%

コラボレーションはコンプライアンスにも及びます。セキュリティチームの全員がコンプライアンス対応を業務に組み込むべきだと思うかという質問に対して「非常にそう思う」と回答した割合が先進的な組織では49%にのぼり、セキュリティプログラムへの取り組みが途上の組織の27%を大きく上回りました。

先進的な組織はデジタルレジリエンスの重要性もよく理解しています。取り組みが先進的な組織では多くの回答者が、デジタルレジリエンスの強化がイノベーションの促進(41%)、ビジネス中断の防止(39%)、コンプライアンス違反の回避(39%)につながると考えています。このことから、セキュリティ業務をビジネス成果と深く関連付けていることが伺えます。

> **経営幹部の積極的な関与がなければサイバーセキュリティの成熟度向上は果たせません**
>
> — Splunk CISO、Jason Lee

生成AIを活用したイノベーションに積極的である

取り組みが先進的な組織はAIを活用したイノベーションにも積極的で、48%が重要な取り組みとしている一方、取り組みが途上の組織では30%でした。取り組みが先進的な組織ではセキュリティチームでのAI導入も進んでいて、ほとんどのチームメンバーが生成AIを利用していると回答した割合が75%にのぼり、取り組みが途上の組織の23%を大きく上回りました。

取り組みが先進的な組織での生成AIの活用は、取り組みが途上の組織と比べて実験的な意味合いが薄く、むしろ本格的な取り組みとして行われています。

- **生成AIに関するセキュリティポリシーが確立していると回答した割合は、取り組みが先進的な組織では82%であったのに対して、取り組みが途上の組織では46%にとどまりました。**
- **サイバーセキュリティのユースケースで生成AIの正式な利用計画があると回答した割合は、取り組みが先進的な組織で55%であったのに対して、取り組みが途上の組織では15%にとどまりました。**

インシデントの検出と対応が速い

サイバーセキュリティの成熟度が高いからといって、攻撃を受ける頻度が減るわけではありません。それでも、取り組みが先進的な組織は脅威をすばやく検出して対応することで、攻撃による影響と被害を緩和しています。

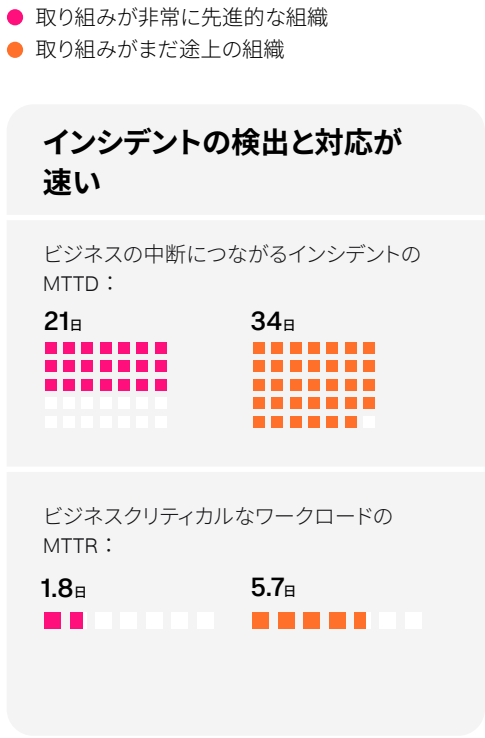
ビジネスの中断につながるインシデントのMTTD (平均検出時間)は、取り組みが先進的な組織で平均21日であるのに対し、取り組みが途上の組織ではネットワークに侵入した脅威を検出するのに平均で1カ月以上(34日)もかかっています。また、取り組みが先進的な組織は復旧も迅速で、ビジネスクリティカルなワークロードのMTTR (平均復旧時間)は44時間強と短く、取り組みが途上の組織の平均5.7日を大きく引き離しました。

「検出時間や対応時間の短さは、セキュリティプログラムの成熟度をよく表しています。取締役会や経営幹部が指標としてMTTDとMTTRを重視するのはそのためです。長期的な成功指標として大きな意味を持つのです」と、Splunkのセキュリティ調査チームであるSURGeのグローバルセキュリティアドバイザー、Mick Baccioは説明します。

> **検出時間と対応時間の短さは、セキュリティプログラムの成熟度をよく表しています。取締役会や経営幹部が指標としてMTTDとMTTRを重視するのはそのためです。長期的な成功指標として大きな意味を持つのです**
>
> — Splunkグローバルセキュリティアドバイザー、Mick Baccio

先進的な組織の取り組み

自社のサイバーセキュリティプログラムが非常に先進的と評価している組織は、4つの主要な能力において他の組織を常に上回っています。



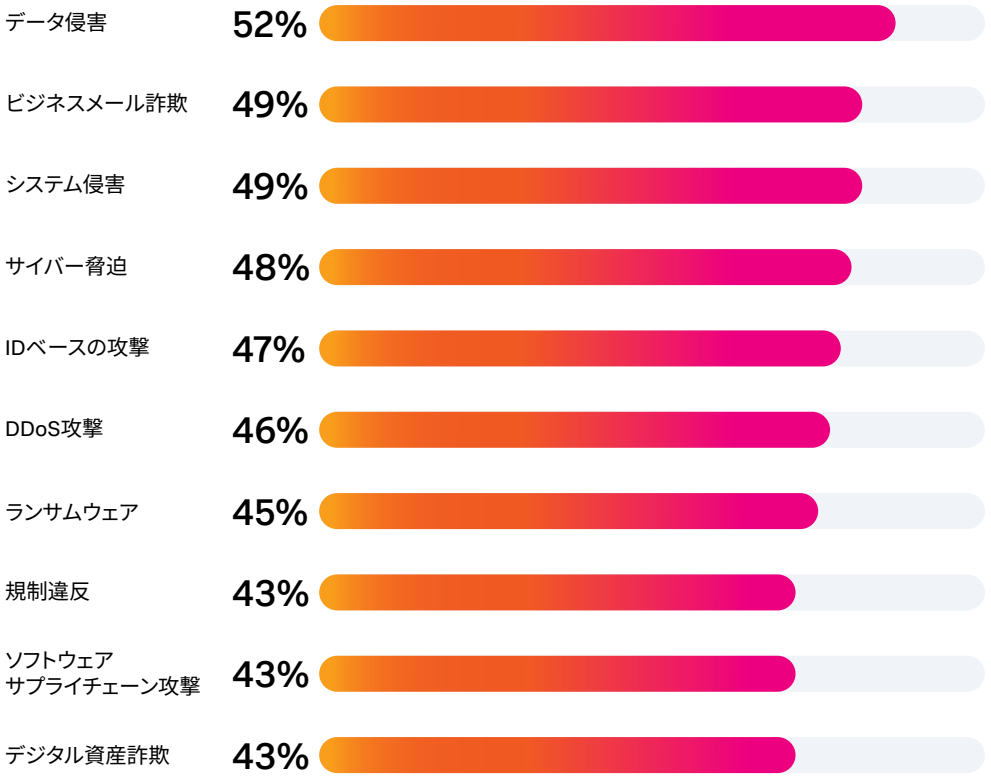
拡大する脅威の状況

セキュリティチームは善戦していますが、攻撃者はその最善の防御をすり抜ける方法をいずれ見つけ出すでしょう。調査では、2021年以降、データ侵害が13ポイント、ランサムウェア攻撃が14ポイント増加したことが明らかになり、攻撃者の勢いが衰えていないことが証明されました。

