Qualys

超優先順位付けと自律的修復の運用化

(Operationalize Hyper-prioritization and Autonomous Remediation)

「ポスト・ミュトス時代」における
脆弱性の急増への対処

Mythos、プロジェクト Glasswing、そしてその影響

Anthropic Claude Mythos プレビュー

Mythos: 脆弱性を自律的に発見し、エクスプロイトを開発する最先端のモデル。他のモデルもそれに追随しつつある。

Glasswing: 広く普及しているソフトウェアの脆弱性を特定し、修正するプロジェクト。

43% CISA KEVの43%はGlasswingのローンチパートナーの製品に起因している。

Qualys製品はCISA KEVには掲載されていません

Mythosとその他のモデルの影響

1. 脆弱性が指数関数的に増加する中、**NVDが強化されることはない**
2. 開示から悪用までの時間は数時間以内です

修復の壊れた物理学: プレMythos

6.5倍	過去4年間における重大な脆弱性の増加
18日	リスクの高いエクスポージャーを悪用するまでの期間の中央値
67日	MTTRの中央値

Source: Qualys TRU Research

CVEの1%未満が武器化されている

0.74%

2025年の武器化されたCVE

自社のセキュリティ対策に基づいて、環境内で実際に悪用可能な脆弱性を優先的に特定していますか？

数字で見る脆弱性ノイズ

年	開示済み	武器化済み	割合
2022	25,043	131	**0.52%**
2023	28,816	185	**0.64%**
2024	39,964	218	**0.55%**
2025	48,172	357	**0.74%**

