ホワイトペーパー

人間主導の脅威インテリジェンスでSOCを強化する

先進的で執拗なハッカーからの無限の攻撃の波をかわし、セキュリティオペレーションセンター（SOC）の担当者は、インテリジェンスデータをフィードし、エンドポイントデバイスのセキュリティのためにプロセスを対応させて、プロセスの自動化を一層進めています。しかし、それだけで十分とはいえません。自動化ツールを使う人間のハッカーは、自動化ベースの防御を備えた人間の防御者と対決するべきです。そのため、インテリジェントSOCを構築する最善の方法は、脅威インテリジェンスの実践に有能かつ自動化によってサポートされた人間のアナリストを配置することです。

SOCにおける自動化の制限

もしも物理的な施設が泥棒の標的にされていたら、すべてのアクセスポイントにカメラとセンサーを設置するだろう。次に、警備員を雇って、昼も夜も入口を監視し、事件が展開すれば迅速に対応する。

セキュリティオペレーションセンター（SOC）は、CCTV制御室に相当するサイバーセキュリティを体現している。CCTVカメラやセンサーの代わりに、ファイアウォール、侵入防止システム、その他のセキュリティ検出および応答ツールを管理する。ちょうど物理的なセキュリティ対応と同様である。こうしたITセキュリティコントロールからの情報は、セキュリティ情報およびイベント管理（SIEM）ソリューションにまとめられる。このソリューションは、企業全体に及ぶ単一の統合セキュリティ重視コントロールパネルとして機能し、SOCスタッフが脅威の進化に応じて攻撃を軽減したり、攻撃に対応できるようにする。

SOCは運用上の施設として設計されている。運用上の考え方では、ダッシュボードのすべてのライトが緑色に点灯していれば、何も問題はない。ライトの1つが赤く点滅していたら、問題を見つけて修正する。すべてのライトが赤く点滅している場合は、計器にシステム上の問題があるか、深刻な問題が発生していて、さらにサポートが必要となる。

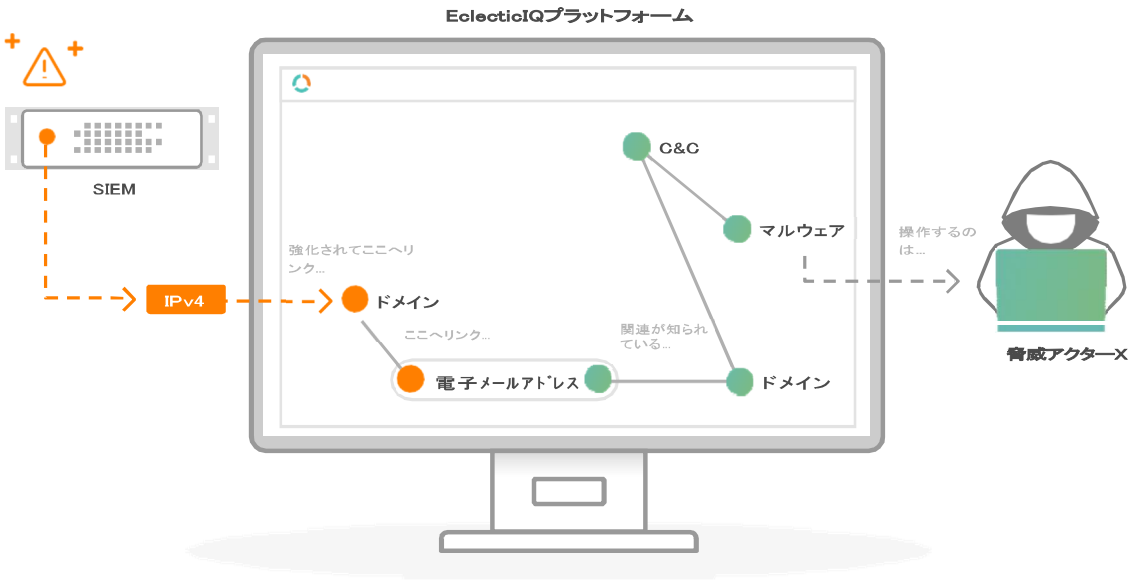
現在、SIEMには計装の問題がある。オンラインの顧客とチャネルの拡大、モバイル機器の企業BYODポリシー、IoT機器の急速な普及、メッシュベースのサービスファブリック、および一般的なデジタル化などがあるため、SOCは急速に増加するボリュームや、さまざまなアラートとセキュリティイベントに対処してこなければならなかった。重要でない軽微な事項が多すぎると、SIEMダッシュボードが赤く点灯し、オペレーターが重要なものと些細なものを区別できなくなるほど、アラートが絶え間なく発生する。