2024年に入ってからも、受信者をだますビジネスメール詐欺(BEC)や、ブルートフォースによるDDoS攻撃など、さまざまな戦術を使った攻撃が報告されています。戦術は多様でも目的はただひとつ、混乱を引き起こすことです。

サイバーセキュリティインシデントは今日でも、組織の評判低下や規制違反、収益減少など幅広く悪影響を及ぼしますが、組織はダメージを軽減する方法を学び、さらには、全体としてより多くの攻撃に耐える力を身に付けているようです。実際、調査では、インシデントの修復に多くの時間と人手がかかると回答した割合は44%で、昨年から13ポイント低下しました。また、生産性の低下や機密データへの侵害の被害に遭った回答者の割合も減っており、デジタルレジリエンス強化の取り組みが功を奏しているとみられます。

過去2年間に最も多く発生したインシデント



サイバー攻撃に対する不安と現実にはずれがある

数百万ドル規模の身代金の支払い、CISOの起訴、ゼロデイ攻撃といった出来事はニュースで大きく取り上げられますが、件数はあまり多くありません。サイバーセキュリティ関係者に「発生を懸念している脅威」と「**実際に発生した脅威**」を尋ねると、実際の状況は恐れているほどひどくないことが度々あります。

たとえば、最も懸念している攻撃ではAIを活用した攻撃が1位になりましたが、実際に受けたことのある攻撃では、データ侵害、ビジネスメール詐欺、システム侵害、IDベースの攻撃が上位に入りました。

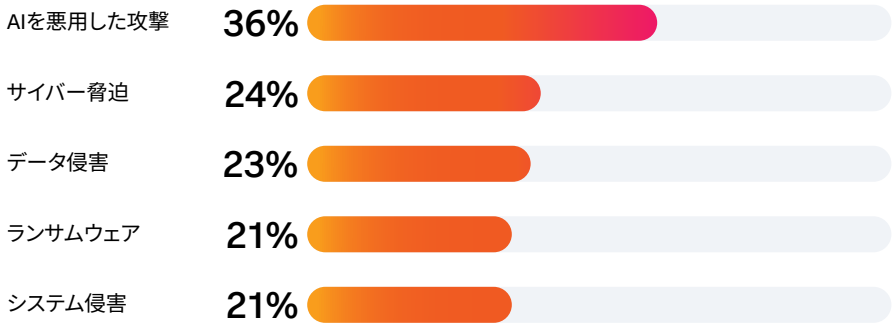
逆もまた真なりで、あまり警戒していない攻撃が実際には頻発していることもあります。ビジネスメール詐欺を最も懸念していると回答した割合は18%でしたが、2024年の発生件数では2位でした。

もちろん、一部の不安は現実と一致しています。たとえばデータ侵害は、懸念される攻撃でも実際に発生した攻撃でも上位に入り、過去2年間にデータ侵害のインシデントが1回以上発生した組織は52%にのぼります。

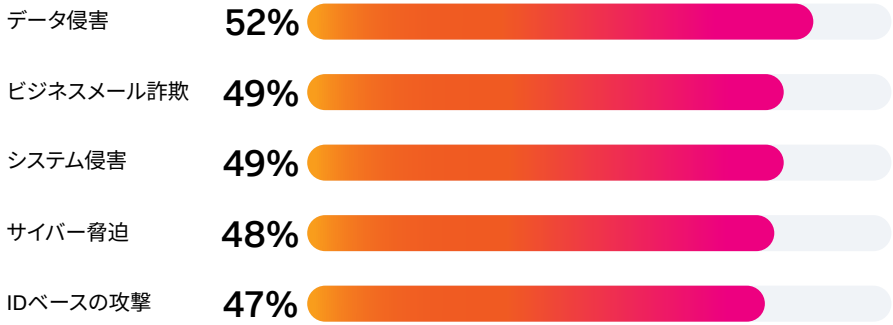
未知なるものには恐怖心を抱くものです。データ侵害などの既知の攻撃に対処するためのプロセスや手順は確立されていますが、AIを悪用した攻撃については、もし起きたとして止める術を知りません

— Splunk SURGeディレクター、Marcus LaFerrera

最も懸念しているサイバー攻撃



経験したことのあるサイバー攻撃



すべてに共通する要因は人間

攻撃者はどのようにして組織に侵入するのでしょうか。自動化や生成AIの導入が進んでも、人間が弱点として残ります。システムの設定ミスは、最もよく悪用される脅威ベクトル(38%)と最も懸念される脅威ベクトル(35%)の両方で上位に入っています。

不安と現実が一致しているということは、セキュリティチームが設定ミスを問題視していながら(ならば監視してください!)効果的に対応できていないことを示唆しています。システムの複雑化と慢性的な人材不足が問題を悪化させている面もあり、設定ミスを排除することは今やモグラたたきのようです。

最もよく悪用される脅威ベクトル

38%
システムの設定ミス

31%
自社開発
アプリケーションの
脆弱性

30%
ゼロデイ脆弱性

29%
既知のソフトウェア
脆弱性

28%
ラテラル
ムーブメント

金銭目的の攻撃は健在

金銭目的の三大攻撃とも言えるランサムウェア、データ侵害、脅迫は、相変わらず猛威を振るっています。実際、データやシステムを人質に取られたことがあると回答した割合は、2022年の35%から2024年には42%に増加しています。さらに、ランサムウェア攻撃の戦術のひとつであり、盗んだデータをインターネットで暴露すると脅すサイバー脅迫は、ランサムウェア自体よりも増えています。サイバー脅迫を受けたと回答した割合は48%で、ランサムウェアの被害に遭った割合の45%を上回っています。

サイバー脅迫の増加には、2021年に起きたColonial Pipeline社への攻撃の成功と、ロシアを拠点とするランサムウェアグループ「Clop」によるMOVEitを悪用した攻撃での、7,500万〜1億ドルに達するとみられる身代金支払いが影響している可能性があります。

組織がバックアップテストの重要性を再認識し始めた今、サイバー犯罪者は、データを暗号化するよりも流出させて脅迫する方が手間がかからず、より多くの身代金を獲得でき、バックアップがないことが前提となる不確定要素もないため、有効な手段だと考え始めているのかもしれません。

国際情勢の緊迫化がサイバー空間に飛び火する

2024年は世界的な混乱が続いています。国際情勢の緊迫化はサイバー空間にも影響を及ぼし、政治とは無関係と思われる組織にも混乱をもたらしています。2023年には、ペンシルベニア州の水処理施設がハクティビスト(政治的な目的でハッキングを行うサイバー犯罪者)による攻撃を受け、国家を後ろ盾とした攻撃グループやテロリスト集団からは誰も完全には逃れられないことを印象づけました。