The Broken Physics of Remediation, Research Report from Qualys TRU

脆弱性悪用は、最も多いアクセス経路です

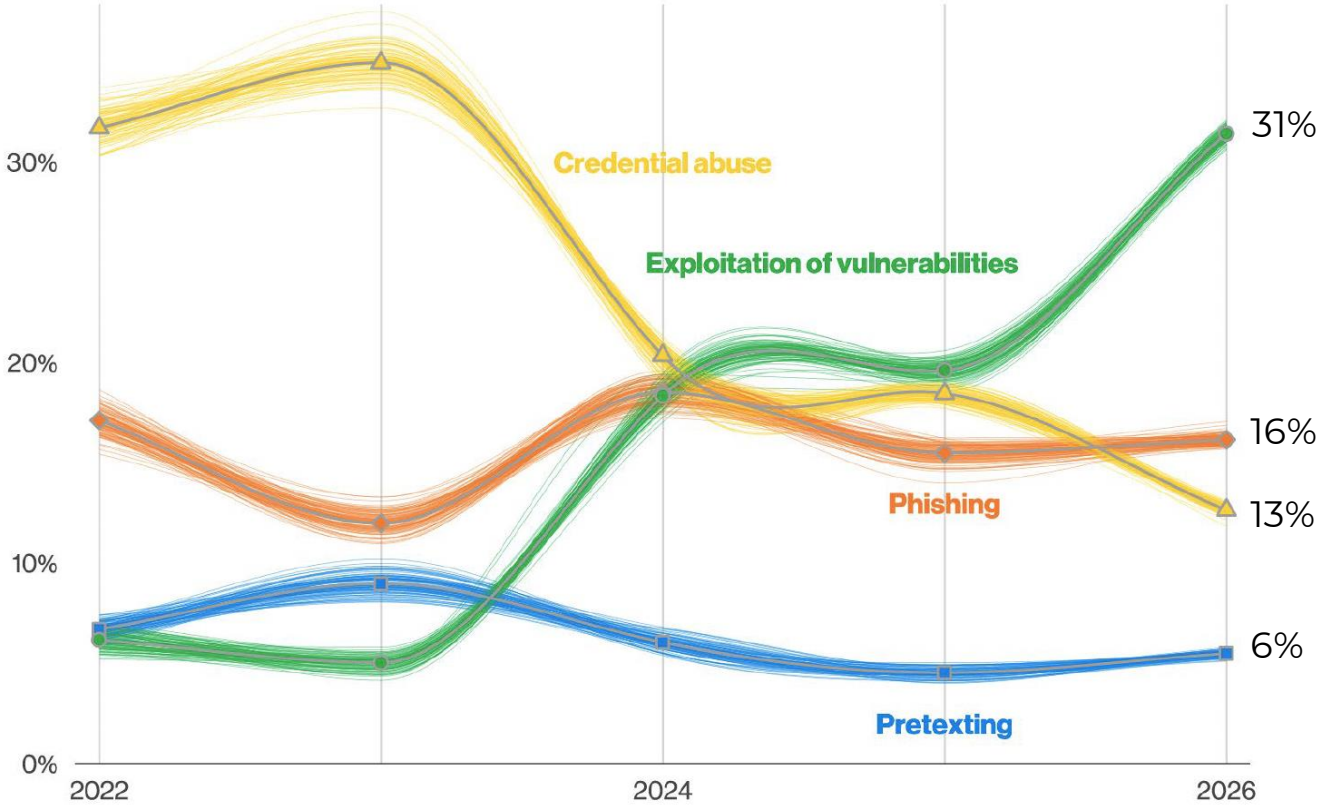


図5. エラーや不正使用以外の侵害における既知の初期アクセスベクトルの推移
（2026年のデータセットの数n=19,905）

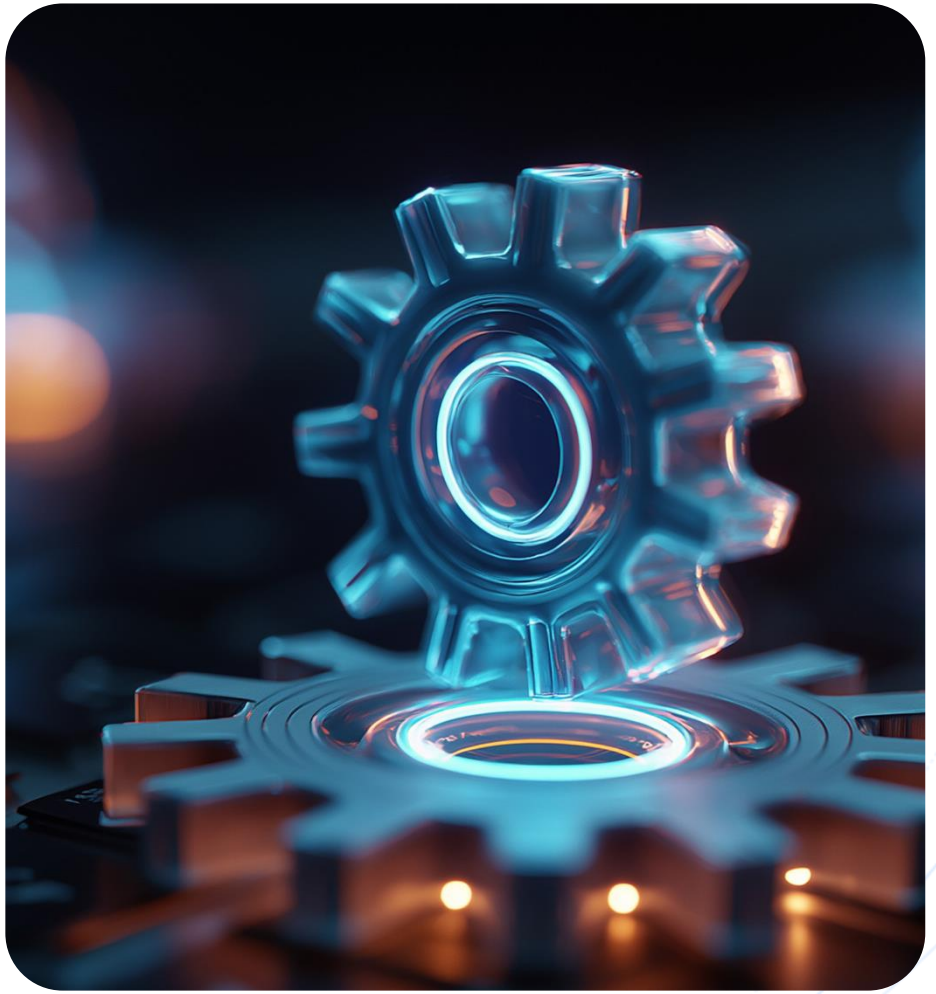
今後の展望

攻撃者は情報公開後数時間以内に悪用するため、環境内の悪用可能な脆弱性に対する修復速度は、マシンの速度と同等でなければなりません。

Risk Operations Center (ROC)

