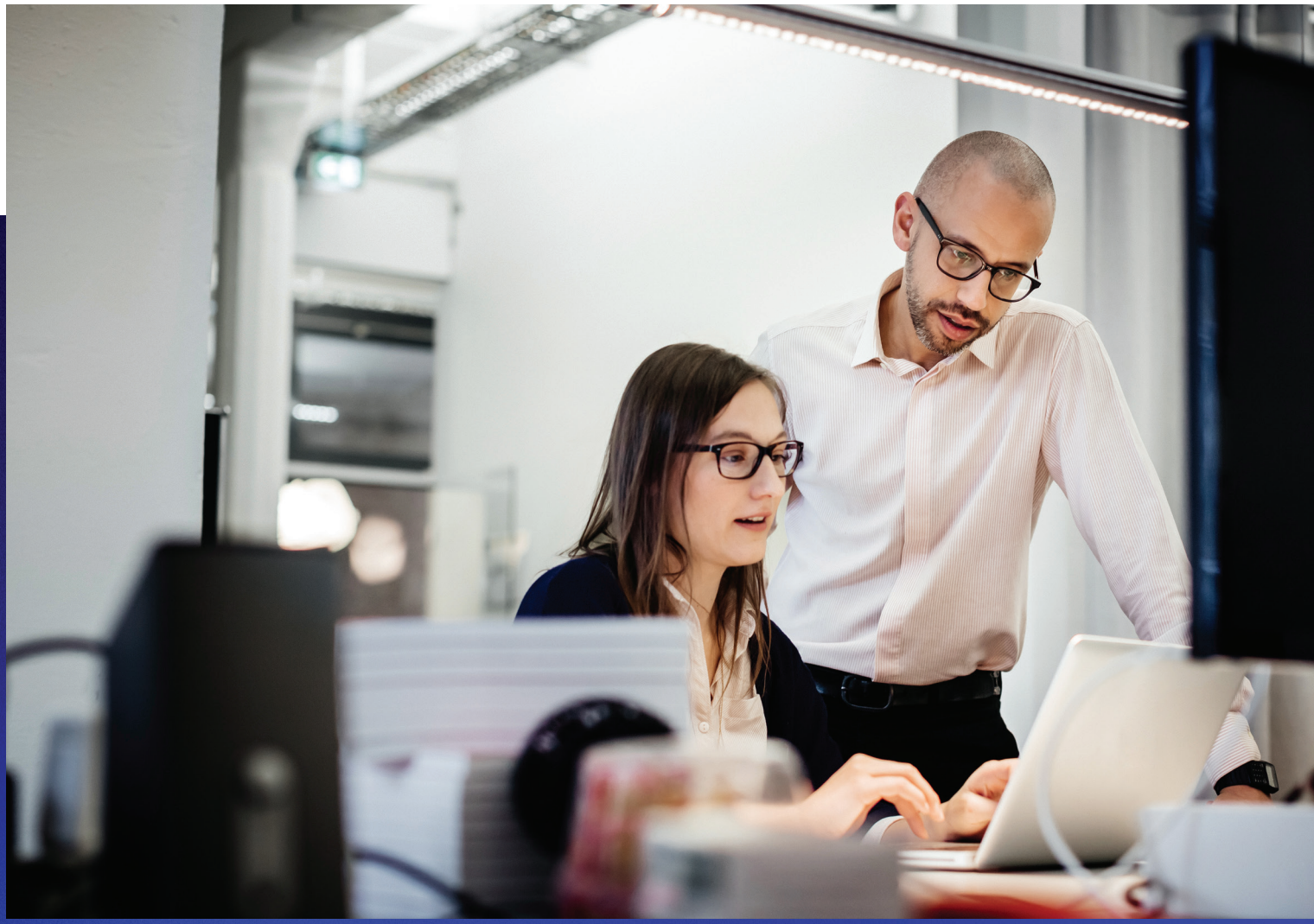
Secureworks®

ホワイトペーパー

IT 運用におけるセキュリティアラート対応疲れの解消

XDR はサイバーセキュリティのアラートノイズを
適切に管理し、間違いのない防御運用を実現します



セキュリティチームは、日々膨大な量のアラートログを管理する必要があります。この作業は、個々のアナリストはもちろんのこと、どのチームにとっても圧倒される作業量となり得ます。最近の調査では、SOC チームの70% がIT 運用においてセキュリティ脅威アラートへの対応作業に心理的圧迫感を感じていることが示されており、半数以上が膨大な量のアラートに正しい優先順位を付けて対応する自信がないと回答しています[1]。増大するアラートノイズにより、その対応優先順位付けは難しくなり、真の脅威や潜在的な侵害を見逃すリスクは増大します。Forrester の最近の調査では、攻撃がより頻繁に発生している昨今の状況下で、セキュリティチームはインシデント対応に対して大幅に人員不足であることが明らかになっています[2]。

70%

のSOC チームは、膨大な量のセキュリティ脅威アラートの対応作業に心理的圧迫を感じています。

サイバーセキュリティの脅威は引き続き進化を続けており、その攻撃対象は拡大しています。アラートノイズを分類しそこから実際の脅威を見つけ出さなければならないセキュリティチームにとって、これは何を意味するのでしょうか。セキュリティ運用環境がどのように変化してきているかを理解することが、この課題に対処するための最初のステップなのです。

過去を振り返って

セキュリティ業界がここまで来た道のりを整理し、これからどこに向かうのかを理解するためには、歴史的な観点でそれを振り返って検討する必要があります。20 年ほど前、セキュリティ業界には、パケットフィルタリング用の標準ファイアウォール、ディープパケットインスペクション用のスニフィングIDS、従来型のAV アラート、およびサーバログがありました。