Operationalize Autonomous Remediation for the Post-Mythos Vulnerability Surge

The rules of vulnerability management have broken.

The past approaches to vulnerability management are now obsolete.

Anthropic's Claude Mythos can autonomously discover vulnerabilities that evaded human experts and develop working exploits by chaining multiple vulnerabilities within hours of disclosure. Other frontier AI models will follow soon. This is expected to create a surge in vulnerabilities and patches from software vendors, including the Mythos preview partners through project Glasswing. Organizations that rely on legacy, manual vulnerability workflows face an existential exposure gap.

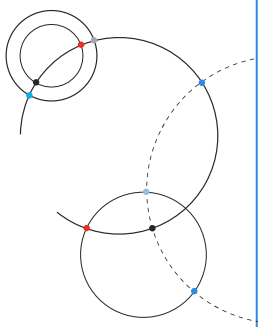
The Broken Physics of Remediation, Pre-Mythos

Even before Mythos, the volume of vulnerabilities had surged 6.5X over last 4 years, while the mean-time-to-exploit collapsed to -7 days in 2025 from patch availability driven by higher volume of zero-days. Current approach to remediation of is already falling behind with median MTTR many times higher than the median time-to-exploit for the CISA KEVs.

6.5x
VULN GROWTH
Over last 4 years. Frontier AI will accelerate this.

18 days
MEDIAN TIME-TO-EXPLOIT
Shrinking to hours with frontier AI models.

67 days
MEDIAN MTTR
Frontier AI models will hunt the long tail.



Source: The Broken Physics of Remediation, Qualys Threat Research Unit (the largest study of its kind based on years of data from 10,000+ organizations)

ONLY
.74%
Weaponized CVEs in 2025

The Vulnerability Noise and Wasted Cycles

While the vulnerability volume has continued to grow rapidly over the years, less than 1% of these get weaponized by attackers. In 2025, only 357 out of the 48,172 vulnerabilities were weaponized and added to CISA KEV, a mere 0.74%. Even out of these, majority are not exploitable due to compensating controls. Organizations are playing whack-a-mole and spending cycles in fixing the wrong vulnerabilities.

The Path Forward

With vulnerability discovery and exploitation going AI speed, remediation must be done at machine speed. The solution for this is via an operational transition to autonomous remediation for the riskiest vulnerabilities. The Risk Operations Center (ROC) enables autonomous remediation by providing these capabilities:

The Risk Operations Center (ROC) enables autonomous remediation by providing these capabilities:

AI-speed detection of vulnerabilities in first and third-party applications, as well as misconfigurations and identity risks:

1. AI-speed detection of vulnerabilities in first- and third-party applications, as well as misconfigurations and identity risks
2. Hyper-prioritization to identify the truly exploitable vulnerabilities based on threat, business, and asset context for theoretical risk filtering, and exploitability validation through compensating controls to surface validated risks.
3. Zero-day remediation with native patch and patchless options while maintaining operational resiliency through reliability scores, deployment waves, and rollback options.

Qualys provides a unified, AI-powered platform to power the ROC, providing industry leading solutions for detection, prioritization, and remediation, delivered at machine speed. No more bouncing across multiple tools. Seamless collaboration between security and IT. This is the future of risk management.

AI-Speed Detection

Detect vulnerabilities before attackers can weaponize.

Qualys VMDR

VMDR is industry leading vulnerability detection supported by multiple Pwnie award winning 120+ threat research team.

- **Six Sigma** detection accuracy
- **45-day** advantage: over industry-standard CVSS-based prioritization
- Automated signature pipeline backed by **120+** dedicated threat engineers
- Digital certificate and CIS configuration assessment built-in
- Detect exposures in first party apps

130K+ CVEs covered — #1 in detection coverage industry-wide
99.4% CISA KEV coverage with prioritization 45 days ahead, best in the industry
12 hours median critical/zero-day signature delivery; under 6 hrs for high-priority vendors

Hyper-Prioritization

Cut 99% of the noise. Focus on what matters.

Qualys (ETM) Enterprise TruRisk Management

ETM operationalizes CTEM with Agentic AI to surface the riskiest exposures.

- Unified asset inventory (CASM) & Risk aggregation
- **TruRisk**: aggregates Qualys + third-party findings into a unified, business-aligned risk score
- **TruLens**: threat-based prioritization tracking dark web trends and ransomware activity
- **TruConfirm**: production-safe exploit validation
- **Agentic AI:** Cyber Risk Agents reduce manual analyst burden

95% Noise reduction via threat + business context layering
8M+ TruConfirm exploit validations in last 12 months, zero disruption
45 days On average head start on prioritization before CISA KEV listing

Zero-Day Remediation

Patch, mitigate, and eliminate risks at machine speed.

Qualys TruRisk Eliminate

TruRisk Eliminate is a cybersecurity remediation solution that closes the speed gap in IT patching.

- Native remediation options: Patch, fix, mitigate, uninstall, isolate.
- AI-powered patch reliability score & wave deployment
- Zero-touch patch automation with auto-rollback on anomaly detection
- 100% coverage for ransomware exposures
- Remediate exposures in first-party apps

150M+ Patches deployed in the last 12 months
40M+ Autonomous patches with <0.1% of rollback rate in last 12 months
80% Reduction in average time to remediate

Ready to Operationalize Continuous Risk Reduction?

Learn how Qualys can help you prepare for frontier AI-era disclosure waves.

Request a Demo

 v260505