# 2022年に向けて セキュリティリーダーが学ぶべき 4つのこと

splunk>
turn data into doing®

セキュリティリーダーにとって、この2年間は試練の時でした。2020年は新型コロナウイルスの感染拡大とリモートワークへの慌ただしい切り替えで幕を開け、その後多くの企業を評価と改善の取り組みへと駆り立てることとなった大規模で衝撃的な情報漏えい事件(SolarWinds)で幕を閉じました。セキュリティの専門家にとって、2020年は自分のキャリアの中でも重大な意味を持つ年になることでしょう。多くの人々にとって、この年はパンデミックの前後の生活を明確に区切る年として記憶に残るはずです。

パンデミックによって在宅勤務が急速に拡がり、それを支えるためにクラウドテクノロジーへの移行が飛躍的に加速した結果、セキュリティエコシステムの可視性が低下し、アクセスポイントの管理が困難になりました。それに伴い、攻撃に晒される領域も多様化し、拡大しました。

それでも、2021年のセキュリティの課題はある程度見慣れたものであると言えます。それらは、大きくは一貫性、コスト、複雑さに関わるものです。Splunkでは、調査会社であるEnterprise Strategy Groupと協力して、9つの主要な経済圏の複数の業界に属する535人のセキュリティリーダーを対象に中小企業や大企業が抱える最大のセキュリティ課題が何なのか、新たな戦略はどのようなものかを探る世界的な調査を実施しました。

SolarWindsへのハッキングはサプライチェーン攻撃に対する深刻な不安を呼び覚まし、企業は自社が信頼を置くベンダーが果たして本当に信頼すべき相手なのかという、ほとんど実存的とも言える疑問を抱えています。

- **78%の企業**がSolarWindsと同様のサプライチェーン攻撃が今後も発生すると予想。
- **88%の組織**がセキュリティ関連の支出が増加していると回答(35%は「著しく増加」と回答)。
- **クラウド導入が拡大し**、それが最大のセキュリティ課題となり、セキュリティへの支出が増大。

調査では、セキュリティやIT運用の意思決定者が考えるクラウドネイティブの環境での重要課題として、2つのセキュリティ課題が突出していました。その1つはポリシーの一貫性維持とデータセンターおよびクラウド全体への適用で、回答者の**50%**が課題であると回答しました。もう1つは複数のセキュリティコントロールを行う際のコストと複雑さで、**42%**が課題として挙げました。総じて調査の回答からは、一過性のワークロードや新しいソフトウェア開発モデル、複数のサービスが混在するパブリッククラウドの使用によって生じるクラウドの複雑性が、今後の大きなセキュリティ課題となることが読み取れます。

セキュリティリーダーの多くは、厳しさを増すセキュリティの課題に対応するために行動を起こし始めていると述べています。支出を増やしても、テクノロジーを投入しても、その基盤にある戦略次第です。そのためには、クラウドの複雑性に焦点を絞り、より優れた分析とクリアなデータの可視化を行うことが不可欠です。

では、以上のような状況を背景に2022年にリーダーが取り組むべきセキュリティ上の優先課題とは、どのようなものでしょうか。

01

# SOCの最新化

セキュリティチームは、ますます全貌が捉えにくくなりつつある環境を、多様かつ進化し続ける脅威や攻撃者から保護しなければなりません。そのためには最先端のコマンドセンターが必要です。以下に挙げるテクノロジーや手法はいずれも、単独ではすべてのニーズに応えることはできませんが、これらを組み合わせることで今日の脅威に対抗できる効果的なセキュリティオペレーションセンターを構築できます。

- **ゼロトラスト：**ゼロトラストは、ネットワーク境界ではなくユーザー、資産、リソースにより重点を置くことで、セキュリティリスクを最小限に抑えます。このモデルは3つの原則の上に成り立っています。それは、1)あらゆる人と事象を検証する、2)特権アクセスの付与を最小限にする、3)セキュリティ侵害がすでに発生しているものと仮定するということです。データセキュリティに重点を置いているため、ゼロトラストではエンドユーザーの認証を厳格に行います。断片化と分散化の進むセキュリティ環境では、このような戦略の切り替えが必須です。
- **セキュリティ運用プロセスの自動化：**これは非常に重要です。人間の分析担当者がすべての攻撃に対応することは不可能です。そうする代わりに、分析担当者がルールを記述して、自動化されたソリューションが攻撃を特定して対応できるようにします。人間の介在が不要になり、人間よりも迅速に対応できます。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)とUEBA(ユーザーとエンティティの行動分析)は、自動化の効果が高い場所でよく使用されます。
- **最新のSIEM：**SIEMは、調査で見られたような分析への投資の成果が現れやすい分野です。セキュリティ情報/イベント管理(SIEM)システムではネットワーク内のアクティビティを完全に可視化することができるため、脅威にリアルタイムで対応することが可能になります。
- **トレーニングと人材の拡充：**これはどの組織にとっても悩みの種です。ここで取り上げられているテクノロジーはいずれも、人員の少ないチームがより多くの仕事をこなす上で役立つものです。しかし結局は、増大する脅威を前にして組織が成長するには、そのセキュリティチームも成長させる必要があります。自動化と分析の機能を使用すれば分析担当者が発揮する能力の向上につながり、業務に必要なツールの数を減らせばトレーニングが行いやすくなります。