これらはすべてセキュリティ情報およびイベント管理（SIEM）システムに転送され、リアルタイムで分析されていました。問題は、業界が成長する中で、SIEM プロバイダはさらに多種多様なデータソースをシステムに取り込もうとしてきたことでした。その結果、次世代ファイアウォール、侵入防御システム（IPS）、電子メールセキュリティゲートウェイ、ルータ、スイッチ、ロードバランサ、エンドポイント検出と応答（EDR）などが全て一緒にシステムに追加されました。これらのデータ追加と統合は意図的に行われたものでしたが、それは結果として増加するログノイズとアラートの増加につながりました。時間の経過とともに関連するログとアラートの数は指数関数的に増加し、アナリストが対応できる量を超えていきました。

アラートノイズが増加する背景

今日、セキュリティ環境のアラートノイズ量はますます大きくなってきており、これは内部と外部の両方の要因によるものです。

内部的には考慮すべき問題がいくつかあります。まず、攻撃対象の領域が大きくなりそのテクノロジー範囲が拡大すると、それに応じてアラートの数が増加します。従業員数の増加だけでなく、それぞれの従業員が使用するデバイス数の増加により攻撃対象となる領域は拡大し、すなわち組織が監視しなければならないエンドポイント数が増加します。さらに、デバイスの数、デバイスの種類、また個々のデバイスに行われるカスタマイゼーション、これらはすべてセキュリティチームが対応しなければならないアラートの量に影響を与えます。

拡大し続ける攻撃対象と拡張する防御境界は、必要なセキュリティ制御の種類と数を増加させてきました。これらの新しいセキュリティ制御はこの業界を進化させていくうえで必要なものでしたが、同時にアラートの増加を引き起こしました。また、アナリストが1つのインシデントを調査するために複数の異なるプラットフォームやツールを使用する必要がでてきました。

