ホワイトペーパ

サイバー脅威インテリジェンス（CTI）プラクティスの構築に向けた利害関係者中心のアプローチ

経営幹部、ビジネスの利害関係者、セキュリティ運用、インシデント対応者を脅威インテリジェンスに関与させる方法

目次

要約

サイバー脅威インテリジェンス（CTI）のプラクティスを確立すれば、組織はプロセス、人、テクノロジーを複数の利害関係者に提供でき、サイバー脅威への対抗に威力を発揮する。

本書は以下を示す：

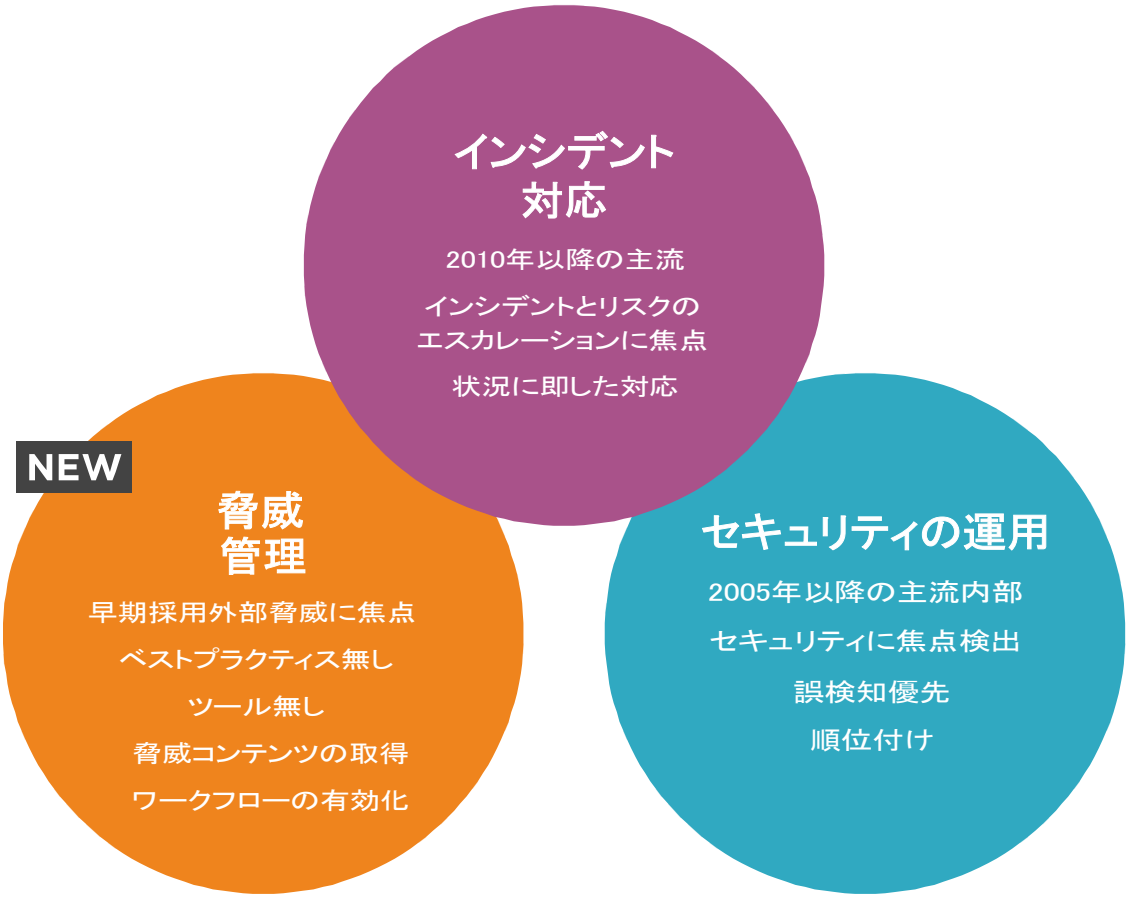
- **サイバー脅威インテリジェンスの実践（プラクティス）によって、サイバー脅威に対抗できる強力なインテリジェンス機能の必要性がどのように満たされるかを説明する**
- **多様なインテリジェンスソースに起因する「情報過多」の問題を掘り下げる**
- **インテリジェンスの手動プロセスの経済的および運用上のコストを明らかにする**
- **サイバー脅威インテリジェンスのベストプラクティスを確立するための推奨事項を示す**
- **サイバー脅威インテリジェンスの実践をサポートする専用プラットフォームの主な機能を概説する**

