Secureworks®

ホワイトペーパー

XDRとSIEMの比較：サイバーセキュリティリーダー向けガイド

サイバーセキュリティ脅威の激化に伴い、SecOpsチームが防御すべきデジタル環境は大規模化し、また複雑化の一途をたどっており、従来型の境界線防御はほぼ破綻したといっても過言ではありません。サイバーセキュリティベンダー各社はこうした状況に立ち向かうべく、次世代ソフトウェアおよびサービスソリューションの展開を進めています。

なかでも2022年に入ってセキュリティ業界を大きく席巻しているのが、これまでにない新たなカテゴリのソリューション「Extended Detection and Response（通称XDR）」です。

XDRは企業・組織のIT環境全体のセキュリティデータを集約するという観点から、「単なるSIEM*進化版に過ぎない」という印象を持たれるかもしれません（*Security Information and Event Management：セキュリティ情報および関連イベントを管理するソリューション）。しかし実際には、XDRは従来型SIEMを大幅に上回る機能を備えており、企業・組織のIT環境全体の可視性、セキュリティ監視実務における脅威情報の調査能力、脅威への対応アクションを向上させる具体的な価値を提供します。

業務量および精度の低いアラートの増加によりSecOpsチームの対応業務量への重圧が高まっているだけでなく、専門的な業務をカバーできるSecOps人材が不足しているという難題もあります。こうした状況下で、XDRとSIEMの大きな違いを検証し、把握しておくことはサイバーセキュリティリーダーの責務だと言えるでしょう。

このガイドでは、XDRとSIEMの主な違いを解説します。

SIEMの定義

「SIEM」という頭字語は2005年にGartner社が提唱した概念[1]ですが、根幹となる機能はそれ以前から存在していました。すでに1990年代から、先見の明をもった組織は「セキュリティ脅威情報の分析を効率化し、またコンプライアンス要件を充足するには、分散しているセキュリティログを単一のシステムに集約すべきだ」と認識していたのです。

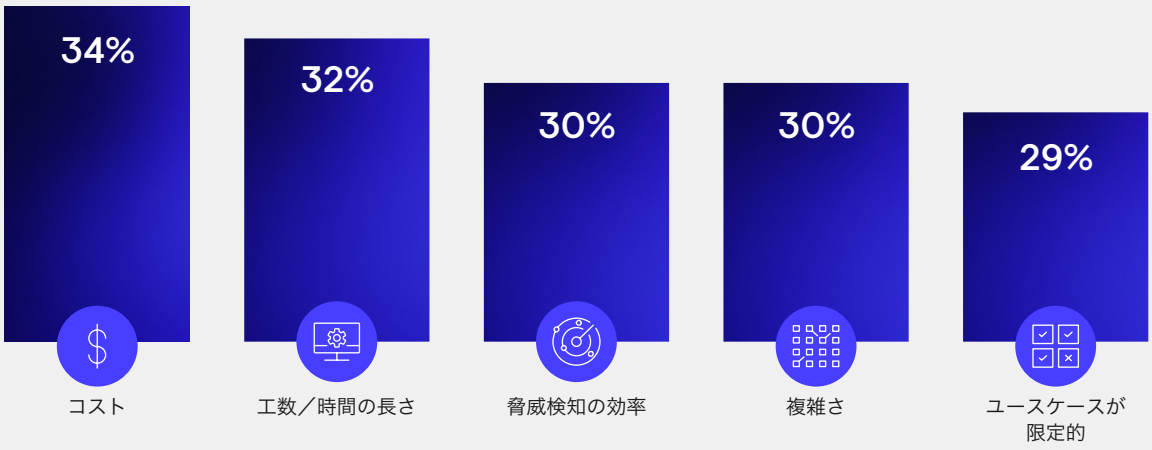
[1]Gartner社の調査レポート「Innovation Insight for Extended Detection and Response」

SIEMソリューションの仕様は製品ごとに異なりますが、基本的にどの製品も以下のような属性を備えています。

- **ログデータの集約：**企業・組織のIT環境全体で収集した監視データを一元化し、SecOpsチームに提供。
- **データ保管の一元化：**フォレンジック分析やコンプライアンス対応に必要な過去データの記録を一般的な保管期間に従って保持すると同時に、分散ログのキャッシュをなるべく頻繁に消去。
- **システム横断的なデータクエリ：**対象環境で進行中かつ未発見の脅威をSecOpsスタッフが特定しやすいよう、セキュリティログやアラートの調査を支援。
- **ダッシュボードとレポート：**SecOpsチームが随時行う対象環境の監視、監査要件の充足、外部関係者（MSSPなど）へのデータ提供時に活用。

