Datasheet

ThreatVision

TEAMT5

脆弱性ソリューション:
パッチ適用と緩和策を同時に実現

脆弱性管理における3大課題

現代の組織は、脆弱性対応と管理において次の3つの大きな課題に直面しています。

- 急増する脆弱性により、追跡が困難
- 複数ソースからの過剰な情報ノイズにより、フィルタリングが複雑化
- パッチ適用の優先順位が不明確で、対応が遅延

これらの課題により、チームは本当に高リスクな脆弱性に集中できません。ThreatVisionは、専門家が精査・更新した脆弱性インテリジェンスと実行可能なパッチ適用ガイダンスを提供し、組織が効果的に優先順位を付け、効率的なプロセスを構築できるようにします。

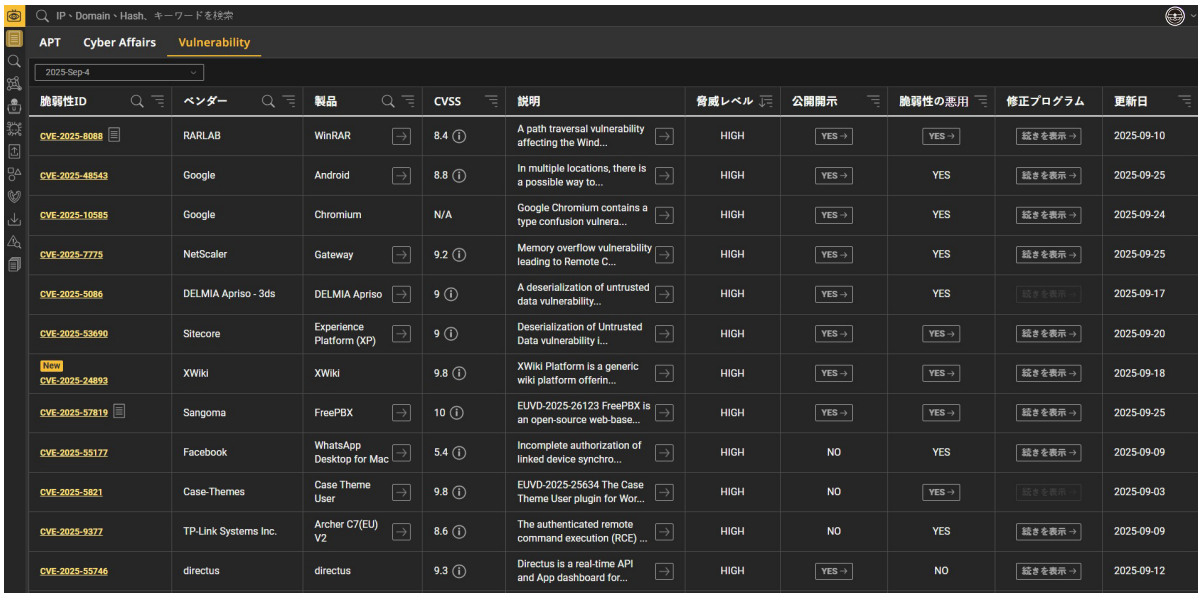
幅広く深い脆弱性インテリジェンス

Vulnerability Insights Report (VIR)

シニアアナリストが作成するVIRは、最近悪用された高リスク脆弱性に焦点を当てます。攻撃シナリオ、関与する脅威グループ、影響を受ける産業を詳細に分析し、リスクと関連性を評価します。各レポートには、CVE ID、CVSSスコア、技術詳細、未修正脆弱性への緩和策や検知ツールを含みます。隔週発行、年間24件。

Patch Management Report (PMR)

各PMRは、約100件の主要な脆弱性を網羅し、CVE、PoCコード、CVSSスコア、影響を受ける製品、パッチ適用ガイダンスを提供します。リソースが限られるチームでも、迅速に優先順位を決めて対応可能です。週次発行、年間52件。



脆弱性ID	ベンダー	製品	CVSS	説明	脅威レベル	公開開示	脆弱性の悪用	修正プログラム	更新日
CVE-2025-8088	RARLAB	WinRAR	8.4	A path traversal vulnerability affecting the Wind...	HIGH	YES	YES	続きを表示	2025-09-10
CVE-2025-48543	Google	Android	8.8	In multiple locations, there is a possible way to...	HIGH	YES	YES	続きを表示	2025-09-25
CVE-2025-10585	Google	Chromium	N/A	Google Chromium contains a type confusion vulnera...	HIGH	YES	YES	続きを表示	2025-09-24
CVE-2025-7775	NetScaler	Gateway	9.2	Memory overflow vulnerability leading to Remote C...	HIGH	YES	YES	続きを表示	2025-09-25
CVE-2025-5086	DELMIA Apriso - 3ds	DELMIA Apriso	9	A deserialization of untrusted data vulnerability...	HIGH	YES	YES	続きを表示	2025-09-17
CVE-2025-53690	Sitecore	Experience Platform (XP)	9	Deserialization of Untrusted Data vulnerability i...	HIGH	YES	YES	続きを表示	2025-09-20
New CVE-2025-24893	XWiki	XWiki	9.8	XWiki Platform is a generic wiki platform offerin...	HIGH	YES	YES	続きを表示	2025-09-18
CVE-2025-57819	Sangoma	FreePBX	10	EUVD-2025-26123 FreePBX is an open-source web-base...	HIGH	YES	YES	続きを表示	2025-09-25
CVE-2025-55177	Facebook	WhatsApp Desktop for Mac	5.4	Incomplete authorization of linked device synchro...	HIGH	NO	YES	続きを表示	2025-09-09
CVE-2025-5821	Case-Themes	Case Theme User	9.8	EUVD-2025-25634 The Case Theme User plugin for Wor...	HIGH	NO	YES	続きを表示	2025-09-03
CVE-2025-9377	TP-Link Systems Inc.	Archer C7(EU) V2	8.6	The authenticated remote command execution (RCE) ...	HIGH	NO	YES	続きを表示	2025-09-09
CVE-2025-55746	directus	directus	9.3	Directus is a real-time API and App dashboard for...	HIGH	YES	NO	続きを表示	2025-09-12