実践としてのCTIの出現

サイバーセキュリティのリーダーは、サイバー脅威に対する防御を強化するべきだと十分に認識している。大規模な組織のテクノロジーセキュリティに関する意思決定者を対象としたForresterResearch社の調査では、回答者の77%が、サイバー脅威インテリジェンス（CTI）の各機能の確立/改善の優先順位を高または重要としている。1

しかし、テクノロジーのリーダーがサイバー防御を自分で処理するだけでは十分ではない。新世代の強力なサイバー脅威に直面する今、「境界」での防御を維持するという古いアプローチはもはや実用的ではない。

サイバー防御は、従来から受け身型のビジネス機能と見なされており、古いソフトウェアパッチや侵入の試みなどの個別の指標に対応する役割を担っている。このアプローチではもはや不十分である。新たなサイバー脅威は、セキュリティオペレーションセンター（SOC）やインシデント対応（IR）チームではなく、サイバーインテリジェンスの実践アプローチで処理する必要がある。

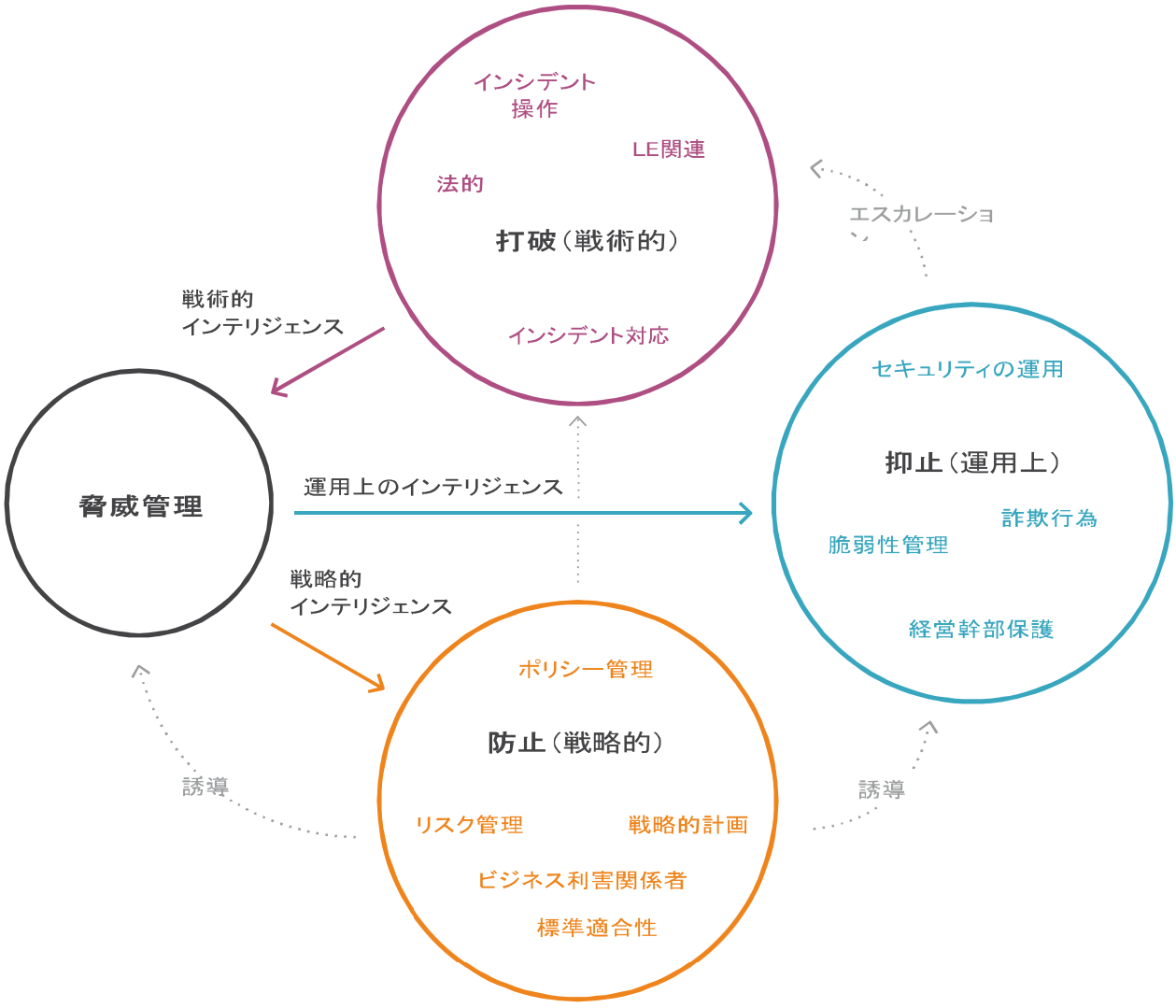


1）Forrester Research社Rick Holland「The State of the Cyberthreat Intelligence Market」2015年6月23日

新しい脅威の環境では、サイバー防御はもはやIT部門に委任できるものではない。代わりに、ビジネスリーダーは、急速に変化する脅威への危険状態を管理するために必要なリソースにアクセスできるようにしながら、組織内に存在するサイバー脅威についての認識を高める必要がある。

サイバー防御への新しいアプローチは、別の協議的な実践としてのCTIに依存している。これは組織内のサイバーセキュリティの継続的な改善に専念するプロセス、人員、およびテクノロジーで構築されている。CTIの実践（プラクティス）によって、CTIと事業部門間の広範な連携を通じて、ビジネスプロセスを継続的に監視するインテリジェンスへの適応がなされる。利用可能な最高のサイバー脅威情報を備えたCTIプラクティスの脅威アナリストは、マネージャーと相談して、さまざまな利害関係者のセキュリティ態勢を改善する。

