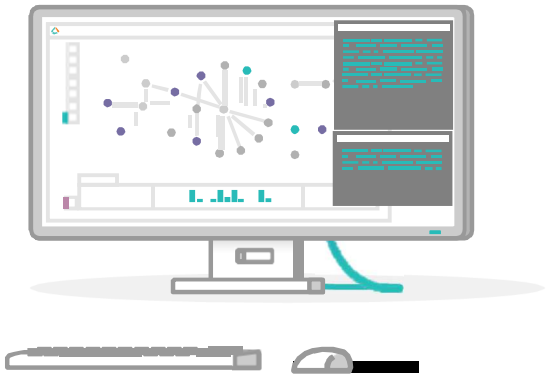
データシート

EclecticIQプラットフォーム

（企業向け）

脅威インテリジェンスのパワーを活用 –

インテリジェンス主導型セキュリティで受け身型から適応型に移行



はじめに

進行中のサイバーセキュリティへの脅威に対処することは、どの企業にとっても課題です。脅威が高まり続ける中、消費者、保険会社、投資家は、より優れたサイバーセキュリティ保護を求めています。そのような状況でこそ脅威インテリジェンスは威力を発揮できます。

脅威インテリジェンスプラットフォーム（TIP）を使用すると、最も重要な脆弱性とサイバー脅威を特定し、優先順位を付ける貴重な知見を発見できます。

EclecticIQプラットフォームはアナリストを中心に据えたTIPであり、オープンソース、商品サプライヤー、業界提携先からインテリジェンスデータを収集して1つの協働アナリストワークベンチに取り込めるように最適化されています。EclecticIQプラットフォームは、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を排除します。その結果、アナリストは最も重要な脅威の特定に集中し、タイムリーな行動を取り、対応方法と同業他社との協働方法について組織に助言することができます。

CTIを自力で組織に取り入れてセキュリティオペレーションセンター（SOC）の効果を改善したい場合でも、脅威インテリジェンスの力を使用することで、あらゆるレベルの決定をガイドしてビジネスリスクを軽減したい場合でも、EclecticIQプラットフォームでは、インテリジェンス主導型セキュリティを組織に導入したり拡大したりすることができます。

主なメリット

アナリスト中心型：協働、分析、作成を実現

EclecticIQプラットフォームを利用すると、アナリストは認定と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。動的なワークスペースは、クエリー、グラフ、フリーテキストを追加したり作業を割り当てたりする機能をご用意して、トピックや関心領域に関わるインテリジェンスを自動的にソートできるようにアナリストを支援することで、協働を推進します。
その結果、脅威の状況に関する実用的なナレッジベースが生まれます。これらの機能を装備することで、ITセキュリティコントロールと防御を既知の脅威に合わせて調整できるため、修復までの時間が劇的に短縮します。

実用的なインテリジェンスを提供することで、対応をさらに迅速化

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。意思決定者は非構造化レポート内のリンクからEclecticIQプラットフォーム内のコンテキストを確認して、より的確な状況認識と迅速な対応を推進できます。

インテリジェンス主導型セキュリティとビジネス決定

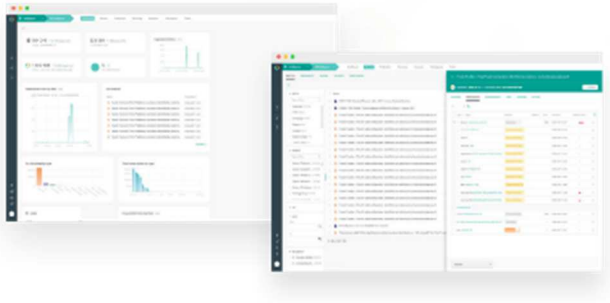
弊社のソリューションは、組織全体でワークフローとデータタイプが利用可能になるという点で他に類を見ないソリューションです。様々な部門や外部ソースからの脅威インテリジェンス
が、作成したケースで統合および強化されるので、企業はインテリジェンス主導型セキュリティを導入でき、その結果、より迅速で多くの情報に基づくビジネス上の決定を支援することができます。

EclecticIQ

データシート

製品概要

協働ワークスペース内で一連の主要なワークフローとプロセスを使用することで、アナリストは適切な実用的インテリジェンスを速やかに特定できます。EclecticIQプラットフォームでは、脅威コンテンツを統合、標準化、強化することで、アナリストが選別、分析、協働、対処方針に集中して取り組めるようにします。



収集および相関付け

- 複数のソースからのインテリジェンスデータ
- 構造化されたSTIXに準拠した非構造化エンティティ
- csv、pdf、独自仕様の形式、STIXなど、非常に多様なデータ形式をサポート

分析および協働

- 自動化された認定、選別、および発見のプロセス
- 直感的なグラフ、ピボットツール、タスク設定を備えた協働ワークスペース
- ウェブサイトからデータをキャプチャして、TIPに直接フィードできるCTIクリップボード

作成および配布

- 人と機械の両方に配布するレポート
- 日次ダイジェストおよび完全なインテリジェンスレポート
- 人が読める形式のレポートのメール送信をサポートする唯一のTIP

企業対応

- あらゆる規模の企業をサポートできるように水平方向に拡張可能
- RHEL、CentOS、およびUbuntuオペレーティングシステムをサポート
- 柔軟な導入オプション：仮想マシンまたは物理敵ハードウェア上の複数の層に単一インスタンスを導入
- オンプレミス型またはホスト型ソリューションとして利用可能
- 高度な設定が可能で、既存のセキュリティインフラに容易に統合
- SIEM、エンドポイント、インテリジェンスフィード、データエンリッチャーなど、様々なセキュリティシステムとインテリジェンスソースへの増え続けるインテグレーションのカタログ

EclecticIQ