近年のモノのインターネット(IoT)の爆発的な増加もあり、攻撃対象の領域が拡大するペースが衰える兆候はありません。また、従業員バッジ、在庫トラッカー、バーコードなど、企業が利用するさまざまな「スマート」ソリューションにより、その攻撃対象はさらに拡大すると思われます。IoT テクノロジーを使用している企業の数は、2014 年から2019 年にかけて13% から25% に増加しました[3]。さらに最近の予測では、2025 年までに416 億台のIoT デバイスが接続され、そこから79.4 ゼタバイトのデータ[4] が生成されると予測されています。攻撃対象の領域拡大に加えて、クラウド利用の拡大もセキュリティチームへ流入するアラートノイズ量と対応の複雑さに影響を与えています。多くの組織ではクラウド導入が急速に進み、その関連ノイズが増加しています。COVID-19 パンデミックの中で、企業はオンプレミスのネットワークからMicrosoft Teams、Zoom、WebEx などのクラウドネイティブアプリケーションを使用するようになりました。これらのプラットフォームが追加されることによりセキュリティ運用がさらに複雑になったことは間違いありません。企業はデータ転送と保存方法について、さらに多くの課題と向き合わなければならなくなりました。以前は一枚の紙やうわさ話による会話が、今ではそれらがデジタルファイルになっているのです。

さらに複雑なことに、業界にはSIEM について「何であれログとして生成されるものは、それをすべてSIEM に取り込む」という共通の考え方が形成されてきました。クラウド環境では大量のログが生成されます。しかしながら、それらすべてのログ情報がセキュリティ運用の観点から重要であるわけではありません。

たとえば、ある組織ではクラウドネイティブサービスを使用してソフトウェア開発のライフサイクル全体を運用管理したいと考えています。従来のSIEM ではこのタイプのアクティビティはモニターされませんでしたが、クラウドネイティブサービスの進化にともない、たとえ最終的にはセキュリティアラートとしての価値がほとんどない場合でも、クライアントはSIEM ベンダーに対してこれらのログも取り込んでその内容を提供することを期待するようになりました。その結果、組織にはアラート対応疲れを避けるための戦略を再検討する必要がでてきたのです。監視可能な情報はすべて監視するという従来の考え方は再検討する必要が出てきました。

また、IT エコシステム内のノイズ量に影響を与えている外部要因もあります。セキュリティ脅威の状況が変化する中で、特定の企業に新たな脆弱性が生まれている可能性があるのです。たとえば、アクティブフィッシングやマルウェア攻撃は金融や製薬などの特定業種を標的にしている可能性があり、COVID-19 パンデミック下で認識されたように、セキュリティ脅威の主体はその時々の状況下での懸念や不確実性を悪用することに重点を置いています[5]。これらすべてが、セキュリティチームのアラートの追加につながっているのです。

アラート対応疲れにより引き起こされること

日常よりアラートノイズの多い環境で業務を行っているIT チームは、しばしばアラート対応への疲労やアラート分析への麻痺に直面します。アラート対応疲れとは、対応必要のない誤検知アラートが大量に繰り返し発生する状況、またSIEM が脅威の真偽を判断できず、アナリストがそれらを都度マニュアルで確認しなければならないような状況と言えます。ESGによる調査は、日々発生するアラートのうち45%が最終的には誤検知であると判断されたことを明らかにしています[6]。またこの調査では、回答者の75%が、組織が真の攻撃への対

41.6 億台

2025 までに 416 億台の接続された IoT デバイスが 79.4ZB のデータを生成します。

75%

の組織は、真の攻撃への対応時間と同等の、また場合によってはさらに多くの時間を誤検知アラートの対応に費やしていると回答しています。

応時間と同等の、また場合によってはさらに多くの時間を誤検知アラートの対応に費やしていると述べています[6]。また、ノイズが大量に流入すると、アナリストが使用ツールをオフにしてしまうことがしばしば発生します。

間違いなく、アナリストにとって、アラート追跡は「回転椅子」での対応、すなわち単一アラートに対して複数のセキュリティコンソールを切り替えての対応となっています。このようなワークフローではアナリストがその業務に燃え尽きる可能性があるだけではなく、多くの場合には対応すべき真の脅威アラートを見逃したり無視したりする結果となります。

アラート対応疲れにより引き起こされる問題を具体的に理解するために、実際に発生した一つの標的型侵害インシデントを参考とすることができます。顧客4,000 万人のクレジットカード情報を危険にさらし注目を集めたある実際のインシデントでは、同社のマルウェア検出ツールは実際にその脅威を検出し、そのアラートを送信していました。しかしながら、セキュリティチームは日々大量に発生するアラートに慣れてしまっており、また高頻度で誤検知アラートを受信していたために、その重要なアラートを無視してしまいました。その結果、その小売り大手企業は合計で3 億ドル近くの対応費用を被ることになりました[7]。