一部のSIEMソリューションにはデータ分析・操作ツールも搭載されているため、SecOpsスタッフによる関連イベントの相関付け、ノイズ／シグナル比率の改善を目的としたフィルターの適用、フォレンジック調査の支援などにも役立ちます。

SIEMを利用する組織から見た「SIEM利用に関する最大の難点」（ESG[2]による調査）



これまでSIEM技術を使った製品には、自組織内で収集中のアラート／監視データを、最新の脅威インテリジェンスによって確認されている実攻撃グループの振る舞い情報と相関付けする機能が搭載されていませんでした。脅威インテリジェンスが組み込まれていないだけでなく、進行中の脅威をSecOpsスタッフが特定し、対応・修復する際の指針となるセキュリティワークフローも内蔵されていません。

[2]ESG社による調査レポート「The Impact of XDR in the Modern SOC」

セキュリティ脅威のリスクを効果的に緩和するにはキルチェーンプロセスをエンドツーエンドで網羅する必要がありますが、全社的な情報をすべてSIEMに一元化している組織の場合には、このプロセスが途切れてしまう恐れがあります。複数のセキュリティツールを組み合わせても侵害を100%防御することはできません。SIEMを利用している組織が攻撃グループに長時間隠密に作業できる隙を与えてしまい、その結果甚大な被害につながりかねない状況が発生した場合でも、すでに疲弊しているSecOpsチームの稼働時間・工数・スキルだけを頼りに対処しなければならなくなる可能性があります。セキュリティ管理の観点においてこれは最悪のシナリオです。

XDRの定義

XDRという用語は、次世代のセキュリティソリューションを表す概念として2018年に誕生しました[3]。Gartner社はXDRを「複数のセキュリティ製品をネイティブに連携し、統合的なセキュリティオペレーションシステムを実現する脅威検知・インシデント対応ツール[1]」と定義しています。

以下は、XDRに分類されるソリューション特有の主な属性です。

- **高効率な監視データの集約：**複数のエンドポイント、サーバー、ネットワーク、クラウド、メール、アプリケーションにまたがる監視データの集約。対象環境内のファイアウォール、侵入検知・防御システム、各種セキュリティ統制システムのデータについても横断的に集約できることが可能。
- **脅威インテリジェンスに照らし合わせたデータ分析および相関付け：**振る舞いについての収集データをもとに、対象環境内で悪意に基づく活動が疑われるケースをあぶり出して特定。
- **機械学習およびヒューマン・インテリジェンスによる知見の継続的活用：**脅威検知の感度・精度を継続的に改善。
- **効果的なインシデント調査・対応を支援するネイティブ機能：**内蔵型のセキュリティ調査ワークフローも提供。
- **脅威特化型ガイダンスへの一元的アクセス：**修復・回復時やアクティブディフェンス対策の強化に役立つ。
- **完全な自動化／自動化によるアシスタンス：**最新のリサーチやベストプラクティスをもとに、脅威に特化した「修復プレイブック」と修復アクションを提供。

[3]Forrester社のブログ記事「XDR Defined: Giving Meaning to Extended Detection and Response」

XDRはまた、2つの重要な側面において従来型EDR（Endpoint Detection and Response）製品より優れています。

1. EDRが収集するエンドポイントの監視データのみならず、XDRではこれまでSIEM経由でしか集約できなかったネットワーク、クラウド、アイデンティティシステム、メール、その他のシステムから収集した監視データを集約。

2. EDRによるリアクティブな（既知の情報にもとづく）マルウェア検知手法やアンチウィルス機能にとどまらず、XDRではプロアクティブな（先手を打った）手法でマルウェアを検知し、進化を続ける高度な脅威（特に、組織のエンドポイント／境界線防御を突破した脅威）に対するキルチェーンプロセスをスピードアップ。

XDRとSIEMの違い

前述のように、SIEMとXDRには機能差および利用目的の点で明らかな違いがあります。またXDRが登場したことで、SIEMの限界が浮き彫りになりました。SIEMを使用すべき状況もありますが、堅牢なセキュリティは実現できません。下表は、両者の違いをわかりやすく比較したものです。

