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

インシデント対応担当者

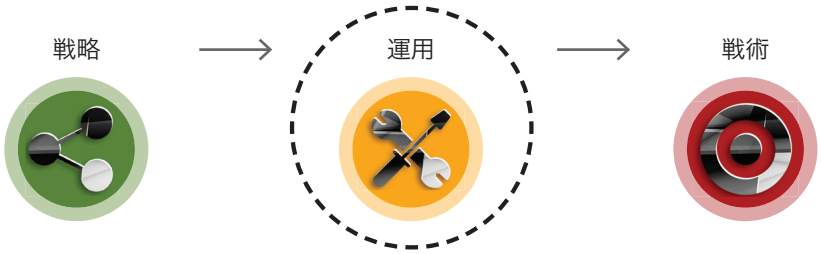
インシデント対応担当者が抱える課題

セキュリティの最前線でサイバー攻撃と戦うインシデント対応担当者は、セキュリティ侵害の疑いがあるインシデントの調査、高度な攻撃の検知と解析、フォレンジック調査の実施、被害の復旧などの作業を担当します。一般に、インシデント対応（IR）チームのメンバーは経験豊富なセキュリティ・アナリストで構成され、組織によっては、レベル2/レベル3アナリストとしてセキュリティ・オペレーション・センター（SOC）に所属している場合もあります

今日のインシデント対応担当者は、次のような課題に直面しています。

- 本物のセキュリティ侵害であるインシデントを速やかに検証し、リスクの大きさに基づいて優先度を判断する必要がある。
- インシデントを特定の攻撃グループや攻撃キャンペーンに関連づけることが困難。
- 高度な攻撃や攻撃グループが使用するツール、技術、手順（TTP）についての詳細情報を探し出すため、膨大な時間を費やしてデータベースやナレッジベースを調査する必要がある。
- 経営陣が正しく理解し、適切な対策を講じられるよう、セキュリティ問題についてビジネス視点で説明する必要がある。

ある調査によると、企業各社が誤検知への対応に費やす年間費用は平均127万ドルに上ります。



インシデント対応担当者によるサイバー脅威インテリジェンスの活用

インシデント対応担当者がサイバー脅威インテリジェンスを利用すれば、深刻な脅威の確実な検知、「いつ/誰が/何を/何の目的で/どのように」の速やかな把握、対応および復旧のスピードアップを実現できます。また、ネットワークの水面下で展開されている高度な攻撃を予防的に発見することも可能になります。

表1：ユースケース - ユースケース - IRチーム

ユースケース	主な目標	必要なインテリジェンス
インシデントの検証と優先度の判断	• 組織に大きなリスクをもたらす可能性が高いインシデントを特定し、ビジネスへの影響が特に大きいインシデントを判断する	• 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
インシデントの解析	• 攻撃の「いつ/誰が/何を/何の目的で/どのように」を把握する • 攻撃が現在も継続中かどうかを判断し、その影響を特定する	• 攻撃グループ、攻撃キャンペーン、標的についてのコンテキスト情報に関連づけられた脅威インジケーター • 過去の攻撃やその手口についての詳細情報を提供するインテリジェンス・ナレッジベース
封じ込めと復旧	• 攻撃者による通信を遮断する • マルウェアを駆除し、改変を復元する • 脆弱性を解消する	• 過去の攻撃やその手口についての詳細情報を提供するインテリジェンス・ナレッジベース
ハント・ミッション	• 目下のインシデントに関連する未確認の攻撃活動や、特定の業種、地域、アプリケーションなどを標的とする脅威を被害の発生前に発見する	• 攻撃グループ、攻撃キャンペーン、標的についてのコンテキスト情報に関連づけられた脅威インジケーター • 過去の攻撃やその手口についての詳細情報を提供するインテリジェンス・ナレッジベース

1. インシデントの検証と優先度の判断：ビジネスへの潜在的な影響を評価

SOCのレベル1アナリストがIRチームにインシデント対応を要請してきた場合、インシデント対応担当者は、そのインシデントの優先度を判定し、詳細な調査が必要かどうかを判断する必要があります。サイバー脅威インテリジェンスは、自組織を標的とする攻撃グループに関係している思われるインシデントや、ビジネスに悪影響を及ぼす可能性が高い攻撃を見極める際に役立ちます。

サイバー脅威インテリジェンスを使用すると、攻撃のインジケーターをコンテキスト情報に関連づける脅威の概要データに基づいて、上記のプロセスを効率化できます。コンテキスト情報として提供される情報には、攻撃の実行者と推測されるグループ、その動機（金銭目的、産業スパイ、イデオロギー的な主張など）、標的、過去に発生した攻撃による被害などがあります。この概要データから、インシデントの標的が他の業種の組織や一般消費者であると判明した場合、インシデント対応担当者は、インシデントの優先度を下げ、重要なビジネス・プロセスや価値ある情報資産を脅かす別の攻撃への対応に、貴重なインシデント解析リソースを振り分けることができます。

2. インシデントの解析：攻撃活動の詳細を調査

インシデント対応担当者は、インシデントの優先度を判断した後、攻撃が現在も継続中かどうか、システムやアプリケーションに対する改変が行われていないか、データの窃取や業務の中断などの被害が発生していないかを確認する必要があります。サイバー脅威インテリジェンスを利用すると、発生した攻撃の全体像を把握し、「いつ/誰が/何を/何の目的で/どのように」を明らかにできます。