XDR によるアラートノイズの除去

セキュリティチームの運用において、真のアラートとその必要のないノイズが正確に区別できるように、どのようなアクションが取られているでしょうか。今日のセキュリティ業界では、そのようなアラート対応疲れを最小限に抑えて、脅威への対応アクションの効率を最適化する取り組みが進んでいます。

ユーザーSOC 運用やマネージドセキュリティサービス提供の観点から、またEDR（エンドポイント検出および応答）開発の観点から、セキュリティベンダーは新しい拡張された検出および応答（XDR）プラットフォームの構築に注力しています。XDR プラットフォームはIT およびビジネスインフラの包括的なセキュリティ管理ツールです（クラウド、ネットワーク、エンドポイント、およびビジネスアプリケーション全てを対象とします）。XDR は早期予防に基づくフレームワークによりセキュリティ攻撃と脅威を阻止することを目的としており、攻撃が発生した場合には組織に与える影響を最小限に抑えることができます。

XDR はセキュリティ運用スタッフの有効性と作業効率性を向上させることを目的とした専用ツールです。セキュリティアナリストやオペレータが直面している課題に対処するため、企業ネットワークで使用されることが多い平均45 種類のセキュリティツールの情報を統合することで、すべてのアラート調査を1 つのツール上に集約することができるのです。その結果、セキュリティ運用の複雑さが大きく改善されます。

ある調査によると、セキュリティ侵害のうち平均80% が新規または未知の「ゼロデイ攻撃」であることが示されています[8]。これらの高度な攻撃手法と脅威に対抗するために、XDR は強力なAIベースの検出とセキュリティ分析機能を持ち、それらを最新の脅威インテリジェンスと組み合わせることで、これまで困難と思われた高度に効果的で効率的な脅威対応を実現します。

また、XDR はセキュリティ監視データを選択的に呼び出して関連付け、その情報をアラート検証と優先順位付けに使用することで、膨大な量のアラートノイズと誤検出の問題を解決します。これにより、セキュリティアナリストと運用部門は、IT エコシステム内で発生する真の攻撃に対応の焦点を当てることができます。

フルXDR ソリューションの機能

IT 運用環境において、セキュリティ脅威の予防、検出、対応を一つに統合するためのXDR プラットフォームには多くの機能が求められます。そこでは、以下の機能が不可欠なものと考えられます。

- **相関** – 既存システムの関連するセキュリティデータを参照分析します。
- **検出** – 既知および未知の脅威を検出し、自動的に環境全体を様々な脅威から保護します。
- **データ補完と強化** – 関連するユーザーやアセット情報を付加することにより、対応判断を迅速化します。
- **マッピング** – 脅威とアラートをMITRE ATT &CK フレームワークにマッピングし、攻撃を停止させたキルチェーン内のポイントを明確にします。
- **協調サポート** – "Do it yourself" XDR ではなく必要に応じてセキュリティ専門家により提供される迅速なサポートが利用可能です。
- **自動化** – 脅威の封じ込めと防止のための自動対応。(これを人間が実施すると、対応が遅すぎてしまいます)。
- **インテリジェンス** – 外部の脅威対応インテリジェンス、また他のXDR プラットフォームユーザーからの情報が収集され提供されます。
- **フォーカス** – XDR は、アラートを詳細に検証する機能を提供し、誤検知でなく対応が必要な真のアラートをセキュリティオペレーターに示します。

XDR は脅威を迅速かつ正確に検出し、攻撃を遮って後の調査に必要となるコンテキストを提供するように設計されています。検出機能は攻撃対象領域全体をカバーし、また攻撃防御の仕組みをバイパスするような脅威も検出します。(注 :今日では多くの攻撃は、防御のための検出制御を回避するように設計され、テストされています。) また、XDR は脅威についての詳細な調査情報とあらゆる観点から攻撃対処するために必要な情報を提供します。