説明	XDR	SIEM
様々なソースから収集した監視データやセキュリティ関連データを集約するオープンプラットフォーム	✓	製品によって異なる
複雑なログの保管やガバナンス・リスク管理・コンプライアンス（GRC）に対応するユースケース	✗	✓
コンプライアンスおよび監査に必要なデータの長期保管	製品によって異なる	✓
振る舞いデータを脅威インテリジェンスと相関付けした、高度な脅威検知・特定能力	✓	✗
機械学習と日々導き出されるヒューマンインテリジェンスを併用し、脅威検知・特定の仕組みを継続的に改善・更新	✓	✗
SecOpsチームと外部パートナーが緊急時のキルチェーンおよび修復プロセスを迅速に実行できるよう、インシデント調査における両者の連携作業を促進	✓	✗
自動アクションおよび実証済プレイブックで、SecOps部門によるセキュリティ課題の対応・修復を迅速化・効率化	✓	アドオンが必要
ライセンスの算定基準	カバー範囲	データ量

多額の予算を投じてSIEMを導入した組織（特に、データ保護に関して厳格な規制を受ける金融業界やヘルスケア業界などの組織）は前述の比較を理解したうえで、コンプライアンスや監査目的でSIEMを使い続けても良いでしょう。

一方でXDRは、攻撃対象領域が拡大し、セキュリティの境界線が消滅しつつある新時代のサイバーセキュリティリスクを緩和する最強プラットフォームです。なかでもSecOpsの社内リソースが乏しく、外部のインテリジェンスやサイバーセキュリティサービスに大きく依存する組織にとっては強い味方となります。

SIEMに大きな投資を行っていない組織、またサイバーセキュリティ予算の再編／配分見直し戦略の一環として現行SIEMを廃止予定の組織にとって、XDRは「SecOps業務の基幹プラットフォーム」および「コンプライアンス／監査報告に必要なデータの一元リポジトリ」という二つの役割を同時に果たせる可能性があります。XDRを使えば、SIEMの現行プラットフォームを維持管理するための継続投資も必要ありません。

XDRとSIEMを比較するうえで、他にも着目すべきポイントが3つあります。

1. SIEMのライセンスは通常、データ量によって決まるため、**多層防御などの優れたサイバーセキュリティプラクティスを取り入れる場合、ライセンスコストは増大するという経済的ペナルティが生じます。**組織の環境が拡大・多様化し、保管対象の過去データの量が増えるにつれ、このコスト負担は経年的に肥大化していく可能性があります。また、SIEMは導入コストが高く、継続的なチューニングや保守の手間がかかるほか、オプショナルなライセンスコストも必要になります。ITシステムの意思決定者は、こうした長期的ライセンスコストを考慮したうえで予算を適正に配分し、費用対効果の最適化を図る必要があります。

2. サイバーセキュリティは主に「個々の組織内において実践するもの」という捉え方もありますが、実際はその逆です。サイバーセキュリティとは本来、集合体による取り組みです。自組織での対策が失敗すると、関わりのある外部組織すべてが脆弱化してしまいますが、奏功するとこれらの組織すべてを保護することができます。同様に、脅威インテリジェンスも本質的には集合体レベルの取り組みです。なぜなら、当該インテリジェンスの質は「既知の情報を共有できる範囲」によって大きく左右されるからです。

3. セキュリティ全般の観点から見ると、SIEMはXDRとは全く異なるエコシステムを形成しています。SIEMには「孤立した島」のような隔離効果がありますが、その守備範囲のすぐ外側には無数のセキュリティリスクが存在します。一方、相互接続システムとして機能するXDRを使うと、リスクの波及やコストの増大を招くことなく、対象環境のあらゆる側面で脅威インテリジェンスのメリットを享受できます。

XDRの本質は、脅威インテリジェンスの集合知の利用とそこへの貢献を容易にし、また脅威の調査・対応における真のコラボレーション環境を提供することにより「集団的サイバー防衛」を促進します。XDRを利用する組織と接点を持つあらゆる組織が危険に晒されないようリスクを軽減する、という簡単な役割もこの点で役立ちます。

対称的にSIEMは、セキュリティ調査・対応ではなくログ管理を目的に開発された自己完結型・非公開型であるという特性を備えています。そのため、集団的サイバー防衛への貢献度はXDRに比べてはるかに劣ります。

なぜ今、XDRとSIEMの違いを理解することが重要なのか

XDRは市場で大きな注目を集めていますが、組織は以下のような新たな現実にも直面しています。だからこそ、XDRとSIEMの違いを明確に理解しておくことが重要なのです。