調査では86%の回答者が、国際情勢の緊迫化によって自分の組織が標的になる可能性が高まっていると危惧しています。特にテクノロジー企業は懸念を募らせており、この考えに「非常にそう思う」と回答した割合が、他の全業界で29%であったのに対して、テクノロジー業界では42%にのぼりました。SolarWinds製品の脆弱性悪用のような、国際情勢と結び付く重大な攻撃を目の当たりにして、テクノロジー企業、特にITサービスプロバイダーは、政治的な動機を持つ犯罪集団が幅広い標的に攻撃を行うために自社を踏み台として利用する可能性があることを痛感したのでしょう。

興味深いことに、行政・公共機関では、国際情勢の緊迫化によって自分の組織が標的になる可能性が高まっているという考えに「非常にそう思う」と回答した割合が17%にとどまりました。その理由として、行政機関は以前から政治的動機による攻撃の標的になってきた(そして今後もそうである可能性が高い)ことが考えられます。

「ハクティビズムは必ずしも洗練されていません」と、Splunk SURGeのセキュリティストラテジストであるAudra Streetmanは言います。「政治的な動機を持つ攻撃者は、古い脆弱性やデフォルトのパスワードなど、比較的安易な方法で攻撃を行うことが多いので、サイバーハイジーンを徹底することがこれまで以上に重要になります」

> **国際情勢の緊迫化によって今後もリスクが高まり続けるでしょう。政治とは一見無関係の組織も例外ではありません。サプライチェーンのグローバル化の副作用として、デジタルのつながりを通じてリスクが波及するからです**
>
> — Splunkグローバルセキュリティアドバイザー、Mick Baccio

厳しさを増すコンプライアンス対応

セキュリティ関係者にとって、規制やコンプライアンスは死や税金と同じ、つまり絶対に避けられないものです。実際、調査では62%が、重大なインシデントの開示に関するコンプライアンス義務の変化の影響をすでに受けていると回答しています。

セキュリティ担当者は、規制の強化がセキュリティ業務に変化をもたらすことを十分に理解しています。そこには、意図した変化もあれば、意図しない変化もあるでしょう。たとえば、87%の回答者が、今後1年間でコンプライアンスへの対応方法が大きく変わると考えています。一方で、コンプライアンスとサイバーセキュリティは決して相反するものではないものの、コンプライアンス対策のために特定のセキュリティ対策を断念せざるを得ないという、意図しない状況に陥る可能性もあります。調査では、86%が、予算配分においてセキュリティのベストプラクティスの導入よりもコンプライアンス規制への対応を優先すると回答しています。

この結果はSplunkが2023年10月に公開した『CISOレポート』の調査結果を反映しています。このレポートでは、84%のCISOがサイバーセキュリティインシデントに対する個人の法的責任について不安を感じていると回答し、同じく84%が、取締役会や理事会にとって強力なセキュリティとは、セキュリティの従来の成功指標よりも規制コンプライアンスを意味すると回答しています。

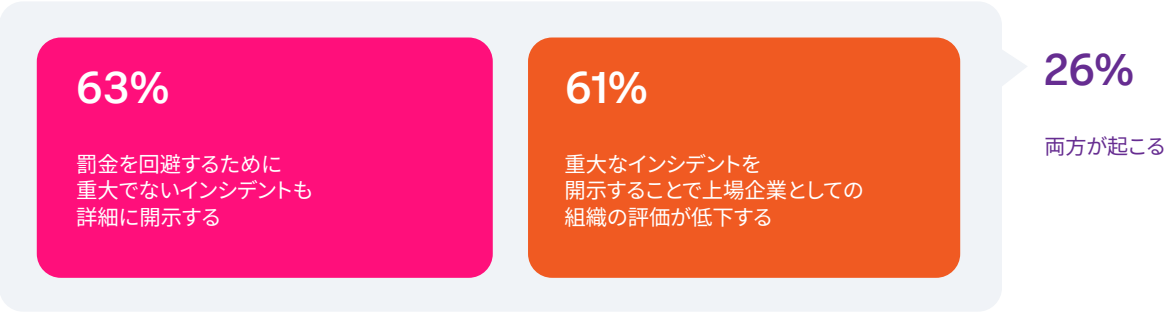
その理由は明らかです。米国証券取引委員会(SEC)による新しい規則では、上場企業に対して、「重大」だと判断されるすべてのサイバーセキュリティインシデントを開示し、詳細を報告することと、自社のリスク管理プログラムについて年次で報告することを義務付けています。これらの規則に違反すると、経営幹部に高額な罰金の支払いが求められたり、経営幹部が起訴され、場合によっては懲役刑が科される可能性があります。EUのNIS2指令では、インシデント対応を担当する正式なチームを設置し、情報交換を目的とした情報システムを構築することが求められています。それに違反した場合は、幹部個人が責任に問われる可能性があります。

セキュリティリーダーは板挟みの状況です。被害を過小評価すれば、不正行為の疑惑をかけられて懲役刑を受ける可能性があります。逆に被害を過大評価すれば、株価が急落して取締役会の不信を買う恐れがあります。

これは一種の道徳的ジレンマです。インシデントを過少申告して、気づかれないことを祈るか、組織の株価が大打撃を受けるのを覚悟して、自分自身を守るためにインシデントを過剰に報告するか、皆様ならどちらを選ぶでしょうか。

今や、セキュリティ戦略の中心はコンプライアンス対応です。机上演習などのシミュレーション訓練は、セキュリティの不備を見つけ出すと同時に、継続的な改善に投資していることを規制当局に証明して、悪いニュースで見出しを飾らないように備えるために役立ちます。

重大なインシデントの開示に関する新しい規制がもたらすと考えられる影響



セキュリティ、法務、コンプライアンスのチーム連携が鍵を握る

かつて、コンプライアンス対応は主に事務処理的な仕事でした。コンプライアンスチームは独立して業務を行い、セキュリティチームと連絡を取り合うことはほとんどなく、セキュリティチームの役割をよく理解していないことすらありました。セキュリティチームもまた、コンプライアンスチームの役割をよく理解していませんでした。

