

高精度インテリジェンスフィードが 次の脅威を見抜く

お客様が直面する課題

アナリストは、一般的なフィードから大量のアラートが送られてくることで、ノイズに埋もれ、本当に重要なものが見えなくなっています。高精度のインサイトがなければ、SOCは常に後追い対応を続けるしかありません。必要なのは、ノイズを取り除き、実際に発生している・新たに台頭している脅威を明確に示す“本物の”インテリジェンスです。

750,000

日次で受信する
不審サンプル数

500,000

日次ブロックされる
URL 数

2,500,000,000

日次で分析するURL 数

60,000,000

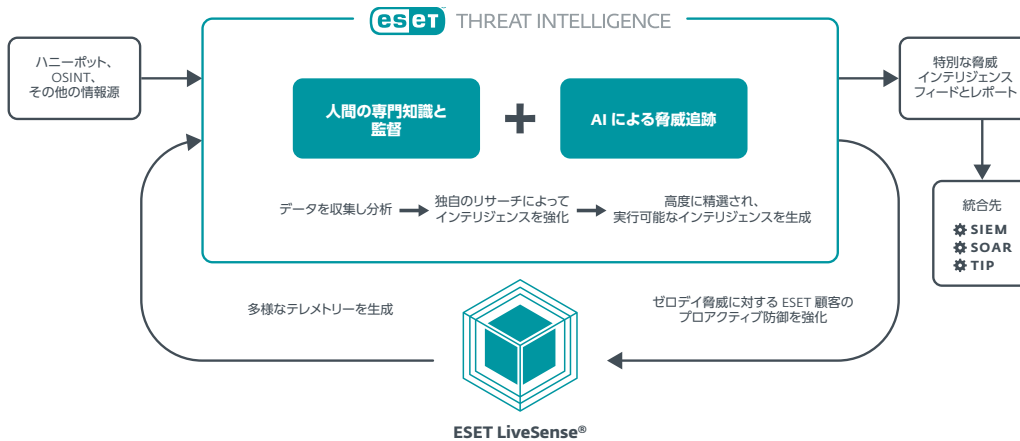
日次処理される
メタデータレコード数

課題への解決策

ESET THREAT INTELLIGENCE FEEDS

ESET Threat Intelligence Feeds は、単なるデータ量の追加ではなく、明確さ (Clarity) をもたらしめるために構築されたインテリジェンスです。グローバルテレメトリと専門家分析を基盤とし、高い信頼性とタイムリーなインテリジェンスを提供することで、滞在時間の削減、検知力の強化、標的型脅威の予測を実現します。

仕組み



主な価値

高信頼 IoC によるセキュリティ強化

ノイズを除去し、セキュリティスタック全体の検知精度を向上させるため、厳密に精選された IoC を提供します。

行動可能なインテリジェンスで迅速対応

フォーカスされたフィードにより、SOC は重要かつ価値の高い脅威情報だけを受け取り、トリアージや調査スピードを向上させます。

他では得られない可視性を獲得

ESET のグローバルテレメトリと地域専門知識により、他社が見逃す脅威やインフラを特定し、新たなリスクを予測できます。

データフィード一覧

- マルウェアデータフィード
- ボットネットフィード
- APT IOC フィード
- Android インフォスティーラーフィード
- Android 脅威フィード
- 悪意あるメール添付フィード
- ランサムウェアフィード
- ドメインフィード
- URL フィード
- IP フィード
- クリプト詐欺フィード
- フィッシング URL フィード
- 詐欺 URL フィード
- スミッシングフィード
- SMS 詐欺フィード
- eCrime フィード
- 望ましくないアプリ(ツール悪用検知)フィード
- 望ましくないアプリ(不要アプリ・アドウェア) フィード

お客様の既存ツールと容易に統合

TIP・SIEM・SOAR を、ESET のテレメトリで簡単に強化できます。

- JSON
- STIX/TAXII

といった標準フォーマットに対応。API とドキュメントも完備しているため、導入後すぐに価値を生み出せます。

お問い合わせ

イーセツジャパン株式会社
jp-marketing@eset.com

www.eset.com/jp