AhnLab
CONNECT PLUS

AhnLab TIP

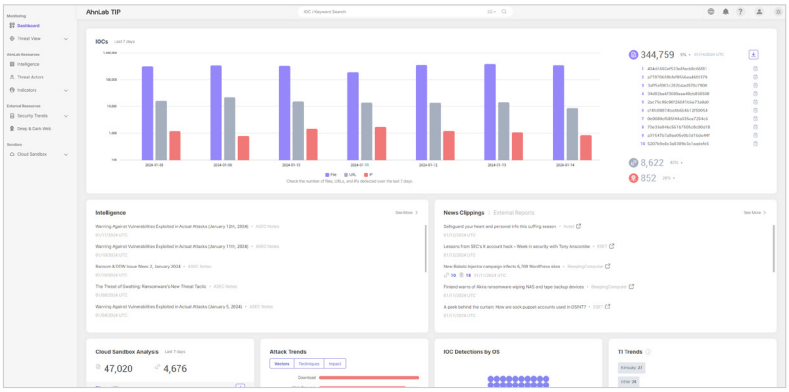
高度化されたサイバー脅威に対応する
次世代脅威インテリジェンスプラットフォーム

緊急かつ重要な脅威に対応できるように、可視性と対応策を提供し
最適な意思決定を支援

概要

AhnLab TIP (Threat Intelligence Platform) は、アンラボのマルウェア対応技術とノウハウに基づいて、脅威相関分析と洗練された脅威情報を提供します。発生済み、または未来に発生する脅威の背景と目的を包括的に分析して合理的な意思決定を下すことができるように、アンラボだけの差別化された脅威インテリジェンスをご提供いたします。

専門技術とノウハウを組み合わせた優れたセキュリティインフラベース
THREAT INTELLIGENCE PLATFORM



包括的な脅威インテリジェンスプロセス	・さまざまなソースから収集された情報をタイプ別に分類し、体系的に保存 ・人工知能と動的分析システムを活用した多次元分析の進行 ・意思決定者、上級管理者、実務者別の状況に合った脅威インテリジェンスを提供
脅威の相関分析	・さまざまな脅威分析情報と影響度の把握による能動的な対応が可能 ・脅威間の相関分析により、あらゆる脅威に対する検知と対応のギャップを解消 ・キーワード登録による顧客に合わせてカスタマイズされた脅威情報の確認と対応 ・提供される脅威インテリジェンスをセキュリティ構築プロセスに反映
より多くの脅威情報を提供	「プライベートソース情報」のモニタリングと相関分析 ・現在だけでなく、発生可能性のある脅威を予測してセキュリティポリシーを策定 ・脅威対応ソリューションと方法を提示し、防御能力を強化 ・攻撃動向の常時モニタリング

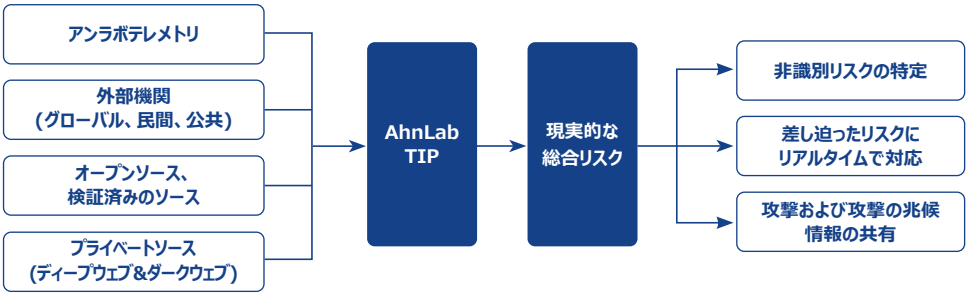
リリース背景

従来の脅威情報（Threat Information）は、平面的な脅威データがさまざまなソースから提供され、分析と対応効率が低下し、セキュリティ担当者の主観的な判断に頼るしかありませんでした。

プライベートソース（ディープウェブ&ダークウェブ）情報の確認が困難

導入効果

AhnLab TIP は、単一チャネルでさまざまな脅威インテリジェンスを提供することで、顧客のセキュリティ担当者が最新の脅威情報と洗練された分析結果に基づいて、脅威に対する可視性を確保し、拡散の有無と組織の影響度を把握して迅速に対応できるようにします。



