

専門的インテリジェンスで意思決定を支援し、レジリエンスを強化

ThreatVision 脅威インテリジェンスプラットフォーム

20年以上にわたるAPAC脅威研究を基盤とするThreatVisionは、マルウェアやAPTグループに関する高品質かつ焦点を絞ったインテリジェンスを提供します。戦略的・運用的・戦術的インテリジェンスを統合し、意思決定者、リスク管理者、IRチームが脅威環境を理解し、防御を強化できるよう支援します。ThreatVisionはまた、ディープウェブやダークウェブに関するインテリジェンスを提供し、早期警告やデータ侵害リスクを検知します。フォーラム、マーケットプレイス、ソーシャルメディアをカバーし、自動アラートやカスタムレポートにより、脅威が拡大する前に組織が能動的に対応できるようにします。

主要数値



ThreatVisionのコアバリュー

| | | |
|---|--|---|
| 迅速な脅威特定 複数のIoCソースを統合し、隠れた攻撃を素早く特定、防御効率を強化。 | 精緻な脅威分析 サンプル提出と分析により、悪意のある特性を迅速に特定、IRや調査を支援。 | 完全な攻撃コンテキスト マルウェアを敵対者と関連付け、攻撃の背景・目的を再構築。 |
| APACインテリジェンス専門性 地域特有の攻撃手法・標的・進化する脅威環境に関する専門分析を提供。 | リアルタイムアクセス IP、ドメイン、サンプルを即時クエリし、Raw Intelligenceやカスタムレポートへアクセス可能。 | 迅速な統合と自動化 TIPやSIEMプラットフォームと接続し、インテリジェンスの自動配信とインシデント対応を加速。 |

脅威インテリジェンスの重要性

ThreatVisionは、経営層から最前線の防御担当者まで、幅広い役割を支援する3つのインテリジェンスレベルを提供します。

| 戦略的インテリジェンス (経営層向け) | 運用的インテリジェンス (セキュリティチーム向け) | 戦術的インテリジェンス (現場防御者向け) |
|--|---|--|
| CISOに脅威環境の全体像を提示し、サイバー脅威をビジネス影響と結び付け、戦略策定やリソース配分を支援。 | 敵対者のTTP、動機、キャンペーンを詳細に示し、優先度付けや対応の最適化を可能に。 | 即利用可能な技術データを提供し、IT・セキュリティチームが検知・防御に活用。 |

ThreatVisionレポートの概要

ThreatVision は、APAC APTインテリジェンス、脆弱性、中文インターネット世界・中国サイバー政策、サイバー犯罪インテリジェンスに関する4種類の主要レポートを提供し、組織の意思決定を支援します。

APT in Asiaフラッシュレポート

最新APT攻撃事例を分析し、技術詳細やIoCを提供。週2回発行、年間100件以上。

APT in Asia月次レポート

APAC地域のAPT動向を月単位で総括。地政学的状況と攻撃行動を関連付け、13~16件の事例を掲載。年12件発行。

APTキャンペーントラッキングレポート (CTR)

脅威グループや攻撃戦術・標的範囲を詳細分析。CTRは四半期ごとに2回発行され、年間では8本のレポートが公開されます。そのうち6本は攻撃者グループの分析レポートで、残り2本は年2回発行の脅威情勢レビューです。

サイバー情勢隔週レポート

中国のサイバー能力、政策、規制、事件を分析。隔週発行、年間24件。

脆弱性インサイトレポート (VIR)

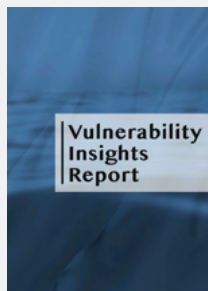
重要な脆弱性を1件ずつ詳細に分析。隔週発行、年間24件。

パッチマネジメントレポート (PMR)

約100件の高リスク脆弱性を収録。PoCや影響製品、パッチ推奨を提供。週次更新、年間52件。

サイバー犯罪インテリジェンスレポート (CCレポート)

サイバー犯罪インテリジェンスレポート (CCレポート) は、TeamT5によるディープウェブ・ダークウェブ・犯罪コミュニティの長期的な調査と監視に基づいて作成されています。このシリーズには、サイバー犯罪キャンペーン (Cybercrime Campaigns / 毎月発行・年間12本) のほか、フォーラム活動 (Forum Activities) およびランサムウェア活動 (Ransomware Activities) (それぞれ月4回以上発行・年間合計48本以上) が含まれます。