ROCは、
自律修復
を可能にするソリューション
を運用化します。

Autonomous Remediation



自律的な修復を運用するための手順

AIによる高速検出

- 情報開示速度の速い脆弱性検出
- 資産インベントリ – 内部資産および外部資産

超優先順位付け

- 脅威、ビジネス、資産コンテキストに基づいて優先順位を決定
- 補完的な対策と照らし合わせて悪用可能性を検証

ゼロデイ修復

- パッチ適用型およびパッチレス型の修復・緩和策を提供
- 運用上の回復力を維持しながら自動化を実現

Qualysの自律型修復ソリューション

AIによる高速検出

- 情報開示速度の速い脆弱性検出
- 資産インベントリ – 内部資産および外部資産

VMDR

超優先順位付け

- 脅威、ビジネス、資産コンテキストに基づいて優先順位を決定
- 補完的な対策と照らし合わせて悪用可能性を検証

ETM

ゼロデイ修復

- パッチ適用型およびパッチレス型の修復・緩和策を提供
- 運用上の回復力を維持しながら自動化を実現

TruRisk Eliminate

統合プラットフォームによる最先端AI時代のリスク管理

カテゴリリーダー

AIスピードによる高速検出
VMDR

ベースライン脆弱性管理

価値

- オンプレミス環境とクラウド環境、コンテナインフラストラクチャ全体にわたる脆弱性の高精度検出。
- リスク管理とコンプライアンスワークフローの基盤となります。

主要な機能

- No.1カバレッジ: 13万件以上のCVEをカバー
- 99.4%: CISA KEVカバレッジ
- デジタル証明書評価
- 構成評価（CISベンチマーク）
- 資産インベントリ
- 脅威ベースの優先順位付け (TruRisk)

カテゴリリーダー

超優先度設定
ETM

Agentic AIによる運用可能なCTEM

価値

- 攻撃者が攻撃を仕掛ける前に、最もリスクの高い脆弱性に対処するため、エクスポージャーノイズを98%削減します。
- セキュリティポスチャーを3倍向上
- ビジネスへの影響に合わせたリスクの統合ビュー

主要な機能

- 統合資産インベントリ (CSAM)
- QualysおよびQualys以外のセンサーからの統合リスクビュー
- 資産およびビジネスコンテキストに基づく優先順位付け (TruRisk)
- 新たな脅威 (TruLens)
- 悪用可能性の検証 (TruConfirm)
- サイバーリスクの定量化
- サイバーリスクワークフローのためのAIエージェント

カテゴリリーダー

ゼロデイ修復
TruRisk Eliminate

パッチ適用とパッチレスによる修復

価値

- 機械並みのスピードで修復
- セキュリティとIT部門の連携を円滑化
- 運用上の回復力を実現

主要な機能

- 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
- マルチベンダー対応: Zscaler, SCCM/Intune, CrowdStrike, ServiceNow.
- ルールベースのオーケストレーション
- 100%カバレッジ: ランサムウェア対策

超優先順位付け
(Hyper-Prioritization)

Qualys®

AIネイティブのリスクオペレーションセンターで優先順位付け

Qualys Enterprise TruRisk Management (ETM)

885 Critical TruRisk™ Score

統合資産インベントリ → リスク要因の集約 → 脅威インテリジェンス → ビジネスコンテキスト → リスクの優先順位付け → リスク対応オーケストレーション → コンプライアンスおよび経営報告

セキュリティとリスクの調査結果 | リスクの特定

QUALYS

- 脆弱性
- アプリセキュリティ
- コンフィグレーション
- 資産管理
- コンプライアンス
- アタックサーフェス
- クラウドセキュリティ
- AI セキュリティ

