

Raw Intel: 脅威理解の出発点

TeamT5エキスパートチームによる — ThreatVision Raw Intel

TeamT5アナリストが最前線の調査で収集した Raw Intelは、潜在的リスクを持つ未公開の観測情報を提供します。セキュリティチームはこれを用いてリアルタイムに不審な活動を発見し、詳細なインテリジェンスレポートが利用可能になる前に、タイムリーかつ詳細性のギャップを埋めることができます。例えば、追跡中に発見された不審なIP、ドメイン、ハッシュはRaw Intelとして記録されます。アナリストはこれらの手掛かりを照会・相互参照し、さらなる調査を導き、防御ロジックを強化し、脅威特定を加速できます。

情報 vs インテリジェンス

ThreatVisionのRaw Intelは「情報」であり「インテリジェンス」ではありません。

情報（Information）とは、初期観測を意味し、タイムリーだが完全には検証されていないため、アナリストによる確認や相互参照が必要です。

インテリジェンス（Intelligence）とは、処理・構造化され、信頼でき、行動に移せる洞察を提供します。Raw Intelは、完全なレポートが公開される前のギャップを埋めます。

不審なIoC、マルウェア、インフラといった予備的な発見は、調査の早期手掛かりを提供します。セキュリティチームはこの情報を分析の指針や進行中のケースの支援に活用できます。

また、TeamT5は、初期ワークフローにRaw Intelを組み込みつつ、より深い検証やコンテキストが必要な場合には完全レポートを依頼することを推奨します。

Raw Intelの利点

レポート公開前にタイムリーな手掛かりを入手

最新の未公開観測データにアクセス

不審活動の早期検知

インシデント対応とリスク評価の加速

Two Steps to Obtain ThreatVision Raw Intel

ステップ1: 検索結果から特定

キーワード検索（IP、ドメイン、ハッシュ）を行うと、「Raw Intel」タブに一致するRaw Intelが表示され、予備的な内容を閲覧可能。

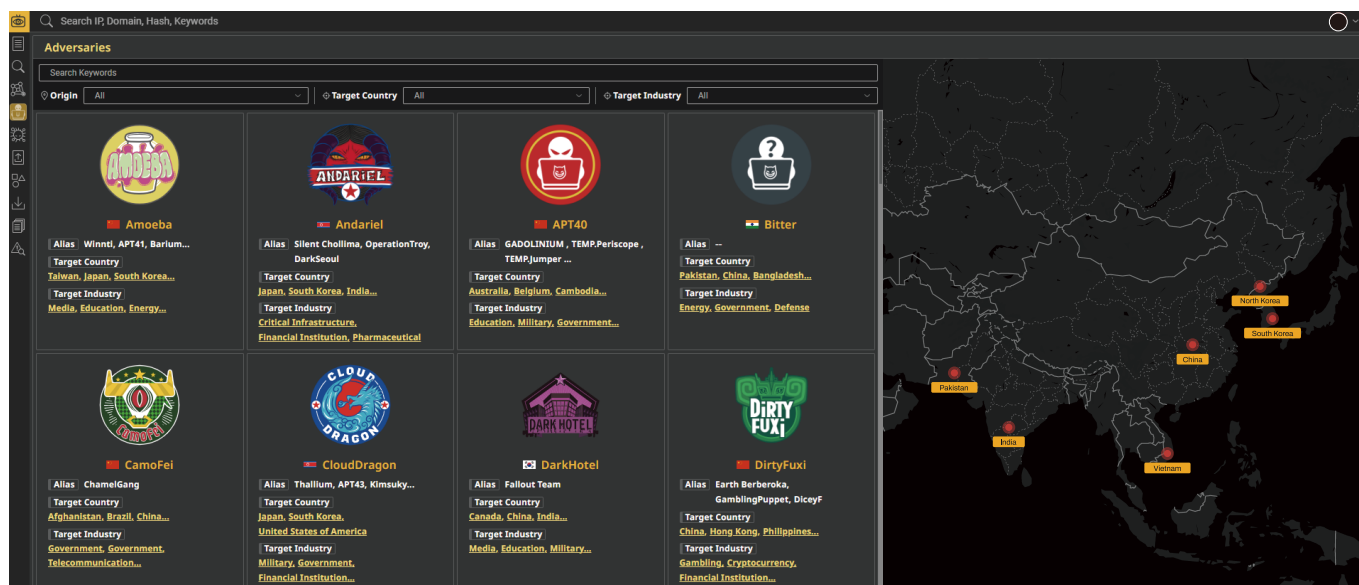


ステップ2: クレジットを使用して詳細を解放

詳細情報は初期状態ではマスクされています。クレジットを使用すると、対象・敵対者・マルウェア・悪用状況を含む完全な情報が解放され、ユーザーは脅威のコンテキストを迅速に把握できます。

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。