Microsoft Security

統合型の脅威対策に移行するべき 3 つの理由

目次

イントロダクション

現在、平均的な企業では 30 種類以上のセキュリティ ツールが使用されており、多くの場合ばらばらに後付けされています。

セキュリティは転換期を迎えています。組織が人材不足やコスト バランス調整からハイブリッド ワークのプレッシャーまでにわたる課題に対処し続ける中、サイバー攻撃はますます高度化しています。

一方、セキュリティ市場はこれまで以上に細分化され、複雑化しています。現在、平均的な企業では 30 種類以上の異なるセキュリティ ツールが使用されています。これらは多くの場合、ばらばらに後付けされているため、セキュリティ オペレーション センター (SOC) は可視性が乏しく、十分なインサイトを得られません。

セキュリティとコンプライアンスのリーダーは、最新のリスクと脅威についてより深く理解したいと思っていますが、何がうまくいっていて何がうまくいっていないのか、どこにギャップがあるのかを把握する必要もあります。

セキュリティの課題は、もはや大きすぎて手に負えないと感じるかもしれません。ですが、セキュリティ運用の効率を改善し、効果を高めるような、CISO が探し求める方法は必ず見つかります。その答えは、統合的なエンドツーエンドのアプローチでサイバー脅威からの保護を行うことです。これによって、組織は次のようなことを実現できます。

理由 1: より少ないリソースでより多くの成果を上げる

ポイント ソリューションを統合し、セキュリティ運用 (SecOps) のオーバーヘッドを削減することができます。

理由 2: SecOps が価値の高いタスクに集中できるようになる

効率性を高めるツールを活用して、経験の浅いアナリストにも、これまで以上に能力を発揮させることができます。

理由 3: 従業員の生産性の向上

従業員が恐れずに創造と革新を行えるような方法で、組織を保護することができます。

このアプローチは、拡張検出および応答 (XDR) ソリューションを、AI (人工知能) と自動化機能を使用するクラウドネイティブなセキュリティ情報およびイベント管理 (SIEM) システムに統合することによって実現します。この統合的なソリューションによって、SOC は企業全体の攻撃に対する予測性、先見性、防御性を高めることができます。

マイクロソフトの統合ソリューションにツールを集約することで、使用した分だけ料金を支払うことができ、節約にもなります。

理由 1

より少ないリソースでより多くの成果を上げる

多くの組織では、セキュリティ ツールの導入に際して、最善のポイント ソリューションに重点を置いて取り組んできました。残念ながら、このアプローチでは、セキュリティ担当者が迅速に脅威を特定して対応することが、むしろ困難になってしまう可能性があります。また、IT 支出やエンド ユーザーの生産性に悪影響を及ぼすおそれもあります。

より少ない負担でより多くの効果を上げたい企業にとって、マイクロソフトの SIEM や XDR などの統合されたアプローチは有効です。個々のツールを統合して、複雑さを軽減できます。また、クラウドネイティブな統合ソリューションは、パフォーマンスとスケールを向上させることもできます。

マイクロソフトの統合ソリューションにツールを集約することで、使用した分だけ料金を支払うことができ、節約にもなります。また、自動化と統合を進めることで、ソリューションの管理に必要な SecOps のオーバーヘッドを削減することもできます。

> ギャップが大きくなることが予想されるため、新しいセキュリティ ツールの導入プロセスを開始するのは簡単です。そこから進んでいくうちに、さまざまなベンダーのツールを使えば、その役割が重複する可能性があることにすぐに気づきます。このような重複は、抑制と均衡の観点からは望ましいかもしれませんが、**多額の金銭的コストを伴う可能性があります**”
>
> MITA、最高技術責任者、
> **Jonathan Cassar 氏**

160 万ドル

ベンダーの統合によって実現した年間節約額

マイクロソフトは Forrester Consulting に委託して Total Economic Impact ™ (TEI) 調査を実施し、マイクロソフトの SIEM と XDR を展開することで企業が実現できる投資利益率 (ROI) を検証しました。以下は、総従業員数 8,000 名、セキュリティ担当者 10 名の架空の複合組織を対象にした主な検証結果です。

- **ベンダーの集約によって、年間約 160 万ドルの節約を実現。**マイクロソフトの SIEM と XDR に投資することで、この複合組織は以前の SIEM (56 万ドル)、関連するオンプレミス インフラ (36 万ドル以上)、3 つの XDR ポイント ソリューション (19.2 万ドル)、これらを管理するための継続的な人件費 (48 万ドル) のコストを削減できます。