NON-QUALYS

- 脆弱性管理
- コンプライアンス
- ランタイムセキュリティ
- アプリケーションセキュリティ

（脅威情報フィードを内蔵し、社内の脆弱性調査を強化）

脅威インテリジェンス

（CMDB、カスタムデータソース）

ビジネスコンテキスト

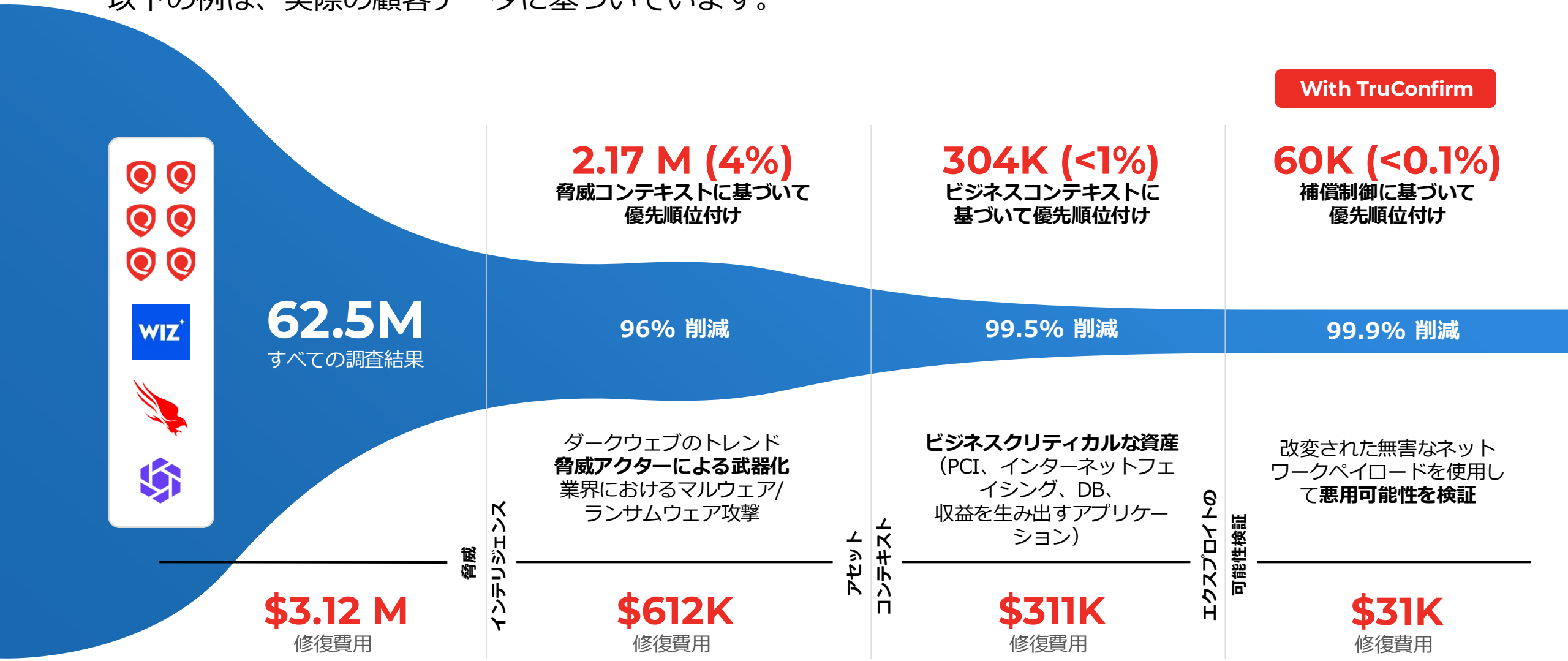
測定 | ビジネス用語でサイバーリスクを定量化する

伝達 | エグゼクティブレポートとチケット発行

排除 | パッチ、緩和、追跡

検出から優先順位付け、そして超優先順位付けへ

以下の例は、実際の顧客データに基づいています。



Qualys ETM が Agentic AI で CTEM を運用可能

統合資産インベントリ (CSAM)

外部および内部の攻撃対象領域全体をリスクコンテキストとともに包括的に可視化します。技術資産を、重要度および関連リスクとともに、ビジネスエンティティに自動的にリンクします。

TruRisk: ビジネスにおけるサイバーリスクの定量化

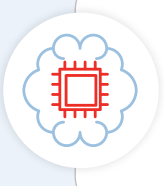
脅威、資産、ビジネスコンテキストに基づいて優先順位付け。
ビジネスへの影響に基づいて**定量化**。
環境要因とリスク軽減策に基づいて**リスクをカスタマイズ**。

エクスポージャーの集約

Qualysおよびサードパーティ製セキュリティツールから得られたセキュリティ検出結果を集約、正規化、重複排除することで、リスクの統合ビューを実現します。

TruLens: 脅威ベースのリスク優先順位付け

QualysのTruLensモバイルアプリを使えば、**業界における新たな脅威やトレンド**を常に把握し、リスクの優先順位付けと軽減計画を可視化することで、常に先手を打つことができます。外出先でも状況を把握可能です。



ネイティブなエージェント型AI

TruRiskのインサイトを活用したQualysのすぐに使える**サイバーリスクエージェント**と**サイバーリスクアシスタント**は、セキュリティチームを戦略的なオーケストレーターへと変革します。

