CSIRTを進化させる次の一手

再考、スレットインテリジェンス

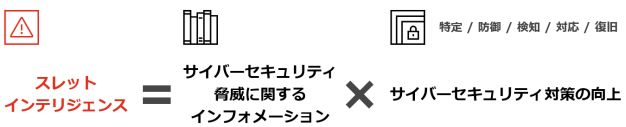
PwCコンサルティング合同会社　ディレクター　村上 純一

1. スレットインテリジェンスを「意思決定の知見」として活用するために

近年、スレットインテリジェンスまたは脅威インテリジェンスと呼ばれる情報および情報提供サービスが注目を集めています。以前からCVE（Common Vulnerability Enumeration）に代表されるソフトウェア脆弱性に関する情報を提供するサービスは存在しています。また、IoC（Indicator of Compromise）のように実際のサイバー攻撃で悪用されたマルウェアのハッシュ値や通信先IPアドレスなどを提供するサービスも近年登場しています。こうした取り組みとスレットインテリジェンスはどこが違うのでしょうか。

インテリジェンスは一般的に、インフォメーションを特定の目的で分析して得られる意思決定のための知見を意味します。そのためインテリジェンスを語る上で「分析の目的は何か？」は欠かすことができない問いと言えます。スレットインテリジェンスは、文字どおりサイバーセキュリティ脅威に関するインフォメーションを対象とし、自組織のサイバーセキュリティ対策向上を目的とした分析により得られた、意思決定のための知見と考えることができます。サイバーセキュリティ対策という概念をどのように捉えるかにはさまざまな考え方がありますが、代表的なものとしてはNISTサイバーセキュリティフレームワーク（NIST CSF）が挙げられます。そのため同フレームワークを構成する5つの要素（「特定」、「防御」、「検知」、「対応」、「復旧」）それぞれの観点からサイバーセキュリティ脅威に関するインフォメーションを分析したものが、スレットインテリジェンスと考えることができます。

図表1：スレットインテリジェンスの定義



「スレットインテリジェンスサービスが有用だと聞いてと契約したが、有効な使い方が分からない」という声を聞くことがあります。こうした場合、「どのようなセキュリティ課題を改善するか・高度化するか」という課題・目的の設定、そのためにどのような知見が必要か、知見を得るためにはどのような情報・分析が必要か、という検討プロセスがおろそかになっていることが少なくありません。冒頭の脆弱性情報の場合、「自社システムに関連する、深刻度の高い脆弱性情報の把握」、「自社システムに関連する、実際の攻撃での悪用が確認されている脆弱性情報の把握」、「自社システムに関連する、同業他社を狙った攻撃が確認されている脆弱性情報の把握」では分析の目的が異なり、必要となる知見や情報も異なります。インテリジェンスが「意思決定のための知見」であることを踏まえると、企業や組織においては、徹底して自組織で活用することを前提とした目的設定が必要だと言えます。

2. 乱立するスレットインテリジェンスサービスとその分類

昨今、さまざまなスレットインテリジェンスサービスが提供されています。冒頭の脆弱性情報やIoC、APT（Advanced Persistent Threat）の詳細解析情報、ダークウェブのモニタリング情報、地政学リスクとサイバー攻撃の分析情報など、内容は多岐に及びます。こうしたスレットインテリジェンスサービスの全体像は、次の3つに大きく分類することができます。

ストラテジック型

政治・経済・社会・技術などのマクロ要因とサイバー攻撃の関係性を分析し、情報提供するサービス。実際に発生したサイバー攻撃の背景、攻撃者像、各国・組織のサイバーセキュリティ関連動向の分析を行うことで、将来的に想定されるサイバー攻撃のリスクを洗い出す。