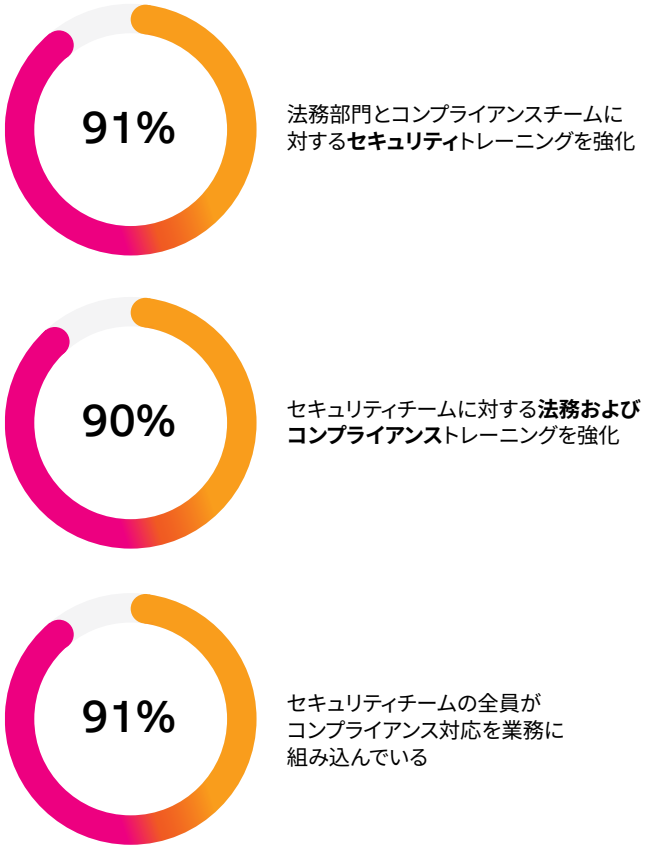
しかし、規制が不十分であったために、コンプライアンスの欠如が深刻な結果を招くようになり、こうした日々は終わりを告げることになります。2023年10月にSECは、SolarWinds社がサイバーセキュリティ対策に関する情報開示で投資家を欺き、2020年の壊滅的なサイバー攻撃を招いたとして、詐欺行為と内部統制の不備を理由に同社の元CISOを起訴しました。今日では、取締役会、法務部門、コンプライアンスチーム、セキュリティチーム間のコミュニケーションは不可欠であり、互いを理解して適切に連携する方法を学ぶことが必須です。

インシデントは「起きるかどうか」ではなく「いつ起きるか」の問題です。組織と取締役会は、実際にインシデントが起きた場合に誰が最終責任を取るかについて、よく考える必要があります。一般的には、最終責任者はCISOになるでしょう。ただし、CTO、CIO、さらには取締役会のサイバーセキュリティ担当者も、株主代表訴訟で起訴されたり追加調査の対象になったりする可能性があります。

こうした動きはセキュリティ担当者にも伝わっています。調査によると、大多数の回答者が、セキュリティ対策の強化と、法務部門やコンプライアンスチームとの連携促進にすでに取り組んでいます。

チーム間で認識を共有することには追加のメリットもあります。優先項目、役割、責任をチーム間で共有することで、セキュリティ態勢をより強化するとともに、法務部門とコンプライアンスチームにより多くの権限を付与して自立性を高めることができます。

セキュリティチームとコンプライアンスチームの連携



コンプライアンスが個人の問題に

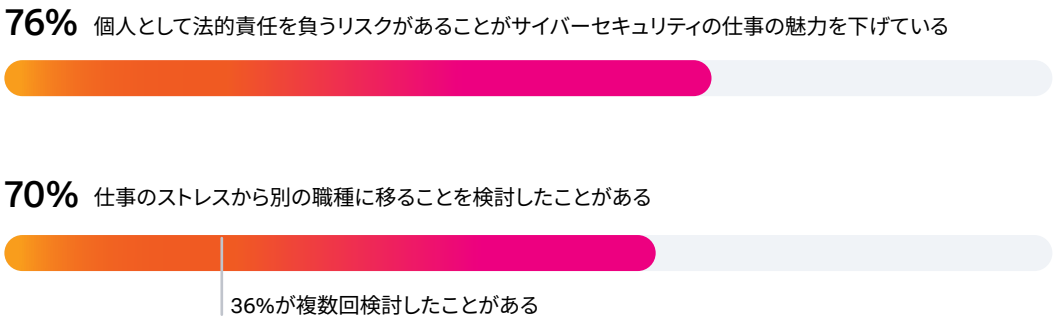
SECがサイバーセキュリティインシデントに関連して初めてCISOを起訴したSolarWinds社の事例は重要な転機になりました。この前例のない措置は、サイバーセキュリティに対する考え方を変え、今後、セキュリティリーダーとセキュリティチームに長期にわたって影響を与えることになるでしょう。サイバーリスクは今や、ビジネスリスクと同義になったのです。

SECは、経営幹部をはじめとするステークホルダーに説明責任を課し、厳しい監視の目を向けています。組織のセキュリティ義務を強化する新たな法規制が世界各地で制定される中、セキュリティチームは、インシデントを迅速に報告する体制を整備する必要があります。EUのNIS2指令では猶予は24 ～ 72時間ですが、SECの規則では4営業日以内とやや余裕があります。いずれにしても猶予期間は短くなっています。その対応のために、多くのベテランセキュリティ担当者が駆り出されることになるでしょう。

インシデントに関する説明責任の強化は、セキュリティ対策の強化につながる反面、セキュリティ関係者を委縮させる可能性があります。仕事のミスで刑務所に入りたい人はいないでしょう。

刑務所は大げさだとしても、責任の追及が不安をあおることは確かです。セキュリティチームが人材不足にあえいでいる今、コンプライアンス違反に対する恐怖心は、人材を遠ざける新たな要因になり得ます。

コンプライアンス対応への重圧がキャリアに及ぼす悪影響



将来の展望

2024年、サイバーセキュリティには、新たなコンプライアンス規制の施行や国際情勢の緊迫化など、世界レベルのさまざまな困難が待ち受けています。しかし、希望もあります。AIを積極的に取り入れて活用法を果敢に開拓することは、セキュリティチームの利益につながります。AIツールの利用に関するリスクを緩和し、統制を維持できれば、導入効果がさらに高まります。

将来に向けたもうひとつの明るい兆しは、組織がサイバーセキュリティへの投資を増やしていることです。調査ではほぼすべて(96%)の組織が、今後1～2年でサイバーセキュリティ予算を増やすと明言しています。

最後のアドバイス

テクノロジーの変化と進化がますます進む中で、組織はどこに重点を置くべきか迷うところでしょう。そこで、Splunkのエキスパートから今年の調査結果を踏まえたアドバイスをご紹介します。

組織全体で生成AIの導入を推進する

生成AIの導入は、組織全体でも(93%)、セキュリティチームでも(91%)すでに進んでいます。導入を躊躇していると、競争に取り残される可能性すらあります。生成AIの利用を全面的に禁止することは、イノベーションへの扉を閉ざすと同時に、シャドー AIへの扉を開くことになります。

イノベーションを妨げないように注意しながら生成AIに関するポリシーを作成する

リスクや影響を考えずに生成AIの導入に突き進むのは間違いです。生成AIに関するポリシーを作成し、ビジネスとセキュリティのユースケースについて適切な計画を立てれば、正式なポリシーを作成していない34%の組織の先を行くことができます。生成AIについて特に懸念されるリスクを洗い出し(調査では49%がデータ漏えいを挙げています)、それらの問題に具体的に対処するためのポリシーを策定しましょう。