TruConfirm: 脆弱性の悪用可能性を検証

セキュリティ対策を検証しながら、**脆弱性の悪用可能性を確認**します。
悪用可能性が確認された脆弱性を優先的に処理することで、脆弱性の修復を迅速化します。

TruConfirm と Agent Valによる悪用可能性検証の紹介

TruConfirm

実証済みの本番環境向けエクスプロイト検証

実際の構成、実際の制御システムを用いて、稼働中の資産における脆弱性の悪用可能性を検証します。

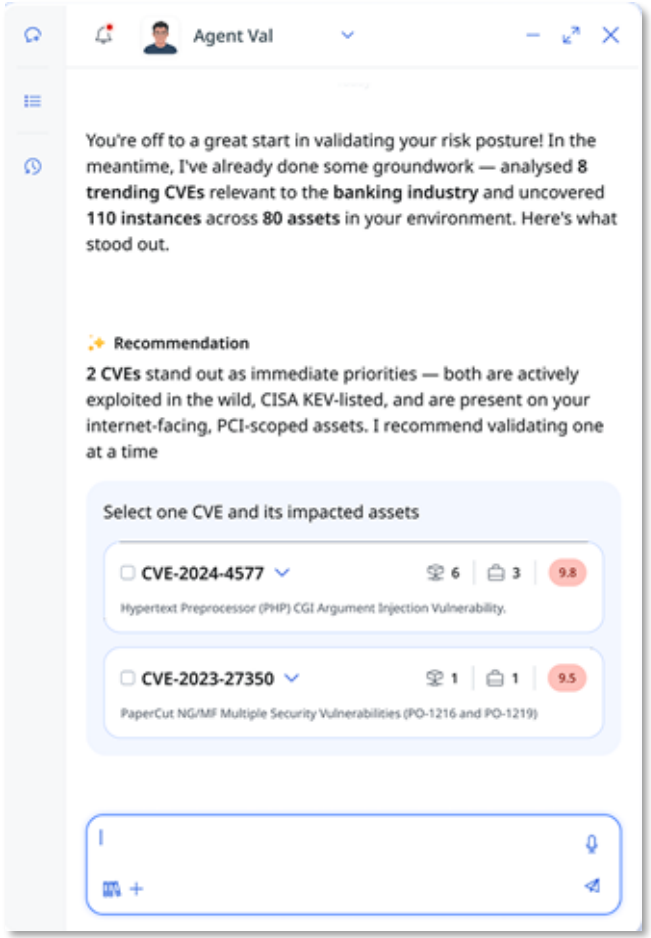
以下の**3つ**の結果を生成します:

A. 悪用可能
B. 制御システムによりブロックされている
C. 到達不能

Agent Val

業界初の、エクスプロイト検証のためのエージェント型AI

次のターゲットを継続的に選択し、本番環境でTruConfirmを安全に実行し、修正を推進し、完了を再検証します。



TruConfirm: 安全で実績あり

800万件以上の TruConfirm 認証を実施。

過去12か月間における実施件数。

中断ゼロ

本番環境

安全第一のアーキテクチャ

- データの抜き取りなし
- ディスクへの書き込みなし
- 持続性なし
- 非ブロッキング非同期
- プライバシー・バイ・デザイン

*EternalBlue*は、*SMBv1*が実際に有効になっている場合にのみ悪用可能と判断されます。*Log4Shell*は、*JNDI*パスが有効な場合にのみ悪用可能と判断されます。

ゼロデイ修復
(Zero-day Remediation)

Qualys®

Qualys TruRisk Eliminate は、ゼロデイ攻撃対策に不可欠な修復ソリューションです。

ITパッチ適用におけるスピードギャップを埋めるためのサイバーセキュリティ対策ソリューションがあることを、経営陣に確信させましょう。

自律型修復への信頼構築方法

運用上の回復力への信頼

パッチが上手く適用されるかどうか、どうすれば分かりますか？	パッチ信頼性スコア
パッチが利用できない場合、またはパッチが信頼できない場合は、どのように対処すればよいですか？	パッチレスの修復
重要度の低いマシンから重要度の高いマシンへと段階的にデプロイすることは可能ですか？	導入の波
異常な動作が発生した場合、修復措置を元に戻すことはできますか？	ロールバック機能

TruRisk Eliminate: シックスシグマ精度で修復する

AIベースのレコメンデーションエンジン

自社製ソフトウェアおよびサードパーティ製ソフトウェアの脆弱性と対策をマッピングする

パッチ

- Windows、macOS、Linux
- サードパーティ製アプリ
- ゼロタッチパッチ自動化
- **AIベースのパッチ信頼性スコアによる各パッチの信頼性評価**