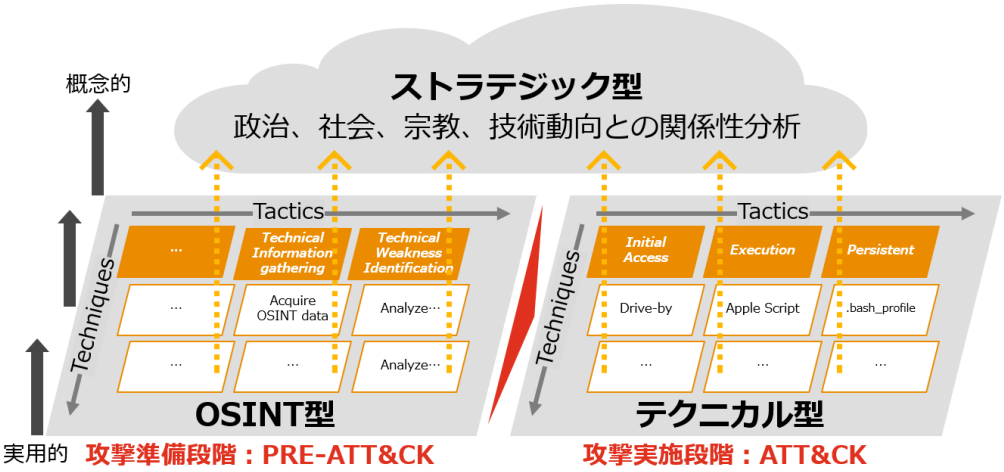
OSINT（Open Source Intelligence）型

ダークウェブを含むインターネット上の公開情報を対象として、情報を収集・分析し、情報提供するサービス。サイバーセキュリティ対策を行う上で認識すべき脆弱性情報、漏えい情報、攻撃の予兆、インターネットに露出したShadow ITデバイスなどの攻撃者にとって有益な情報を提供する。攻撃者から見た場合、攻撃準備段階に相当する（MITRE-PRE-ATT&CKで説明される戦術に相当）。

テクニカル型

実際に発生したサイバー攻撃やAPTを詳細に解析し、情報提供するサービス。最新の攻撃手法を明らかにし、その対策や攻撃に関連したIoCなどを提供する。攻撃者から見た場合、攻撃実施段階の手口に相当する（MITRE-ATT&CKで説明される戦術に相当）。

図表2：スレットインテリジェンスの全体像



こうしたスレットインテリジェンスサービスを活用するためには、前述のとおり、分析の目的が明確になっていることが重要です。サービス側で必要な分析が行われており、提供される情報が自組織にとって必要な知見である場合は、追加の分析は必要ありません。一方で業界または自社特有の情報、特性を考慮する必要があるといった理由でサービス側での分析が不十分な場合は、追加での分析が必要となるため、事前にアウトソース・インソースする内容を見定めておくことが必要です。

3. CSIRTでスレットインテリジェンスをどう活用するか

CSIRTでのスレットインテリジェンスの活用を考える場合、外部のスレットインテリジェンスサービスの利用有無、インソースでの追加分析の有無に関わらず、分析により得られた知見を活用するためには、既に一定水準でCSIRTの活動が定義・運営されている必要があります。

この前提において、初めに自組織のCSIRTがサイバーセキュリティ対策のどの機能を担うのかを明らかにする必要があります。例えば、NIST CSFの一要素である「特定」を考えた場合、「サイバーセキュリティ資産管理」によるCSIRTパフォーマンスの最大化でも紹介したように、IT資産管理が各業務部門に分散しているケースもあれば、サイバーセキュリティ資産管理の導入により必要な情報がCSIRTにより管理されているケースも考えられます。また、「対応」「復旧」についてもCSIRTが中心になるケース、インシデントが発生した事業部門が中心となるケース、インシデントに応じて組成された対応組織が中心となるケースなどが考えられます。そのため、まずはCSIRTが行う活動において存在する課題、高度化が必要となる項目を明らかにし、分析の目的を設定します。一例を以下に示します。

- 自組織のビジネス戦略に基づいて採用するIT技術に対してどのような攻撃が行われているのか、想定されるのかを明らかにする。これにより、「防御」「検知」の仕組み、対応体制を準備する。
- 自組織の資産管理から漏れているShadow ITを特定する。これによりShadow ITへの対策を促す。
- 自組織に関する漏えい情報、漏えい時期、漏えい元を特定する。これにより見逃していたインシデントを特定し、被害範囲の把握、原因究明、再発防止策を実施する。また、外部サイトからの情報流出の場合は、利用サービスの見直し、選定基準の改訂などを促す。
- 同業他社を狙った最新の攻撃手法を把握する。これにより、導入すべき検知、防御の仕組みを明らかにし、対策を実施する。
- 日々発見される脆弱性について、実際に自社への攻撃が想定される脆弱性を特定する。これにより、当該脆弱性について例外的な対処を行う。

上記の例は、現実には一筋縄ではいかず、課題として認識されているものの改善されないまま放置されていることが少なくありません。スレットインテリジェンスは「自組織の意思決定のための知見」である以上、自組織固有の特性を含んでおり、異なる組織間で共通して活用できることはあっても、それが一般化されることはありません。「目の前にある情報をどう有効活用するのか」ではなく、問いに相当する「分析の目的」の設定と、その答えに相当する「実装と運用」のサイクルを継続的に回し、双方のレベルを段階的に上げていく必要があるのです。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表） Mail：jp_cyber_inquiry@pwc.com

© 2020 PwC. All rights reserved. PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.