- **重大な侵害のリスクを 60% 削減。**調査と対応に関する対応ワークフローの効率化、セキュリティ対応の自動化の改善、すべてのコンピューティング環境を保護する能力の向上 (マルチクラウド保護など) により、この複合組織は侵害のリスクを低減し、年間 160 万ドルを節減できます。

- **207% の ROI を達成。**代表インタビューと財務分析によると、この複合組織は、3 年間で 1,768 万ドルの利益を実現し、一方コストは 576 万ドルと、1,192 万ドルの正味現在価値 (NPV) を実現していることがわかりました。

理由 2

SecOps が価値の高いタスクに集中できるようになる

SIEM と XDR を連携させることでアラートを関連付け、重要な脅威に優先して対応しながら、企業全体でアクションを調整することが非常に重要です。

SecOps チームは、分析しなければならないシグナルの量に圧倒されています。その中には、手動で検出して軽減することが不可能ではないにしても困難な、忠実度の低いシグナルが多数含まれています。脅威が増えるほど、過剰な負担を抱えた SOC はついていけなくなります。特に複数のポイントソリューションのデータを分析しようとする場合は大変です。人員を増やして問題を解決しようと考えるのは賢明とは言えません。高度なスキルを持つセキュリティ担当者は簡単には見つからないからです。

そのため、SIEM と XDR を統合してアラートを関連付け、最大の脅威を優先して、全社的にアクションを調整することが重要であり、脅威を事前に検出して修復するための高度な AI と自動化が必要です。

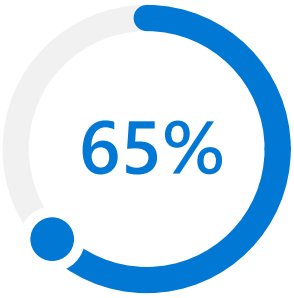
たとえば、単一の優先度の低いシグナルは、従来の SIEM であればあまり警戒されないことを考えてみましょう。しかし、AI を活用するクラウドネイティブな SIEM は、このシグナルを組織全体の他のソースから来たシグナルと自動的に比較し、複数のデータセットを相関させることで、多段階の攻撃を発見することができます。

SIEM と XDR の統合によって、SecOps のリソースを解放すると同時に、経験の浅いアナリストにも、より多くの能力と自信を持たせることができます。

その後、システムはデータの正規化、分析、関連付けによって、攻撃者によるインフラへの侵入方法や、サイバー攻撃拡大のタイムラインなど、コンテキスト情報を生成します。これにより SOC チームは、1 つのコンソールで侵害を可視化し、効果的に対処できます。

> 多くの CISO が、**20 種類のガラス窓を使うことでチームにかかるオーバーヘッド**、つまり、ポイント ソリューションとそれに関連する年間コストに気付いていません ... 私たちは 1 つのベンダーを利用することで、ツールにまつわる多くの疲労を解消することができました”
>
> Thycotic、最高情報セキュリティおよびプライバシー責任者、
> **Terence Jackson 氏**

セキュリティ ソリューションの価値を引き出すために、組織に深い専門知識が必要であってはなりません。SIEM と XDR の統合によって、SecOps のリソースを解放すると同時に、経験の浅いアナリストにも、より多くの能力と自信を持たせることができます。



マイクロソフトの SIEM と XDR の統合的なアプローチにより、脅威の調査にかかる時間が 65% 削減されました。

マイクロソフトの委託による Forrester Total Economic Impact ™ 調査では、その複合組織において、次のような SecOps の効率化が見られました。

- **脅威の調査にかかる時間を 65%、脅威への対応にかかる時間を 88% 短縮。**マイクロソフトの SIEM と XDR では、統合的なアプローチでセキュリティ脅威の調査と対応を行うため、これらのワークフローが複合組織のセキュリティ担当者にとってより効率的になります。脅威を特定するために複数のツールを駆使する必要がなくなり、同時にセキュリティ自動化機能によって対応ワークフローがさらに強化されます。

- **ワークブックの新規作成にかかる時間を 90%、新しいセキュリティ担当者のオンボーディングにかかる時間を 91% 削減。**マイクロソフトの SIEM と XDR の統合的なアプローチにより、セキュリティ担当者の追加ワークフローもさらに効率化されます。SIEM のログは一連のソリューションを通じて統合されているため、ワークブックの作成はほぼ自動で行われます。さらにログインが 1 つに統一されることで、新しいセキュリティ担当者のオンボーディングが約 16 週間早くなります。

理由 3

従業員の生産性の向上

SIEM と XDR の統合ソリューションによって、組織はエンド ユーザーの生産性を高めることができます。

SIEM と XDR の統合ソリューションは、より少ないリソースでより多くの効果をもたらし、SecOps の効率性を高めるのに加えて、エンド ユーザーの生産性を高めることができます。

