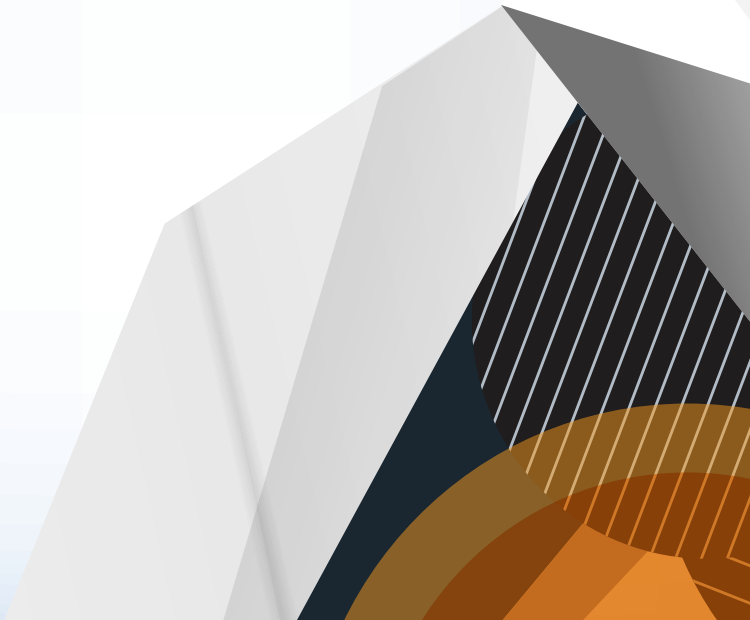
FIREEYE™

ホワイトペーパー

セキュリティ・オペレーションの主導権を握る

あらゆる組織で統合セキュリティを実現



セキュリティ・オペレーションを刷新する新たなアプローチ

新たな脅威が毎日のように出現する中、多くの企業は、セキュリティ関連の予算とリソースを増やして防御体制を強化するという賢明な決断を下しています。その理由は単純です。情報や資金、サービスなど、攻撃者が目を付けるような資産を保有する企業は、規模の大小にかかわらず、いずれ狙われることになるからです。しかし、強固なセキュリティ体制を構築するための負担は、決して小さくありません。特にリソースが限られる小規模企業にとっては深刻な問題です。小規模企業は、大規模企業とは比較にならないほどの少ない予算と人材で、大規模企業と同じレベルのリスクに対処しなければならないのです。

財政上の制約は別にしても、単に新しいアプライアンスやサブスクリプション・サービスを導入するだけでは、企業が望むような改善効果はほとんど得られません。単機能製品は、環境の複雑化、必要な人員の増加、手作業に伴うミスなどの発生原因になる上、導入が適切でない場合には、逆にリスクを増大させるケースさえあります。比較的新しい製品でも、このような喫緊のニーズへの対応は驚くほど進んでいません。

しかし、ご安心ください。今日では、強固なサイバー・セキュリティを実現する、より総合的なアプローチが登場しつつあります。

セキュリティ・オペレーション・プラットフォーム

セキュリティ・オペレーションにおける課題を解決する革新的な手段の1つが、セキュリティ・オペレーション・プラットフォームです。このプラットフォームは、セキュリティ・オペレーション・センター（SOC）において管制塔のような役割を果たします。セキュリティ・オペレーションを統合、自動化できるように設計されており、セキュリティ脅威の迅速な防御と運用コストの削減を実現します。ただし、セキュリティ・オペレーション・プラットフォームを名乗るすべてのソリューションが同様の機能を備えるわけではありません。

たとえば、セキュリティ・オペレーション・コンソールとしての役割転換が行われつつあるセキュリティ情報およびイベント管理（SIEM）ソリューションが実際に提供するのは、戦術的な機能に限られます。コンテキスト解析や自動化などの機能を備えていないため、大量のアラートを1か所に集約するだけに終わり、むしろSOCアナリストの手間を増やしかねません。

本ホワイトペーパーでは、セキュリティ・オペレーション・プラットフォームに必要不可欠な機能を検証し、ベンダーの選定時に考慮すべきポイントについて解説します。強固なセキュリティを実現するためには、優れたテクノロジー、プロセス、人材が欠かせません。セキュリティ・オペレーション・プラットフォームは、セキュリティ・オペレーション全体の統合を可能にします。そしてセキュリティ・オペレーションの統合は、コンピューター・ネットワークを大幅に効率化、簡素化し、セキュリティ向上という成果を組織にもたらします。

