

Threat Intelligenceポイント： インテリジェンス価値の最大化

多様なセキュリティニーズに応えるため、ThreatVisionはリアルタイムクエリから高度な分析までカバーする2つのポイント仕組みを提供します。

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。

AAP (Automated Analysis Points)

リアルタイムクエリやサンプル分析用。既知の攻撃活動との関連性を判定。

RAH (Request for Assistance Hours)

レポート、ツール、カスタムインテリジェンスへのアクセス用。

ThreatVision Automated Analysis Points (AAP)

AAPは迅速なリアルタイムクエリを可能にし、脅威を早期に検出します。代表的な用途は、アラートのトリアージ、IoC（侵害の兆候）の検証、サンプル分析です。

AAPの利用例：

IP／ドメイン／サンプルのクエリ

不審なIP／ドメイン／ハッシュを、関連する敵対者・マルウェア・レポートと照合。

Raw Intelアクセス

未公開の観測情報（攻撃者活動、IoCなど）を取得し、早期警告に活用。

不審サンプルの分析

ファイルをアップロードし、悪性プログラムを自動解析してトリアージや対応を支援。

補足：

- ポイントは前払い制で、必要に応じて購入可能。
- サンプル分析実行前に差し引きポイントを表示。
- アラート分類やサンプル検知など、迅速対応シナリオに最適。

// ThreatVision Request for Assistance Hours (RAH)

RAH は高度なサポートを提供し、特定のレポート種類へのアクセス、ツールのダウンロード、カスタマイズされたインテリジェンスサービスをカバーします。特定の攻撃や脅威動向の詳細調査に特に有用です。

RAH の利用例：

レポートアクセス	脅威ハンティングツール	カスタマイズインテリジェンス 依頼 (RFI)
サブスクリプションに応じ、過去公開済みレポートを解放。	YARA、Snort、Sigmaルールをダウンロードし、即時展開による迅速な検知・追跡を実現。	業界・地域・攻撃活動に関するTeamT5独自調査を依頼可能。

補足：

- ポイントは前払い制で、必要ポイントは事前に表示。
- 利用履歴は管理・監査用に確認可能。
- 背景調査、攻撃帰属分析、キャンペーン分析に最適。

// AAPとRAHの選び方

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。

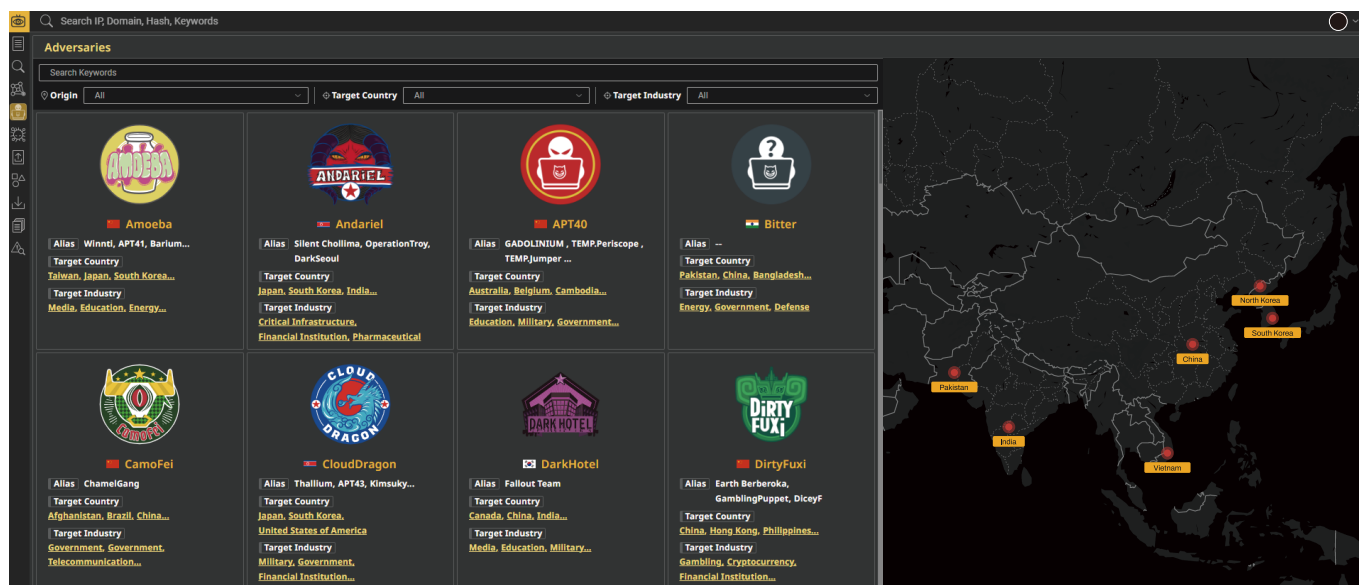
AAP	RAH
• 不審なIP／ドメインを照会し、悪意ある活動を確認。 • サンプルをアップロードし、自動分析を実行。 • Raw Intelへアクセスし、新興脅威への曝露を評価。	• 特定のレポートやハンティングツールにアクセス。 • 特定トピックに関するカスタム依頼を提出。 • 攻撃手法やキャンペーンの分析を実施。

// 最大限のインテリジェンス価値を即時活用

インシデントレスポンス、SOCアナリスト、迅速なリスク評価を求めるCISOなど、AAPとRAHは柔軟な選択肢を提供します。導入に関してはTeamT5のセールsteamまでお問い合わせください。

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。