サイバー脅威インテリジェンスでは、アラートやインジケーターを過去に発生したイベントや攻撃の痕跡に関連づけることができます。たとえば、あるマルウェアが見つかった場合は、そのマルウェアに関連づけられたIPアドレスの有無を確認できます。また、攻撃グループが使用するC&Cサーバーの既知のIPアドレスに接続するかどうかを調べることも可能です。インシデント対応担当者は、これらの情報をもとにネットワーク・ログをチェックし、C&Cサーバーに接続しているシステムや侵害されている可能性のあるシステムが他にないかどうかを確認できます。

脅威インテリジェンスがナレッジベースで管理されている場合は、攻撃者の素性や標的、TTP、攻撃を受けた場合の影響などの詳細情報をナレッジベース経由で入手できます。IRチームは、この情報を参考に、攻撃の証拠（攻撃を実行しているグループ、これまでの攻撃活動、手口、攻撃が継続中かどうかなど）を探すべき場所を判断できます。

3. 封じ込めと復旧：被害の拡大を阻止、脆弱性を解消

インシデント対応担当者は、攻撃を封じ込め、被害の復旧に役立つ情報を他のIT担当者に提供する必要があります。

脅威インテリジェンスのナレッジベースでは、インシデントに関与している攻撃グループの目的、手口、インフラストラクチャに関する情報が提供されます。この情報を使用すれば、外部のC&Cサーバーとの通信を遮断する、フィッシング攻撃で窃取されたユーザー認証情報を無効にするなどの方法で、攻撃の進展を食い止めることができます。

特定の攻撃グループによるシステムの侵害手法やそのグループが使用するマルウェアの振る舞いなどの情報は、感染システムの特定、マルウェアの駆除、レジストリやファイルに加えられた改変の復元、脆弱性の解消による被害の再発防止に役立ちます。

4. ハント・ミッション：水面下の攻撃を予防的に調査

「保護システムや検知システムですべての攻撃を防ぐことは不可能であり、気づかぬうちに攻撃者がネットワーク内に潜んでいる場合もあり得る」。この認識は、今日ではほとんどの組織で共有されています。このような攻撃を予防的に発見するのが、「ハント・ミッション」というプロセスです。

受動的なハント・ミッションでは、サイバー脅威インテリジェンスを利用して、現在発生しているインシデントに関係する未確認の攻撃活動を調査します。たとえば、目下のインシデントでフィッシング攻撃が行われている場合、脅威インテリジェンスによって、その攻撃の実行グループが別のフィッシング攻撃キャンペーンや水飲み場型攻撃にも関与しているという事実が判明する場合があります。この情報から、当該のグループは複数の攻撃手法を用いている可能性が高いと判断できるため、ハンティング・チームは、他のフィッシング攻撃キャンペーンが行われている証拠や、水飲み場となっているWebサイトにアクセスした社員の調査に乗り出すことができます。

予防的なハント・ミッションでは、まず、「特定の業種に属する組織や特定のシステムを運用する組織を標的とする攻撃グループは、同じ業種に属する組織や同じシステムを運用する組織を狙う可能性が高い」というような仮説を立てます。脅威インテリジェンス（特に、包括的なインテリジェンス・リポジトリ）では、仮説のような、自組織を狙う可能性が高い攻撃グループについての正確かつ詳細な情報や、攻撃グループが組織のネットワークに侵入している証拠を探すべき場所についての有用な情報が提供されるため、これらの情報を利用して、被害の発生を未然に防止できます。

iSIGHT脅威インテリジェンスがインシデント対応担当者にもたらすメリット

- 市場でも有数の詳細なインテリジェンス、厳密に検証されたインテリジェンス、関連するインジケーター
  - 攻撃グループ、攻撃キャンペーン、TTPに関する、コンテキスト情報を豊富に含むインテリジェンス
  - サイバー犯罪やサイバー・スパイ、ハクティビズムなど、幅広い攻撃活動に対応
  - 世界各地から情報を収集、解析
  - 8年分の履歴データベース
- 既存のツールやプロセスとの統合を可能にする強力なAPIとSDK
- パートナーが提供する主要なインシデント対応ツールと統合
  - 解析：Splunk、BAE、Palantir、Maltego
  - エンドポイント：Tripwire、Ziften
  - 脅威インテリジェンス・プラットフォーム：ThreatConnect、Anomali、ThreatQuotient
  - インシデント対応：Resilient Systemsなど

まとめ

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。インシデント対応担当者がこのインテリジェンスを利用して迅速かつ的確に意思決定を下せば、次のようなメリットが実現します。

- 即時の調査が必要なイベントを特定する。
- 個々のインジケーターを攻撃グループや攻撃キャンペーンに関連づけ、攻撃の実行者や標的を直ちに把握する。
- 広範囲にわたって的確かつ詳細な調査を実施し、攻撃の「いつ/誰が/何を/何の目的で/どのように」を把握する。
- 現在も継続中の攻撃を遮断し、ビジネスへの影響を抑える。
- 同様のインシデントによる被害の再発を防止する。
- ハント・ミッションを実施し、ネットワークの水面下で展開されている攻撃を発見する。

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。