SecOps チームも知っているように、セキュリティを厳しくすると、人々はそれを回避するようになります。したがって、エンド ユーザーのエクスペリエンスによって社員の生産性が高まるどころかむしろ阻害される場合、企業はより多くのセキュリティ リスクにさらされ、コストも増加する可能性があります。脆弱なパスワードや、パスワードの紛失、個人のデバイスを介した安全性の低いアクセス、機密データの自由な共有などは、その一例にすぎません。

> [以前は] 誰かが問題を疑った場合、単刀直入な方法で対応していました。色々なものをシャットダウンしてアクセスを遮断していたので、業務に悪影響を与えていました。一時的に仕事ができなくなるのですから、誰にでもわかることです。Microsoft Sentinel には、起きている問題に対して外科的に対応するためのメスが備わっています。**企業はたいてい、私たちが脅威に対応していることを知りさえしませんが**、これは私たちの成功の非常に重要な指標なのです”
>
> Wedgewood、最高情報責任者、
> **Rick Gehringer 氏**

約
68,000
マイクロソフトの SIEM と XDR によって、他の従業員の生産性が年間合計で約 68,000 時間向上しました。

SIEM と XDR の統合型アプローチにより、社員の日常のあらゆる場面で、生産性と安全性を両立させるシームレスなユーザー エクスペリエンスを提供することができます。サービスの停止や、マシンの分離と再イメージ化を行わなければならないなどの、生産性への悪影響を減らすことができます。また、SIEM と XDR の統合によって、セルフサービス セキュリティ サポートの増加、ダッシュボードとレポート作成の改善、応答性の向上、実行するセキュリティ エージェントの数が減ることによる起動時間の短縮など、エンド ユーザーの生産性を高める新たな機会が生まれる可能性もあります。

マイクロソフトの委託により実施された Forrester Total Economic Impact ™ (TEI) 調査では、総従業員数 8,000 名の架空の複合組織において、マイクロソフトの SIEM と XDR を展開したことにより、従業員の生産性が向上しました。

- **他の従業員の生産性が年間合計で約 68,000 時間向上。** マイクロソフトの SIEM と XDR は、非効率的なセキュリティ プロセスによる他の従業員への悪影響を防ぎます。たとえば、この複合組織では、IT 担当者がセキュリティ更新プログラムや推奨事項に関してセルフサービスを行うことができるようになることで、年間 4,000 時間を節約できます。また、従業員のマシン上でセキュリティベースのリモート トラブルシューティングを行えるようになり、実行するセキュリティ エージェントの数が減るため、エンド ユーザーの生産性を年間約 64,000 時間節約できます。

セキュリティは、技術的な成功を実現するために不可欠なものとなっています。そのため、組織には、最新の攻撃に対する回復力をできる限り高めるセキュリティ対策が必要です。それによって、成長の原動力となる生産性とイノベーションを守り、実現することができます。

SIEM と XDR を活用し、統合的なサイバー脅威対策を実現する

業界をリードする製品を統合することにより、サイバー脅威からの保護、検出、対応を単一の包括的なソリューションで実現します。

マイクロソフトが提供する最初で唯一の統合された SIEM および XDR ソリューションは、すべてのクラウドとプラットフォームにわたるエンドツーエンドの可視性をもたらします。業界をリードする製品を統合することにより、サイバー脅威からの保護、検出、対応を単一の包括的なソリューションで実現します。

マイクロソフトの SIEM と XDR は、AI と自動化のパワーはもちろん、サイバー脅威の検出と分析に向けた深く継続的な取り組みを反映しています。また、専門家のインサイトと毎日 43 兆のシグナルの可視化を提供します。これらの製品を統合することで、SOC チームはこれまで以上にコンテキストを持ち、重要なサイバー脅威をより迅速に解決できるようになります。

