ソリューションの概要

深く調査して、サイバーアンダーグラウンドの脅威を検知、防止

Intel 471のサイバー犯罪インテリジェンスをEclecticIQプラットフォームに統合することで、脅威の状況を攻略。

共同ソリューションの特長

統合の自動化

Intel 471がサイバー犯罪アンダーグラウンドから得た、閉じられた情報源からの、信頼性の高いインテリジェンスの自動ダイジェストを入手できます。

脅威パターンの視覚化

EclectiqIQのデータ構造化、エンリッチメント、Intel 471の敵対者インテリジェンスの統合で、悪意のある脅威パターンを素早く視覚化します。

- 脅威アクターの足跡
- 悪意のあるインフラとフォーラムアクティビティ
- 組織固有のアラートと実践的で観察可能な挙動

単一画面

CTIとインシデント対応(IR)を単一画面から推進します。EclecticIQはIntel 471の脅威アンダーグラウンドフィードを第三者の構造化/非構造化インテリジェンスとシームレスに織り交ぜることで、チームの能力を向上させます。

チームのメリット

CTIへのメリット

- 深部に潜入しているアンダーグラウンドの敵対者とマルウェアのインテリジェンスを収集、コンテキスト化、統合することで、より幅広い脅威の背景に合わせて素早く対応します。
- アンダーグラウンドアクターの正体、目的、理由、方法を先見的に配布することで、CTIの実用性を高めます。

SOC/IRへのメリット

- Intel 471の知見をEclectiqIQワークフローに織り交ぜることで、状況認識を推進します。
- 信頼できるマルウェアインフラIOC(ファイルハッシュ、URL、IP ADDR、ドメイン、C2データなど)でSOC/IRの対応に優先順位を付けます。

セキュリティリーダーへのメリット

- ビジネスと第三者への直接的なリスクを深度に及ぶまで先見的に可視化します。
- セキュリティについてより的確な決定を下して、侵害を最小限に抑え、組織的なリスクを軽減します。

脅威アンダーグラウンドを発見し、先見的に防御

EclecticIQはそのプラットフォームを最適化して、オープンソース、商業、業界提携のインテリジェンスデータを収集、統合、分析します。Intel 471のサイバーアンダーグラウンドの脅威インテリジェンスがシームレスに統合されるので、アナリストは敵対者とマルウェアのインジケーターを特定することで、最新のインテリジェンスを強化して最も重要な脅威に真っ先に集中することができます。チームは協働可能な作業環境で一連のワークフローを使用しながら、適切な対処方針への取り組み、選別、分析、協働を行って、アンダーグラウンドの敵対者か地上の敵対者かを問わず、あらゆるサイバー犯罪者から組織とその資産を先見的に保護できます。

ソリューションの概要

EclecticIQとIntel 471のユースケース

脅威アクターの追跡

課題：
脅威アクターによるサイバー攻撃の協働、やり取り、計画が行われる、閉じられた情報源への侵入とアクセスの維持がなくても、サイバー犯罪のアンダーグラウンドの脅威がもたらす敵対者とマルウェアの追跡は不可能です。

協働ソリューション：
EclecticIQプラットフォームの構造化インテリジェンスデータモデルでは、Intel 471の敵対者インテリジェンスとマルウェアインテリジェンスを他のデータソースと統合し、敵対者のTTP、マルウェアインフラをより幅広い脅威に合わせて調整します。

成果：
CTIアナリストは、捉えにくいアンダーグラウンドの敵対者とマルウェアを追跡します。Intel 471のインテリジェンスとEclecticIQ TIPの組み合わせによって、実用的なワークフローと共同作業が推進されて、より積極的な防御を行うことができます。

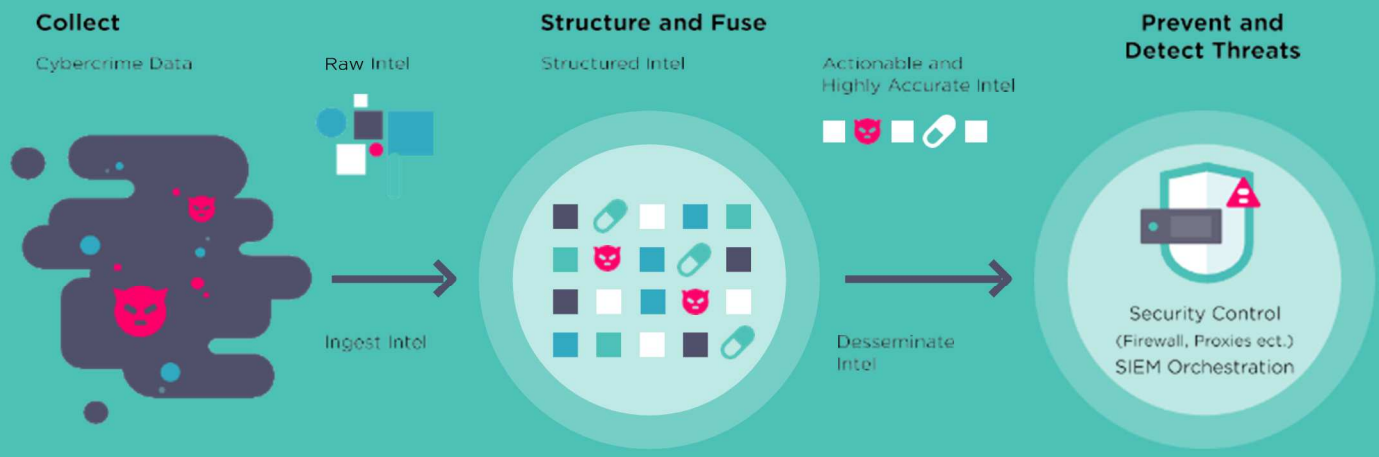
高信頼のインジケーターに基づくアクション

課題：
インジケーターの信頼性が低いと、サイバー脅威チームはイベントに対する関心が薄れて、真の脅威を見抜けなくなります。敵対者がアンダーグラウンドに潜伏している場合、高信頼のインテリジェンスを得ることはなおさら困難になります。

協働ソリューション：
Intel 471の脅威アンダーグラウンドインテリジェンス（閉じられた情報源を含む）との統合によって、アナリストは重要なインジケーターと豊富なコンテキスト（期限、信頼度、MITRE ATT&CK戦術、マルウェアインテリジェンス、YARAルールなど）を入手できます。

成果：
EclecticIQのTIPからは、関連性のあるタイムリーなインテリジェンスが提供されるため、SOCは自組織のSIEMに高信頼のインジケーターを取り入れて、ファイアウォール、IDS、エンドポイント保護ソリューションからの自動対応を促進できます。

サイバー犯罪の防止と打破



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

Intel 471について

Intel 471は、先進的なインテリジェンス、セキュリティ、詐欺対策チームに向けて敵対者やマルウェアに関するインテリジェンスを提供します。弊社の敵対者インテリジェンスは、脅威アクターによるサイバー攻撃の協働、やり取り、計画が行われる、閉じられた情報源への侵入とアクセスの維持に焦点を置いています。
弊社のマルウェアインテリジェンスは敵対者インテリジェンスとアンダーグラウンドの能力を利用して、マルウェアと敵対者のインフラについてタイムリーなデータとコンテキストを提供します。