ホワイトペーパー

導入前に押さえたい運用基盤としての SIEM 活用ポイント

目　次

SIEM と運用の効率化

SIEM とは

標的型攻撃対策、ログの活用、セキュリティ監視強化、そして導入済みのセキュリティ投資の有効活用など、SIEM の導入に至る経緯は様々です。SIEM とは Security Information and Event Management の略で、セキュリティデバイスやセキュリティに役立つログが得られるデバイスから、ログ情報やイベント情報を収集、集約してセキュリティ運用を支援するシステムです。

無理を承知で一文で言い表すと、「セキュリティ運用において負担の大きな、監視、調査、対応に関する作業をできるだけ楽に、効率良く、素早くできるようにするためのシステム」です。

セキュリティ人材の確保が難しい中でセキュリティ強化を実現するには、セキュリティチームの生産性向上は欠かせません。攻撃の巧妙化に伴い検知強化にどんなログを使うかなどの視点で注目されがちですが、このドキュメントでは主に SIEM がセキュリティ運用効率化の実現基盤として、どのように運用効率化に貢献するのか、運用ノウハウをどこで得るか、導入を成功させるための注意点について紹介します。

効率化

効率化とは具体的にどのような事でしょうか。SIEM の活用で得られる具体例を挙げてみます。もし、現在 SIEM を使用せずに運用していて手間がかかっているものがあれば運用の効率化が期待できます。現在の行っていない作業をセキュリティ強化のために追加して行うのであれば作業自体は増えますが、SIEM が有る場合と無い場合で比較することになります。

自動化

これまで手作業で行っていたことが不要になる。

スピードの向上（時間の短縮）

これまでより短い時間で作業を完了する。

できなかった事ができるようになる

これまでできなかったことができるようになったり、必要だった作業人数が減る。

上記は関連する部分も多くありますが、SIEM は特に複数の異なるデバイスのログを使用して検知したり、調査したりする際に大きく貢献します。

効率化：運用のどんな作業が楽になるのか？

効率化の具体例

ログが統合集約して保存されることによる効率化例

- 必要なログにすぐアクセスできるため、他の担当者にログの提供や調査の依頼が不要
- 異なるデバイスの同様イベントの重複を自動的に排除
- 異なるデバイスの同一時間帯のログの一覧性が高く調査しやすい
- あるログの情報を使用して、異なるデバイスのログの関連する情報を検索しやすい
  （例：関連 IP アドレスが含まれるログ）
- 複数の異なるデバイスのログを組み合わせて条件を設定してイベントを発生させやすい

ログのフォーマットを自動的に統一（正規化）されることによる効率化例

- 調査時（検索、条件設定時）にログの表現の違いの意識や知識が不要
  日付のフォーマットの違い（YYYYMMDD と YYYY-MM-DD など）や同様イベントでも異なる表現（ログインとログオン、Permit と Allow）など。
- 自動的に同様イベントをグループ化
  ログイン成功、ログイン失敗は認証としてグループ化して認証関連のログとしてグループ化して扱うなど。
- デバイスにより異なるイベントの重要度（優先度）を統一

パーツが用意されていることによる効率化

- 運用画面はパーツの選択と条件設定で作成できたり、必要な操作（ドラックして範囲指定、データを選択して表示データに絞り 込み、ドリルダウン など）はパーツに備わっていている。
- 必要とされがちな運用を想定した画面、相関ルー ル、フィルタ、インシデント管理機能などが用意されている。

SIEM と他システム連携による自動化例

- 他システムと連携した一次対応
  SIEM で表示されたイベントに対して一次対応（エンドポイントの隔離など）を実行できるように連携できる。
- 調査作業の自動化
  ネットワーク上で検知した未知のマルウェアをサンドボックスで解析した結果（IoC 等利用）で SIEM の過去のログにバックトレースを自動実行し侵害を調査する。

