ポスト・ミュトス脆弱性急増に対する自律的修復の運用化

脆弱性管理のルールが破られた。

従来の脆弱性管理手法はもはや時代遅れです。

Anthropic 社の Claude Mythos は、人間の専門家が見逃した脆弱性を自律的に発見し、複数の脆弱性を連鎖させることで、公開後わずか数時間で実用的なエクスプロイトを開発できます。他の最先端 AI モデルも間もなくこれに追随するでしょう。これにより、Glasswing プロジェクトを通じて Mythos のプレビューパートナーを含むソフトウェアベンダーから、脆弱性情報とパッチが急増すると予想されます。従来の脆弱性管理ワークフローに依存している組織は、存続に関わるリスクに直面することになります。

修復の破綻した物理法則、Mythos 以前

Mythos 以前から、脆弱性の数は過去 4 年間で 6.5 倍に急増し、ゼロデイ脆弱性の増加に伴うパッチの普及により、平均悪用時間は 2025 年には-7 日にまで短縮されました。現在の修復アプローチは既に時代遅れとなっており、CISA の重要脆弱性（KEV）の平均悪用時間よりも、平均修復時間（MTTR）の中央値の方がはるかに長くなっています。

6.5 倍

脆弱性の増加

(過去 4 年間の増加率)

フロンティア AI はこの増加をさらに加速させる。

18 日間

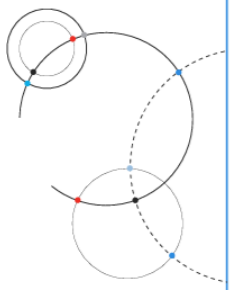
エクスプロイトまでの期間の中央値

最先端の AI モデルにより、数時間に短縮。

67 日間

MTTR (平均修復時間) の中央値

最先端の AI モデルはロングテールを狙います。



ソース: The Broken Physics of Remediation, Qualys Threat Research Unit
(1 万以上の組織から得られた長年のデータに基づく、この種の研究としては最大規模のもの)

0.74%

2025 年に、武器化された CVE の割合

脆弱性のノイズと無駄な時間

脆弱性の数は年々急速に増加していますが、攻撃者によって悪用されるのはそのうちの 1%未満です。2025 年には、48,172 件の脆弱性のうち、悪用され CISA KEV に登録されたのはわずか 357 件、つまり 0.74%に過ぎません。しかも、これらの脆弱性の大部分は、対策によって悪用されることはありません。組織は、いたちごっこに終始し、間違った脆弱性の修正に時間を浪費しています。

今後の展望

脆弱性の発見と悪用が AI のスピードで進む中、修復も機械のスピードで行わなければなりません。この課題を解決するには、最もリスクの高い脆弱性に対して自律的な修復を行う運用体制への移行が必要です。リスクオペレーションセンター（ROC）は、以下の機能を提供することで自律的な修復を可能にします。

リスクオペレーションセンター（ROC）は、以下の機能を提供することで、自律的な修復を可能にします。

1. 自社およびサードパーティ製アプリケーションにおける脆弱性、設定ミス、ID リスクを AI で高速検出。
2. 脅威、ビジネス、資産のコンテキストに基づいて、真に悪用可能な脆弱性を特定するための超優先順位付けを行い、理論的なリスクフィルタリングを行い、補完的な制御を通じて悪用可能性を検証し、検証済みのリスクを顕在化させる。
3. 信頼性スコア、展開ウェーブ、ロールバックオプションによる運用上の回復力を維持しながら、ネイティブパッチおよびパッチレスオプションによるゼロデイ脆弱性の修復。

Qualys は、ROC（リスク管理）を強化する統合型 AI プラットフォームを提供し、検出、優先順位付け、修復のための業界最先端のソリューションを機械速度で提供します。複数のツールを行き来する必要はもうありません。セキュリティ部門と IT 部門間のシームレスな連携を実現します。これこそが、リスク管理の未来です。

AI による高速検出

攻撃者が悪用する前に
脆弱性を検出します。

Qualys VMDR

VMDR は、数々の Pwnie 賞を受賞した 120 名以上の脅威リサーチチームに支えられた、業界をリードする脆弱性検出ソリューションです。

- **シックスシグマ**レベルの検出精度
- 業界標準の CVSS ベースの優先順位付けよりも **45 日**先行
- **120 名以上**の専任脅威エンジニアによる自動シグネチャパイプライン
- デジタル証明書と CIS 構成評価機能を内蔵
- ファーストパーティアプリの脆弱性を検出

13 万件以上の CVE をカバー: 業界全体で検出カバレッジ No.1

CISA KEV を **99.4%**カバー、優先順位付けは 45 日先まで先行、業界最高水準

クリティカル/ゼロデイ脆弱性に対するシグネチャ配信の中央値は **12 時間**、優先度の高いベンダーでは 6 時間未満

超優先順位付け

不要な情報を 99%排除。
本当に重要なことに集中する。

**Qualys (ETM)
Enterprise TruRisk Management**

ETM は、エージェント AI と連携して CTEM を運用化し、最もリスクの高いエクスポージャーを明らかにします。

- 統合資産インベントリ（CASM）とリスク集約
- **TruRisk:** Qualys とサードパーティの調査結果を統合し、ビジネスに即したリスクスコアを算出
- **TruLens:** ダークウェブの動向とランサムウェア活動を追跡し、脅威に基づいた優先順位付けを実施
- **TruConfirm:** 本番環境で安全に動作するエクスプロイト検証
- **Agentic AI:** サイバーリスクエージェントが手動アナリストの負担を軽減ファーストパーティアプリの脆弱性を検出

脅威とビジネスコンテキストのレイヤリングにより、ノイズを **95%**削減

過去 12 ヶ月間で **800 万件以上**の TruConfirm エクスプロイト検証を実施、業務中断ゼロ

CISA KEV リスト掲載前に、平均 **45 日間**の優先順位付けの先行

ゼロデイ修復

マシンスピードでリスクを
修正、軽減、排除します。

**Qualys
TruRisk Eliminate**

TruRisk Eliminate は、IT パッチ適用におけるスピードギャップを解消するサイバーセキュリティ対策ソリューションです。

- ネイティブな修復オプション: パッチ適用、修正、緩和、アンインストール、隔離
- AI を活用したパッチ信頼性スコアとウェーブ展開
- 異常検知時の自動ロールバック機能を備えたゼロタッチパッチ自動化
- ランサムウェアの脆弱性を 100%カバー
- ファーストパーティアプリにおける脆弱性を修復

過去 12 ヶ月間に **1 億 5000 万件以上**のパッチを適用

過去 12 ヶ月間に **4000 万件以上**の自動パッチを適用、ロールバック率は 0.1%未満

修復にかかる平均時間を **80%**短縮

継続的なリスク軽減策を実用化する準備はできていますか？

Qualys が、AI 時代の情報開示の波に備えるためにどのように役立つかをご覧ください。

デモを依頼する

v260505