

IoC (侵害の兆候): 脅威を遮断するための精緻な特定

セキュリティチームが 直面する課題

セキュリティチームは、大量のアラートに圧倒され、調査コストの増大、リソースの浪費、侵害の見逃しにつながっています。外部サービスに依存すると、持続可能な防御には遅すぎる上に高額になりがちです。

ThreatVisionの高精度IoCは、検知精度と対応効率を向上させ、チームの負担を増やすことなく継続的に効果的な防御を実現します。

// 5つの主要機能

シナリオ横断型IoC応用

高精度データソース

精緻なアラートトリガー

関連インテリジェンス統合

自動統合

// 4つの主要メリット

誤検知とアラート疲れを軽減

脅威を攻撃源やコンテキストに結び付け

プロアクティブな脅威検知と追跡を支援

迅速な導入で防御を強化

// ThreatVision IoCが特別な理由

TeamT5が長年にわたり追跡してきたAPACの脅威を基盤に、APT (高度持続的脅威) およびサイバー犯罪 (CC) のIoCは、一次観測を独自の行動コンテキストで強化されたインジケータへと変換します。アナリストが検証したIoCは既存防御に直接統合され、アラートのトリアージを大幅に改善し、インシデント対応を加速します。

ユーザーは任意のインジケータを照会することで、関連する攻撃・マルウェア・敵対者の全体像を把握し、迅速かつ適切な対応と防御強化が可能になります。

// ThreatVision APT/CC IoCの特徴

APT IoC	CC IoC
- 国家支援型やミッション指向型APTに焦点 - 敵対者、マルウェア、技術に関連する完全なコンテキストを提供 - 政府・防衛など高感度業界のリスク監視・分析に最適 - 週に1回、年間合計52件を発行	- 大規模で非標的型のサイバー犯罪活動をカバー - ランサムウェア、フィッシング、認証情報窃取などを検知 - アラート品質を改善し、多発する攻撃への防御を強化 - 週に1回、年間合計52件を発行

補足：APT調査中にサイバー犯罪関連インテリジェンスが判明する場合がありますが、IoCの分類はAPT攻撃として特定されたかどうかに基づきます。

// ThreatVision IoCの多様な応用

組織のニーズ

効果的な検知には複数の脅威ソースのカバーが必要。

脅威認識を向上させるために、信頼できるインジケータが必要。

リアルタイム防御のために、より高いアラート精度が必要。

防御効率を高めるために、自動化されたフィードが必要。

攻撃コンテキストを伴う、より迅速なインシデント調査が必要。

統合を容易にするために、標準化されたフォーマットが必要。

適用例

ハイテク製造業は、APT & CC IoCをカスタマイズしたロジックで適用し、アラート精度と効率を改善。

政府機関は、APT IoCを使用して国家レベルのアクターを監視し、リスク分析のための追跡可能なインテリジェンスを確保。

金融サービス企業は、CC IoCを用いて異常なログインを検知し、データ侵害リスクを低減。

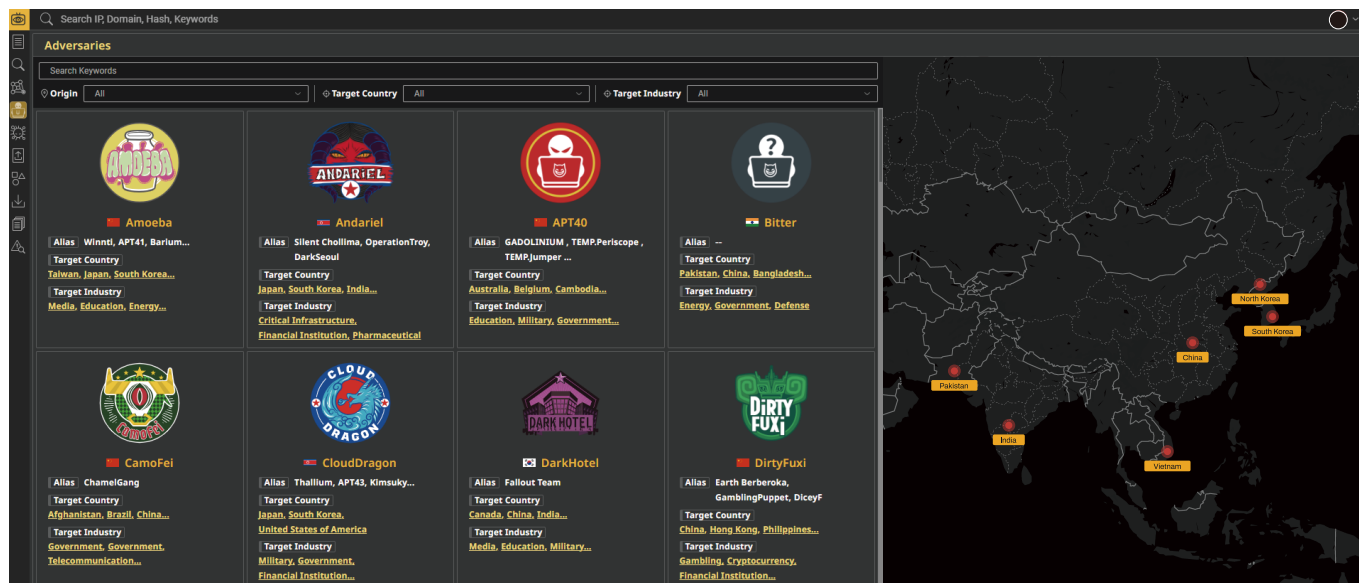
大企業はIoCをAPI経由でSIEMに投入し、リアルタイム更新を可能にし、手作業を削減。

インシデントレスポンスはThreatVision内でIoCを照会し、マルウェアやアドバーサリデータを取得し、迅速にコンテキストを構築。

MSSPはIoCをSTIXおよびCSV形式で取り込み、迅速な顧客展開と自動レポートングを実現。

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。