「 定量的・定性的判断基準を提供し、独自のセキュリティ対応力を強化 」

影響度および拡散程度の確認

異常行為または疑わしい脅威検知時の独自の分析および対応

流入と拡散の防御

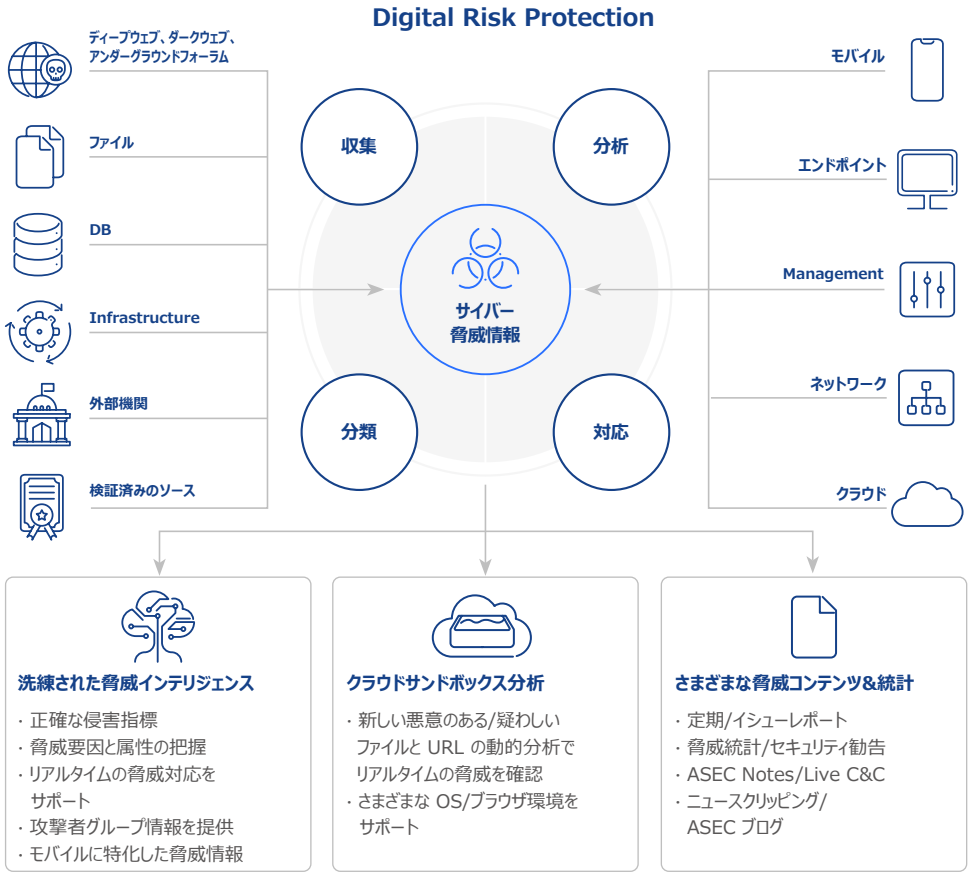
さまざまな脅威シナリオの設計とテスト

検知および対応ポリシーの強化

新しい悪意のある・疑わしい検知ポリシーとパターンのリアルタイム適用

主要機能

AhnLab TIP による情報識別の目的は、許可されていない情報収集、脆弱性を利用したセキュリティ制御の無力化/迂回、情報漏洩などの攻撃行為に迅速に対応することです。これを実現するために、洗練された脅威インテリジェンス、クラウドサンドボックスを活用した動的脅威情報分析、およびさまざまな脅威インテリジェンスコンテンツを提供します。



AhnLab TIP は、以下の主要機能を「中央集中型シングルダッシュボード」として提供します。シングルダッシュボードですべての IOC (Indicators of Compromise) の確認と検索が可能であり、深刻度と信頼レベル別に IOC を要約し、脅威対応の優先順位の設定に貢献します。