一般的なインテリジェンスプラクティスと同様に、CTIプラクティスは次に示すように、運用上、戦術的、および戦略的なあらゆる達成目標を掲げる組織をサポートする。



インテリジェンスの実践では以下のことを行う。

- **セキュリティの取り組みの計画を通知するための戦略的インテリジェンスの可用性を確保**
- **運用上のインテリジェンスを統合して、既知の脅威を確実に抑止**
- **「脅威ハンティング」を介して新規や新興の脅威を発見**
- **インシデントが発生した場合に、迅速かつ最小限の影響で対処できるように、戦術的インテリジェンスを準備**
- **適切なガバナンスと制御を確保するために、各ステップで組織への露呈を評価**

CTIにはサイバー脅威に関連して独特で前例のない側面があるため、次に示すとおり、通常インテリジェンスプラクティスが直面する課題よりも先に進んでいる。

サイバー脅威は毒性が強い。サイバー攻撃には、光ファイバインターネットトラフィックの速度でグローバルネットワーク全体に広がる能力がある。さらに、重要なシステムがデジタル制御下に置かれている範囲を考えると、サイバー脅威にさらされる危険の可能性は
巨大であり、日ごとに増加している。このことは大規模で複雑な組織に特に関係する。小規模で単純な組織よりも、電子経路を介した相互作用点が多く、魅力的なターゲットが多い傾向があるためである。

サイバー脅威は絶えず進化している。攻撃者が持ちそうな動機としては、顧客データや資金を盗む金銭的動機、政策や慣行を変えようとする政治的動機、スパイ活動の一形態として企業情報を盗む商業的動機、または敵側に損害を引き起こすための軍事的動機
などが考えられる。こうした脅威はすべて過去から存在してきたが、今日、サイバー脅威はグローバルに、同時に、即時に存在する。