02

# データを統合して表示する

最新のSOCは最高のツールを備えており、それらをカスタマイズすることができます。しかし、そのことが、複数ソースからのデータに関与するインシデントを把握する能力やトレーニングという観点では新たな悩みの種となる場合もあります。マルチクラウドで複数のサービスを実行する複雑な環境では、従来のセキュリティデータだけでなく、すべてのデータを横断的に把握できることが必要です。この俯瞰的かつエンドツーエンドの視点は、セキュリティやコンプライアンスの取り組みだけでなく、開発や運用での成功にとっても不可欠なものです。 データを統合して表示することで、セキュリティチームとITチームにとっての単一情報源を構築できます。

03

# サプライチェーンの脅威に対するアプローチを見直す

SolarWindsハッキングの発生後、誰もが心配したのは、攻撃者が取引先を利用して自社のシステムやネットワークを悪用するのではないかということでした。最も重要な原則となるベンダーの監査は、言うほど簡単ではありません。というのも、「ビデオ会議ベンダー」や「支払処理ベンダー」は1つであっても、実際には外部のAPIやサービスを通じて複数のビジネスシステムで構成されていると考えられるためです。そのためすべてのデータコンポーネントとフローを把握する必要があります。さらに、セキュリティ侵害が発覚した時に最速で対応する方法を心得ている必要があります。この対応にはシャットダウンと侵害されたデータの特定が含まれます。

サプライチェーンの脅威やその他の類似する脅威では、ネットワーク内の疑わしいラテラルムーブメント(横展開)を見つけ出す能力を向上させることが不可欠です。理想的なのは、攻撃者の侵入手段がベンダーのソフトウェアパッチであるか従業員から盗んだ資格情報であるかを問わず、攻撃者が獲物を求めてネットワークに忍び込んだ時点でそれを発見できることです。

脆弱なパスワード、多要素認証として効果的でない方法、シングルサインオンを使用していないことなどは、この戦略の抜け穴となる恐れがあります。これに対して組織は、SOCを最新化するだけでなく、明確に定義され厳しい監視下に置かれたアイデンティティポリシーを用意し、強力に適用して監視し続けることで、このギャップを埋める必要があります。

04

# コラボレーションを促進する

新型コロナウイルスの災害対応では迅速な行動が求められ、セキュリティチームとITチームのコラボレーションが促進されました。セキュリティチームの使命は潜在的な障害を軽減させることであるため、この変化をさらに推し進めていく必要があります。この取り組みが十分に実を結ぶと、組織はDevSecOpsを実現することができます。DevSecOpsは相互に関連する3つの分野を融合させるものですが、これらの相互連携が期待通りに機能していないというのが現実です。

DevOpsの実践は、開発チームと運用チームとの間に従来あった壁を取り払い、ソフトウェア開発が加速して、ソフトウェアの提供とデジタルエクスペリエンスの品質が向上します。そして、その次のステップが、そこにセキュリティを統合したDevSecOpsです。DevSecOpsでは、3つの分野で目標と測定基準、ツールとプラクティスを共有することで、それまでサイロ化していた3つのグループ間の摩擦を減らし、フローを1つに統合します。これにより、セキュリティの自動化が可能となり、開発プロセスの初期の段階からセキュリティを組み入れることができるようになります。

組織がこの大きな発想の転換を受け入れる準備がまだできていなかったとしても、この2年間の得難い経験は、ITとビジネスのあらゆるステージでセキュリティを統合するという考え方の重要性を提唱する根拠となるでしょう。

結局のところ、2022年、さらにはその先がどのようになっていくのかは誰にもわかりません。

セキュリティトレンドに関する詳細なインサイトと、世界のセキュリティリーダーのベストプラクティスについては、無料の「セキュリティの現状」レポートをご覧ください。

レポートをダウンロード



21-22064-Splunk-4 Lessons of Security Leaders for 2022-LS-JA-202203

splunk> turn data into doing®