こうなるとSOCには、次のような最適とはいえない2つの応答のいずれかが残される。その1つは、最も明白な攻撃にのみ応答することでアラームのしきい値を上げ、もっと危険な他の脅威を確認せず放置すること（つまり、検知漏れ過多）。2つめは、生産性の低いインテリジェンスのリードを追うために膨大な時間を費やすこと（つまり、誤検知過多）である。

手に負えないほどの頻繁な通知に圧倒されて、SOCは、アラートと通知に対する応答の処理、選別、および手作業を介さない誤検知排除を自動化することに目を向けてきた。ここで自動脅威分析の全体的なソリューションのカテゴリーが登場して、SIEMデータに基づいてパターンを検出し、異常な動きを特定し、さまざまな脅威を自動的に検出するようになった。テクノロジープロバイダーは、今後3～5年以内に機械学習などを使って自動化されるような、脅威インテリジェンスとセキュリティ運用のバラ色の未来を描いている。この根底にあるメッセージは、自動化によって、警報ベルを鳴らすのをやめて実務に戻れるということだ。

しかし、自動化自体が潜在的なセキュリティの弱点を表している。最も価値の高いターゲットは、最も才能あるハッカーから攻撃される。彼らは最も洗練された自動化アルゴリズムさえも通過できる十分なリソースを備えている。現実には、サイバー攻撃に対する防御は、自動化やAIが簡単に解決できる問題ではない。AIベースのアプローチには不確実性が多すぎ、すぐに使用できる攻撃方法が多すぎ、データセットが希薄すぎるため、最も危険なハッカーを相手に包括的に防御するには不十分である。多くの場合、利用できるデータからのAIの学習方法には必然的な傾向があり、その傾向の理解と学習は、防御とプロセスに対抗する敵対者側でも利用できることがある。

スマートな攻撃者には、スマートな防御者が対抗しなければならない。身を守るためには、適切に管理され、十分に監視された自動化の支援を受ける、献身的な人間のインテリジェンスが今でも必要である。



なぜSOCはインテリジェンスの処理が不得意なのか？

多くのSOCは、受け取る脅威の状況に関する実質的なデータを含む、良質なインテリジェンスフィードをすでにサブスク契約している。しかし、こうしたフィードの内容に常に関与しているSOCアナリストは珍しい。

第1の障害は、複数のフィードに異なる視点の重複データが含まれることである。複数のフィード間でデータの正規化と重複排除を行い、近接する脅威を微細に理解したうえで対処方法に優先順位を付けなければ、インテリジェンスはノイズと解釈されやすい。

十分に正規化したインテリジェンスフィードであっても、SOCによくあるやり方は静的な対応でしかなく、受け取ったデータを複数のITセキュリティエンドポイントにコピーすることである。たとえば、特定の攻撃でIPアドレス「1.2.3.4」が使用されたという情報をSOCが受け取った場合、SOCは「IP1.2.3.4」を企業のファイアウォールに迅速に送信してブロックする。このようなプロセスは簡単に自動化できる。

それでも、最高の自動化でさえ、IPアドレスを切り替えてしまう攻撃者を止めることはできない。そのため、攻撃方法や攻撃者の動機についてさらに情報を得るためにIPアドレスを調査し、適切な対策を講じられる人が必要となる。

最も重要な課題は、SOCにあるのは、運用上の問題を抑え込むための短期的な視点ということである。批判するわけではない。実際、それこそがまさにSOCが設計された理由である。それでも、組織があらゆる種類の攻撃者を撃退するには、SOCの短期的な視点を、サイバー防御の長期的な計画と戦略に特化した別の組織機能と組み合わせる必要がある。そしてこれこそが、脅威インテリジェンスプラクティスの役割である。

