Cybersecurity
Progress. Protected.

IOC検索とサンプル解析で脅威調査を迅速化

課題

セキュリティチームは、日々、不審なファイルやIOC（侵害指標）に直面しています。しかし、それらに対して次に何をすべきかを判断することは、必ずしも容易ではありません。ツールによって判定結果が異なったり、なぜ脅威として検出されたのかを判断するための十分な情報が得られなかったりする場合があります。アナリストには、機密性の高いサンプルを外部にさらしたり、高額なプライベートサービスに依存したりすることなく、不確実性を減らすための、より明確で信頼性の高い情報が求められています。同時にSOCには、大量のアラートを迅速にトリアージしながら、優先度の高いファイルについては詳細な調査を行える仕組みが必要です。

5分
最新のESETデータと照合

20種類のフィード
20種類の専門フィードから得られる固有のIOC

900名以上の社内エキスパート
ESETの脅威インテリジェンスアナリスト、マルウェア研究者、AIスペシャリストの専門知識を活用

ソリューション

ESET THREAT INTELLIGENCE INVESTIGATION LAB

ESET Threat Intelligence Investigation Labは、不審なファイルやIOCの調査から、確信を持った意思決定へとつなげるためのサービスです。ESETのテレメトリ、レピュテーションデータ、長年にわたる脅威解析の知見を活用し、**信頼性の高いセカンドオピニオンを提供**します。また、機密性の高い調査のプライバシーも維持します。**IOC Search**を利用すれば、大量のIOCを迅速に確認し、必要な情報を効率的に取得できます。さらに詳細な挙動情報やコンテキストが必要な場合には、サンプル送信によって、より深い分析を行えます。

仕組み

シグナルの発見から意思決定までを、より迅速に

Investigation LabはAPIを通じて、既存のセキュリティツールと連携できます。
アラートに脅威情報を付加して次のアクションを判断し、より詳細な挙動分析が必要な場合にはサンプルをサンドボックスへ送信できます。

セキュリティ環境
- SIEM
- SOAR
- TIP
- Firewall
- XDR

→ APIまたは手動検索 →

Investigation Lab
まず迅速に確認
必要に応じてサンプルを送信し、詳細なサンドボックス挙動解析を実施

→

確信を持って対応
- 情報付加（Enrich）
- ブロック
- 隔離
- 調査
- クローズ

INVESTIGATION LABが選ばれる理由

幅広い地域の脅威を可視化

ESETのグローバルテレメトリにより、十分に報告されていない地域についても独自の可視性を提供します。米国中心の情報ソースだけでは得られない、信頼性の高い情報を活用できます。

より迅速な調査

ESETが長年にわたり構築してきたインフラストラクチャに、グローバルテレメトリ、AIによる処理、高度な解析パイプラインを組み合わせることで調査を迅速化し、より早く対応につながる情報を得ることができます。

専門家による監修

AIによって解析を高速化すると同時に、ESETの専門家が結果を精査・レビュー。確認されたIOCが正確かつ関連性が高く、実際の対応に活用できる情報となるよう品質を確保しています。

Cybersecurity
Progress. Protected.

ESET Threat Intelligence Investigation Labのサービス内容

項目	Investigation Lab	Investigation Lab Advanced
このようなチームにおすすめ	信頼性の高いIOC情報の付加と、必要に応じた詳細なファイル解析を必要とするチーム	調査件数が多く、より高度な解析を必要とするチーム
APIへのフルアクセス	○	○
IOC Search（ボットネット、C&C、ドメイン、IP、URL）	1,000件/日、5,000件/週	10,000件/日、50,000件/週
ESETデータベースの高度な検索	○	○
Sample Submission	50件/日、250件/週	500件/日、2,500件/週
詳細な挙動解析	○	○
サンドボックスのカスタマイズ	×	○
Sandbox processing priority サンドボックス処理の優先度	標準	高
サンプルのプライバシー	標準：サンプルを削除、判定結果とハッシュ値は保持	高：サンプル、判定結果、ハッシュ値をすべて削除

お問い合わせ

イーセットジャパン株式会社

jp-marketing@eset.com

www.eset.com/jp