チーム間のコラボレーションとツールの統合に重点を置く

デジタルレジリエンスを向上させるには、ソフトウェアエンジニアリング、エンジニアリング運用、IT運用のサイロ化を解消する必要があります。IT運用については特に重要です。先進的な組織では76%が、今年、デジタルレジリエンスを向上させる目的でIT運用とのコラボレーションを強化したと回答しています。チームの負担を減らすことも大切です。ツールを統合して多数のダッシュボードを巡回する手間を省けば、チームは重大な脅威への対応に集中できます。調査では43%の回答者が、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ることを問題に挙げています。

法務部門やコンプライアンスチームと足並みを揃える

今年はコンプライアンスの新時代とも言える年になります。セキュリティリーダーにとっては、法務部門やコンプライアンスチームと緊密にコミュニケーションをとって最大限の連携を図ることが急務です。調査では、91%の組織が、すでにセキュリティチームの業務にコンプライアンス対応を組み込んでいると回答しています。机上演習などのシミュレーション訓練を実施すれば、セキュリティやコンプライアンスの不備を見つけ出すと同時に、継続的な改善に投資していることを規制当局に証明できます。

今後2年間のサイバーセキュリティに関する優先項目

1. サイバーセキュリティとIT運用の担当者にセキュリティ運用トレーニングを実施する

2. 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

3. 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

4. 既存のツールに加えてクラウドベースのセキュリティ分析/運用テクノロジーを調査、テスト、導入する

5. セキュリティ運用での外部リソースの利用を増やす(マネージドセキュリティサービスを提供するサードパーティプロバイダーなど)

セキュリティリソース拡充の重要性を効果的に伝える方法を学ぶ

サイバーセキュリティの成熟度はトップの能力が大きく左右します。取り組みが先進的な組織では、95%が問題を解決するために必要なリソースと権限を確保していると回答しています。特にCISOは、ビジネスの観点でセキュリティリスクを捉え、わかりやすく説明する能力を身に付けることが重要です。これにより、役員会議に常に呼ばれるようになり、サイバーセキュリティへの投資がビジネスの価値につながることを取締役会に明確に伝えることができます。その際には、サイバーセキュリティインシデントがビジネスに及ぼす影響と、法的または財務的に重大な結果につながるコンプライアンス要件を明確に示すことが大切です。

既存の枠にとらわれない考え方で人材不足を補う

調査では、先進的な組織が採用やトレーニングについて従来の方法にこだわらないことも明らかになりました。AIと機械学習を活用して人材不足を補っていると回答した割合は、取り組みが先進的な組織で53%にのぼり、取り組みが途上の組織の28%を大きく上回りました。こうした組織は、セキュリティ以外の職務に就く人にSOCでのシャドウイングを行うなど、創造的な採用およびトレーニング戦略を取り入れることで、スキル不足を解消すると同時に、セキュリティチームに必要な多様性を実現しています。

基本を忘れない

サイバーセキュリティの脅威が巧妙化する一方で、従来の実証済みの攻撃技法もいまだ多用されています。また、よく悪用される脅威ベクトルの1位は2024年もシステムの設定ミスでした。これらの点を踏まえると、基本的な対策をしっかりと講じることで最大限のROIを引き出せるとともに、長期的にはコンプライアンス要件への対応を容易に実現できるようになります。調査では76%の回答者が、IT資産のインベントリに時間がかかりすぎることに不満を抱いていますが、それは有意義な時間の使い方です。組織が所有する資産とそれらの依存関係の最新状況を把握することで、リスクとしての盲点を洗い出して解消できます。

サイバーセキュリティに影響する世界的な動きを注視する

サイバーセキュリティには社会の動向が深く関わります。政治、国家間の紛争、コンプライアンス義務の強化は、脅威の状況に直接的または間接的に影響を及ぼします。調査では、86%の回答者が国際情勢の緊迫化によって自分の組織が標的になる可能性が高まっていると懸念し、62%がコンプライアンス義務の変化の影響をすでに受けていると回答しています。こうした状況の変化を常に把握しておけば、それに起因する問題に直面してもすばやく対処できます。

Splunkを活用したデジタルレジリエンスの強化方法を学ぶ

日本語ブログ - セキュリティ情報サイト

2024年以降のサイバーセキュリティのトレンドについて、さまざまな業界のリーダーが、AI、新たな脅威、コンプライアンス環境の変化など、今日の喫緊のセキュリティ課題にどう取り組んでいるかをご紹介します。

詳細はこちら

デジタルレジリエンスの構築

セキュリティチームは今日、サイバー脅威、変化し続ける規制、国際情勢の緊迫化など、常に重圧にさらされています。混乱の時代に回復力だけでなく成長力を高める方法もご紹介します。

詳細はこちら

業界別の特徴

世界共通の代表的な6つの業界について主要なインサイトをご紹介します。

製造

製造業界では、重視する取り組みとしてクラウドセキュリティを挙げた組織の割合が40%にのぼり、他の業界を上回りました。ゼロデイ脆弱性の対策も優先度が高く、39%の組織が最も懸念する脅威に挙げています。これはおそらく、基幹インフラへのパッチ適用が難しいという業界固有の事情によるものと思われます。

進化を続ける脅威への対応に苦戦する組織が多い点も特徴です。

- **製造業界のセキュリティ担当者の51%が、過去1年間でセキュリティ要件への対応が難しくなったと回答しています。**
- **回答者の50%が、脅威の巧妙化にまったく対応できていないと答えています(全業界の平均は38%)。**

苦戦の原因は、組織としての投資不足にあるかもしれません。サイバーセキュリティ予算が大幅に増額されると見込む回答者の割合は、全業界の平均が48%であるのに対して、製造業界では36%にとどまりました。

一方で、セキュリティ人材の確保は他の業界よりも順調です。

- **27%が、仕事のストレスが原因で自身または他のチームメンバーがサイバーセキュリティ職を離れることを複数回検討したことがあると回答しています(全業界の平均は36%)。**
- **27%が、スキル不足が原因で重要なプロジェクトが複数回遅延したことがあると回答しています(全業界の平均は37%)。**

サイバーセキュリティ予算の問題を抱える製造業界のセキュリティリーダーがまず取り組むべきは、経営幹部や取締役会に対して、インシデントが発生した場合の財務的影響を明確に示し、リスクの重大さを強く訴えて賛同を得ることでしょう。

金融サービス

金融サービス業界は、他の業界に比べてサイバーセキュリティ要件への対応能力に自信を持っているようです。過去1年間で対応が楽になったと回答した割合は、全業界の平均が41%であったのに対して、金融サービス業界では50%にのぼりました。

楽になったと感じる要因は、IT運用チームやエンジニアリングチームとのコラボレーションが進んでいることにあるかもしれません。金融機関のセキュリティチームで、デジタルレジリエンスを強化するためにエンジニアリング運用と緊密に連携していると回答した割合が64%にのぼり、全業界の平均である46%を大きく上回りました。

人材不足を補うための生成AIの役割について期待が大きいのも特徴です。特に以下の点を期待しています。

- **63%が、人材の獲得とオンボーディングの迅速化に役立つと回答しています(全業界の平均は58%)。**
- **71%が、ベテランのセキュリティ担当者の生産性向上に役立つと回答しています(全業界の平均は65%)。**

