

専門性の高い脅威インテリジェンスで 意思決定を支援し、防御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

ThreatVisionは、TeamT5が20年以上にわたり蓄積してきた、APAC地域におけるマルウェア、APTグループ、サイバー脅威に関する研究を基盤とした脅威インテリジェンスプラットフォームです。APACに特化した質の高いインテリジェンスを提供し、戦略・運用・戦術の各レベルのインテリジェンスを組み合わせることで、意思決定者、リスク管理担当者、インシデント対応チームによる脅威情勢の把握、攻撃者の特定、防御体制の強化を支援します。

また、ThreatVisionはディープウェブやダークウェブに関する脅威インテリジェンスも提供しています。ディープ・ダークウェブ上のフォーラム、マーケットプレイス、中国語圏のアンダーグラウンドコミュニティ、ソーシャルメディアなどを対象に、早期警戒や情報漏えいリスクの把握を支援します。毎週の自動アラートやカスタム監視・分析レポートを通じて、脅威が顕在化し実際のリスクとなる前の段階から状況を把握し、早期対応につなげます。

主要数値

2,500+	700 万以上	2,700 万以上	3,300+	350+
レポート	IoC	脅威サンプル	マルウェア	アドバイザリー

ThreatVision の主な特長

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。	精度の高い脅威分析 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。	攻撃の全体像を把握 マルウェアと脅威アクターを関連付け、攻撃の背景・目的を再構築。
APAC特化のインテリジェンス APACを継続的に研究する専門チームが、地域特有の攻撃手法・標的・進化する脅威情勢を詳しく解説する分析レポートを定期的に提供。	リアルタイムアクセス IP、ドメイン、サンプルを即時検索し、Raw Intelligenceを取得できるほか、カスタムレポートやツールもアクセス可能。	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迅速化。

脅威インテリジェンスの重要性

TeamT5では、脅威インテリジェンスを3つのレベルに分類し、経営層の意思決定から最前線の防御まで、さまざまな役割を支援します。

戦略的インテリジェンス (経営層／意思決定者向け)	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 (最前線での現場担当者向け)
CISOや経営層にとって、戦略的脅威インテリジェンスは、サイバー脅威が事業へ与える潜在的な影響を把握するうえで重要です。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します。	運用的インテリジェンスでは、脅威アクターのTTP、動機、キャンペーンを詳細に示し、SOCやインシデント対応チームによる対応の優先度付けや最適化を支援します。	戦術的インテリジェンスは、すぐに活用できるTTPなどの技術情報を提供します。ITチームや最前線のセキュリティ担当者による検知・防御の調整に活用できます。

ThreatVision が提供する多様な脅威インテリジェンス

ThreatVisionは、APAC APT脅威インテリジェンス、脆弱性インテリジェンス、中国語圏のサイバー情勢・中国のサイバー政策、サイバー犯罪インテリジェンス、の4種類の主要レポートを提供します。これにより、組織のよりの確な意思決定を支援し、迅速な対応につなげます。

APT in Asiaフラッシュレポート (APT in Asia Flash Reports / Flash Report)

最新APT攻撃事例に焦点をあて、攻撃手法や技術的な詳細を分析し、関連するIoCを提供。週2回発行、年間100件以上提供。

APT in Asia月次レポート (APT in Asia Monthly Report / Monthly Report)

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て分析し、平均13～16件の事例を掲載。毎月1回、年12件発行。

APTキャンペーントラッキングレポート (APT Campaign Tracking Reports / CTR)

脅威グループ、攻撃戦術、標的範囲を詳細分析。APAC地域の重要な脅威グループや攻撃活動に対する包括的な理解を支援します。CTRは四半期ごとに2回発行され、年間では8本のレポートを公開。そのうち6本は脅威グループの分析レポート、2本は半年ごとの脅威情勢分析レポートです。

サイバー情勢隔週レポート (Cyber Affairs Biweekly Report / Biweekly Report)

新興大国である中国のサイバー能力や、中国語圏のオンライン環境におけるサイバーセキュリティニュース、政策・規制、セキュリティインシデントを詳細に分析。2週間に1回、年間24本発行。

サイバー犯罪インテリジェンスレポート (Cybercrime Reports / CC Report)

