EclecticIQプラットフォームおよびMISP

サイバー脅威インテリジェンスを補足

常に変化し、ますます巧妙化するサイバー攻撃から自衛する最善策は何でしょうか？最も肝心なのは、自身を取り巻く脅威の現実を理解することです。結局のところ、個々の不具合や脅威ベクトルごとに備えをすることは、実行可能な対策ではないし、経済的に妥当なことでもありません。

サイバー脅威インテリジェンス（CTI）の力を活用すれば、不要な情報をカットして、自分に最も直結した脅威を特定できます。脅威インテリジェンスプラットフォームは、データを収集、フィルタリング、分析して実用的なインテリジェンスを生成し、脅威がもたらすリスクに関する知見を提供する上で重要な役割を果たします。

脅威の状況を明確に把握すれば、最も必要とする部分にリソースを割り当て、発生する可能性が最も高い攻撃へのセキュリティ体制を強化できます。

どの脅威インテリジェンスプラットフォームを選びますか？

市場には要件に応じて多数のTIPの選択肢があります。
以下に例を挙げます。

- 商業ソースまたはオープンソース
- 状況に即した実用的な脅威インテリジェンスまたはセキュリティ侵害インジケーター（IOC）指向型
- アナリスト中心の協働またはコミュニティ共有

両方の良いところを選択

市場の多くのTIPの中で、選択肢は1つだけとは限りません。EclecticIQプラットフォームでは、たとえば、MISP（Malware Information Sharing Platform）も選択できます。これらの製品は排他的ではありません。事実、それぞれの強みを享受できる、補完的ソリューションです。

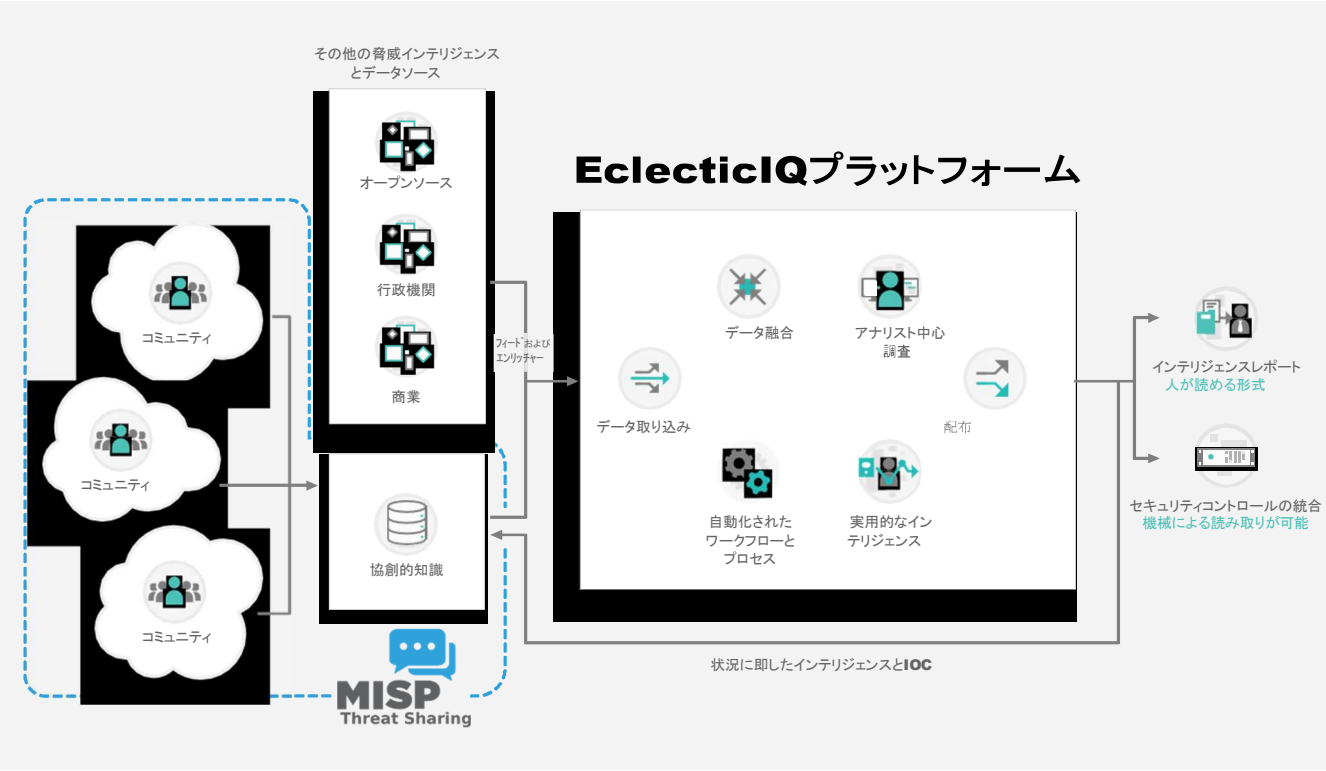
EclecticIQプラットフォームは、アナリストを中心に考えられたTIPであり、オープンソース、商品サプライヤー、業界提携先からのインテリジェンスデータを1つの協働アナリストワークベンチに取り込みます。EclecticIQプラットフォームを使用すると、複数のインテリジェンスフィードの処理に伴う手動の繰り返し作業がなくなるため、アナリストは最も重大な脅威を特定し、タイムリーに対策を講じ、組織に対処方法をアドバイスし、同業他社と協働することができます。EclecticIQプラットフォームは、業界のベストプラクティスがベースになっており、CTIワークフローと産業スパイ活動などに関するノウハウを中心に据えて開発されています。

MISPはオープンソースの脅威共有プラットフォームで、コミュニティのメンバーとマルウェアのナレッジベースで構成されています。ユーザーは、既存のマルウェアと脅威に関する協創的知識のメリットを享受できます。標的型攻撃のIOCを保存したり、相関付けたりすることができ、信頼できるコミュニティ内でマルウェアの技術的特徴を共有できます。共有の観点から見ると、
信頼できるコミュニティとは、自組織、特定のコミュニティ、つながりのある複数のコミュニティ、あるいはすべてのコミュニティであると言えます。

EclecticIQ

仕組み

MISPをEclecticIQプラットフォームに統合することで、MISPの強力な共有機能と広範なコミュニティのつながりによる恩恵を受けられるだけでなく、EclecticIQプラットフォームのアナリストを中心に据えた機能も活用できます。



既存のマルウェアと脅威に関するMISPの豊富な協創的知識は、EclecticIQ Platformが取り込む多くのソースの1つに過ぎません。

マルチソースの相関関係により、脅威の状況を包括的に確実に把握できます。EclecticIQプラットフォームはデータの融合により、脅威コンテンツを統合、標準化、強化します。EclecticIQ プラットフォームを利用すると、アナリストは認定、選別、検出のプロセスを自動化することで、大量の脅威インテリジェンスを日々処理することができます。動的な協働ワークスペース、直感的なグラフ、検索およびピボットツールを利用することで、アナリストは大量のデータを解読して、関係性、パターン、傾向を特定できます。検証される仮説が増えるにつれ、組織内でインテリジェンスへの要求にタイムリーに対応できるようになります。

EclecticIQプラットフォームは、プラットフォーム自体の中で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作成できる唯一のTIPです。レポートとデータはITセキュリティコントロールにメールで、または直接送信されます。最新のセキュリティ侵害インジケーター(IOC)や、脅威アクターとその侵入セット、関連するキャンペーン、ツール/技法/手順(TTP)などに関連する、STIX準拠のインテリジェンスを受け取ることができます。

EclecticIQプラットフォームとMISPの双方向の統合により、この実用的なインテリジェンスはMISPに容易に転送されて、関連するコミュニティ内で共有されます。

EclecticIQプラットフォームを選択すると、アナリストを中心に据えた実用的なインテリジェンスで強化した、コミュニティの協創的知識の共有といった、両方の良いところを享受できます。

EclecticIQ