可視性

可視性とは、攻撃を検知して担当者に通知し、その影響を把握する組織の能力を指します。より具体的には、組織が直面している脅威を明確にし、最もリスクの大きい脅威を把握することです。効果的なセキュリティには可視性が欠かせません。インフラの死角は、深刻な問題の発生源になりかねないからです。

セキュリティ脅威トレンドは常に進化しているため、仮に万全の可視化を実現したとしても、ネットワークに新たな死角が生じることは十分にあり得ます。たとえば、今日の企業ネットワークは従来とは異なり、取引先や子会社などのネットワークと相互接続されているため、これらの接続についても可視化が必要となります。

クラウド・インフラの利用が急増していることも、脆弱性と可視性の間にずれを生じさせています。組織がパブリック・クラウドを使用して重要な業務を遂行したり機密データを保持したりしている場合、ユーザーの認証情報や設定を一元的に管理することが難しいため、データのセキュリティ保護はさらに難しくなります。

高度な可視化を実現するには、セキュリティ・オペレーション・プラットフォームを使用して、セキュリティ侵害の迅速な検知、脆弱性の予防的な特定、攻撃者の行動を予測するためのセキュリティ・データの一元化と統合を行う必要があります。

セキュリティ侵害の迅速な検知

当然ながら、攻撃を受ける側の組織は攻撃を防ぎたいと思っています。しかし、技術的な脆弱性に加えて人間の弱点を突く攻撃者の手口は高度化する一方であり、セキュリティ侵害を完全に防ぐことはほぼ不可能な状況となっています。そこで重要になるのが、いかにしてセキュリティ侵害の発生期間を最小限にとどめるかです。ある調査によると、セキュリティ侵害の発生から検知までに要した日数は、依然として世界全体で99日（中央値）となっています[1]。約3か月あれば、攻撃者は余裕を持って機密情報を窃取し、侵害の証拠隠滅を図ることさえできるでしょう。

セキュリティ・オペレーション・プラットフォームでは、迅速な検知をベースに、攻撃に使用されているマルウェアの把握、被害の程度や範囲の迅速な評価、セキュリティ・オペレーション・プロセス全体への情報提供を実現し、強固な防御体制を構築できる必要があります。セキュリティ侵害が発生した場合には、1分あたり数百ドルから数千ドルもの損失が発生します。早い段階での侵害の検知は、この損失を最小限に抑えることにつながります。

膨大なアラートの検証

膨大なアラートの中から、本物の脅威を発見する能力も重要です。ある調査によると、組織で週ごとに発生するマルウェア・アラート1万7,000件のうち、信頼できると考えられるアラートは19%、実際に調査されるケースはわずか4%しかありません。不正確なアラートは単にわずらわしいだけでなく、運用コストの増大を招きます。不正確なアラートや誤検知への対応に費やされる時間と労力は、平均で年間127万ドル相当にも及んでいるのです[2]。

適切なコンテキスト情報が提供されないアラートでは、十分な情報に基づいて的確な判断を下せません。優れたセキュリティ・オペレーション・プラットフォームでは、脅威を検知して解析した後、自動アラート検証を実施して誤検知を排除できます。また、膨大なアラートに潜む脅威に優先度を設定できるため、それに基づいて緊急性の高い脅威に素早く対処することが可能です。

攻撃者の行動の把握と今後の予測

従来型のシグネチャ・マッチング技術は、ここ数年で急速に検知率が低下しています。その最大の要因は、不正なコードを変異させ、シグネチャによる検知を回避する攻撃者側の能力が向上しているためです。また別の要因として、窃取した認証情報を使うなど、不正なコードをまったく使用しない攻撃手法への移行が徐々に進んでいる点も挙げられます[3]。

このため、セキュリティ・オペレーション・プラットフォームには、過去に出現していない未知の脅威を検知できる能力が求められます。たとえば、攻撃者の行動をモデリングする高度な解析技術によって、今後の行動を予測的に検知できる必要があります。攻撃者の行動を体系化するためには、解析、インテリジェンス、そして現場での実践的な経験という3つの要素を組み合わせることが重要です。セキュリティ・オペレーション・プラットフォームでは、機械学習技術やユーザー振る舞い解析（UBA）にとどまらず、これら3つの要素を提供することによって、脅威の優先度の判定、脅威の隔離、適切な復旧策の判断を支援できる必要があります。

1 FireEye (2017). M-Trends 2017: A View from the Front Lines.
2 Ponemon Institute (January 2015). The Cost of Malware Containment.
3 Joshua Goldfarb (October 26, 2016). 20 Endpoint Security Questions You Never Thought to Ask.