アンインストール

- 最終使用状況と依存関係に基づいてリスクを高める**不要な**ブロートウェア*をアンインストールする

*ブロートウェア: 予めインストールされている試用版や不要なソフトウェア

緩和

- パッチが利用できない場合や危険な場合は、エクスポージャーを減らす

カスタム

- 複雑なケースに対応する既成スクリプト
- 自社開発アプリ向けに独自のスクリプト作成が可能

隔離

- 最終手段としての封じ込め
- 高リスク機器を封じ込め、遠隔でパッチを適用する

TruRisk Eliminate: 最高水準の実績

世界中で実証され、信頼されている

1.5億以上
過去12ヶ月間に展開されたパッチ数

#1
GigaOm ランキング

機能する自動化

4000万以上
自動パッチ適用済み数

0.1%未満
ロールバック率

AIを活用したパッチ信頼性スコア

ウェーブ
1 → 4 インテリジェント展開

98.2%
初回パス成功

パッチ適用不要の修復に関する顧客事例

92K
Zoomの9万2千インスタンスが**アンインストール**され、管理者管理環境へ安全に移行されました

40K
16日間で4万件のサポート終了脆弱性が**アンインストール**されました

27K
わずか**3日間**で2万7千件のWinVerifyTrustの脆弱性を**修正**

10K
1万件のBirthday Attackの脆弱性を**6日間**で**修正**

TruRisk Eliminateによる顧客への影響

80%

修復にかかる
平均時間の短縮

1日未満

ゼロデイ脆弱性の
修復にかかる平均時間

0.1%未満

自律パッチ適用時の
ロールバック率

アプリとAPIの脆弱性を修正 (自社開発)

Claude Securityを含む、DAST/SAST/SCAから脆弱性を取り込む

TotalCloudと
TotalAppSecを使用して
脆弱性を検出する

01

脅威、資産、および
ビジネスコンテキストに
基づいてETMの使用を
優先する

02

TruRisk EliminateとTotalCloudの
QFlowを使用して
修復を行う

03

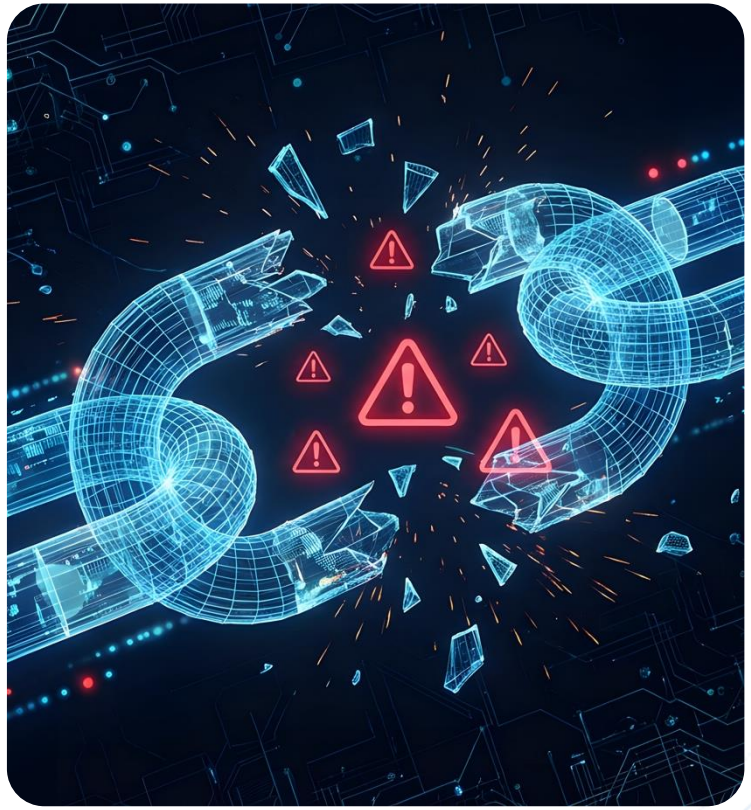
AIスピードの検出
(AI-Speed Detection)