新しいアクターは、攻撃者として一瞬で信頼を手にする。開発されたツール、開始されたキャンペーン、実行された攻撃に関する知識が広まっているため、新しい動機を持つ新しい攻撃者は、必ずしも高度なコンピュータスキルがなくても、新しいターゲットを攻撃できる。

防御には専門性の高い知識が必要である。攻撃の検出や防止には、知識と専門的技術に多大な投資を要する。さらに、防御側は、攻撃による損害を軽減するために、ビジネスシステムの実践的な経験が必要となる。

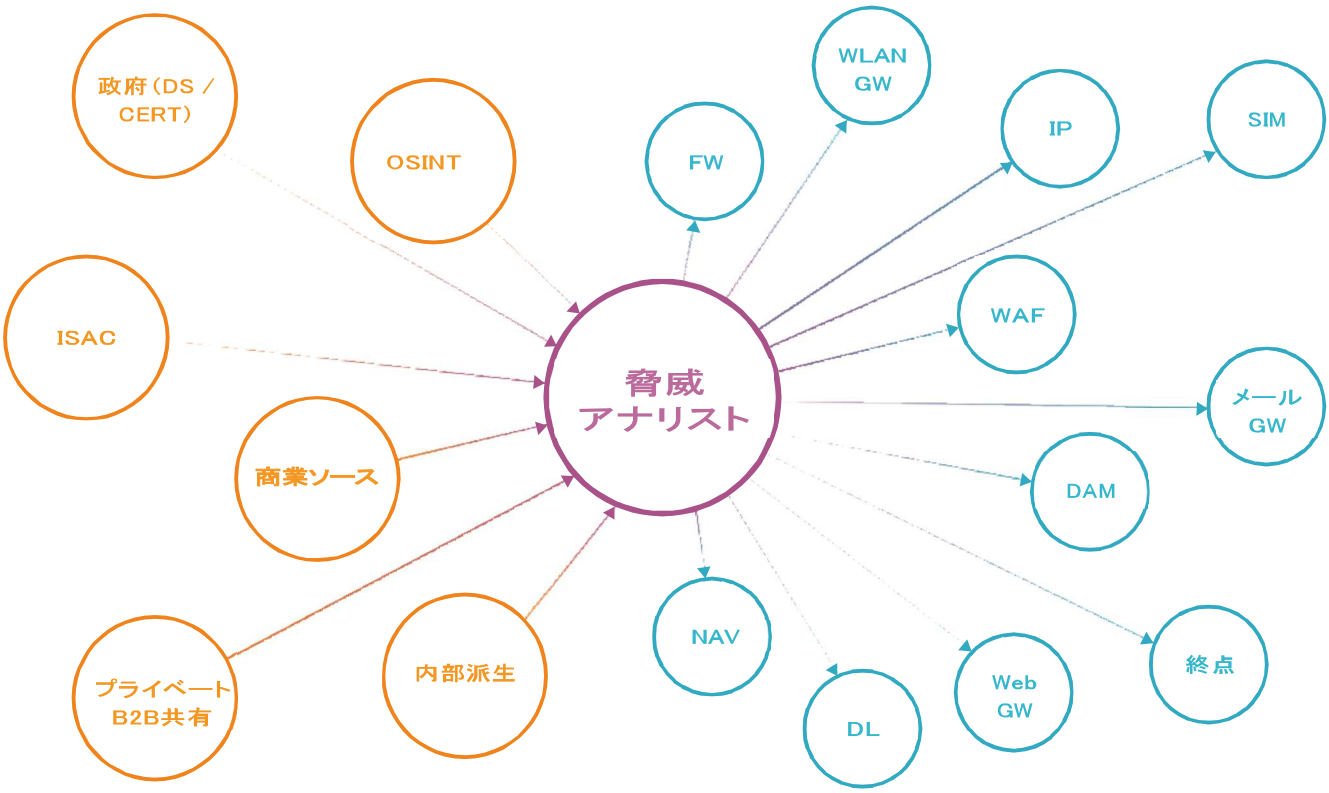
CTIプラクティスは、従来のインテリジェンスプラクティスの機能から拡大して、サイバー脅威がもたらす固有の課題にまで及ぶ。