基盤：ログの統合、ノウハウ共有、情報共有

様々な効率化の手段が用意されている理由

SIEM に効率化の仕組みが備わっているのは、単に決まった監視や調査を効率良くするためだけではありません。脅威も変われば、組織内の IT 環境も変わります。セキュリティ製品に提供されるソフトウェアのアップグレードやシグネチャ等の更新も重要ですが、組織で必要な作業を素早く運用に取り込むことが大切になっています。より組織に合った運用を効率よく取り込めることが望ましいからです。調査等で検知や運用改善のアイデアがあっても、ログが入手できない、ログのフォーマットの違いを調べなければならい、運用画面を作るの時間要するとなれば、途中であきらめて負荷の高い運用を続る可能性があります。

一方で、素早く容易に改善できる手段があれば、運用を継続的に改善できます。できるだけ早いタイミングで検知できれば早期発見の仕組みが手放せなくなります。手作業を自動化して、検知できなかった事を検知できるようになったり、一次対応をある程度定型化しておくことで運用の属人化を避けることもできるようになります。

また、監視をしていれば時には白黒つけがたい場合がありますが、監視レベルを上げてしばらく継続的に監視を続 けるような柔軟性の高い運用も可能になります。

ログの統合管理と運用ノウハウの共有

ここまで紹介したように SIEM はログを統合管理するだけでなく、SIEM を運用ノウハウの共有基盤として活用することが重要です。他にも、実際の運用現場と、運用現場を管理する担当者で効率的な情報共有が行えます。現場と管理側の情報共有というと不都合な印象を持つ人もいるかもしれませんが、報告のために多くの時間を費やすことが避けるられます。ある一定レベル以上のアラートの発生状況や、インシデント対応状況など、いちいち他のツールで報告書を書くことなく、管理者も運用者と同じ情報を見ることができる環境のが整備できます。特に優秀な人は調査に時間を使いたいのに、報告書作成に時間をとられるような状況を改善し生産性を向上することができます。報告作業の効率化はセキュ リティ運用に限らず様々な場面で実現されていることです。

不安：使いこなせるのだろうか？

運用ノウハウの活用方法

既に日ごろインシデント調査をしている場合は、調査で得たノウハウや洞察の活用など想定しやすと思います。しかし、これから運用強化に SIEM を活用しようと考えると、どんなログがどのような攻撃の検知に有効か参考情報が欲しくなります。

外部提供情報の活用

情報処理推進機構（IPA）や JPCERT コーディネーションセンター等からログ分析に関連する多くの情報が提供されています。基本的なログの活用方法から、実際に発生したインシデントの調査を基にしたログ分析方法などが提供されています。

SIEM にあらかじめ入っている相関ルールを活用する

多くの SIEM はベンダーが提供している相関ルールがあるので、その相関ルールを活用したり、相関ルールの中身を見てどんなログを組み合わせて条件を設定しているか参考にしたりカスタマイズしたりできます。

ベンダーやコミュニティの活用例を利用する

特定の運用を想定してノウハウが提供されている場合があります。マカフィーの SIEM の場合はコンテンツパックを提供していて、ベンダー自身がテストして無償提供されています。

- マカフィーのコンテンツパックに含まれるもの
  - ビュー（運用に使用する画面）
    監視対象の情報や、操作で必要になるドリルダウン等が予め設定されたもの。
  - 相関ルール
    監視対象イベントを検知するための相関ルール。
  - 他
    運用時に継続的に監視したい対象を登録するウォッチリスト（フィルタの条件に使える）や、イベント発生時に特定の人にメールを送付するアラー ムが含まれる。
- コンテンツパック例
  - 外部への情報流出や不審活動の監視、インシデントレスポンス、ユーザの振る舞い分析、各種 コンプライアンス、他

他にも SIEM 導入実績の豊富なサービス提供者のサービスを利用してエキスパートのノウハウを早期に運用に取り込んだり、マネージドサービスが利用されることも良くあります。

