

脆弱性インテリジェンス パッチ適用と緩和策を同時に実現

脆弱性管理における 三大課題

現代の組織は、脆弱性対応と管理において主に3つの課題に直面しています。

- 脆弱性の数が急増し、追跡が困難
- 複数ソースからの過剰な情報ノイズにより、必要な情報の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

こうした課題により、セキュリティチームは、本当にリスクの高い脆弱性を効果的に特定することが難しく、限られたリソースの中で適切に対応の優先順位を付けることも困難になります。

ThreatVision は、専門家が精査し、継続的に更新する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、組織が高リスクな脆弱性に優先的に対応し、より体系的で効率的な脆弱性管理プロセスを構築できるよう支援します。

深さと幅広さを兼ね備えた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、大規模に悪用されている高リスクな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、影響を受ける業界を詳細に分析し、脆弱性のリスクや攻撃との関連性を評価します。各レポートには、CVE ID、CVSSスコア、技術情報に加え、すぐにパッチを適用できない場合の緩和策や検知ツールを含みます。2週間ごとに発行され、年間24本提供されます。

Patch Management

Patch Managementは、高リスクな脆弱性に関する重要なインテリジェンスを継続的に更新・集約します。TeamT5の脅威ハンティング研究チームは、リスク評価モデルを適用し、信頼できる複数のインテリジェンスソースを照合することで、公開済みの脆弱性のうち、実際の攻撃で悪用されているものや、利用可能な攻撃ツールが存在する高リスクな脆弱性を特定します。

影響を受ける製品の詳細、パッチ情報、PoCコードを提供し、リスク評価やパッチ適用の優先順位付けを支援します。既知の脆弱性に加え、TeamT5はゼロデイ脆弱性も積極的に追跡し、ユーザーがより早い段階でリスクを把握して、プロアクティブな防御を検討できるよう支援します。

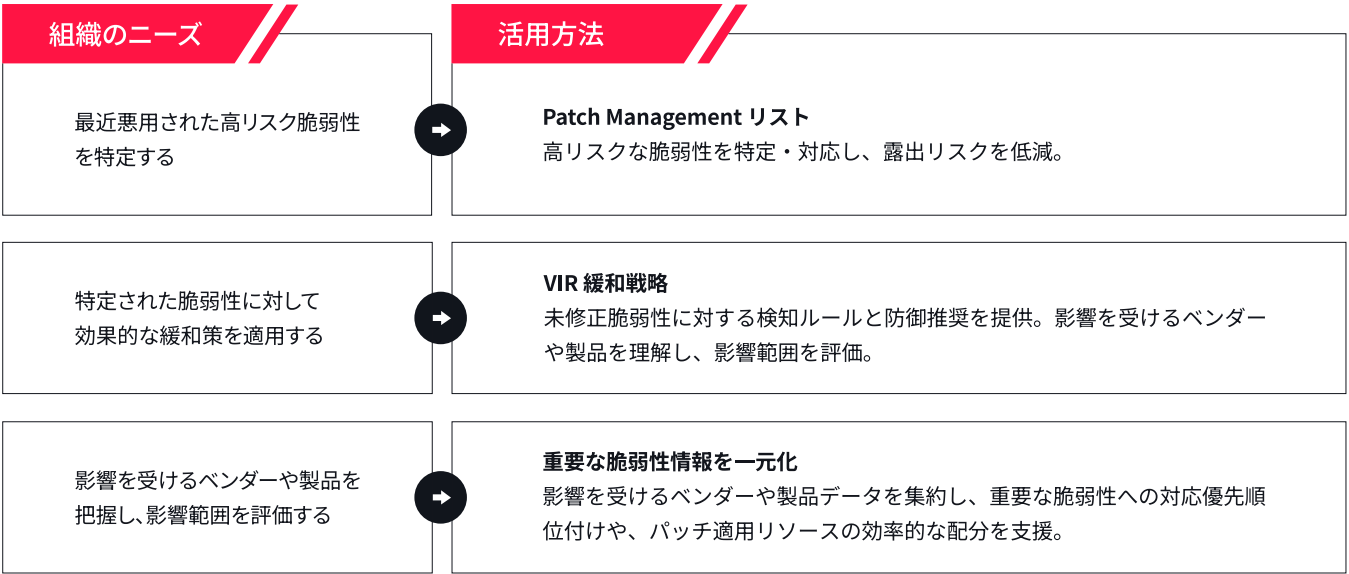
Patch Management										
Search Vuln ID, Vendor, Product										
Threat Level: 制限なし Publicly Disclosed: 制限なし Exploited: 制限なし Visibility: All Items Update Date: 制限なし										
7773 total results										
脆弱性ID	ベンダー	製品	CVSS	説明	脅威レベル	公開開示	脆弱性の悪用	修正プログラム	更新日	
New CVE-2025-53296	Linux	Kernel	8.8 [CVSS:3.1]	In the Linux kernel, the following vulnerability ...	HIGH	YES	YES	修正を表示	2026-09-22	
New CVE-2025-39964	Linux	Kernel	7.8 [CVSS:3.1]	In the Linux kernel, the following vulnerability ...	HIGH	YES	YES	修正を表示	2026-09-22	
New CVE-2025-60004	Gitea	Gitea	9.8 [CVSS:3.1]	Gitea before 1.27.1 allows remote code execution ...	HIGH	YES	YES	修正を表示	2026-09-22	
New CVE-2025-85706	GitLab	Community Edition and Enterprise	10 [CVSS:3.1]	GitLab has remediated an issue in GitLab CE/EE af...	HIGH	YES	YES	修正を表示	2026-09-22	
New CVE-2025-84645	Jenkins Project	Jenkins	8.8 [CVSS:3.1]	In Jenkins 2.579 and earlier, LTS 2.568.2 and ear...	HIGH	YES	NO	修正を表示	2026-09-22	
New CVE-2025-67276	Mikrotik	RouterOS	9.2 [CVSS:4]	ELUVD-2025-72034 RouterOS does not compare the comp...	HIGH	YES	NO	修正を表示	2026-09-22	
New CVE-2025-19598	sc0ttkclark	Pods - Custom Content Types an...	9.8 [CVSS:3.1]	The Pods - Custom Content Types and Fields plugin...	HIGH	YES	NO	修正を表示	2026-09-22	
New CVE-2025-77812	DJI	Avata 360	9.4 [CVSS:4]	ELUVD-2025-63973 DJI drones transmit DUMML (DJI Univ...	HIGH	YES	NO	修正を表示	2026-09-22	
New CVE-2025-72773	Zyxel	GS1900 Series Switches	8.8 [CVSS:3.1]	Zyxel GS1900 series switches contain a stack-base...	HIGH	NO	YES	修正を表示	2026-09-22	
New CVE-2025-39682	Linux	Kernel	9.8 [CVSS:3.1]	In the Linux kernel, the following vulnerability ...	HIGH	YES	YES	修正を表示	2026-09-21	
New	Adobe	Adobe Commerce	10 [CVSS:3.1]	Adobe Commerce is affected by	HIGH	YES	YES	修正を表示	2026-09-21	

