



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	公開済み	脆弱性の適用	修正プログラム	更新日
CVE-2025-6898	RARLAB	WinRAR	8.4	A path traversal vulnerability affecting the Win...	HIGH	YES	YES	修正プログラムあり	2025-09-10
CVE-2025-6949	Google	Android	8.8	In multiple locations, there is a possible way to...	HIGH	YES	YES	修正プログラムあり	2025-09-25
CVE-2025-10889	Google	Chromium	N/A	Google Chromium contains a type confusion vulner...	HIGH	YES	YES	修正プログラムあり	2025-09-24
CVE-2025-7779	NetScaler	Gateway	9.2	Memory overflow vulnerability leading to remote C...	HIGH	YES	YES	修正プログラムあり	2025-09-25
CVE-2025-5886	DELLMA Apptec - Sds	DELLMA Apptec	9	A deserialization of untrusted data vulnerability...	HIGH	YES	YES	修正プログラムあり	2025-09-17
CVE-2025-5890	Sitacore	Experience Platform (XP)	9	Deserialization of Untrusted Data vulnerability...	HIGH	YES	YES	修正プログラムあり	2025-09-20
CVE-2025-24893	XWiki	XWiki	9.8	XWiki Platform is a generic wiki platform offeri...	HIGH	YES	YES	修正プログラムあり	2025-09-18
CVE-2025-51819	Sangoma	FreePBX	10	EUV2-2025-28123 FreePBX is an open source web-base...	HIGH	YES	YES	修正プログラムあり	2025-09-25
CVE-2025-58177	Facebook	WhatsApp Desktop for Mac	5.4	Incomplete authorization of linked device synchron...	HIGH	NO	YES	修正プログラムあり	2025-09-09
CVE-2025-5861	Case Themes	Case Theme User	9.8	EUV2-2025-15604 The Case Theme User plugin for Wo...	HIGH	NO	YES	修正プログラムあり	2025-09-03
CVE-2025-58177	TP-Link Systems Inc.	Archer C7500 V2	8.4	The authenticated remote command execution (RCE)...	HIGH	NO	YES	修正プログラムあり	2025-09-09
CVE-2025-58176	directus	directus	9.3	Directus is a real-time API and App dashboard for...	HIGH	YES	NO	修正プログラムあり	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	毎週約100件の脆弱性リスト
実際の攻撃シナリオと緩和方法	影響製品の詳細とパッチ適用ガイド
緩和策とTeamT5独自の検知ツール	公開PoCコードを収録
重大脆弱性からのリスク低減	実際の悪用事例を追跡
隔週発行 (年間24件)	週次発行 (年間52件)
英語版提供	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

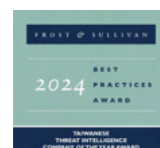
世界中の300以上の顧客に信頼され、政府、テクノロジー、製造、金融、医療、軍事、通信など幅広い業界を支援しています。

世界的な専門チーム

TeamT5のメンバーは脅威インテリジェンス研究や先進セキュリティ技術における世界的リーダーであり、HITCON(台湾)、Black Hat(米国)、Code Blue/AVTOKYO(日本)、Troopers(ドイツ)、Hack In The Box、FIRSTなどの国際会議で最新研究を発表しています。

業界からの認知

TeamT5はBloomberg、CNN(米国)、産経新聞、朝日新聞(日本)、ET News(韓国)など主要メディアで取り上げられています。2022年には、JAFCO(日本最大のベンチャーキャピタル)、伊藤忠(日本最大の総合商社)、マクニカ(日本最大のセキュリティソリューションプロバイダー)から出資を受けました。



TeamT5 | Tel +886-2-7706-1299 | E-mail SALES-ADMIN-JP@teamt5.jp



[Website](#)



[X \(Twitter\)](#)



[YouTube](#)