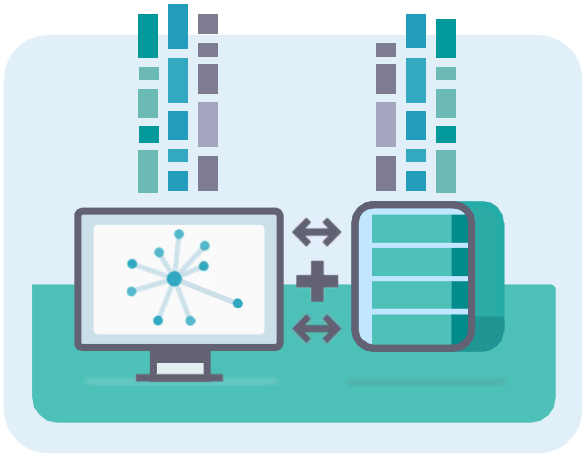
データシート

# EclecticIQ インテリジェンスフィード

*オープンソースと商業ソースからの、EclecticIQプラットフォーム用に最適化され、キュレートされたEclecticIQのフィードで主要な脅威を追跡。*



## はじめに

あらゆる組織が、セキュリティ上の弱点、多形マルウェア、フィッシング、ランサムウェアなど一連の主要な脅威に直面しています。サイバー脅威インテリジェンス（CTI）チームがこれらの脅威に対処するには、脅威インテリジェンスプラットフォーム（TIP）に信頼性の高い実用的な脅威データを取り入れる必要があります。これらのチームは通常、数百もの選択肢（オープンソースと商業ソース）がある市場からデータを収集します。

アナリストはこれらの市場からのフィードで過負荷状態になり、誤検知に対処したり、TIPの運用能力を最大限に高めるためにデータの構造化とタグ付け機能に取り組んだりして何時間も費やしています。しかも、画一的な方法は通用しません。CTIプラクティスを始めたばかりの組織は、高額な主流の脅威フィードを入手する準備ができていないし、より成熟した組織は、脅威の状況をもっとよく把握するために多様なフィードを求めています。

EclecticIQはこれらの課題を受けて、主要な脅威を対象にキュレートされ、EclecticIQプラットフォーム用に最適化された2種類の脅威データフィードを提供します。プラットフォームにはオープンソースフィードが付属しています。商業ソースフィードは、先進的な専門分野脅威データベンダーとEclecticIQ脅威インテリジェンスのオリジナルデータを持つ、コスト効率に優れたアドオンです。

## 主なメリット

### 市場からのしかかる過負荷を打破

EclecticIQの社内脅威調査チームは、主要な脅威を対象とする、キュレートされた信頼できるオープンソース脅威インテリジェンスと商業脅威インテリジェンスを提供します。これらのフィードによって、CTI運用が活性化し、主流の脅威フィードの認知が強化されます。

### CTI運用を加速

CTIチームは、フィードの質のモニタリングや、TIPに応じたフィードの最適化に貴重な時間を無駄にせずに、分析や対応を迅速化しています。また、EclecticIQの脅威インテリジェンスを利用して、主要な脅威を検証し、価値の高い調査内容を素早く、簡単に配布します。

### コスト効率に優れた単一の調達源

EclecticIQは複数の商業ソースで関係を管理しているため、大規模組織向けの調達を合理化し、コスト効率に優れた先進的な専門分野脅威データを提供します。

EclecticIQ

# EclecticIQインテリジェンスフィード

## フィードの特長

| | | オープンソースフィード | 商業ソースフィード |
|---|---|---|---|
| **キュレートされたフィード群により、貴重なCTIアナリストの時間を節約** | • 常に更新されている一連の信頼できるデータプロバイダーからの、主要な脅威を追跡するキュレートされたオープンソース脅威データフィード。 | ✓ | |
| | • 先進的なソースをまとめ合わせることで、企業ネットワーク、分散型コンピューティングプラットフォーム、オペレーティングシステムを狙う多形マルウェアとDDOSボットネットなど、主要な脅威について深い知見をお客様に提供する、キュレートされた商業ソース脅威データフィード。 | | ✓ |
| | • 機械学習、商業ソースプロセスデータを利用<br>5億5,500万以上のセンサー、サンドボックス、ハニーポット、ネットワークアナライザー、ウェブクローラー、トラップ、監視対象ボットネット、およびダークウェブ。 | | ✓ |
| **タグ、観察可能な挙動に関するルール、テーマを使って、プラットフォーム用にフィードデータを最適化** | • フィード固有のルールとタグを使って、誤検知を減らし、フィードを最適化します。 | ✓ | ✓ |
| | • 企業ITへの一般的な脅威、高度で持続的な脅威、ハクティビズム、重要インフラ、金融犯罪など、敵対者ターゲット向けにEclecticIQのアナリストが開発したインテリジェンスタグ。 | ✓ | ✓ |
| | • STIXに準拠したフィードで提供される脅威データ。 | ✓ | ✓ |
| **脅威インテリジェンスと調査により、調査とインテリジェンスの配布を迅速化** | • フィードには、戦術的、戦略的な週次運用ダイジェスト、およびEclecticIQプラットフォーム上の構造化されたビジュアライゼーションへのリンクがあるインテリジェンスレポートなど、EclecticIQ脅威インテリジェンスアナリストからの実用的な脅威インテリジェンスが含まれています。 | | ✓ |
| | • EclecticIQのアナリストが開発したインテリジェンスは、マルウェア/ツールの機能特定を促進するために、TTPのタグを介してMITRE ATT&CKを参照します。 | | ✓ |
| **EclecticIQプラットフォームに統合された、主要な脅威をターゲットとするコスト効率に優れたバンドル** | • EclecticIQにバンドルされた、信頼できるオープンソースフィード。 | ✓ | |
| | • EclecticIQプラットフォームに簡単に統合して主要な脅威を可視化できる、コスト効率に優れた商業ソースアドオンフィード。 | | ✓ |
| | • 単一の調達源により、企業規模や無契約といったフィード調達の課題解決を支援。 | | ✓ |

## 弊社のキュレーターをご紹介

EclectIcIQには、脅威インテリジェンスアナリストの社内チームがいます。チームは調査のために、信頼できるオープンソースフィードと貴重な商業フィードを常に探しています。アナリストは、EclecticIQプラットフォームにフィードを取り込んで、誤検知を最小限に減らし、脅威データの関連性と正確性を確保するプロです。

## EclecticIQについて

EclecticIQは、行政機関と一般企業を対象に、インテリジェンスで強化したサイバーセキュリティを実現します。お客様のサイバーセキュリティの焦点を脅威の現実に合わせる、アナリストを中心に考えた製品とサービスを開発しています。その結果、インテリジェンス主導型セキュリティ、検知と予防の向上、コスト効率に優れたセキュリティ投資が実現します。

EclecticIQのポートフォリオの詳細：www.eclecticiq.com
EclecticIQへのお問い合わせ：info@eclecticiq.comまたは
+31 (0) 20 737 1063

EclecticIQ