効果的な脅威インテリジェンスプラクティスを構築する

SOCがアラートに苦心している場合、差し迫って必要なのは、代わりに脅威アナリストが選別を行うことである。そのための最初の業務は、政府、業界、第三者、およびオープンソースから組織に送られる複数のインテリジェンスフィードを、整理して正規化することである。社内のインテリジェンスアナリストがスプレッドシート、基本的なプログラム、または不十分な社内ソリューションを使いつつフィードの番をして日々を費やすことには、ビジネス上の価値はもちろんのこと、セキュリティ上のメリットもない。

これは脅威インテリジェンスプラットフォーム（TIP）の役割である。TIPの自動化機能を使用すると、脅威アナリストは複数のフィードの取り込みと処理を簡素化でき、外部ソースからの侵害の痕跡（IOC）を分類でき、それらのIOCを内部SIEMからの情報と比較でき、そしてSOCを介してセキュリティコントロールを適宜更新できる。これらのタスクはおそらくSOCアナリストでもできるだろうが、そうすると、専任の脅威アナリストがTIPによって実現できる、はるかに効果的なやり方の可能性を断つことになってしまう。

つまり、高度な脅威から組織を守るためには、受け取ったフィードの自動処理が必要であるが、それで十分ではない。

脅威分析者には、効率的なデータ処理だけでなく、効果的な調査を実施するためのツールも必要である。脅威インテリジェンスプラクティスの最も重要な責務は、事後対応ではなく事前に、より優れた防御を創り出すことである。そのためには、企業を裏の裏まで理解し、脅威の状況を十分に理解して全体像を把握できる人間のアナリストが必要である。アナリストは、受け取ったさまざまなデータフィードを利用して複雑な調査を実施する必要がある。そうすることで、軽微なインシデントとして最初にSIEMに表示され得るイベントの背後の、隠れた脅威を明らかにする。

脅威アナリストの自動化は、SOCアナリストの調査のワークフローを支援して調査を強化するべきである。また、組織の短期的で戦術的な防御と長期的な防御の両方に役立つ改善結果を得られるようにすべきである。

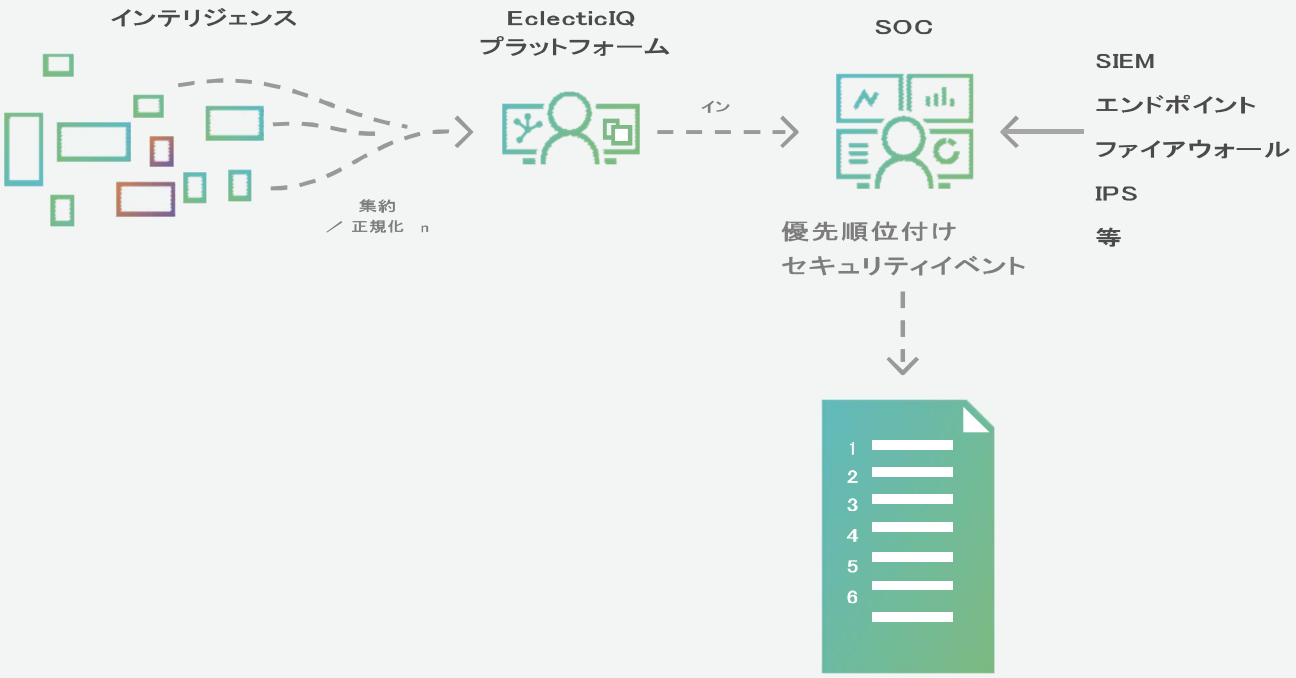
インテリジェントSOCにはインテリジェントTIPが必要

人間の脅威アナリストには、想像力と経験を組み合わせて戦略を練る能力がある。自動化すれば、こうした取り組みを企業規模で運用できる。TIPの自動選別ツールと自動検出ツールを使えば、脅威アナリストの働きが強化されて、SOCの円滑でさらに効率的な運用を即座にサポートできると同時に、セキュリティ機能と防御機能に長期的なメリットが生まれる。

TIPとSOCの統合により、脅威アナリストは、受け取ったインテリジェンスに基づいて、セキュリティツールとエンドポイントデバイスを自動的に更新できるようになる。たとえば、脅威アナリストが特定のIPアドレスに関するインテリジェンスを受け取った場合、最初のステップは、SOCの標準的な運用手順に従って、そのIPアドレスをブロックすることである。

さらに進んだところでは、脅威アナリストは、その後さまざまなインテリジェンスソースを調べて、関連するオブジェクト（たとえば、そのIPアドレスを使用するマルウェアやそのマルウェアに関連付けられたドメイン）を見つけることもできる。この調査結果に基づいてアナリストは、SOCが取る複数の対処と、必要に応じてIT担当者や会社に配布できる説明的な書面による警告を並べていく場合もある。このアプローチによって、SOCの適用範囲が大幅に拡大し、受け取ったインテリジェンスに対して幅広く効果的に対応できるようになる。

こうした分析タスクは、SOCが実行しない、実行するものとされていない、そして実行してはならない業務である。つまり、インテリジェントなSOCを構築するための最良の方法は、自動化を活用した脅威インテリジェンスの実践を支援することである。



インテリジェンス/SOCワークフロー
集約と優先順位付け

自動化を活用した脅威インテリジェンスの実践

例えるなら、プロボクサーが頭脳と腕力を組み合わせる方法だと考えてほしい。SOCが強靭な筋肉（ファイアウォール、侵入防止システムなど）と高速な反応時間を表すなら、自動化された脅威インテリジェンスプラクティスは意識的な頭脳を表し、そこで次の攻撃予測を試みる状況認識を育んでいる。パンチをブロックする（または避ける）には、素早くかつ強くあらねばならない。もしも対戦相手の戦闘スタイルとフットワークがわかっていれば、実に簡単なことである。プロボクサーや他のアスリートが対戦相手の動きの映像を熱心に何度も見るのと同じように、組織はサイバー攻撃者の動きの研究に時間を注ぐものである。

脅威インテリジェンスをSOCから分離すると、特に脅威レベルが上昇している期間には、その価値が証明される。大規模なサイバー攻撃を受けた時、セキュリティ防御を維持するか、または次の攻撃の到達場所を予測するか、SOCアナリストに選択を迫りたくないはずである。SOCが火消しで手が離せない時が、まさに他の人（この場合は脅威アナリスト）が必要な時であり、全体像に目を光らせておかねばならない。

企業から見た統合インテリジェンス主導型のサイバー防御のメリット

脅威インテリジェンスの実践でSOCをサポートする方法の重要ポイントを以下に挙げる。

1. 自動化中心ではなく、アナリスト中心のアプローチを採用して、サイバー脅威から保護する。
2. 脅威アナリストとSOCアナリストに別々の役割を割り当てる。
3. ワークフロー全体を自動化するTIPで脅威アナリストをサポートする。
4. 脅威アナリストに徹底調査を行う裁量を与える。
5. 受け取ったインテリジェンスを自動的に処理する、TIPとSOCのインテリジェントな統合を確立する。