一方で、生成AIのリスクについてもよく認識しています。生成AIの影響を十分に理解するための教育が不足していると回答した割合は76%にのぼり、全業界の平均である65%を上回りました。この不安は、最も懸念する脅威としてAIを悪用した攻撃を挙げた割合が39%にのぼったことにも表れています。

コンプライアンス対応の負担が増してセキュリティチームだけでは担いきれず、専門チームの設置が不可欠になっていると回答した割合は、全業界の平均である39%をやや上回り、43%にのぼりました。金融サービス業界の性質上、この結果は当然でしょう。また、最も多く発生したインシデントとして54%がサイバー脅迫を挙げています(全業界の平均は48%)。

調査方法

調査は、2023年12月から2024年1月にかけて、1,650人のセキュリティ幹部を対象に行われました。対象となった国は、オーストラリア、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、米国の9カ国です。対象となった業界は、航空宇宙・防衛、ビジネスサービス、消費財、教育、金融サービス、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、テクノロジー、メディア、石油・ガス、リテール(小売り)・卸売り、通信、運輸・輸送・物流、公益の16種類です。

通信・メディア

通信・メディア業界では、自社のサイバーセキュリティプログラムを「非常に先進的」と評価した回答者の割合が57%で最も高くなりました(全業界の平均は47%)。一方で、課題に対処するために必要なリソースや権限を確保できていないと回答した割合も最も高く、16%にのぼりました(全業界の平均は8%)。

そのほかに目立った課題には以下のものがあります。

- **82%が、攻撃対象が頻繁に変化および拡大するため、セキュリティハイジーンや態勢の管理が難しいと回答しています(全業界の平均は71%)。**
- **62%が、SOCで扱う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ると回答しています(全業界の平均は43%)。**
- **47%が、適切なスキルを持つ人材を獲得または維持できないことが原因で、自身または他のチームメンバーがサイバーセキュリティの職を離れることを複数回検討したことがあると回答しています(全業界の平均は36%)。**
- **74%が、コンプライアンス義務の変化の影響を受けていると回答しています(全業界の平均は62%)。**

一部のインシデントの発生頻度が高まっているのは、これらの課題が原因と思われます。発生回数が増えたという回答が他の業界よりも多かった脅威は、インサイダー攻撃の55% (全業界の平均は42%)、デジタル資産詐欺の59% (同43%)、ソフトウェアサプライチェーン攻撃の57% (同43%)、標的型攻撃の54% (同44%)でした。システムの設定ミスも大きな課題で、過去2年間にシステムの設定ミスが根本原因になったことがあると回答した割合は44%にのぼります。

通信・メディア企業が今後重視すべきは、経営幹部の賛同を得て、サイバーセキュリティプログラムの成熟度をさらに上げることでしょう。セキュリティチームが問題解決に必要なリソースと権限を確保できれば、より効果的に脅威を防止できるはずです。

テクノロジー

テクノロジー業界では、環境の複雑化が大きな課題になっています。その結果、以下の影響が出ています。

- **36%が、サイバーセキュリティ要件への対応が難しくなっている理由としてセキュリティスタックの複雑化を挙げています(全業界の平均は26%)。**
- **37%が、連携しない多数のツールと人材不足によって手動作業が滞ると回答しています(全業界の平均は26%)。**
- **インシデントの根本原因になりやすい問題として、34%が既知のソフトウェア脆弱性、同じく34%が自社開発アプリケーションの脆弱性を挙げています。**

規制環境の変化も悪影響を及ぼしており、41%が対応が難しいと回答しています(全業界の平均は28%)。

国際紛争はさらに深刻な影響をもたらしています。国際情勢の緊迫化によって自分の組織が標的になる可能性が高まっているかという質問に対して「非常にそう思う」と回答した割合は42%にのぼり、全業界の平均である29%を大きく上回りました。

良い点としては、セキュリティ予算が大幅に増額されると見込む回答者の割合が63%にのぼり、全業界の平均である48%を大きく上回りました。

環境の複雑化に苦しむテクノロジー企業にとっての最優先事項はシンプル化でしょう。最新テクノロジーにすぐに飛びつきがちなこの業界では、ツールの統合が有効かもしれません。

医療・ヘルスケア

医療・ヘルスケア業界ではMTTDが大きな問題で、推定で数カ月と回答した割合が31%にのぼり、全業界の平均である19%を大幅に上回っています。また、ランサムウェア攻撃にも悩まされており、過去2年間でランサムウェア攻撃を受けたことがあると回答した割合が56%にのぼり、全業界の平均である45%をかなり上回っています。さらに、インシデントの根本原因になりやすい問題として、33%がアカウントへの過剰な権限の付与を挙げています。

人材不足の問題も他の業界に比べて深刻です。

- **44%が、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たことがあると回答しています(全業界の平均は39%)。**
- **44%が、人手不足が原因で重要なプロジェクトやイニシアチブが遅延したことがあると回答しています(全業界の平均は37%)。**

コンプライアンス義務の変化の影響をすでに受けていると回答した割合も67%にのぼります。さらに、新たなコンプライアンス義務に対応するために24時間365日無休で待機状態にあるシニアレベルの担当者が増えたと思うかという質問に対して「非常にそう思う」と回答した割合が44%でした(全業界の平均は35%)。

医療・ヘルスケア業界は総じて、生成AIについて懐疑的です。生成AIは攻撃側により多くのメリットをもたらすと考える回答者が52%にのぼり、全業界の平均である45%を上回りました。また、生成AIを悪用した攻撃に対抗するためにこちらも生成AIを活用することに関心が低く、AIを優先事項として挙げている割合が37%にとどまり、全業界の平均である44%を下回りました。

脅威検出、ランサムウェア対策、人材不足が大きな課題となっている医療・ヘルスケア業界では、基本的なサイバーセキュリティ対策に立ち返ることが最も効果的な解決策と言えるでしょう。これによって少ないリソースで多くのことに対応できます。

行政・公共機関

行政・公共機関の結果からまずわかるのは、知識不足です。セキュリティ意識向上のためのトレーニングを重視する回答者の割合が24%と高く、全業界の平均である17%を上回りました。それに関連して、サイバーセキュリティに関する経営幹部の知識や取り組みへの関与が不足していることを最大の課題に挙げた割合が28%にのぼりました(全業界の平均は20%)。

昨年の調査では、セキュリティチームの負担軽減のために従来タイプのAIを活用することに消極的でしたが、今年は生成AIに期待する声が高まっています。

- **55%が、生成AIがビジネスの「ゲームチェンジャー」になる可能性があると考え(全業界の平均は47%)、同じく55%がセキュリティチームに最もメリットがあると予想しています(同46%)。**
- **この業界の77%のセキュリティチームが、AI活用に関するポリシーの策定を主導しています(全業界の平均は66%)。**
- **生成AIに期待するセキュリティユースケースとして、46%が脅威検出(全業界の平均は35%)、42%が侵入テスト(同29%)、44%がセキュリティチームのトレーニング(同34%)を挙げています。**