- ますます**激化・巧妙化するサイバー攻撃**
- IaaSクラウドが混在し、利用するSaaSアプリの数が増加しているような組織では特に、SecOpsチームの保護対象**環境が拡大・複雑化**の一途をたどっている（結局、最終責任を負うのはSecOpsチーム）
- **サイバーセキュリティ要員の**慢性的な人材不足による**勤続年数の短期化・離職率の上昇**
- 稼働中の現**SecOpsスタッフを常に維持**し、適正配置を保つための負担（良好な職場環境づくり、過労の防止など）
- **コンプライアンスチェック項目の充足にとどまらず**、データやシステムの安全性を維持する強固な防御態勢を確保しなければならないという日常的なプレッシャー
- コロナ禍および「場所に縛られない働き方」という就業方針がもたらした**リモートアクセス**の普及・定着
- **CXOレベルの経営幹部は**、セキュリティ侵害による自社業務、顧客リレーション、ブランド価値、株価への悪影響について懸念を深める一方で、SecOps部門が自由に使えるような予算は絶対に承認しないというジレンマ

つまり、サイバーセキュリティのニーズとリソースの均衡が崩れ、このままでは立ち行かなくなる、という分岐点を迎えているのです。

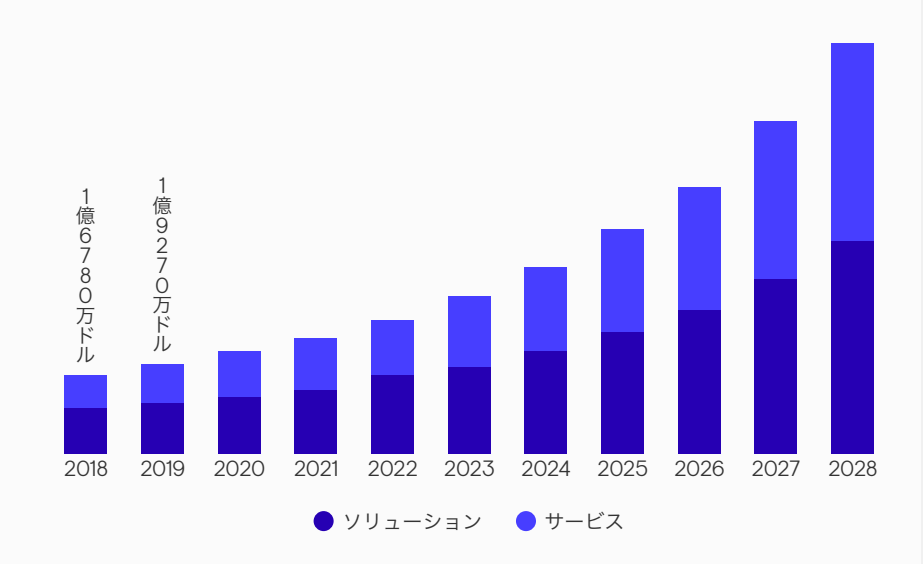
そのため、サイバーセキュリティリーダーは今後、難しい決断を迫られることになるでしょう。長期的に健全で安心な組織を実現するための意思決定に携わる人々は皆、XDRとSIEMのメリット・デメリット、および両者がSecOpsチームのリソース効率に与える影響を明確に理解しておく必要があります。

> セキュリティ情報およびイベントを管理するSIEMの技術が陳腐化し、効果が薄れつつあります。こうした状況のなか、カスタム検知機能を備えたセキュリティ分析プラットフォームをクラウド経由で配信できるか否かによってベンダーの優劣が決まるでしょう[4]。
>
> **FORRESTER**

> セキュリティスキルの格差拡大や攻撃者の動向に対応すべく、セキュリティオペレーション業務の生産性や検知精度を向上させるための拡張型検知・対応（XDR）ツール、機械学習（ML）、自動化機能が登場しています[5]。
>
> **GARTNER**

サイバーセキュリティの厳格化要求に伴い、XDRの採用も増加

XDR市場の年平均成長率は19.6%の見込み[6]



[4]The Forrester Wave: Security Analytics Platforms（2020年第4四半期版レポート）
[5]Top Security and Risk Management Trends（2020年6月版）
[6]XDR Market Size, Share & Trends Analysis（Grand View Research社が2021年4月に公表した調査）

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ド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