いきなり第5のポイント（偶然にも、最も簡単に自動化テクノロジーで解決できる問題）に飛ぶのではなく、統合サイバー防御の作成に関連する組織設計、協力、および人材管理の各側面に注意深く取り組むこと。

この二重のアプローチは、他のインテリジェンス分野で機能することが証明されている。インテリジェントSOCが、既知の脅威に対する危険状態の可能性を重点的に軽減する場合でも、自動化TIPから権限を受けた脅威アナリストが、未知の脅威に重点を置くことができる。

以下に概説するように、企業全体にメリットがある。

SOCアナリスト

- **自動選別**：受け取るインテリジェンスによって誤検知が大幅に減り、時間を節約でき、リソースを維持できる。
- **質の高い情報**：IOCおよびその他の脅威データによって、複数のフィードを手作業で照合するという無駄なタスクに、労力が不要となる。
- **受け取ったインシデントの優先順位付け**：SOCアナリストが最も重要な脅威に集中できるようになる。
- **エンドポイントデバイスの自動更新**：最新の脅威インテリジェンスを活用する。
- **対処事項**：脅威アナリストの実践的な調査によって決定される。
- **運用重視の指示**：イベントの発生時にインシデントチームが迅速に対応できるようになり、望ましい事業成果につながる。

脅威アナリスト

- **調査の重視**：独自の洞察が得られ、より効果的に脅威を特定できる。
- **自動取り込みと融合**：複数のフィードを使用して、外部インテリジェンスデータとの完全な接続を確保する。

- **SIEMソリューションおよびエンドポイントデバイスへの統合**：脅威アナリストに対して、調査に不可欠なフィードバックループと、運用上の防御に関するリアルタイムビューを提供する。（たとえば、次のように想定してみる。脅威アナリストがインテリジェンスをSOCに提供すると、SIEM内のセキュリティイベントが発生し、組織が現在攻撃を受けていることが通知される。これを受けて脅威アナリストは、既知の脅威に再び焦点を当て、より関連性の高いインテリジェンスとIoCデータを提供できる。）
- **実用的で詳細な分析**：外部ソースを内部の計測と組み合わせる。
- **計測の改善**：SOCとの自動コラボレーションを通じて、脅威インテリジェンスをさらに効果的に監視する。

脅威インテリジェンスの上部

- **IOCの最適管理**：効果的かつ効率的なサイバーセキュリティ防御を確保する。
- **十分な調整**：TIPとSOCの計画を同期する。
- **報告の徹底**：検出したセキュリティイベントと取られた措置の詳細と概要。

CISO

- **戦略的概要の改善**：過去の脅威と差し迫った脅威に関する報告。
- **競合分析**：同等の組織に関して、サイバー攻撃をかわす企業のパフォーマンスを、利用可能なコミュニティデータから学ぶ。
- **測定基準の改善**：検出された脅威の数、重大度、および優先度を監視する
- **リスクモデル**：継続的な予算、人数、および投資レベルに対応。

会社の幹部

- **理解の向上**：脅威の状況の全体像を把握する。
- **意識の向上**：特に出張中にハッカーの標的とされやすい企業幹部について、個々の脆弱性への責任を育てる。
- **状況的コンテキスト**：セキュリティの問題を考慮してビジネスの意思決定が行われるようになる。

取締役会

- **危険状態管理とリスク管理**：過去および将来のサイバーリスクのエビデンスに基づいて、法的な、セキュリティ上の、および金融資産の影響に対する危険状態（エクスポージャ）を管理する。
- **サイバーリスク評価**：サイバーリスクの知識で意思決定を支援する。
- **意識を高める**：進行中のセキュリティ運用と潜在的な脅威について高レベルな概要を伝える。

EclecticIQは企業と協力して、自動化と人間主導型インテリジェンスプログラムを最適に組み合わせ、サイバーセキュリティプログラムを創りあげます。

これからインテリジェンスフィードの取り込みと使用を自動化し始める場合でも、脅威インテリジェンスプラクティスをゼロから構築する場合でも、既存のインテリジェンス機能を補完する外部機能を見つけようとする場合でも、EclecticIQには脅威インテリジェンスの課題を解決するための適切なソリューションとリソースがあります。

詳細については、以下をご覧ください。

EclecticIQプラットフォーム
www.eclecticiq.com/platform

EclecticIQフュージョンセンター
www.eclecticiq.com/fusion-center

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。