ThreatVisionの主要機能

APT/サイバー犯罪IoC

国家支援型攻撃や大規模サイバー犯罪に対応。2種類のIoCリストを、それぞれ週に1回、年間合計52回を発行。

脅威ハンティングツール

アナリスト設計ルールで環境をスキャン、調査を加速。

RFI(情報要求)

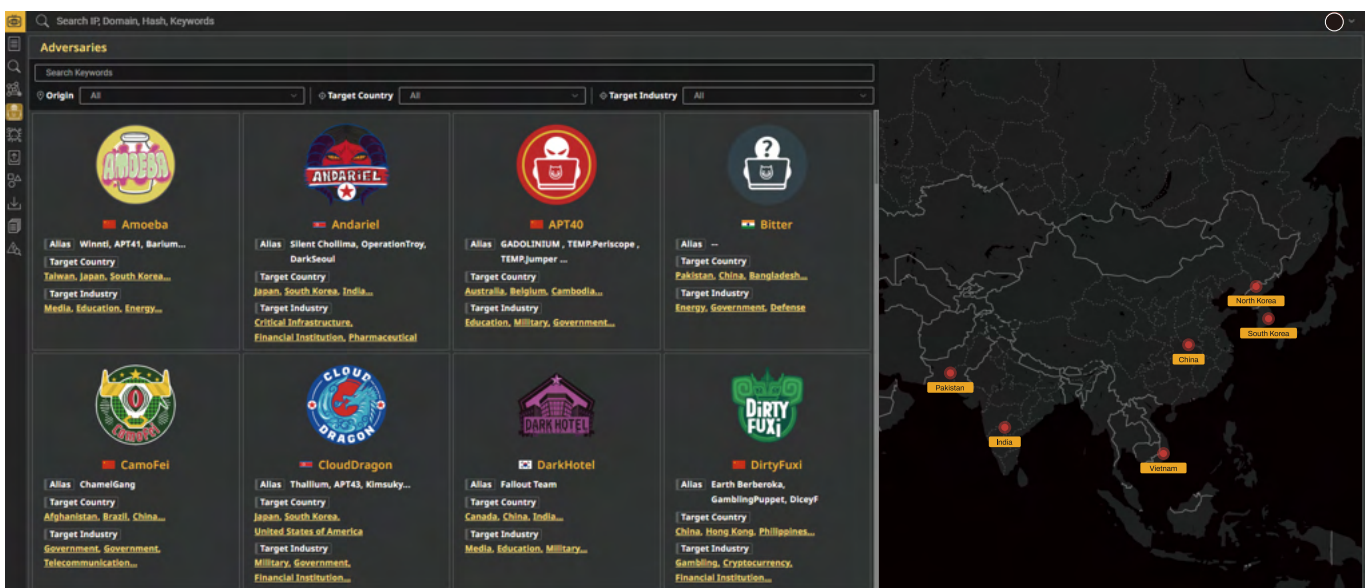
特定トピックや攻撃キャンペーンに関するカスタム調査を提供。

API対応

既存プラットフォームに自動統合し、迅速な展開と安定運用を実現。

ThreatVisionプラットフォーム概要

ThreatVisionの多様なインテリジェンスは、さまざまな役割やタスクを支援し、敵対者の行動パターンを理解して能動的に防御戦略を展開できるようにします。戦略策定から最前線防御までを網羅する最適なソリューションです。



ThreatVisionを始めるには

ThreatVisionの14日間トライアルアカウントをご希望の方は、TeamT5セールスチームまでお問い合わせください。詳細は SALES-ADMIN-JP@teamt5.jpまでメールでご連絡ください。貴社のサイバー脅威防御を支援できることを楽しみにしています。

TeamT5 について

v.202605

政府機関、テクノロジー、製造、金融、医療、軍事、電気通信、その他の業界を含む、世界中の550を超える顧客から広く信頼されています。

TeamT5は、マルウェアと高度な持続的標的型攻撃 (APT) とマルウェアに関する20年以上の経験があります。言語と文化的な利点により、当社はアジア太平洋地域におけるサイバースパイ活動に関する具体的な専門知識を有しており、米国のBlack Hatや日本のCode Blue / AVTokyo、ドイツのTroopers、そしてHack In The BoxとFIRSTを含む、世界クラスのサイバーセキュリティカンファレンスで最新の研究を発表するため頻りに招待されています。また、脅威インテリジェンスの研究と先進的なサイバーセキュリティ技術の分野で世界をリードするチームとして、当社は米国のBloombergとCNN、日本の産経新聞と朝日新聞、韓国のET Newsからインタビューを受けています。