

ディープ & ダークウェブ リスクモニタリング

情報漏えいとサイバー 犯罪リスクを早期に検知

企業の機密データ、アカウント認証情報、侵害された端末に関する情報は、ディープ・ダークウェブ、地下フォーラム、Telegramなどのサイバー犯罪コミュニティで売買、共有される可能性があります。

「ThreatVision ディープ&ダークウェブリスクモニタリング」は、こうした地下チャネルを継続的に監視し、企業に関連する情報漏えいやサイバー犯罪リスクの特定を支援します。また、定期アラートやカスタマイズ分析レポート、専門家によるコンサルティングサービスを通じて、影響範囲の把握やリスク分析、対策計画の策定を支援します。

/// 主な特長

15億件以上の 漏えいデータを収集・分析

ディープ&ダークウェブや地下チャネルで流通する認証情報、アカウント情報、機密データを継続的に収集・分析。

7,700万件以上の 侵害端末を追跡

認証情報の窃取、情報漏えい、または後続攻撃に関連する侵害端末を追跡。

140万件以上の ディープ&ダークウェブ情報源を監視

ディープ&ダークウェブサイト、地下フォーラム、犯罪コミュニティなど幅広い情報源を監視。

400以上の Telegramチャンネルを追跡

地下コミュニティでの犯罪関連の議論や漏えい情報の流通状況を追跡。

APAC地域の中国語圏 地下チャンネルを網羅

APACのサイバー犯罪コミュニティや地下チャネルをカバー。そのうち50%以上が中国語で運用されています。

金融およびECに関する 犯罪リスクを監視

金融やEC分野に関連するサイバー犯罪活動を重点的に監視しています。

カスタマイズレポートお よびコンサルティングサービス

専門アナリストによるディープ&ダークウェブの分析、リスク評価、対策提案、コンサルティングサービスを提供します。

/// 主な利点

● プロアクティブなリスク監視

定期的な監視を通じて、ディープ&ダークウェブ上の潜在的なリスクを早期に検知し、脅威が深刻化する前の対応を支援します。

● インシデント対応力の強化

定期的な監視とタイムリーなアラートにより、情報漏えいリスクの兆候を早期に把握します。また、カスタマイズレポートを通じて、対応計画の策定、関係者への説明準備、業務調整を支援します。

● ブランドと信頼の保護

想定される漏えいデータの範囲と影響を早期に把握することで、対応の優先順位付けを支援し、ブランド毀損や信頼関係の悪化を最小限に抑えることにつなげます。

ThreatVisionはどのように企業のディープ&ダークウェブリスクへの早期対応を支援するのか

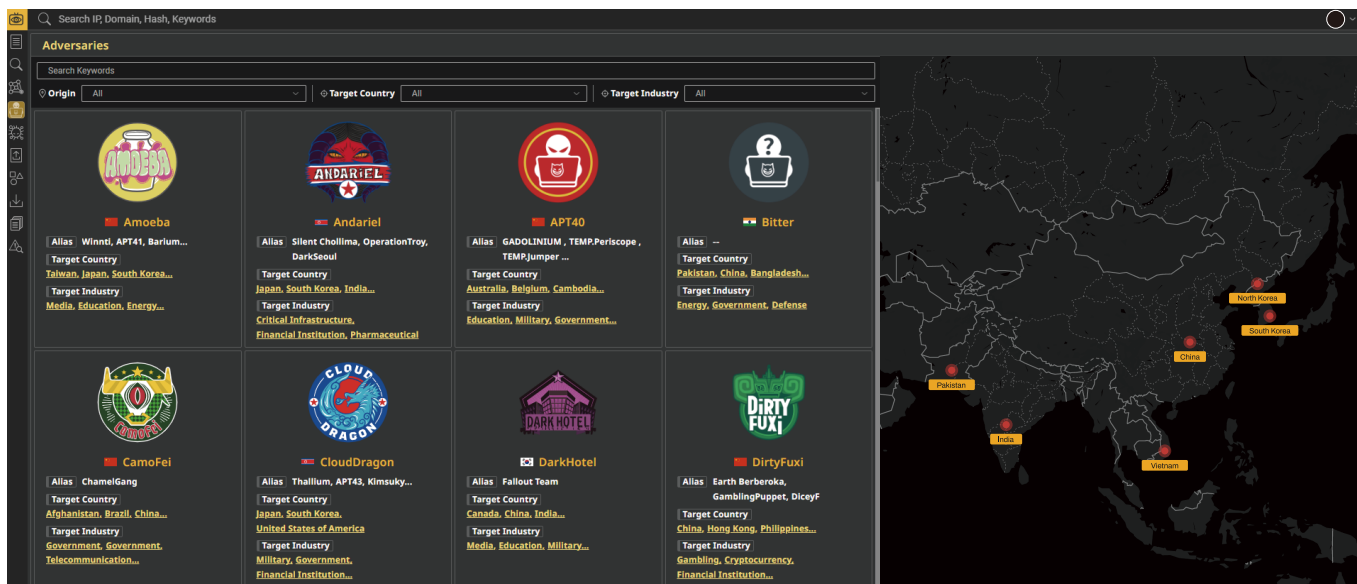
企業の課題	ThreatVisionによる支援
当社のアカウント、認証情報、機密データは漏えいしていないか	企業ドメイン、ブランド名、認証情報などのキーワードを対象にディープ&ダークウェブを監視します。監視結果は毎週メールで通知され、ThreatVisionにも自動反映されます。
漏えいしたデータは当社の事業、顧客、または社内システムに関係しているのか	企業ごとにカスタマイズされた監視分析レポートを通じて、漏えいデータとの関連性、影響範囲、リスクレベルを評価します。
地下フォーラムやTelegramで当社に関連する情報の売買や議論が行われていないか	ディープ&ダークウェブ、ハッカーフォーラム、Telegram、中国語圏の地下チャンネルを継続的に追跡し、漏えいデータの流通や犯罪活動の動向を把握します。
漏えいの兆候を発見した後、深刻度や対応優先度をどのように判断すればよいか	専門アナリストがディープ&ダークウェブの分析、リスク評価、推奨対策を提供し、適切な対応判断を支援します。
監視結果はどのように提供され、どのように活用できるのか	監視結果は毎週メールで通知され、ThreatVisionへ自動反映されます。漏えいデータはCSV形式でエクスポートでき、検索や照合に活用できます。
情報漏えいによるインシデントは、より大規模な犯罪活動と関連している可能性があるのか	漏えいの兆候がランサムウェア活動、犯罪コミュニティ、攻撃ツールと関連している場合、「ThreatVisionサイバー犯罪インテリジェンス」を活用し、追加リスクや防御優先順位を評価できます。

サービスパッケージ

ディープ&ダークウェブ リスクアラート	ディープ&ダークウェブ カスタマイズレポート
<ul style="list-style-type: none">ディープウェブ/ダークウェブを監視・スキャンし、週1回のアラート通知漏えいした認証情報やデータをカバー監視結果を毎週メールで配信、またThreatVision上でも自動的に更新流出したデータはCSV形式で簡単にエクスポート可能	<ul style="list-style-type: none">企業に特化したモニタリング分析レポートと、専門的なレポートコンサルティングサービスを提供専門アナリストによって作成されたレポートとディープ&ダークウェブインテリジェンス分析やリスク評価、推奨対策の提案レポートでは、APAC地域の犯罪コミュニティや中国語圏の地下チャンネルを分析対象とし、ハッカーフォーラム、Telegramチャンネル、招待制コミュニティなど幅広い地下情報源をカバー

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。