Microsoft Sentinel

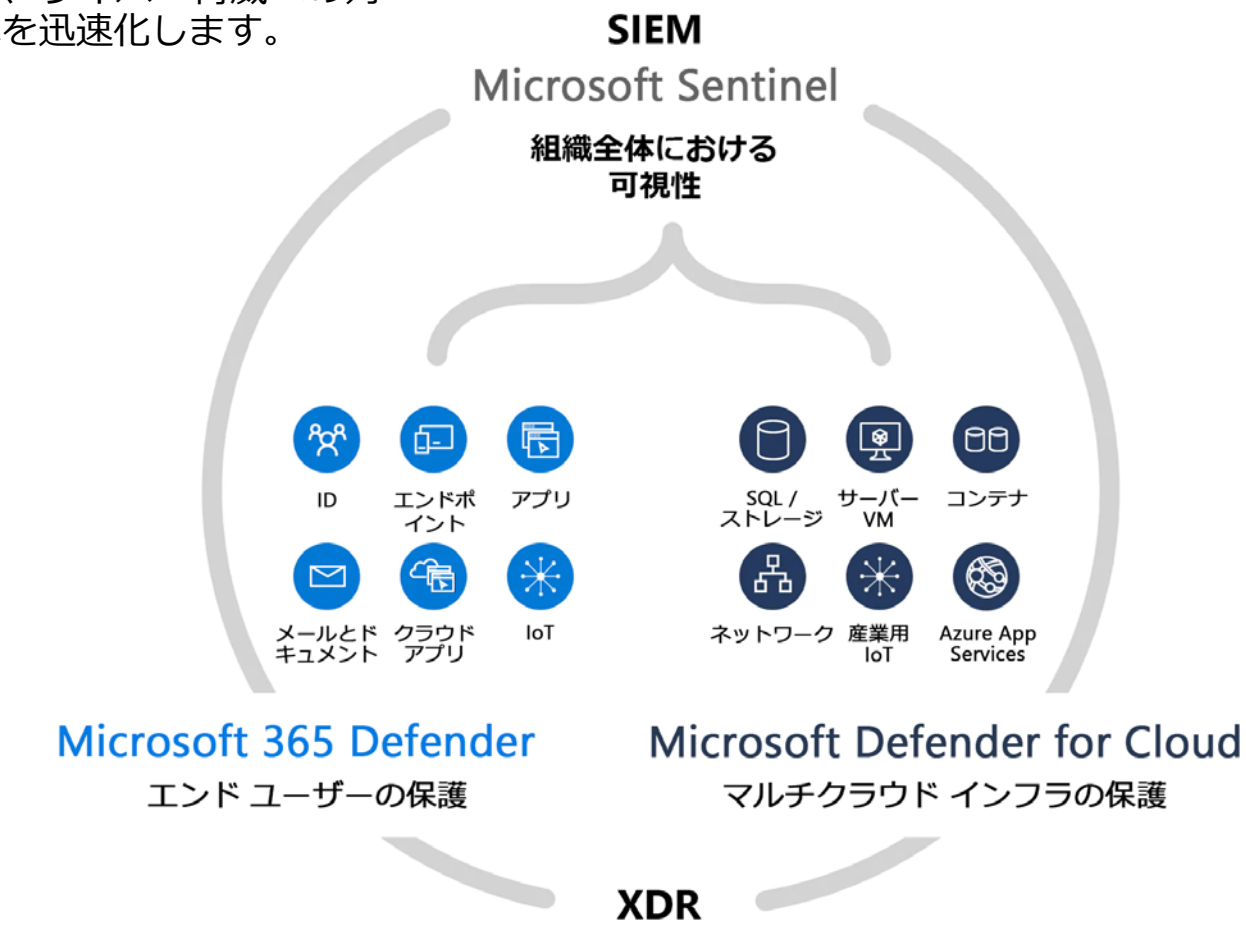
マイクロソフトのクラウドネイティブな SIEM では、企業全体を俯瞰することができます。搭載されたオーケストレーションと自動化の機能によって、事実上あらゆるソースからのセキュリティデータを集約し、AI を適用して正当なイベントとノイズを切り分け、複雑なサイバー攻撃チェーン間でアラートを関連付けて、サイバー脅威への対応を迅速化します。

Microsoft Defender XDR

XDR 機能を使用して、ID、エンドポイント、アプリ、メール、データ、クラウド アプリにわたるサイバー攻撃を防止・検出します。クラス最高レベルのすぐに使える保護機能で、サイバー攻撃の調査と対応を行います。単一のダッシュボードから、脅威を探して対応を簡単に調整できます。

Microsoft Defender for Cloud

搭載された XDR 機能を使用して、マルチクラウドとハイブリッド クラウドのワークロードを保護します。サーバー、ストレージ、データベース、コンテナなどを保護できます。アラートに優先順位付けをすることで、最も重要なものに集中できます。



セキュリティは後付けせず、組み込みましょう。

適切なツールとインテリジェンスを適切な人材に提供しましょう。エンドツーエンドのクラウドネイティブな統合ソリューションでは、最新の攻撃から防御することができます。

マイクロソフトの SIEM と XDR ソリューションによる、統合型のサイバー脅威対策に関する詳細情報 >

Microsoft Security