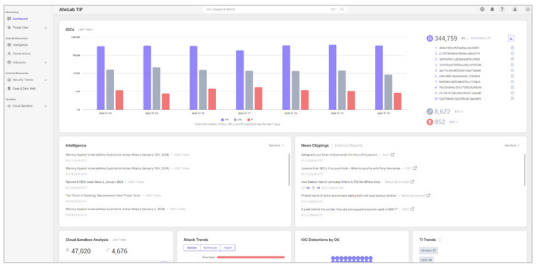
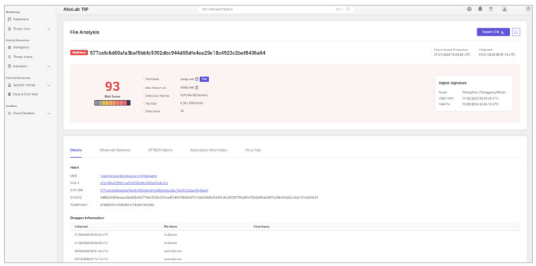
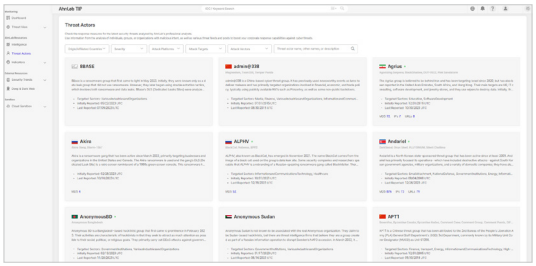
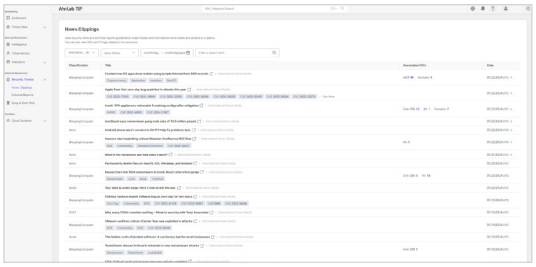
洗練された脅威インテリジェンス	・Threat Lookup: URL、ドメイン、IP アドレス、ハッシュ、脅威の種類、攻撃者などの情報を提供 ・IOC フィードによる脅威情報分析の最適化 ・マルウェア経由及び配布経路の把握による対応効率の向上 ・脅威イベントおよび攻撃フローを提供し、対応/措置案を提示 ・最適化された別の RESTful API を提供することによる製品とサービスの連携 ・ディープ/ダークウェブ上で収集された情報ベースの脅威関連分析
クラウドサンドボックス分析	・経路別の脅威検知状況と収集状況の提供 ・マルチ OS 環境/ブラウザ環境と使用プログラムベースの分析 ・脅威状況情報の可視化と行為別の脅威レベル情報を提供 / 幅広いファイルタイプのサポート
さまざまな脅威コンテンツ	・最新のセキュリティ脅威を分析する過程で収集および分析された情報の共有 ・定期&イシューレポートを通じて定期的に脅威動向情報を共有 ・さまざまな脅威統計情報を提供し、状況分析を最適化 ・悪意のある意図を持って活動している個人、グループ、組織に対する自己分析データの確保 ・配布の多いマルウェアを選別し、自動分析システムを介して確認された C&C 情報を提供 ・脆弱性、影響を受ける製品、対応案を盛り込んだセキュリティ勧告の共有 ・国内外の主要セキュリティニュースなどの脅威関連情報を提供
プライベートソースから収集された脅威情報	・Tor/IP2 ネットワークソース情報、漏洩した電子メールとファイル内容情報 ・重要クレデンシャル漏洩情報 / 侵害され漏洩したデータセット情報

活用案

アンラボの脅威インテリジェンスプラットフォーム活用「TIP」

A. リアルタイムセキュリティ脅威対応とセキュリティ戦略の設計

侵害指標はもちろん、攻撃タイプ、攻撃者情報、新規脆弱性分析情報、プライベートソース情報などのさまざまな脅威トレンドを習得して企業内のセキュリティ戦略を設計

B. さまざまな API 連携による包括的な脅威対応能力の強化

さまざまなセキュリティ製品およびサービスと連携して新種マルウェア対応&リアルタイム遮断

このほか、AhnLab TIP を以下のように活用すれば導入効果を最大化できます。

企業内部のセキュリティ戦略の設計	・脅威予測情報を通じて今後の脅威状況をセキュリティ戦略に反映 ・戦略的対応優先順位を設定してサイバーセキュリティ投資を進める
セキュリティ対策の策定差し迫った脅威に対応	・AhnLab TIP プラットフォームで新規サイバー脅威分析情報を取得 ・差し迫った脅威の影響を受ける資産、脆弱性分析および対応策 ・まとめた情報をもとに事前予防対策の実行と被害の最小化
包括的な脅威対応能力の強化	・IP アドレス/ドメイン/URL リスクを把握した後、IPS、IDS、ファイアウォールなどに遮断リストとして適用 ・SOAR と XDR システムの連携によるファイル、IP アドレス、URL などに対するリアルタイムの脅威検証 ・国内外の主要セキュリティニュースを分析し、社会的なセキュリティ問題に迅速に対応

〒108-0014 東京都港区芝4丁目13-2 田町フロントビル3階
ホームページ: www.ahnlab.com/jp
TEL: +81 3-6453-8315 FAX: +81 3-6453-8316

AhnLab