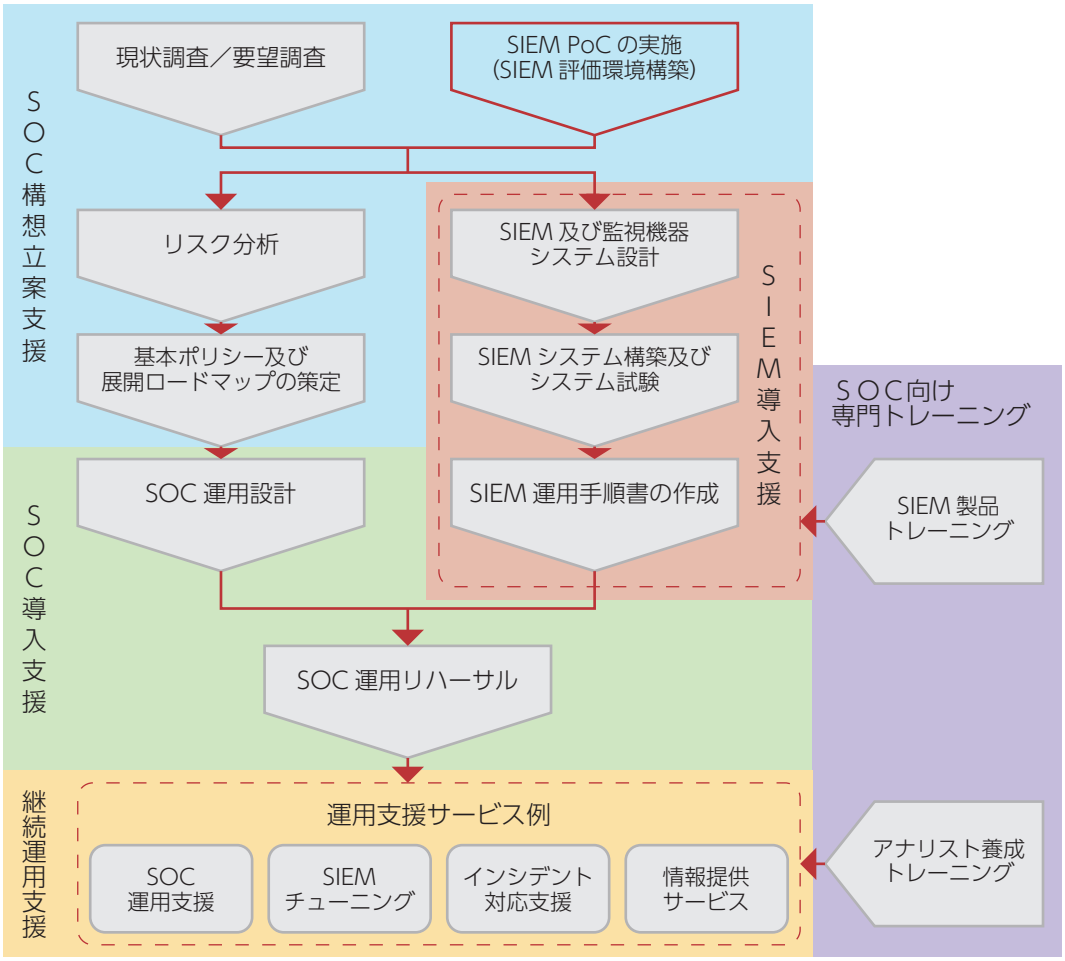
注意！：SIEM の有効活用は導入前に決まる?

SIEM 導入に失敗しないための注意事項

ここからは、SIEM の導入を成功させるためにカギとなる注意事項について紹介します。SIEM の導入による運用の効率化において重要なのは、事前の計画と運用設計です。また、導入して継続的に運用効率を向上させることを前提にしておくことが大切です。以下は押さえておきたい重要ポイントです。

- 現状把握と目的を整理しておく
- 運用リソースを考慮した現実的な運用
- 監視や検知はもちろん、検知後のプロセスも含めた運用プロセス
- ルールの修正や追加のために定期的に時間を確保