脆弱性向けに設計された脅威ハンティングツール

TeamT5は、VIRで取り上げた脆弱性を対象に、YARA、Snort、Sigma、スクリプトなどの検知ツールを開発。攻撃試行を検出し、対応を支援することで防御を強化します。

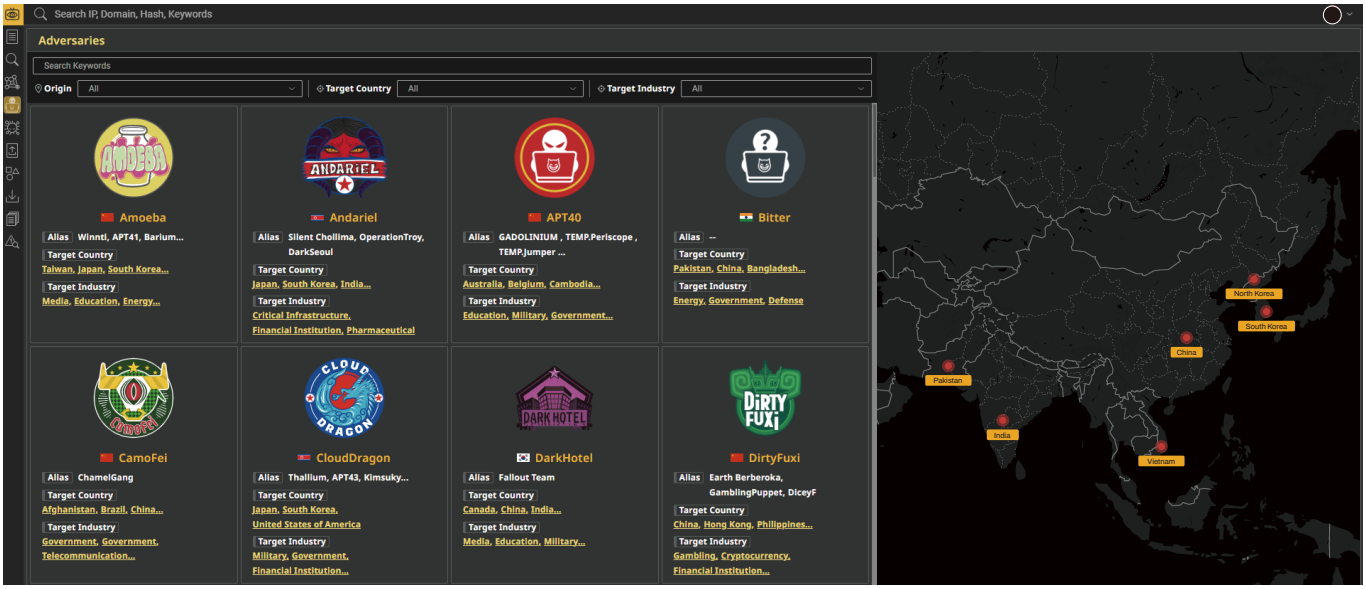
VIR	PMR
・ 高リスク脆弱性の詳細分析 ・ 実際の攻撃シナリオと緩和方法 ・ 緩和策とTeamT5独自の検知ツール ・ 重大脆弱性からのリスク低減 ・ 隔週発行（年間24件） ・ 英語版提供	・ 毎週約100件の脆弱性リスト ・ 影響製品の詳細とパッチ適用ガイド ・ 公開PoCコードを収録 ・ 実際の悪用事例を追跡 ・ 週次発行（年間52件） ・ 英語版提供

ThreatVision PMR + VIR: 脆弱性対応の最適解

組織のニーズ	適用方法
最近悪用された高リスク脆弱性を特定する	**PMR 脆弱性リスト：** 高リスク脆弱性を特定・修正し、被曝を低減
特定された脆弱性に対して効果的な緩和策を適用する	**VIR 緩和戦略：** 未修正脆弱性に対する検知ルールと防御推奨を提供。影響を受けるベンダーや製品を理解し、影響範囲を評価
影響を受けるベンダーや製品を把握し、影響範囲を評価する	**PMR + VIR の統合インテリジェンス：** 影響ベンダーや製品データを集約し、優先順位付けとリソース配分を最適化

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セールスチーム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。

E-mail sales-admin-jp@teamt5.jp

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA