TotalAppSec

ポスト・ミュトス時代における アプリケーション層のセキュリティ確保

最先端のモデルはアプリケーション脅威を生み出したのではなく、それを産業化させたのです。AI 時代の攻撃者は、ソースコードなしで、Web アプリケーションや API を機械速度で悪用し、システム全体で稼働しているシステムをテストします。TotalAppSec は、AI による高速検出、ハイパープライオリティ化、ゼロデイ修復によって、リスクオペレーションセンターをアプリケーション層に拡張します。

50%
スキャン時間の削減

95%
ノイズ除去

80%
MTTR 短縮

AI スピードの検出

機械レベルの速度で、
より広範囲な検出を実現

- 既知のアプリ、シャドウアプリ、不正アプリ、忘れ去られたアプリおよび API の **継続的な検出**
- **自動シグネチャ生成**: 新規 CVE およびゼロデイ脆弱性
- **AI を活用した DAST** による、実行中のアプリケーションごとの AI スキャン最適化による、確認済みアプリケーションリスクの検出
- **ディープラーニングによるマルウェア検出**（精度約 99%）
- **TTR と検出リリース速度が 2 倍向上**
- **カスタムシグネチャ**: LLM、AI エージェント、MCP サーバー

超優先順位付け

実行時に確認された検出結果を、ビジネスコンテキストに基づいてランク付け

- **TruRisk™スコア**は、CVSS だけでなく 25 種類以上の脅威インテリジェンスフィードに基づいて算出されます。
- **DAST による悪用可能性の検証**は、本番環境で確認します。
- **BOLA**、認証バイパス、ロジックチェーンは、本番環境で確認します。
- **攻撃経路分析**: 個別の CVE ではなく、攻撃チェーンを分析します。
- **Claude/Mythos による検出結果**は、Qualys ETM に取り込み可能。
- **脆弱性の相関分析と**重複排除は、Qualys ETM に反映されます。**

ゼロデイ修復

脆弱性の悪用可能性を検知し、
緩和と修復を実施

- GitHub Actions、Azure DevOps、Jenkins との **CI/CD 連携**
- **Jira** および ServiceNow のチケット発行を**自動化**する ITSM 連携
- シフトレフトとシフトライトを実現する **QFlow™ノーコード自動化**
- **PCI-DSS、GDPR、HIPAA** への継続的なコンプライアンス
- アプリケーションの脆弱性のための **TruRisk Eliminate** 連携**
- アプリケーションの脆弱性のための**緩和可能な QID 拡張と QQL** フィルタ**

包括的な Web アプリケーションおよび API 環境の検出

オンプレミス、マルチクラウド、API ゲートウェイ、マイクロサービスなど、あらゆる環境における既知、未知、シャドウ、不正、そして忘れ去られた Web アプリケーションと API を継続的に検出します。

ランタイム DAST はコード理論を凌駕する

外部からデプロイ済みアプリケーションをテストします。攻撃者が見つけるであろう、静的解析では検出できないランタイム設定ミス、認証失敗、論理的欠陥などを検出します。

TruRisk™による優先順位付け

25 種類以上の脅威インテリジェンスフィードを活用し、実行時に確認された検出結果を、収益への影響、コンプライアンス範囲、資産の重要度に基づいてランク付けします。

AI 攻撃対象領域のカバレッジ

アプリケーションに組み込まれた LLM、AI エージェント、MCP サーバーを検出します。これらは Mythos が完全に無視する、拡大し続ける攻撃対象領域です。

リスクオペレーションセンターを アプリケーション層に拡張する

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。

 v260528

今すぐ試す

** ロードマップの機能は、計画されている製品の方向性を反映したものであり、優先順位に基づいて変更される場合があります。