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

CISOおよびIT部門上級幹部

CISOが担う4つの役割

- **戦略家：**ビジネス戦略とサイバー・リスク戦略の足並みを揃え、意味のある投資を通じてリスク管理の変革を促進する
- **助言者：**ビジネス担当者と連携し、サイバー・リスク管理に関する取り組みについて啓蒙、助言する
- **保護者：**脅威トレンドを理解し、効果的なサイバー・リスク・プログラムを管理して、ビジネス資産を保護する
- **技術者：**組織的なセキュリティ能力を確立するためのセキュリティ技術とセキュリティ基準を評価、導入する

CISOおよびIT部門上級幹部のためのサイバー脅威インテリジェンス

最高情報セキュリティ責任者（CISO）とIT部門上級幹部は、サイバー・セキュリティについて戦略的な意思決定を下す役割を担っています。この両者は、最も大きなリスク軽減効果が期待できる場所に人的リソースと技術的リソースを配分する立場にあります。そのためには、組織を攻撃する可能性が高いグループと、そのグループが狙うであろう資産を把握しておかなければなりません。また、本物の脅威と単なる風評を見分け、IT部門の活動についてCEOや取締役に説明できることも必要となります。

CISOが抱える課題

今日のCISOとIT部門上級幹部は、次のような課題を抱えています。

- プログラム、人材、テクノロジーに関する予算申請のうち、どの投資がリスク軽減戦略として効果的であるかを判断する。
- メディア、アナリスト、ベンダーによる膨大なレポート、解析結果、誇大宣伝をより分け、組織にとって関連性が高く、優先的に対応する必要のある脅威を見極める。
- 経営トップや取締役とコミュニケーションを図り、組織にとっての脅威とIT部門の対応について理解を得る。

iSIGHT Partnersについて

iSIGHT Partnersは、2007年の創業以来、サイバー脅威インテリジェンスのリーダー企業として高い評価を得ています。世界18か国、300人を超える多様な専門家で構成され、業界でも確固たる地位を確立しているiSIGHT Partnersのインテリジェンス・チームは、グローバルな脅威トレンドや攻撃グループ、攻撃手法の解析に特化しており、お客様のセキュリティ・チームやインテリジェンス・チームがインテリジェンス主導のセキュリティ戦略を策定し、インテリジェンスをビジネスの保護に直接活用できるよう支援しています。

表1：ユースケース - CISOおよびIT部門上級幹部

ユースケース	主な目標	必要なインテリジェンス
リスクの優先度の判定	• 特定の業種、地域、組織を標的としている攻撃グループを特定する • 特にリスクの高い情報資産と侵害がビジネスに及ぼす影響を把握する	• 特定の業種や組織に特化した脅威解析 • 攻撃グループやそのグループが標的とする資産、窃取した資産の利用方法を示す脅威診断
新規プロジェクトのリスク診断	• 新しい市場、地域、業界、テクノロジーに関するリスクを判断する	• 新しい市場、地域、業界、テクノロジーの脅威解析 • サイバー・セキュリティ研究者への問い合わせ
計画策定、予算編成、人員配置	• セキュリティ・プログラム、テクノロジー、人員配置の現状を現在および将来の脅威に照らし合わせて評価する	• 組織の業種に特化した脅威解析 • 攻撃グループやその攻撃手法のインテリジェンス・ナレッジベース • サイバー・セキュリティ研究者への問い合わせ
経営幹部とのコミュニケーション	CEOや取締役とのコミュニケーション： • 報道されたセキュリティ侵害のうち、自組織との関連性が高いのはいずれか？ • 現在発生しているインシデントにどう対応するのか？ • 最新の脅威に備えた対策はどの程度整っているのか？	• メディア報道の分析 • 脅威解析 • サイバー・セキュリティ研究者への問い合わせ