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。

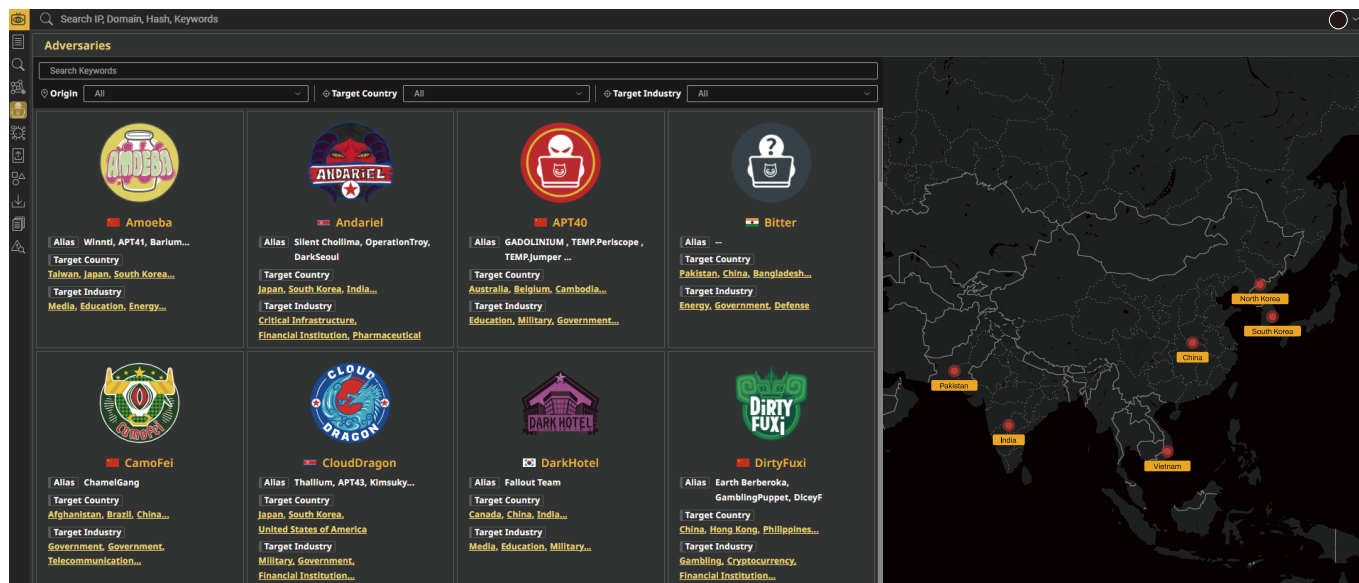
VIR	Patch Management
・ 高リスク脆弱性の詳細分析 ・ 実際の攻撃シナリオと緩和方法 ・ 緩和策とTeamT5独自の検知ツール ・ 重大脆弱性からのリスク低減 ・ 隔週発行(年間24件) ・ 英語版提供	・ 検証済みのインテリジェンスに基づき、高リスクな脆弱性を優先 ・ 公開状況と実際の悪用状況を追跡 ・ 影響を受ける製品情報をもとに影響範囲を評価 ・ パッチ情報と公開PoCを活用して修復を支援 ・ ゼロデイリスクを早期に把握

ThreatVision 脆弱性分析 + 管理: 脆弱性対応の最適解



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。