ソリューション概要

FireEye

脅威インテリジェンスの ユースケース・シリーズ

セキュリティ・オペレーション・センター（SOC）のアナリスト

SOCのアナリストが抱える課題

セキュリティ・ソリューションが生成するアラートやアラーム、イベントの数は増加の一途をたどっており、SOCのアナリストはその中から重要な情報、攻撃キャンペーンや高度な攻撃に関わる情報、緊急の対応を要する情報を見極めるのに苦労しています。膨大なノイズの中から深刻な脅威を見つけ出し、限られたリソースをそのインシデント対応に集中させる必要があります。特に困難な課題は次のとおりです。

- 日々発生する数万～数百万件のアラートをくまなく調査し、その中から深刻な脅威を発見することはほぼ不可能である
- 信頼性や関連性の低いアラートと、組織に深刻なリスクをもたらす脅威に関するアラートを区別するための情報が不足している

ログを集約し、関連アラートを相関分析するツールを使用すれば、解析が必要なアラート数を削減できますが、初動を担当するレベル1アナリストの負担を軽減するためには、それだけでは不十分です。

SOCのレベル1アナリストによるサイバー脅威インテリジェンスの活用

高度なセキュリティ・オペレーション・センター（SOC）では、脅威インテリジェンスを導入する動きが広がっています。その目的は、アラートの対応優先度を判断し、内容を検証して、組織に深刻なリスクをもたらす脅威を速やかに特定することです。脅威インテリジェンスを利用して問題を絞り込み、コンテキスト情報を素早く入手すれば、レベル1アナリストは、インシデント対応（IR）チームによる詳細な解析や対応が必要なアラートを迅速かつ的確に判断できます。

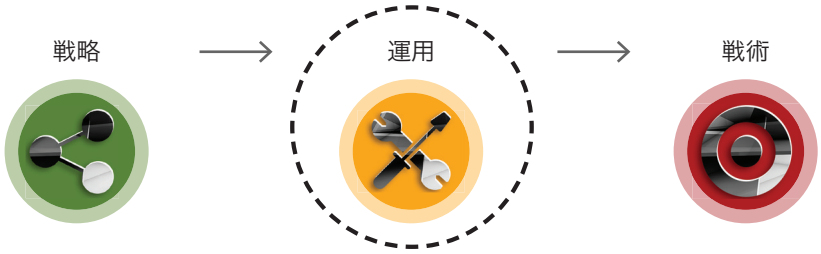

表1：ユースケース - SOCのレベル1アナリスト

ユースケース	主な目標	必要なインテリジェンス
機械処理での優先度判定	SOCのアナリストに提示されるアラートやアラームの優先度を、SIEMや解析ツールで的確に判定できるようにして、初期トリアージのプロセスを自動化する	機械可読の脅威データ：深刻度のスコアとタグを含む脅威インジケーター（タグは、特定の業種や地域、アプリケーションを標的とする攻撃との関連性を示す）
アラート/イベントのトリアージ	優先的に調査する必要のあるアラートやイベントを速やかに判断	コンテキストの把握と状況の認識を可能にする、脅威の概要データに関連づけられた脅威インジケーター
アラート/イベントの解析と検証	イベント情報を検証し、IRチームによる詳細な対応が必要なイベントを判断する	個々のインジケーターとコンテキスト情報（攻撃キャンペーン、攻撃グループ、手口など）を関連づける脅威データ

1. **機械処理での優先度判定：負担の大きい作業はテクノロジーが担当**
   膨大なアラートやイベント情報の中から、本当に重要な情報を見つけ出すにはどうすればよいのでしょうか。SOCチームが直面するアラートの多くは誤検知です。つまり、ビジネスに影響を与えない脅威や、既存のセキュリティ対策で回避できる脅威に過ぎません。発生したアラートを脅威インテリジェンスと照合すると、SIEMやログ管理ツール、セキュリティ解析ツールで、自動的かつ高速にアラートの優先度を判定できるようになります。このような仕組みを構築すれば、日々大量に発生する軽微なアラートや関連性の低いアラートの調査という手間のかかる作業から、SOCのレベル1アナリストを解放できます。

   たとえば、業務ネットワーク上に残された識別可能な脅威インジケーター（ドメインやIPアドレス、ポート、プロトコル、ファイル・ハッシュ、レジストリ設定などの情報）を脅威インテリジェンスと照合するSIEMルールを作成すると、特定の業種や地域、ソフトウェア・アプリケーション、インフラストラクチャ・コンポーネントを標的とする攻撃グループや攻撃キャンペーンを把握できます。この照合結果に基づいて、SIEMが自動的にアラートやイベント情報の対応優先度を高めるので、SOCチームは組織との関連性が高い脅威を速やかに把握できます。

2. **イベントとアラートのトリアージ：人手による優先度判定の効率化**
   機械処理で優先度を判定すれば、負担の大きい作業のかなりの部分を自動化できます。しかし、危険性の高いアラートを見極める困難な作業は依然として残ります。サイバー脅威インテリジェンスは、このプロセスの効率化に効果を発揮します。脅威インテリジェンスで提供される脅威の概要データを使用すれば、コンテキストの把握と状況の認識が可能になります。

   このデータは、個々のインジケーターを攻撃グループや標的に関連づけるタグおよび概要情報として、またはインジケーターを攻撃キャンペーンや段階的な攻撃のコンテキストに関連づける、ストーリーに基づく長めの情報として提供されます。

   たとえば、あるアラートにマルウェアが関連づけられている場合、SOCのアナリストは脅威インテリジェンスを使用して、そのマルウェアが特定のサイバー犯罪やスパイ活動に利用されているかどうかをすぐに確認できます。また、インターネット上のIPアドレスとの不審な通信がアラートに記録されている場合も、脅威インテリジェンスの利用により、特定の業種や地域を標的とする既知の攻撃グループと関連のあるアドレスかどうかを速やかに判断できます。

3. **解析と検証：証拠を収集し、IRチームによる対応が必要なインシデントを判断**
   脅威インテリジェンスは、SOCのレベル1アナリストが脅威を詳細に解析し、イベントを検証する目的でも役立ちます。たとえば、「このイベントは、ビジネスに深刻なリスクをもたらす脅威に関係しているのか」、「このイベントは単発的な出来事か、それとも複雑な標的型攻撃の一環なのか」といった疑問に答えることができます。

   アラートに関連づけられたコンテキスト情報には、関連するマルウェア・ファミリー、ドメインおよびIPアドレス、マルウェアの振る舞い、フィッシングやその他の攻撃の手口に関する情報が含まれます。また、脅威インテリジェンスでは、マルウェアやフィッシング・メールの背後に存在する特定の攻撃グループの素性や、段階的な攻撃を構成する各ステップの解析情報、リスクを軽減するために推奨される対策などの詳細情報やストーリーも提供されます。

   このようなインテリジェンス・リソースを利用すれば、SOCのアナリストは短時間で証拠を集め、アラートやイベントを「組織に深刻なリスクをもたらすインシデント」として扱う必要があるか、インシデント対応チームによる即時かつ詳細な調査が必要かどうかを判断できます。

iSIGHTがSOCに提供する情報

市場で最も詳細なインテリジェンス、厳密に検証された正確なインジケーター

- その他

まとめ

今日のSOCチームは、膨大なアラートへの対応に忙殺されています。iSIGHT Partnersが提供するインテリジェンスは、信頼性が高く、具体的で、コンテキスト情報が豊富に含まれています。SOCのレベル1アナリストがこのインテリジェンスを利用すれば、次のようなメリットが実現します。

- 膨大なセキュリティ・アラートやイベント情報を絞り込む
- 大量に発生する軽微なアラートや優先度の低いアラートを調査する無駄な労力を不要にする
- 組織との関連性が高い脅威に関するアラートを素早く特定する
- 短時間で証拠を収集、評価して、IRチームによる対応が必要なインシデントを的確に判断する

FireEye製品の詳細については、次のWebページをご覧ください。
www.FireEye.jp

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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.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・レスポンスといった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の4割以上を含む、世界67か国以上の6,800を超える組織で利用されています。