Qualys®

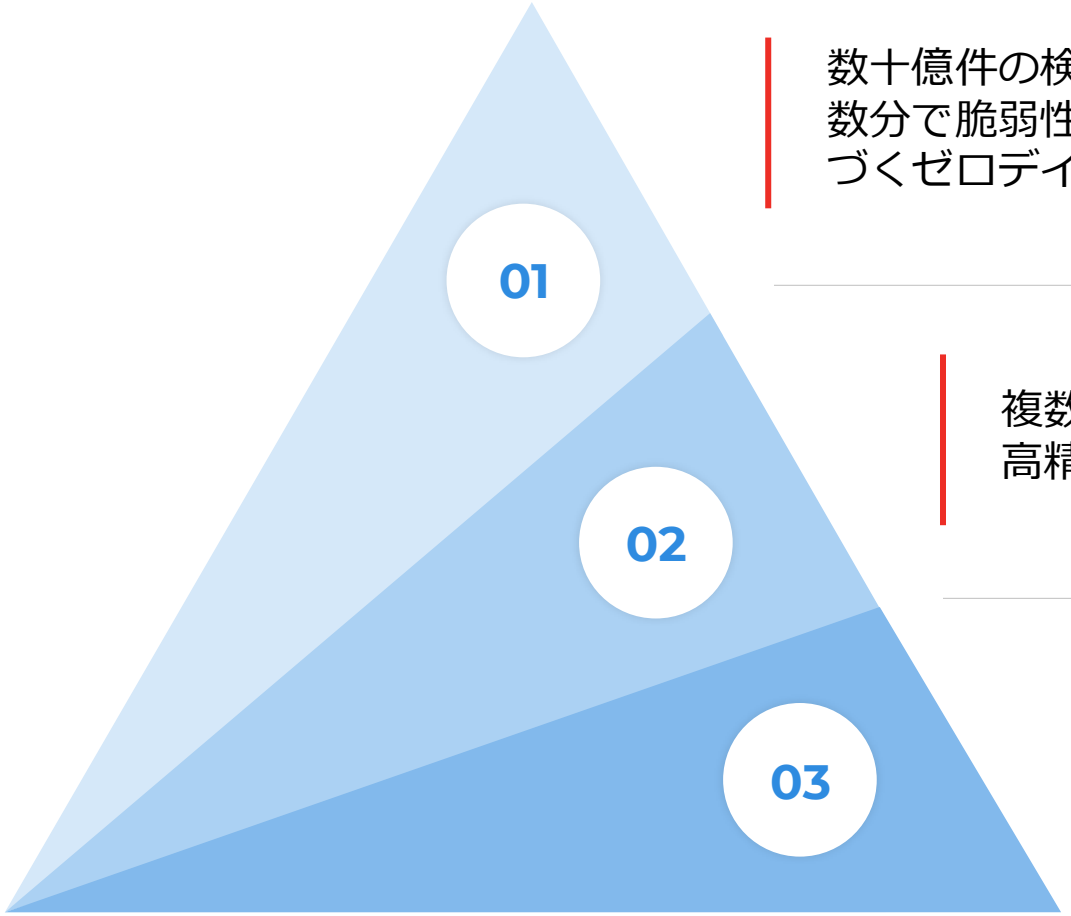
業界トップクラスの脆弱性対応時間

- **重大な脆弱性／ゼロデイ脆弱性に対する**当社の**平均対応時間**は**12時間**です。
- **優先度の高いベンダー**の場合は**6時間**です。
- 10年以上にわたり、**シックスシグマ**レベルの検出精度を維持しています。
- 誤検出を回避します。
- CISA KEVの**99%** をカバーしており、業界トップクラスの実績を誇ります。

競合するスキャナーはシグネチャの追加に数日から数週間かかり、いくつかのCISA KEVをカバーしていない。



検出速度と検出範囲への新たな投資



数十億件の検出データを含むグラフデータベースに基づき、数分で脆弱性を検出：エンドポイント上の悪用指標に基づくゼロデイ脆弱性。

複数のAIモデルを導入し、ノイズを除去することで高精度な検出を実現する。

TruConfirm（あらゆる資産、あらゆるリスク）軽減策の迅速な適用、Agentic AI

包括的かつ柔軟なプラットフォームAI戦略

最適なユースケースに最適なモデルを選択。推論能力とコスト効率の両方を最大限に高めます。

プラットフォームにおけるマルチモデル統合の現状

エージェント型AIおよびサイバーリスクエージェントフレームワークで活用

- オープンソースモデル *(Llama, Mistral)*
- カスタマイズされたSLM *(Phi-4 Mini from Microsoft)*
- Anthropic社のLLM *(Claude Haiku / Sonnet / Opus)*

脅威研究・防御モデル

研究および防御能力に関する既存のパートナーシップ

- Anthropic社のサイバー検証プログラム（CVP）。 *Opus 4.7*
- OpenAI社のサイバー向け信頼アクセス（TAC）。 *GPT-5.5-Cyber*
- ユースケース:
  - 脆弱性調査
  - ゼロデイ攻撃の発見
  - エクスプロイト開発
  - マルウェアのリバースエンジニアリング
  - レッドチーム演習