セキュリティ運用の自動化を望む声も強く、その対象として、43%がSSL証明書の管理(全業界の平均は31%)、53%が異なるセキュリティコントロールをまたぐアクションのオーケストレーション(同38%)、47%がアラートのエンリッチメント(同32%)を挙げています。

基本的なサイバーセキュリティ対策については、最もよく悪用される脅威ベクトルとして設定ミスを挙げた回答者の割合が高く、42%がインシデントの根本原因になりやすい問題として挙げています。また、ラテラルムーブメント(横展開)をかなり警戒していて、39%が最も懸念する脅威に挙げています。

AIに関する知識不足と関心不足は危険な組み合わせです。行政・公共機関には、生成AIを急いで導入する前に、AI導入に関する計画的なアプローチを立て、AIのリスクについてよく学ぶことをお勧めします。

国別の特徴

世界の8カ国についての主要なインサイトをご紹介します。

オーストラリア

オーストラリアの組織は、国内のサイバーセキュリティの状況についてかなり悲観的です。国際情勢の緊迫化がサイバー攻撃の状況を悪化させていると思うかという質問に「非常にそう思う」と回答した割合が44%にのぼり、世界全体の平均である29%を大きく上回りました。また、56%が国家を後ろ盾とした犯罪グループの攻撃を受けたことがあり、やはり世界全体の平均である39%を大きく上回りました。

実際、調査対象となったすべてのタイプの攻撃について、被害に遭ったことがあると回答した割合が平均を上回りました。たとえば、データ侵害が63% (世界全体の平均は52%)、規制コンプライアンス違反が53% (同43%)、インサイダー攻撃が55% (同42%)、ビジネスメール詐欺が59% (同49%)でした。

サイバー攻撃の被害に遭いやすい要因は可視化の遅れにありそうです。セキュリティツールの数と種類が多すぎると回答した割合は72% (世界全体の平均は43%)、攻撃対象を適切に可視化できていないと回答した割合は35% (同20%)にのぼりました。この問題は当然のことながら検出時間に影響し、通常はMTTDが数カ月以上と回答した割合が50%と高く、世界全体の平均である19%を大幅に上回っています。

人材不足の問題も深刻です。

- **52%が、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たことが複数回あると回答しています(世界全体の平均は39%)。**
- **50%が、仕事のストレスが原因で自身または他のチームメンバーがサイバーセキュリティ職を離れることを複数回検討したことがあると回答しています(世界全体の平均は36%)。**
- **52%が、セキュリティに関する重要なプロジェクトやイニシアチブが遅延したことが複数回あると回答しています(世界全体の平均は37%)。**

生成AIの導入とポリシーの作成は他の国よりも進んでいて、従業員が公共の生成AIツールを業務に利用していると回答した割合が69% (世界全体の平均は54%)、生成AIの利用に関するセキュリティポリシーが確立していると回答した割合が73% (同66%)にのぼりました。

フランス

フランスの組織は、過去1年間でサイバーセキュリティ要件に対応するのが難しくなったと回答した割合が56%にのぼり、世界全体の平均である46%を上回りました。サイバーセキュリティの成熟度も低く、自社のプログラムを「非常に先進的」と評価した割合は37%にとどまりました(世界全体の平均は47%)。

サイバーセキュリティ要件への対応が難しくなった理由として、33%がセキュリティスタックで利用するツールやベンダーの数が多すぎることを挙げています(世界全体の平均は26%)。テクノロジースタックの複雑化は設定ミスにつながりがちで、40%が最も懸念する問題として設定ミスを挙げています。

フランスでは、AIや機械学習機能を備えたサイバーセキュリティツールを広く活用している組織の割合が27%で、世界全体の平均が37%であることを考えると他の国に後れを取っています。また、AIの導入に前向きで、優先する取り組みとしてAI活用を挙げた割合が56%にのぼり、世界全体の平均である44%を上回った一方で、生成AIの利用に関するポリシーが確立していると回答した割合は52%にとどまり、世界全体の平均である66%を下回りました。

良い点としては、インシデントの発生率が低く、以下のタイプの攻撃について過去2年間で発生したと回答した割合が世界全体の平均を下回りました。

- **データ侵害：44%**
- **規制やコンプライアンスの違反：37%**
- **DDoS攻撃：37%**
- **ランサムウェア攻撃：40%**

ドイツ

ドイツの組織は、他の国と比べて生成AIのリスクを重く見る傾向があります。

- **生成AIの普及によって攻撃対象が懸念すべきレベルまで拡大するという考えに、41%が「非常にそう思う」と回答しています(世界全体の平均は31%)。**
- **生成AIの普及によって既存の攻撃対象の脆弱性が高まるという考えには、38%が「非常にそう思う」と回答しています(世界全体の平均は29%)。**

ドイツで特に大きな課題となっているのが人材不足です。過去1年間でセキュリティ要件への対応が難しくなった理由として十分なスキルを持つ人材の不足を挙げた割合が33%にのぼり、世界全体の平均である25%を上回りました。

SOCについては、53%がセキュリティツールの数と種類が多すぎることを問題に挙げています(世界全体の平均は43%)。最も懸念するインシデントとして23%がクラウドインフラへの攻撃を挙げていることから、これらのツールの多くはクラウドベースと考えられます。

人材不足とツールの氾濫の影響なのか、MTTDも他の国よりやや長めで、数週間かかると回答した割合が40%にのぼりました(世界全体の平均は35%)。

これらの課題はあるものの、ランサムウェア攻撃に遭ったときのデータやシステムの復旧能力の高さでは際立っています。過去2年間に復旧に成功したことのある組織の割合は調査対象国の中で最も高い58%で、世界全体の平均である44%を大きく上回りました。

このほか、国際情勢の緊迫化によって自分の組織が標的になる可能性が高まっていると思うかという質問に対して「そう思う」と回答した割合が94%にのぼり、世界全体の平均である86%を上回っています。

インド

インドは他の国に比べて自社のセキュリティプログラムを「非常に先進的」と評価する組織の割合が66%と一番高く、世界全体の平均である47%を大きく上回りました。また、組織内でチーム間のコラボレーションが進んでおり、ソフトウェアエンジニアリングチームとは58%、エンジニアリング運用チームとは52%、IT運用チームとは78%がコラボレーションを強化しています。

クラウドセキュリティに対する関心が高いのも特徴で、48%の組織が最も重視する取り組みに挙げています(世界全体の平均は35%)。そのため、最も懸念する脅威としてクラウドベースのインフラに対する攻撃を挙げた組織が25%にのぼり、他の国を上回っています。ただし、最も懸念する脅威で1位になったのはサイバー攻撃による脅迫の37%で、こちらも世界全体の平均である24%を上回っています。

重大なインシデントの開示を求めるコンプライアンス義務への対応が重要課題になっているとみられ、81%がその影響を受けていると回答しています(世界全体の平均は62%)。そのため54%が、セキュリティチームの全員がコンプライアンス対応を業務に組み込むべきという考えに「非常にそう思う」と回答し、世界全体の平均である42%を大きく上回りました。