「情報過多」の問題

脅威アナリストが直面する大きな課題の1つが、現在のまたは可能性のある攻撃に関する圧倒的な情報の洪水である。反復的なデータフィードの多様なセットを組み込む必要があるため、CTIアナリストは、「信号対雑音」比が低いデータプールをふるいにかける必要がある。つまり、ノイズが多すぎる。

商用CTIフィードは主要な情報源であるが、それらのインテリジェンスの正味価値を完全に評価することは困難であることが多い。アナリストは、各プロバイダーが独自の機能や情報へのアクセスを提供している範囲を判定し、利害関係者の情報ニーズを常に満たせるかを判断する必要がある。

情報共有・分析センター（ISAC）はさまざまな業界に設立されており、サイバー脅威インテリジェンスに関連する貴重なデータを提供する。しかし、この種のインテリジェンス交換や共有コミュニティは、提供する情報が少ないのではなく、多いという点で誤りがちである。ISACに参入すると、無関係なデータが大幅に取り込まれる可能性があるため、これを人手で確認するには人材への多額の投資が必要となる。



内部のプロセス、人、およびシステムについても、可能性のあるインテリジェンスデータの膨大な集積が生まれる。サーバー、接続、およびアクセスログは豊富なデータソースであり、異常な動作に関連する警告を検出して重要視していくためのさまざまな分析手法がある。業界によっては、人とプロセスによって実用的なデータをCTIアナリストに提供することもできる。

ほとんどの組織は、収集された脅威データの中から最も関連性の高い情報を探し出すために格闘している。

関連性を判断する正式なテクノロジー主導の方法がない限り、組織は大量のインテリジェンスの処理を人手に頼らねばならない。うまくいけば、労働重視の方法で、誤検知からなる大きな作業負荷に取り組むことになる。しかしありがちなのは、最終的に情報過多となり、回避できたはずのサイバー脅威に利害関係者をさらすことである。

さまざまな利害関係者がさまざまな方法で情報過多を経験することになるだろう。
次のような状況が起きやすい。

- **セキュリティオペレーションセンター（SOC）が受け取る脅威関連の警告信号が多すぎるため、最も重要な脅威を判別したり、それに対応したりすることができない。**
- **脆弱性管理チームの気付きによれば、ITシステムの脆弱性のうち、影響の小さいものと大きいものを区別するのが難しい。あるいは、既知の搾取ベクトルへの対応が遅れている。**
- **インシデント対応および運用（IR）チームにおいて、攻撃前や攻撃中のある時点で、組織の詳しい状態を正確にまとめ上げるのは困難である。**
- **ビジネスの利害関係者は、何かが起こる前は脅威レベルにほとんど気づいていなかったり、何が起こったのか漠然としかわからなかったりする。**
- **IT設計者は、最初からベストプラクティスを組み込む場合に比べて、セキュリティ強化の改造にコストがかかるようなITインフラストラクチャの決定を下す。**
- **経営幹部と意思決定者は、インシデント発生前の組織の危険状態をあまり理解していない。そのため、実際の脅威に見合うようにではなく、主に規制や評判につながる事柄に反応して対応する。**

インテリジェンスにおける手動プロセスの高コスト

CTIアナリストの仕事は困難で要求が厳しい。なかでも、受け取るインテリジェンスの関連性を判断し、新しい脅威を発見し、既知の脅威と新しい脅威を関連付けなければならない。これらの任務はすべて、気が遠くなるほど遅くて非効率的な手動プロセスに頼る場合、さらに悪化する。

他の一般的な労働集約型の任務とは異なり、インテリジェンスの問題に対して多くの人員を投じることは、通常は非現実的である。アナリストの人材が不足しているのは、サイバー脅威インテリジェンスに関連する任務を実行する新しい職員を探し、評価し、訓練することが困難なためである。したがって、CTIの慣行は、素質と処理能力が限られるわずかな人材バンクの制約を受ける。

アナリストは最終的に、利害関係者のニーズを満たす責任があるため、組織が利用できるインテリジェンスの価値を十分に活用する。反復の手作業は時間の浪費となる。それよりも、適切な情報を適切な人に、適切な場所とタイミングで確実に届けられるように時間を使うほうがよい。