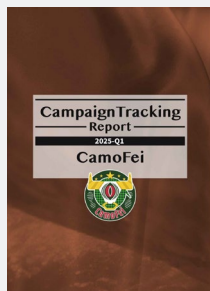
サイバー犯罪インテリジェンスレポート（CC Report）は、TeamT5によるディープウェブ、ダークウェブ、犯罪コミュニティの長年の追跡・研究に基づいて作成されています。
このシリーズには、サイバー犯罪キャンペーン（Cybercrime Campaigns / 毎月発行・年間12本）のほか、ダークフォーラム動向（Forum Activities）、ランサムウェア動向（Ransomware Activities）（それぞれ月4回以上発行・年間合計48本以上）が含まれます。

脆弱性インサイトレポート (Vulnerability Insights Reports / VIR)

脆弱性インサイトレポート（VIR）は、毎回1件の重大な脆弱性に焦点を当て、詳細な技術情報に加え、想定される攻撃シナリオや検知ツールを提供します。VIRは2週に1回発行され、年間24本提供されます。

パッチマネジメント (Patch Management)

パッチマネジメントでは、重要な脆弱性情報を継続的に更新し、公開済みの脆弱性のうち、実際の攻撃で悪用されているものや、利用可能な攻撃ツールが確認されている高リスクな脆弱性を整理して提供します。影響を受ける製品、パッチ情報、公開されているPoCコードなどを確認できるほか、TeamT5はゼロデイ脆弱性についても継続的に追跡します。これにより、ユーザーが早期にリスクを把握し、プロアクティブな防御策を検討できるよう支援します。



ThreatVision の主な機能

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、調査を迅速化。

RFI(情報要求)

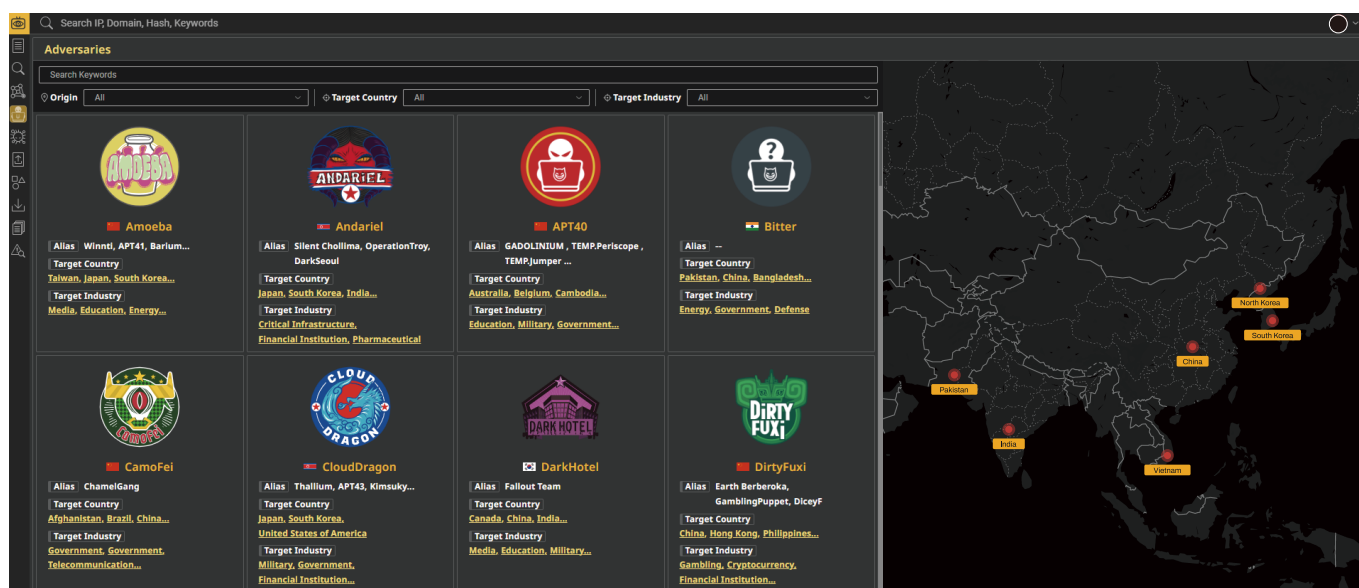
特定トピックや攻撃キャンペーンに関するカスタム調査を提供。

API対応

既存プラットフォームに脅威インテリジェンスを自動統合し、導入の迅速化と安定運用を実現。

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、さまざまな役割や業務を支援し、組織が脅威アクターの行動パターンを包括的に理解し、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日間トライアルや詳細をご希望の方は、TeamT5セールsteam（sales-admin-jp@teamt5.jp）までお問い合わせください。皆さまの組織をサイバー脅威から守るために、ご支援できることを楽しみにしています。

TeamT5 について

v.202609

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繁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。