効果的で効率的なXDR ソリューションは、セキュリティ運用を活性化し、攻撃を阻止し、システムとユーザーのダウンタイムを最小限に抑え (例えばランサムウェア攻撃)、インシデント対応のワークロードを最小限に抑えることができます。

将来を見据えて

サイバー脅威が進化するなかで、企業の防御境界はますます不明確なものになり、攻撃対象となる領域は拡大し続けています。今日、圧倒的な量のアラートノイズが存在することは明白であり、セキュリティリーダーは新しいアプローチによってそれに対応する必要があります。詰まるところ、旧来型のSOC SIM/SIEMアプローチは、クラウド、ネットワーク、そしてエンドポイントのITインフラストラクチャを広くカバーするXDR：拡張されたセキュリティ検出、防御、およびインシデント対応のための単一ソリューションとして考慮された設計はなされていませんでした。

今でも多くの組織が「ログの量は多ければ多いほど良い」という考えにあり、XDR 導入への意思決定には時間がかかります。市場で入手可能な数多くのツールや製品からはさらに多くの情報が取り込まれ、状況を悪化させる一つの要因となっています。また、コンプライアンスの要件は“ログ”ビッグデータの問題を生じさせてその運用コストは大幅に増加し、コンプライアンスログやそこから生成されるアラートにはセキュリティとの関連性が無いものばかりであるという誤った考え方を生みだしています。ログの量を削減し調整しすぎると、調査対応する必要のあるものまで削除してしまう可能性があります。一方で、それを十分に削除し調整しなければ、アラートノイズと誤検知の海に溺れてしまうという問題に立ち戻ってしまいます。適切なバランスによりこの両方のリスクを管理することは、今すべての組織にとっての最優先事項となっています。XDR は、ほとんど使われることのない情報のデータレイクを生成するのではなく、必要なログ情報を選択的に使用し脅威に迅速に対応する環境を提供します。

セキュリティリーダーは、集中し、脅威から組織を保護するための最も効率的な方法を見つけ出せるようにするため、セキュリティ運用の戦略を緊急に再評価する必要があります。主にビジネス観点からセキュリティ優先順位に焦点を当てる内部チームに加えて、インシデント対応やフルマネージドXDR などの外部のセキュリティ専門リソースを組み合わせたハイブリッドXDR 運用モデルは、この課題に対する有望な実装可能オプションと考えられます。

Forrester が明確に指摘しているように[2]、XDR はIT 環境全体においてセキュリティツールとビジネスツールの両方から集められたテレメトリ情報を統合し、サイバー脅威に対応するためのよりシンプルで効果的な手段をセキュリティチームに提供します。また、XDR によりクラウド上に構築されたビッグデータインフラストラクチャ、機械学習機能、高度なセキュリティ分析を利用することにより、さらなる柔軟性とスケーラビリティ、そして運用自動化の機会が得られます。さらに、分析機能とサードパーティツールとの統合機能は、ビジネスのすべての領域を通してセキュリティの可視性と制御を可能とし、また脅威と関連性のないノイズを排除することで、今日の拡大するサイバー脅威の環境下で企業や組織が必要とする堅牢なサイバー防御を実現します。

Sources:

[1] Trend Micro, A global study: Security Operations on the backfoot

[2] Forrester, Adapt or Die: XDR is on a Collision Course with SIEM and SOAR

[3] McKinsey, Growing opportunities in the Internet of Things

[4] IDC, Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023

[5] DHS, CISA, NCSC, COVID-19 Exploited by Malicious Cyber Actors

[6] ESG, Reaching the Tipping Point of Web Application and API Security

[7] Infosecurity Magazine, Target Sues Insurer Over Data Breach Costs

[8] Ponemon-Sullivan Privacy Report, The state of endpoint security risk

Secureworks®

SecureWorks®（NASDAQ：SCWX）は、20年以上にわたり実環境で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たクラウトネイティブのセキュリティ分析プラットフォームSecureworks®Taegis™により、高度な脅威の検知、合理化された協調モデルによる調査、また脅威に対する適切なアクションを自動的に実施する能力を強化し、お客様のビジネス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。

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2−1
Otemachi One タワー17階
+81-3-4400-9373
www.secureworks.jp