また、協議的なCTIプラクティス内でアナリストの役割が拡大される可能性を考えると、手動プロセスに依存しすぎると、インテリジェンス機能とビジネス機能の統合がしにくくなり、コストがかかる。

CTIプラクティスがうまく機能すると、効果的な検出、防止、および対応の各機能を備えたさまざまな社内事業のプラクティスを支援できる可能性がある。しかし、そのようなレベルの統合には、圧倒的なアナリストチームでも叶わないようなレベルの尽力が求められる。

アナリストは、CTIの新しい分野のベストプラクティスに遅れずについていき、その教訓を組織内の状況に適用する必要がある。さらに、脅威データの評価を安全なリポジトリ経由で、関与する利害関係者に配布し、脅威環境を考慮して組織のプロセスが十分に保護されるようにしなければならない。

こうした可能性が常にあるため、インテリジェンスの手動プロセスのコストは、労働力に対する支払いの直接原価をはるかに超える。コストの実際の計算では、CTIの実践がなく、組織の利害関係者をサポートする最良の機会をアナリストに与えないことによる機会費用を考慮しなければならない。

CTIプラクティスを確立する方法

CTIプラクティスの設定という組織の挑戦では、運用上、戦術上、および戦略上の幅広い問題に注意が必要である。以下に重要な推奨事項を挙げる。

組織図に空きを作る。CTIはITセキュリティに非常に近く関係しているが、別個の機能とみなすべきである。そのような機能において、CTIプラクティスの責任は、明確に定義された自らのプロセスに対して割り当てられ、さらに人員配置と
技術に関して適切なサポートを受けるべきである。また、CTIプラクティスは、セキュリティ運用、インシデント運用、インシデント対応、不正運用、リスク管理など、他のいくつかの既存の組織機能と連携する必要がある。報告、コミュニケーション、責任の境界線は、前もって十分に明らかにしておくべきである。

IT容量を固定する。CTIプラクティスでは、独自のIT開発チームを維持しなくてよいかもしれないが、それでも、CTIフィードの取得など、標準のCTIプロセスおよび手順を設計、計画、および導入できるITリソースの可用性を確保する必要がある。さらに、CTIプラクティスでは、基幹業務システムへの変更やセキュリティ改善の展開を担う、バランスの取れた機能横断的なチームにすぐにアクセスできる必要がある。

バランスの取れたコアチームを構築する。CTIプラクティスには、次のような補完的なスキルセットを備えるリソースが含まれる。

- **テクニカルコレクションアナリスト、コレクションマネージャー、脅威アナリスト、ウォッチセンターアナリスト、インテリジェンスオペレーター、またはインテリジェンスマネージャーなどのインテリジェンスの専門家**
- **インテリジェンスの正規訓練、または批判的思考における同様の訓練**
- **異文化間または組織間の場合を含むプロジェクト管理**
- **変更管理**
- **リスク管理**
- **システムエンジニアリング、セキュリティエンジニアリングなど、実用的なITセキュリティの導入と運用**
- **脆弱性、マルウェア、サイバー脅威、詐欺、ポリシー分析など、1つ以上の主要テーマの分野におけるアナリストの実務経験**

CTIフィードの適切な収集を管理する。CTIフィード、特に商用フィードは、サブスクリプションとテクノロジーにかなりの投資を要することが多い。CTIプラクティスが、利害関係者への価値の観点から、新しいCTIフィードの期待インテリジェンス価値の測定機能を備えるようにする。影響を明確に理解した場合にのみ、CTIフィードへの投資を増やすこと。

テクノロジープラットフォームによる立ち上げ。CTIプラクティスの機能を実施または改善する際の一般的な課題に対応する新しいテクノロジーが登場した。これらのツールによって、ワークフローとプロセスのコアセットを迅速かつ簡単に展開できるようになる。テクノロジープラットフォームのワークフロー機能が、CTIプラクティスのビジネス要件をすべて満たすようにすること。