インシデント対応

適切なインシデント対応は、インシデントの防止と同様に重要です。サイバー攻撃被害がかつてないほど大きく報道されるようになった結果、最近ではセキュリティ関連職以外の人々の間にもこの認識が広がっています。効率的かつ効果的にインシデント対応を実施するためには、高精度のアラート、適切な優先順位が設定された作業キュー、正確な解析、そしてシームレスなケース管理が欠かせません。平均的な企業では、ワークフローの重要性はそれほど高くないと受け止められているようですが、その見方は事実に反することがデータによって証明されています。昨年のある調査によると、高度なサイバー攻撃を受けた企業が攻撃を封じ込めて被害を復旧するまでには、平均で82日かかりました[4]。

この時間を短縮するためには、セキュリティ・オペレーション・プラットフォームですべてのセキュリティ・オペレーションを統合し、インシデント対応におけるインテリジェンスの活用、シームレスなケース管理、スタッフの作業効率向上を実現する必要があります。

すべてのセキュリティ・オペレーションを統合

優れたプラットフォームでは、アラート発生から問題解決に至るオペレーション全体をスムーズに実施できます。ただし多くの場合、対応のスピードはセキュリティ・チームがアラートの検証を開始するタイミングによって決まります。アラートが複数のログ・ソースから発せられる場合に、コンテキスト情報の提供や相関分析が行われないとしたら、そのログ・ソースはほとんど役に立ちません。適切なセキュリティ・オペレーション・プラットフォームでは、複数のログ・ソースを統合し、その結果を脅威インテリジェンスや解析情報と照合して脅威の存在を明らかにできるため、よりスピーディな対応が可能となります。このような連携を可能にするプラットフォームは、各コンポーネントの単純な組み合わせよりも、はるかに効果的に機能します。

インシデント対応におけるインテリジェンスの活用

精度が高く、信頼の置けるインテリジェンスは、セキュリティ・オペレーションの成熟化に欠かせない存在です。ただし、セキュリティ・オペレーションで直接活用できないインテリジェンスなら、あまり意味がありません。つまり、組織を保護するためにインテリジェンスを活用することが困難な場合は、それは役に立たないのです。セキュリティ・プラットフォームが提供するインテリジェンスは、コンテキストに基づく情報、つまりその組織と今起きているセキュリティ侵害に関連した情報でなければなりません。さらに調査活動でより詳細な情報が必要になった場合、オンデマンドで新たなインテリジェンスを入手できると、より効果的な対応が可能となります。

ケース管理機能の提供

多くの組織では、検知の作業をSOCチームの協力者に依存しています。また、調査活動や各種の共同作業では、各チームのメンバーがそれぞれに割り当てられた作業を実施し、報告書を作成して、機密性の高い情報を共有します。しかし、従来型のプロジェクト管理ツールやコミュニケーション・ツールは、SOCチームによるこれらの作業を連携させる目的には不適当です。セキュリティ・オペレーション・プラットフォームは、作業の割り当てと追跡、作業キューの管理、効率的な問題解決に向けた情報交換の促進を実施できるシンプルなツールを備えている必要があります。

スタッフの作業効率向上

セキュリティ脅威の進化に対抗するため、多くの組織がサイバー・セキュリティ担当者の欠員を埋めようと躍起になっており、人材の供給をはるかに上回る需要が発生しています。米国では、20万9,000件ものサイバー・セキュリティ関連職が欠員のままとなっており、求人数は過去5年間で74%増加しています[5]。仮にセキュリティ・オペレーションを24時間体制で運用しようとしても、十分な数の人員を確保するためには、許容できないほどの人件費が必要になるかもしれません。大多数の組織にリソースの限界があるとすれば、従来型セキュリティ・システムが発するアラートの処理をアナリストに担当させるのは、時間や予算の使い道として有効であるとはいえません。この作業を手動で実施するのは非効率的であり、ミスも誘います。繰り返し発生し、時間を浪費するこの種の作業をセキュリティ・オペレーション・プラットフォームで自動化すれば、組織のセキュリティとスタッフの生産性の両方を高めることができます。

総所有コストの計算

サイバー・セキュリティの分野で、総所有コスト（TCO）ほど厳しい目にさらされるトピックはありません。多くの企業は、複数の製品を比較検討する際、価格を基準に置こうとします。たとえ製品の機能が大きく異なる場合でも、その判断基準がまったくの間違いというわけではありません。サイバー・セキュリティ向けの予算を他の重要なビジネス・プロジェクトに振り向けるなど、企業が優先順位に基づいて投資先を判断するのは当然のことです。

