cycode

Mythos: What It Means and How to Be Ready.

Anthropic Mythos is a frontier model that finds and exploits vulnerabilities at a scale humans cannot match. Public release was withheld due to security concerns, with vulnerability disclosures beginning in July. Operational readiness is essential to weathering the impending AI vulnerability storm.

01 · WHAT HAPPENED

A frontier model crossed the **offensive threshold.**

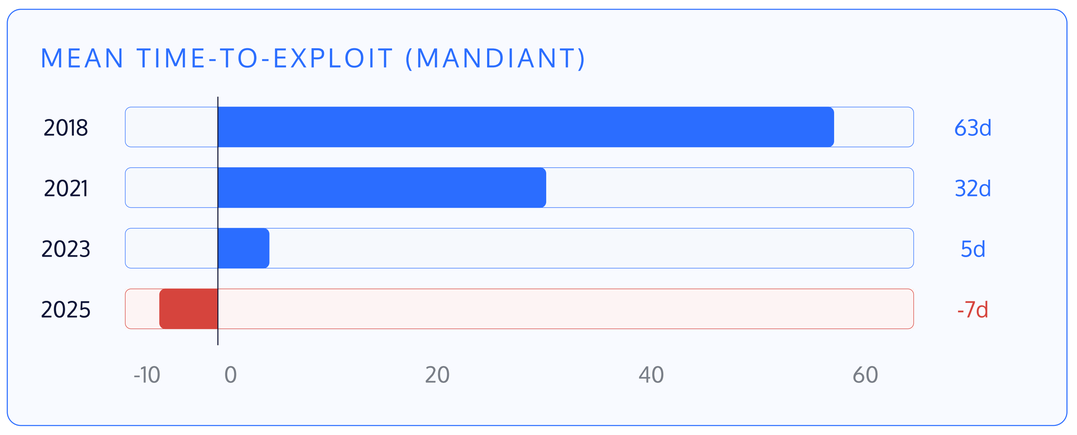
- **Claude Mythos Preview** autonomously discovered thousands of zero-day vulnerabilities across major OSs and browsers — including bugs that survived decades of human review. The oldest was **27 years old.**
- It chained them into working multi-step exploits. **22 Firefox vulnerabilities in two weeks** with Mozilla. **181 working Firefox exploits** vs. ~0 for prior frontier models under identical conditions.
- Public release was withheld. Access is restricted to ~50 organizations under **Project Glasswing** — AWS, Apple, Google, Microsoft, CrowdStrike, Palo Alto, the Linux Foundation, and more — patching critical systems before **initial public disclosures begin in July.**



From announcement to disclosure — the window to prepare is now.

02 · WHY IT MATTERS

More vulnerabilities. **Faster exploits.**



Exploits now precede patches. The window is closing.

-7 days

Time-to-exploit, 2025

Down from 63 days in 2018 (Mandiant). Exploitation now precedes patching.

+263%

CVE volume surge, 2020 → 2025

NIST shifted NVD to triage in April 2026. AI-driven discovery accelerates it further.

03 · WHAT TO DO NOW

Six moves **Anthropic and the CSA** recommend before July.

Close the patch gap

Patch CISA Known Exploited Vulnerabilities (KEV) immediately. Use EPSS to prioritize. Internet-facing systems within 24 hours of exploit availability.

Prepare for 10× volume

Intake, triage, and remediation must scale. Apply the same expectations to your vendors and OSS dependencies.

Find bugs before you ship

Add SAST and AI-assisted review to CI. Automated pentesting in CD. Secure the build pipeline.

Scan your code with AI

Prioritize code that parses untrusted input, enforces auth, or is internet-reachable. Include legacy.

Build VulnOps capability

A permanent Vulnerability Operations function — staffed and automated like DevOps. Continuous discovery and remediation.

Govern Shadow AI

Discover unauthorized AI coding agents, MCP servers, and agentic tools in your dev environments. Manage what you can't see.

04 · THE AGENTIC DEVELOPMENT SECURITY OPERATING MODEL

How Cycode **accelerates readiness.**

AI Risk Detection

Continuous SCA across every repo, container, and deployed service. When a critical CVE or AI discovered zero-day drops, you know within minutes whether you re affected. AI visibility surfaces Shadow AI and and AI code risk detects OWASP LLM Top 10 violations legacy scanners miss.

SCA · AI SAST · ADLC Visibility · AIBOM

Code-to-Runtime Context

The Context Intelligence Graph unifies code, pipelines, dependencies, runtime, and identity. The Exploitability Agent traces from finding to runtime to determine real risk, so triage focuses on what's actually reachable, exposed, and exploitable.

CIG · Reachability · Blast Radius · Ownership

Maestro Orchestration

Specialized agents detect risks, analyze for exploitability, assess business impact and blast radius, generate fixes, and implement preventative controls with minimal human intervention — reducing MTTR on critical vulnerabilities by 99%.

Maestro · AI Teammates · PR-Ready Fixes

Mythos is a signal.
Operational readiness is the answer.

Don't just be Mythos-ready. Be AI-evolved and autonomous. Detect in minutes. Prioritize by real exploitability. Remediate at machine speed.

Shift Left is dead
Welcome to the Shift to AI

Learn more at **cycode.com**