利害関係者重視のCTIソリューションを提供。CTIから事業価値を生み出すには、組織の主要な利害関係者の情報ニーズを微細に理解する必要がある。CTIプラクティスの支援があるとしても、最終的には申し分のない抑止、打破、防止の戦略を実行する責任は利害関係者の肩に掛かっている。CTIの実践がプラスの影響を与えるためには、
実践チームは、主要な利害関係者が誰なのか、彼らが答えるべき質問が何か、インテリジェンスのどのような取り込みと周期を好むかを理解しなければならない。

利害関係者の賛同を得る。CTIの実践を成功させるには、利害関係者は、共有ビジョンと現在のセキュリティの長期計画に満足している必要がある。どの程度、どのようなペースとステップで、どのような事業上の制約において達成したいと考えているかを、利害関係者から理解されるようにしておくこと。測定可能な結果で約束を果たすこと。

利害関係者グループを具体的に支援。CTIプラクティスは、IT機能の内外を問わず、組織内のさまざまな機能を包括的にサポートする必要がある。

- **セキュリティオペレーションセンター（SOC）は、主要な脅威に関連する構造化指標と警告信号を、構造化されて機械で読み取り可能な形式（CSV、STIXやベンダー固有の形式など）で送信するように要求する。**
- **脆弱性管理チームが要求するのは、ITシステムの組織に対する新興で影響力大の脆弱性と既知の悪用ベクトルに関するインテリジェンスの文書である。**
- **インシデント対応（IR）および運用チームが要求するのは、臨時で特注のインテリジェンスである。これらはツール、手口、関連するキャンペーン、アクターの意図と帰属、および侵害ポイントに関するフォレンジックデータに関連する。**
- **ビジネスの利害関係者には、自らの責任範囲に関する主要な脅威と、それらの事業運営への影響の可能性について、定期的な情報更新が必要である。**

- **ITアーキテクト**には、ITインフラストラクチャの構成と進行中のサイバー脅威の現実とが整合されるように、ITセキュリティへの一般的なアプローチに対する主要な脅威について、最新の連絡が必要である。

- **経営幹部と意思決定者**は、組織が直面する危険状態と主要な脅威に関する、継続的でハイレベルなレポートを必要とする。

TIPに依存するサイバー脅威インテリジェンス

CTIプラクティスの技術支援を計画するときは、脅威インテリジェンスプラットフォーム（TIP）が以下の各中核機能に対応していることを確認する。

1 マルチソースの収集と交換

CTIフィードには異世界の多様な雰囲気がある。CTIフィードを利用し、CTI交換やコミュニティを通じて双方向の会話に参加する機能などで、親和性を確保すること。

要件：

- **TAXII、FTP、電子メール、Web API、独自のAPI、その他の送信機構との互換性**
- **STIX、PDF、CSV、JSON、OpenIOCおよびその他のデータ形式との互換性**
- **利用可能なオープンソースデータフィードの即時のサポート**
- **IBM X-Force、Facebook ThreatExchange、RiskIQ PassiveTotal、ThreatConnectコミュニティ、業界、政府後援のISAC、ISAO、およびその他の地域コミュニティなどの、CTI交換およびコミュニティとの互換性**
- **情報源に基づく承認**
- **情報の処理方法のマーキングと表示を含む、ソース格付けのサポート（例：トラフィックライトプロトコル）**

2 統合と正規化

アナリストが利害関係者に代わってインテリジェンスの価値の十分な恩恵を受けられるように、適切なコンテキストにおいて脅威情報の一貫性を確保する。

要件：

- **統合および正規化されたデータ構造を持つ共通参照モデル**
- **一般的エンティティの抽出手法**
- **自然言語処理（NLP）**
- **エンティティの重複排除**
- **エンティティのホワイトリスト／ブラックリスト**

3 強化

内外のデータソースの追加情報でCTIフィードが強化されるため、脅威の相関関係と関連性をさらに判断できるようになる。

要件:

- **内外データソースの簡単な組み込み**
- **一般的なデータ形式のサポート**

4 関連性と選別

CTIアナリストが、組織に影響を与えない脅威にリソースを浪費せずに、関連する脅威インテリジェンスに集中できるようにすること。

要件:

- **高度な検索**
- **CTI処理のためのルールベースまたは発見ベースの推奨エンジン**
- **自動または半自動の選別と認定**
- **選別ワークフロー**

5 複雑な分析

コア分析用の可視化ツールやその他の強力なリソースでアナリストを支援する。要件:

- **グラフの高度な考察**
- **グラフ分析**
- **各機能のエクスポート**
- **第三者の分析ソフトウェアとの統合**

6 脅威の登録

組織全体に影響する脅威についての構造化情報を管理し、現在の理解と予想危険状態を積極的に追跡する。

要件:

- **ケース管理**
- **キャンペーン管理**
- **トピック管理**
- **懸念事項管理**
- **利害関係者管理**

7 IOC管理

重要な懸念事項に関連する侵害の痕跡(IOC)と警告信号を検証し、追跡する。アナリストがIOCと警告信号の有効性をきめ細かく制御できるようにし、結果のデータを使用して検出、防止、および応答機能を改善できるようにする。

要件:

- **指標と警告信号の信頼度**
- **誤指標のホワイトリスト**
- **IOCの署名の動的生成**
- **ITセキュリティコントロールに統合するためのIOCおよび警告信号の変更のサポート**
- **強化による第2および第3レベルの警告信号の自動生成**

8 作成と配布

内部の利害関係者のニーズをサポートするために、内外のインテリジェンスソースを組み込んだレポートを作成する。

要件:

- **構造化インテリジェンスと非構造化インテリジェンスを組み合わせる機能**
- **脅威レポート**

- アクターのプロファイルレポート
- インシデント情報レポート
- キャンペーンレポート
- ツール、技法、手順に関する情報のナレッジ管理
- 脆弱性インテリジェンスと搾取対象
- 対処方針
- 侵害の痕跡と警告信号
- アナリストワークフロー
- 利害関係者へのワークフロー配布
- 非構造化形式への対応（Microsoft Word、PDF、電子メールなど）
- 構造化形式への対応（CSV、Microsoft Excelなど）

9 ITセキュリティコントロールとの統合

インテリジェンスとITセキュリティコントロールがタイムリーに統合されるようにする。

要件：

- 侵入検知システム（IDS）、IDプロバイダー（IdP）、エンドポイント検出および応答（EDR）システム、セキュリティ情報およびイベント管理（SIEM）システムとの統合
- きめ細かなアクセスポリシー
- インテリジェンス統合の監査証跡
- TAXII、FTP、電子メール、Web API、その他の独自のAPIを含む送信機構との互換性
- STIX、CSV、独自の形式を含むデータ形式との互換性
- HP ArcSight、IBM QRadar、LogPoint、Splunkなどの一般的なSIEM形式との互換性

EclecticIQについて

EclecticIQは、応用サイバーインテリジェンステクノロジーのプロバイダーであり、企業のセキュリティプログラムや政府機関が脅威インテリジェンスを立ち上げできるようにします。アナリストが脅威の現実に対して制御を取り戻し、それに応じて危険度を軽減できるようにします。

EclecticIQが目指すのは、サイバー攻撃者との戦いにおけるバランスの回復です。その主力製品であるEclecticIQ脅威インテリジェンスプラットフォームは、セキュリティ情報交換の運用化を実現し、アナリスト共同ワークフローを強化し、確実にサイバー脅威インテリジェンスの検出、防止、および対応機能をタイムリーに統合します。

EclecticIQは、オランダのアムステルダムに本社を置く株式非公開企業で、ロンドンにオフィスを構えています。

2015年EU IPACSOサイバーセキュリティ賞を受賞し、NATO NCIエージェンシーセキュリティインキュベーターのパートナーです。

EclecticIQの詳細については、www.eclecticiq.comをご覧ください。

販売や製品のデモについては、sales@eclecticiq.comにお問い合わせください。または、電話+ 31（0）20 737 1063におかけください。

Twitterは@eclecticiqをフォローしてください。