重要資産のセキュリティ対策に必要な費用は、運用コストの中でも、継続的、不可避的に発生するコストです。そのTCOについて、従来とは多少異なる観点から検証してみれば、より大局的、より戦略的な視点でサイバー・セキュリティを検討することが可能になります。セキュリティ・オペレーション・プラットフォームがもたらすコストとメリットを、総合的な視野で評価できるようになるはずです。

金銭的なコスト

ハードウェアやソフトウェアの購入費用、サブスクリプション・サービスやアップグレードの費用、その導入および保守に必要な費用。通常、これらの費用には厳しい目を向けられます。このような直接的なコストはすぐに目に付きますが、同じような機能のソリューションが複数存在する、未統合で運用管理に手間がかかる、頻繁なアップグレードが必要、長時間のダウンタイムが発生するなど、隠れた無駄や非効率性というコストも存在します。

一方、効果的なセキュリティ・オペレーション・プラットフォームなら、ネットワーク保護、エンドポイント保護、Eメール保護、SIEMとオーケストレーション、ログ管理とフォレンジック調査など、多様な機能を統合できます。さらに、必要に応じて既存の単機能製品を統合または排除して、コストダウンを図ることも可能です。

4 Ponemon Institute (March 2016). "The State of Malware Detection and Prevention."
5 Ariha Setalvad (March 31, 2015). "Demand to fill cybersecurity jobs booming."

運用コスト

コストが発生するのは、アプライアンスの購入時やサブスクリプション・サービスを利用するときだけではありません。有能なセキュリティ担当者の雇用、製品についてのトレーニング、継続的な運用のサポートなどにも、時間と予算という運用コストが発生します。大多数の企業では、これらのコストは避けることができない金銭的なコストとなります。

どこに時間を費やすかは、慎重に判断する必要があります。作業時間の長短や配分の結果は必ず運用コストに跳ね返るからです。セキュリティ・オペレーション・プラットフォームを評価する際には、次の特長を備えているかどうかを確認する必要があります。

- 幅広い機能を備えており、未統合で多数の単機能製品のトレーニングに必要な時間と費用を削減できる
- アラート対応の労力を最小限に抑え、本物の脅威を素早く検知する高度な機能を有している
- セキュリティ担当者が重要な作業に専念できるよう、作業の連携および調査を支援する

アラート検証など繰り返し発生する手動の作業は、自動化機能により最小限に抑えられます。勤務時間の約8割を占めるとされるこの種の作業は、ほとんどのセキュリティ担当者にとって大きな負担であり、離職の原因となっています。セキュリティ・オペレーション・プラットフォームでこのような作業を自動化すると、セキュリティ担当者は脅威のハンティングや防御、実際に侵害を受けた場合の対応と問題解決など、より影響の大きい作業に専念できるようになります。

また、人手不足が課題となっている場合でも、セキュリティ・オペレーション・プラットフォームでセキュリティ関連作業を体系化、自動化すれば、常にベスト・プラクティスを遵守できます。

セキュリティ・オペレーションの継続性も、運用コスト増大の主な要因となります。有能なセキュリティ担当者を確保し続けることは、その雇用と同様に容易ではありません。一般的に人材の雇用は予測可能ですが、離職は必ずしもそうではありません。急に人材を失うことがあれば、セキュリティ・オペレーションを継続できなくなる恐れがあります。スタッフの離職を最小限に抑えるためには、チームのスキル・レベルに応じた適切な機能、情報、ツールをセキュリティ・オペレーション・プラットフォームで提供することが効果的です。

表1: セキュリティ・オペレーション・プラットフォームに必要な機能のチェックリスト

可視性の向上	
セキュリティ侵害を迅速に検知	✓
アラートを集約し、各アラートに優先度を設定	✓
攻撃者の今後の行動を予測	✓
迅速な対応	
インフラ全体を単一のコンソールで統合管理	✓
インシデント対応におけるインテリジェンスの活用	✓
ケース管理機能	✓
コストの削減	
金銭的な投資を合理化	✓
スタッフの作業効率を向上	✓
セキュリティ・オペレーションの継続性を維持	✓

結論

セキュリティ・オペレーション・プラットフォームは、多くの組織に多大なメリットをもたらします。ただし、これはどのような製品にも当てはまることですが、購入にあたってはベンダーに詳しい説明を求め、そのプラットフォームが実際に提供する機能を正しく理解する必要があります。適切な準備を怠らなければ、潤沢な予算に恵まれない小規模組織を含め、どのような組織でも成熟したセキュリティ体制を構築できます。

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

FIREEYE™