CISOおよびIT部門上級幹部によるサイバー脅威インテリジェンスの活用

最近では、CISOやIT部門上級幹部の間に、サイバー脅威インテリジェンスを活用する動きが広がっています。この背景には、ビジネス・リスクを特定して対応の優先度を判断する、計画、予算、人員についての戦略的な意思決定を的確に下す、事業リスクや財務リスク、脅威、セキュリティ体制についてCEOや取締役とビジネスの観点でコミュニケーションを図る、などの目的があります。

サイバー脅威インテリジェンスがもたらすメリット

1. **リスクの優先度の判定：最も危険性の高い脅威に優先的に対応**
   ISOやIT部門上級幹部がサイバー脅威インテリジェンスを利用すれば、膨大な脅威の中から組織に大きな影響をもたらす脅威を見極め、その対応を優先的に実施できるようになります。脅威レポートでは、特定の業種や地域、業態の組織を狙う攻撃グループや、その戦術、技術、手順（TTP）に関する情報が提供されます。脅威診断では、組織の脅威プロファイルを策定し、その組織の資産を積極的に狙う攻撃グループや、戦術的、戦略的な対応の必要性を明らかにできます。これらの情報をもとに、組織が直面するリスクの対応優先度を判断し、リスクを管理するための適切なポリシー、プロセス、テクノロジーを見極めることができます。

2. **新規プロジェクトのリスク診断：転ばぬ先の杖**
   新たな市場や地域への参入（または撤退）や新しいテクノロジーの導入には、予期しないリスクが付きものです。サイバー脅威インテリジェンスは、このような新規プロジェクトのリスクに備える目的にも役立ちます。たとえば、参入先の市場で活動しているサイバー犯罪者、特定の地域で事業を展開する企業を狙うハクティビスト（場合によっては国家政府）、新しいアプリケーションやテクノロジーの脆弱性を悪用する攻撃グループなどの脅威を把握できます。このような情報は、市場や地域、テクノロジーの脅威解析結果や、サイバー・セキュリティ研究者への問い合わせやディスカッションから入手します。

3. 計画策定、予算編成、人員配置：投資と人材採用の意思決定を支援

サイバー脅威インテリジェンスは、CISOやIT部門上級幹部が脅威トレンドを戦略的な観点で理解する際に効果的です。たとえば、組織が直面している攻撃グループや脅威の概略、同じ業種の組織で狙われている情報資産、利用可能な対策を把握できます。これらの情報をもとに、現在のセキュリティ状況を評価して、セキュリティ・プログラムや新しいテクノロジーへの投資、必要なスキルを備えた人材の雇用などについて、重要な意思決定を下すことができます。

4. 経営幹部とのコミュニケーション：関係者全員で同じ認識を共有

今日のCEOや取締役は、サイバー犯罪者やハクティビスト、大規模データ侵害に関する大量のメディア報道を目にしています。CISOとIT部門上級幹部は、組織が直面する実際の脅威と、IT部門が特定のプログラムやテクノロジー、人材に投資する理由について、経営陣と積極的にコミュニケーションを図る必要があります。

脅威インテリジェンスを利用すると、ビジネス上のリスクや脅威、攻撃グループの金銭的・政治的な目標を、技術に不案内なビジネス担当の経営幹部にわかりやすく説明できます。これらの情報を把握しておくと、一般紙や業界紙で報道されたインシデントや、サイバー・セキュリティにおける優先順位について質問を受けても、素早く正確に答えることができます。インシデントの発生時には、脅威インテリジェンスに基づいて今後の対応方法をCEOや取締役に伝えられるため、あらかじめ全員の同意を得たうえで次のステップへ移行できます。

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、戦略的かつ具体的です。CISOとIT部門上級幹部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。
- 組織との関連性が高い脅威インテリジェンスに基づき、リスクを識別して優先度を判断する。
- 新しいビジネス・プロジェクトのリスクを正確に評価する。
- セキュリティ予算と人員配置についての戦略的な意思決定を的確に下す。
- 攻撃グループの素性とその戦術、技術、手順を正確に理解したうえで、効果的なインシデント対応を実施する。
- リスク、脅威、セキュリティ体制、対応方法の認識について、経営幹部の足並みを揃える。

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。