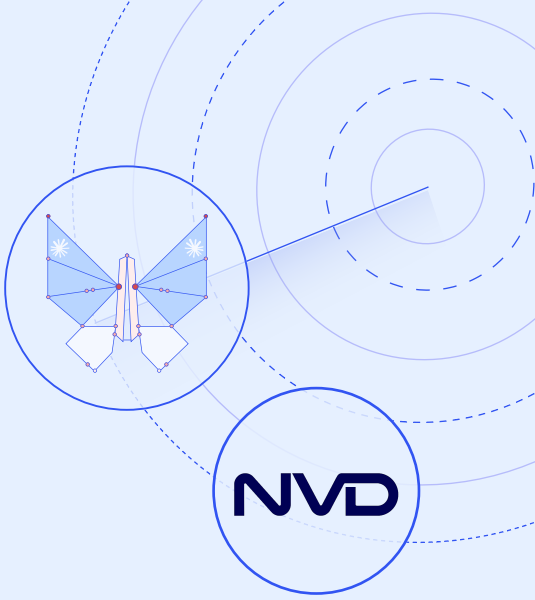
XM Cyber

Claude Mythos & Changes at the NVD:

A Catalyst for Exposure Management



AI-powered discovery and a buckling independent scoring system have accelerated a necessary shift away from CVE-driven risk management

Despite not yet being officially released, Claude Mythos has fundamentally disrupted the Vulnerability Risk Management (VRM) landscape. By finding thousands of deep-seated flaws in major operating systems within hours, Mythos proved that AI can now identify vulnerabilities at a scale and speed that completely outpaces human-led triage.

The fact that many of those discovered were more than a decade old, coupled with the ability for attackers to develop exploits faster than ever has many security teams worried about the impending tsunami on the horizon. Mythos and Project Glasswing have served as an accelerant for an industry that was already grappling with a form of existential uncertainty.

Major Changes with the National Vulnerability Database (NVD)

The NVD is the world's most comprehensive repository of software vulnerabilities. Historically, NVD has played a critical role in the enrichment of reported CVEs, providing necessary context and foundational severity scoring that largely underpins the modern vulnerability management community and process.

In April 2026, NIST officially announced a new "risk-based triage model", through which the NVD now only prioritizes enrichment for three categories:

- CVEs in CISA's Known Exploited Vulnerabilities (KEV) catalog.
- Software used by the U.S. Federal Government.
- "Critical software" as defined by Executive Order 14028.

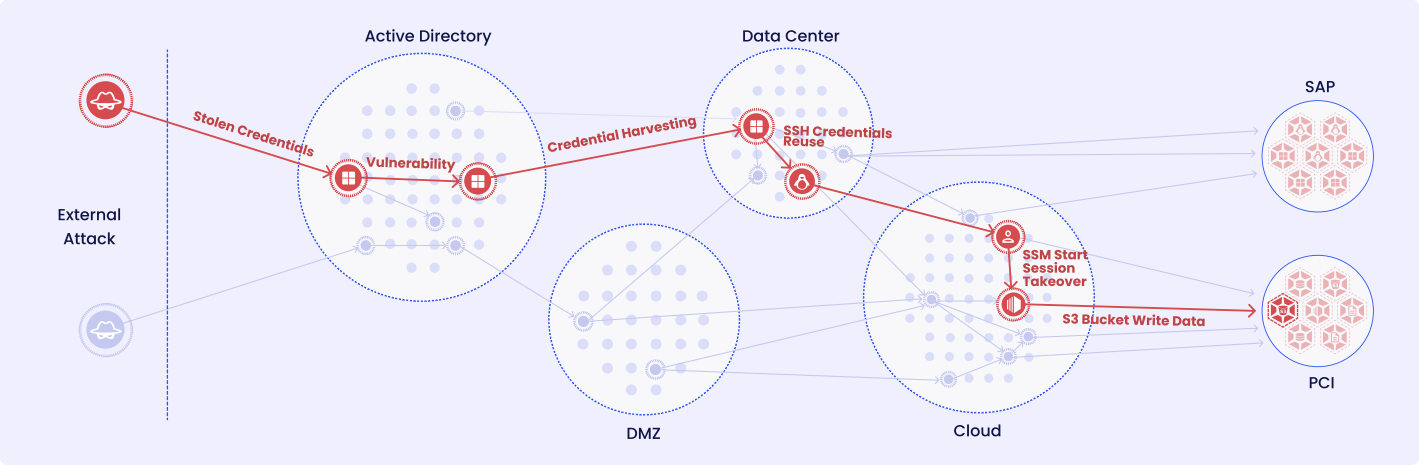
Vulnerabilities outside these categories are now tagged as "Not Scheduled" and may never receive official NIST enrichment. Furthermore, NIST has offloaded its pre-March 2026 backlog into this same "Not Scheduled" category, effectively signaling that the industry can no longer rely on a single government database to score all software risks.

The Time Is Now For Continuous Exposure Management

The discovery explosion powered by Mythos-level tools flooding the ecosystem with new CVEs is a primary reason the NVD recently shifted its enrichment practices. NIST clearly determined it has become mathematically impossible to manually score every bug. Consequently, modern VRM programs are coming to terms with the reality that they must abandon their reliance on CVEs and universal metadata enrichment in favor of focusing on validated exposures that attackers can actually weaponize in their environments.

XM Cyber Continuous Exposure Management Platform

The XM Cyber Continuous Exposure Management Platform discovers, prioritizes, and drives remediation of validated exposures across on-prem and cloud environments. The platform uses a digital twin to dynamically map real attack paths from your external attack surface to internal critical assets. By continuously testing reachability and exploit conditions, taking into account compensating security controls, XM Cyber ensures teams focus on what matters most - validated exposures that put your business at risk.



Exposure Management Across the Entire Hybrid Attack Surface

Map how diverse exposure types (CVEs, misconfigurations, excessive permissions, AI exposures, etc.) interconnect to form validated attack paths

Continuous, Production-Safe Validation to Filter Out the Noise

Build a digital twin of your entire estate, testing reachability and exploitability conditions for every exposure, taking into account existing security controls.

Meaningful Risk and Compliance Reporting

Report on meaningful reduction of risk to business-critical processes and assets, prove effective security operations to leadership, and achieve audit readiness.

Business-Driven Prioritization & Remediation

Drive remediation and risk reduction based on business impact, identifying choke points where a single fix eliminates multiple validated attack paths.

XM Cyber

As the pioneer of exposure management, XM Cyber delivers a continuous and actionable understanding of cyber risk across the entire attack surface, including hybrid, cloud, on-prem, OT, legacy, AI, and container environments. Powered by proprietary Attack Graph Analysis™, the platform continuously validates exploitable exposures against a digital twin of your production environment, applying nearly a decade of offensive security expertise. By revealing the critical choke points where multiple attack scenarios converge, XM Cyber directs security teams to the remediation actions that eliminate the most risk with the least effort. The result is measurable improvement in security posture through prioritized, high-impact remediation, along with clear, business-contextual reporting that enables leaders to communicate risk effectively and demonstrate security ROI.