SASTユースケース向けモデルとの連携

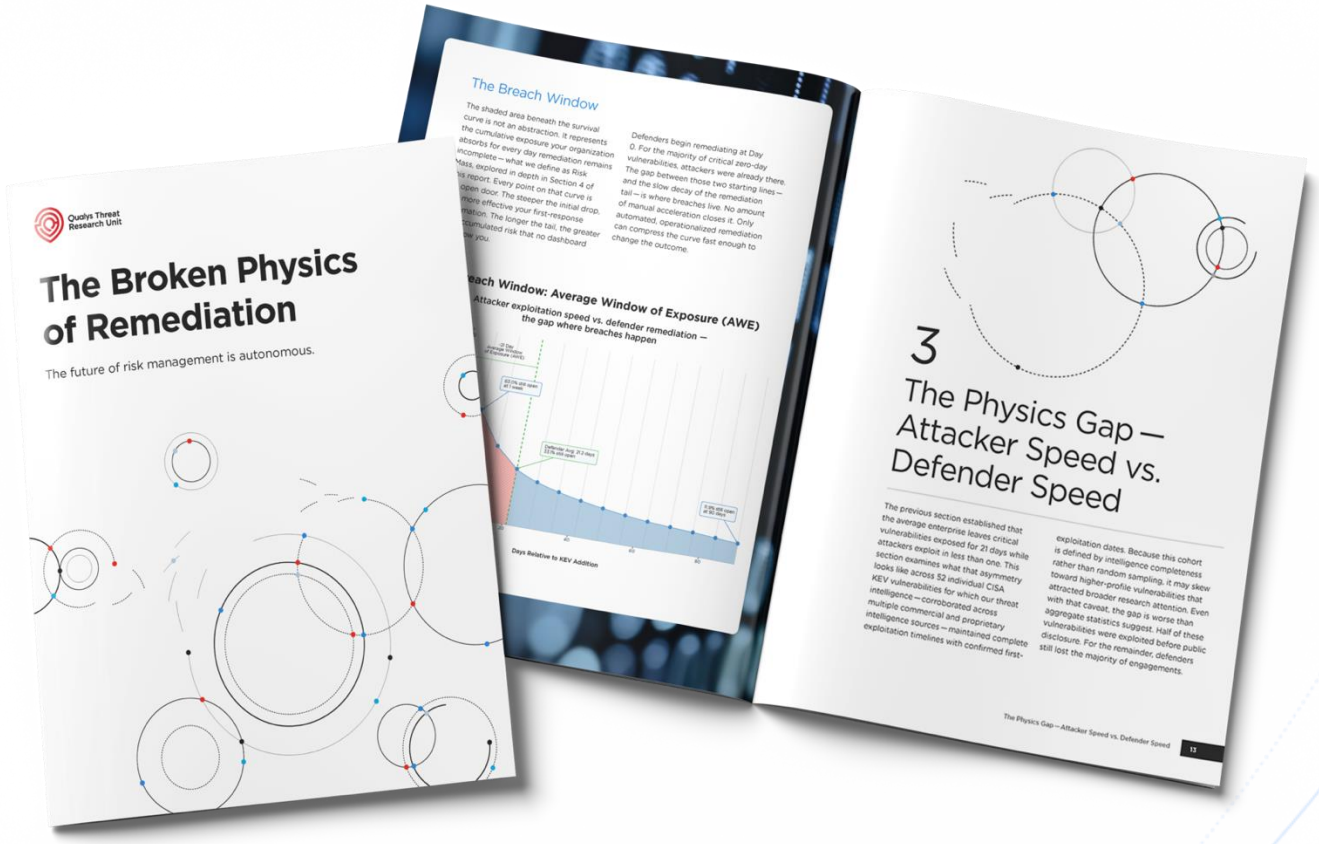
ファーストパーティアプリの脆弱性検出のためのClaude Securityとの連携

- ソースコード内の検出結果をQualys ETMにインポートする
- Qualysでランタイムコンテキストを適用して優先順位付けを行う
- 優先順位付けされた脆弱性にパッチを適用する

ANTHROP\C　Mistral AI　OpenAI　Microsoft　Meta

10億件のCISA KEVデータに基づく、この種の研究としては最大規模の調査。4年間にわたる1万の組織における修復記録を分析。

レポートをダウンロードする



Qualys Research Unit - 修復における理論の限界 (日本語翻訳)
https://cdn2.qualys.com/docs/mktg/jp/qualys-tru-the-broken-physics-of-remediation-japanease.pdf

ソリューション紹介やデモのご依頼は
sales-jp@qualys.comまでお問い合せください。

Qualys®