以下はマカフィーが SOC の体制確立、SIEM 導入、運用に関するサービスを提供する際の手順例です。

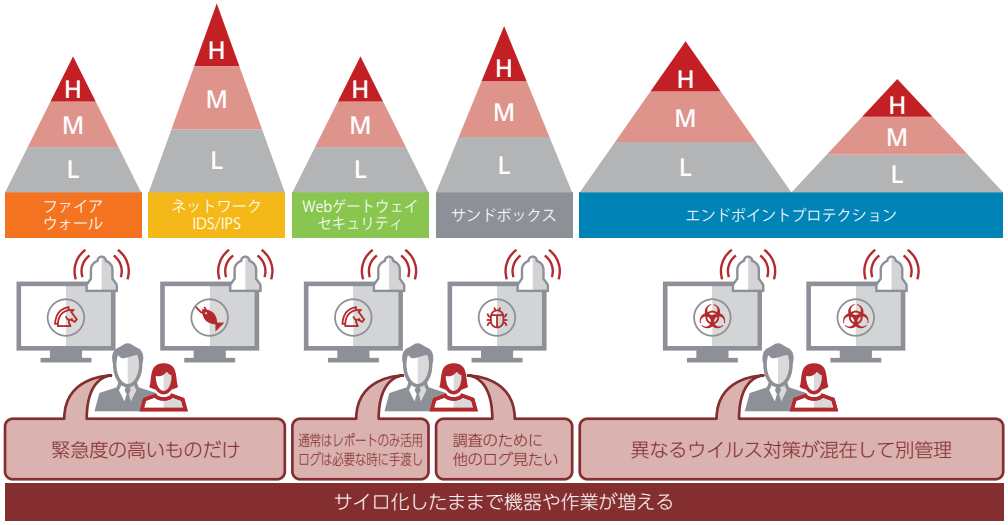


ビフォー・アフター：ログ・ノウハウ・情報の共有基盤化

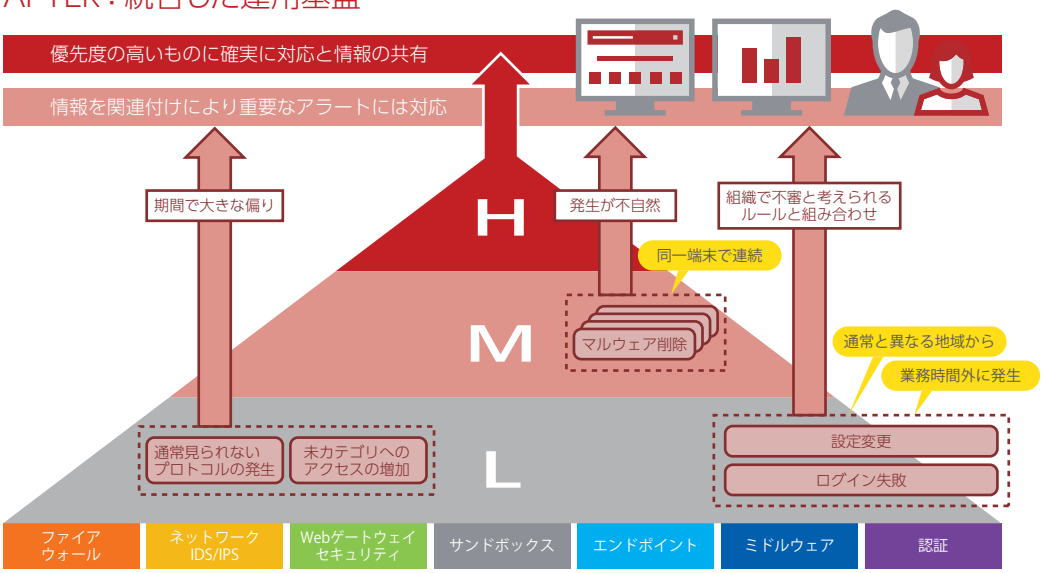
運用基盤のビフォー・アフター

SIEM でログを統合管理すると、バラバラに監視をしていたセキュリティデバイスで発生するイベントをまとめて、より重要なイベントに優先的に対応できます。また、セキュリティ以外のデバイスのログを利用して、セキュリティデバイスでは検知できなかったときにも兆候を把握できる可能性を高めることもできます。脅威が進化したり、導入製品が増えても、運用リソースを無尽蔵に増やせません。SIEM を上手く活用すると、ログの統合管理だけでなく、運用ノウハウの蓄積、情報共有の促進など、まさに運用基盤になり、監視、調査、対応が、より少ない負担で、より速くできるようになります。

BEFORE：独立したシステムの運用



AFTER：統合した運用基盤



定常的発生しがちだが、場合よっては要注意なイベントは組み合わせ条件が成立した監視対象！

SIEM 関連資料

以下の URL からダウンロードすることができます。

https://japan2.secureforms.mcafee.com/wp-siem001-index