生成AIがもたらす変革には最も楽観的で、防御側により多くのメリットをもたらすと回答した割合が51%にのぼり、世界全体の平均である43%を上回りました。また、生成AIの活用が期待されるユースケースとして以下のものが多く挙げられました。

- **脅威の検出/優先順位付け：52% (世界全体の平均は35%)**
- **トレーニング：50% (同34%)**
- **脅威インテリジェンスの分析：55% (同39%)**
- **検出ルールの作成：44% (同30%)**
- **セキュリティデータの要約：54% (同34%)**

生成AIに関するポリシーの作成も進んでいます。エンドユーザー向けに生成AIのセキュリティポリシーを確立している割合は、世界全体の平均が66%であったのに対して、インドでは82%にのぼりました。

日本

日本では、他の国に比べてサイバーセキュリティ要件への対応が難しくなったと回答した割合が高く、54%にのぼりました(世界全体の平均は46%)。楽になったと回答した組織は27%にとどまり、世界全体の平均である41%を大きく下回っています。楽になったと回答した組織のうち、「かなり楽になった」と回答した組織はわずか5%でした(世界全体の平均は17%)。

その要因として、以下の点で世界に後れを取っていることが考えられます。

- **36%が、セキュリティスタックがあまりにも複雑化していると回答しています(世界全体の平均は26%)。**
- **29%が、すべてのセキュリティ関連データを効果的に分析できていないと回答しています(世界全体の平均は21%)。**
- **27%が、攻撃対象を十分に可視化できていないと回答しています(世界全体の平均は20%)。**

さらに要因として考えられるのが、予算不足です。サイバーセキュリティ予算が大幅に増額されると見込む組織の割合は38%にとどまりました。

また、日本では生成AIがSOCチームにもたらすメリットについても懐疑的な傾向がみられます。生成AIがスキル開発に役立つことに「非常にそう思う」と回答した割合は37%で、世界全体の平均である43%を下回りました。

ランサムウェア対策に重点を置く組織の割合は世界トップで、21%が重視する取り組みとして挙げています。その取り組みが功を奏してMTTDを短縮しており、MTTDが数日と回答した割合が43%にのぼり、世界全体の平均である33%を大幅に上回りました。

シンガポール

シンガポールの調査結果からは、組織のサイバーセキュリティプログラムの成熟度が他の国よりも低いことが読み取れます。

- **14%が自社のサイバーセキュリティプログラムを「取り組みが途上」と評価し、世界全体で最も高い割合でした(世界全体の平均は7%)。**
- **77%がサイバーセキュリティの課題に対応するために必要な権限とリソースを確保していると回答し、他の国と比べて低い割合でした(世界全体の平均は91%)。**
- **28%がサイバーセキュリティ予算が大幅に増額されると見込んでいますが、世界全体で最も低い割合でした。**
- **26%がMTTRを把握しておらず、25%がMTTDを計算するためのインシデント後分析を行っていませんでした。**

そのため、デジタルレジリエンスがビジネスに与える影響に対する認識が他の国と比べて低めです。デジタルレジリエンスが顧客維持率の向上につながることに「非常にそう思う」と回答した割合は23%にとどまり、世界全体の平均である33%を下回りました。また、デジタルレジリエンスが重大な業務中断の防止につながることに「非常にそう思う」と回答した割合は25%で、やはり世界全体の平均である35%を下回りました。

コンプライアンスチーム、セキュリティチーム、法務部門間のコラボレーションを重視する組織も少なめです。コンプライアンスチームのセキュリティトレーニングを強化することを非常に重視する組織は29%にとどまり、世界全体の平均である42%を大きく下回りました。セキュリティチームのワークフローにコンプライアンス対応を組み込むことを非常に重視する組織も29%で、世界全体の平均である42%を大きく下回っています。

全体の調査結果から、プログラムの成熟度とAIの優先度には相関関係があることがわかっています。そのため、AIの取り組みを重視する組織の割合は、世界全体の平均が44%であったのに対してシンガポールは36%にとどまりました。また、生成AIのポリシーを確立している組織も48%でした。さらに、AIを悪用した攻撃を懸念する組織も最も少なく、最も懸念する脅威に挙げた組織はわずか23%でした。

英国

英国の状況は、他の国と比べて全体的に良好です。

以下のようにコラボレーションを強化することでレジリエンスを向上させている組織が多いことがわかります。

- **66%が、セキュリティチームとソフトウェア開発チームのコラボレーションを強化していると回答しています(世界全体の平均は54%)。**
- **56%が、セキュリティチームとエンジニアリング運用チームのコラボレーションを強化していると回答しています(世界全体の平均は46%)。**

自動化も他の国より進んでいます。特に、汎用的なプロセス(40%)と脆弱管理(35%)で自動化の割合が高くなっています。

スキル不足の影響も他の国ほど大きくありません。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たことが複数回あると回答した割合は30%で、世界全体の平均である39%を下回っています。さらに、スキル不足が原因でセキュリティに関する重要なプロジェクトが失敗したことが複数回あると回答した割合も23%にとどまり、世界全体の平均である33%を下回りました。

おそらくこうした成熟度の高さのために、以下のタイプの攻撃を経験した組織の割合が他の国を下回っています。

- **規制違反：35% (世界全体の平均は43%)**
- **インサイダー攻撃：37% (同42%)**
- **ビジネスメール詐欺：38% (同49%)**
- **DDoS攻撃：38% (同46%)**
- **アカウント乗っ取り攻撃：34% (同42%)**
- **ランサムウェア攻撃：37% (同45%)**
- **ソフトウェアサプライチェーン攻撃：35% (同43%)**

米国

米国の調査結果は、世界平均とほぼ一致します。その中で平均を大きく上回った領域のひとつが生成AIの利用に関するポリシーで、すでに確立していると回答した割合が、世界全体の平均が66%であったのに対して、米国では72%にのぼりました。逆に、AIの悪用を根本原因として挙げた割合は最も少なく、18%でした。

課題はMTTDの長さで、40%が数週間(世界全体の平均は35%)、22%が通常は数カ月(同19%)と回答しています。ただし、改善は進んでいるようで、30%がプロセスの自動化によってMTTDが短縮されたと回答しています(世界全体の平均は25%)。

今後の優先事項については、サイバーセキュリティの人材不足への対応を挙げた割合がやや高めです。21%がセキュリティ運用担当者の増員を挙げ(世界全体の平均は18%)、25%がセキュリティ運用トレーニングの提供を計画しています(同23%)。

Splunkについて

Splunkは、組織のデジタルレジリエンス向上を支援します。世界の名だたる組織がデジタルシステムのセキュリティと信頼性を維持するために、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を利用しています。Splunkのソリューションを導入すれば、インフラ、アプリケーション、セキュリティに関するインシデントが大規模な問題に発展する前に防止し、障害の発生時にはデジタルシステムを迅速に復旧して、新しいビジネスチャンスをすばやく掴むことができるため、Splunkは多くの組織から信頼されています。

SplunkのSNS

splunk>

24-492903-Splunk-State-of-Security-JA-202405