

脅威ハンティングツール: プロアクティブ防御の強力な資産

インテリジェンス駆動の プロアクティブ防御ツール

ThreatVisionは、組織が潜在的な脅威を迅速に特定し、セキュリティプロセスを強化できるよう、すぐに利用可能な脅威ハンティングツールを提供します。TeamT5アナリストによって開発されたこれらのツールは、攻撃者のツール、バックドア、運用痕跡を明らかにします。

サイバーセキュリティの課題に最適なソリューション

複数の亜種やサンプル タイプをカバー	精選ルールで 分析負荷を軽減	関連インテリジェンスで攻撃 コンテキストを構築	既存システムに 展開可能
YARA、Sigmaなどの検知ルールがマルウェアの亜種を網羅し、多様な攻撃行動を特定。	関連性の低いログやアラートを事前にフィルタリングし、アナリストが異常に集中できるようにして誤検知を削減。	SIEMやTIPにインポートでき、リソースが限られていてもハンティングを加速。	ツールはSIEMやTIPにインポートすることができ、限られたリソースでも脅威ハンティングを加速します。

ワンクリックで必要なツールを入手

対象（マルウェア、脆弱性）や種類（YARA、Snort、Sigma）ごとに分類され、リリース日順に整理されたツールをホームページからワンクリックでダウンロードできます。

利点

脅威状況を迅速に把握	未知の攻撃検知を強化	自動化プロセスへ統合
潜在的な脅威や異常を理解し、対応を円滑化。	更新されたルールでマルウェア亜種や攻撃の検知力を向上。	標準化されたYARA、Snort、Sigmaルールを既存システムやワークフローに組み込み可能。
脆弱性対応を改善	防御範囲を拡大	
危険にさらされたシステムや資産における悪用済み脆弱性のパッチ適用を優先。	マルウェアや脆弱性悪用を検知し、より強力なプロアクティブ防御を実現。	

// 適用対象の役割

セキュリティチーム 脅威ハンティングを導入し、検知と対応を強化。	SOCアナリスト アラートをフィルタリングし、IoCを検証して調査効率を改善。	インシデントレスポnder サンプルやTTPを突き合わせ、攻撃コンテキストと帰属を確立。
セキュリティエンジニア ルールをアーキテクチャに統合し、検知力と自動化を向上。	セキュリティ意思決定者 検知結果に基づきパッチやリソースを調整し、戦略的防御を実現。	

// 多様な適用シナリオ

ThreatVisionの脅威ハンティングツールは、さまざまな検知ニーズやシナリオをカバーし、大きく3カテゴリに分類されます。

多様な検知ルール

YARA、Snort、Sigmaルールにより、ホストや自動化プラットフォーム上でファイルや行動の異常を迅速に検知。

マルウェアハンティングツール

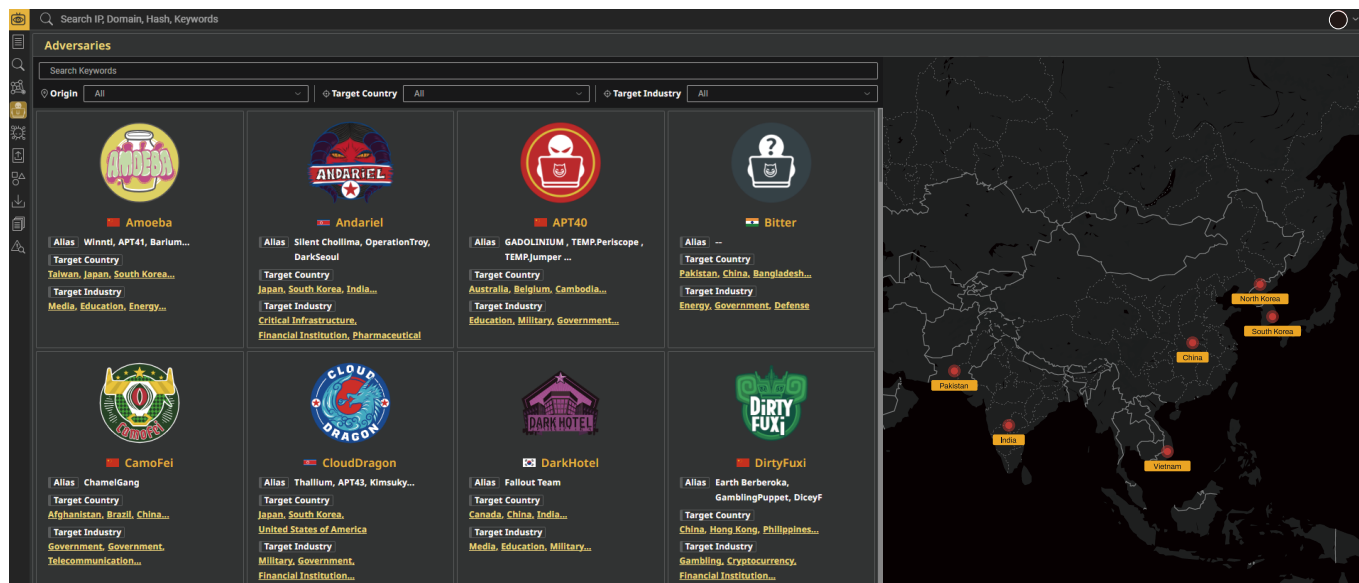
ShadowPADなどの高リスクマルウェアやその亜種を検知し、従来のアンチウイルスを補完。

脆弱性検知ツール

悪用された脆弱性を特定し、影響範囲を評価し、関連する悪意あるプログラムを検知。

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steam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。