SKYHAWK SECURITY

Mythos-Ready Cloud Defense

www.skyhawk.security

⚠ Mythos will flood your team with noise.
Thousands of new zero-days. More CVEs. More alerts. More dilemmas — at machine speed.

Skyhawk shows you only the alerts that matter.
We cut 100,000+ findings to the <1% that are real, weaponized threats to your crown jewels.

The AI Vulnerability Storm is here. Skyhawk is already your Mythos-ready defense.

<1% of alerts are a real threat

Anthropic's Mythos AI (April 2026) discovered thousands of zero-days across every major OS and browser with a 72% exploit success rate. The CSA/SANS CISO community has issued an urgent briefing: security programs must become **Mythos-ready — now**. Skyhawk's Continuous Autonomous Purple Team already delivers what they prescribe.

THREAT LANDSCAPE	**89%** increase in AI-enabled attacks YoY	**29 min** avg. eCrime breakout time · fastest: 27 sec	**72%** Mythos exploit success rate	**82%** of detections are malware-free attacks	**266%** rise in state-nexus cloud targeting
SKYHAWK RESULTS	**99%** alert noise eliminated	**Seconds** to detect & stop threat actors	**78%** faster alert promotion to action	**<1 hr** to deploy; first insights in 24 hrs	**500K→300** critical findings reduced to actionable

Threat data: CrowdStrike 2026 Global Threat Report · CSA/SANS "AI Vulnerability Storm" (April 2026) Skyhawk results: customer deployments

THE CHALLENGE

Mythos changes everything for defenders

Anthropic's Mythos AI discovered thousands of zero-days — across every major OS and browser — in a single run, with a **72% exploit success rate**. Time-to-exploit has collapsed to **under one day**. The CSA/SANS CISO briefing warns: AI-accelerated attacks are now **machine-speed**, while most security teams still operate at human speed. Traditional detection-and-response, CVSS-based prioritization, and quarterly pen tests cannot keep pace. The window to act is **this week**.

THE SOLUTION

Skyhawk: the Mythos-ready defense platform

Skyhawk's **Continuous Autonomous Purple Team** creates a digital twin of your cloud and runs intelligent simulations powered by Adversarial AI — continuously, at machine speed. It answers: not what *could* go wrong, but what an attacker *would* exploit, in what order, and with what consequence. The result: a **weaponized risk picture** that closes the gap between AI-speed attackers and your team — **before** the breach.

HOW SKYHAWK DELIVERS THE MYTHOS-READY PROGRAM

CSA/SANS Priority Action	Skyhawk Capability	Proven Result
PA 1 · Point Agents at Code & Pipelines LLM-driven security review; all code passes AI review before merge	**Adversarial Exposure Validation** Continuously simulates attacker behavior — finds what will be exploited before attackers do	**99%** alert noise eliminated 100,000+ CVEs condensed to dozens of real, weaponized attack sequences
PA 4 · Defend Your Agents Define blast-radius limits, human override, no new privileged agents	**Digital Twin Simulation** AI replica of your cloud runs in SaaS — zero impact to production; no new attack surface	**<1 hr** to full deployment Agentless, read-only API connection — operational in under one hour, first insights in 24 hrs
PA 9–10 · Build Deception & Automated Response Pre-authorized containment, machine-speed response playbooks	**Confident Automated Response** Skyhawk acts — not just alerts — within the attacker's own timeline, closing the 29-min breakout gap	**Seconds** to detect & stop threat actors Adaptive CDR with pre-validated, automated responses — matching Mythos-speed attacks
PA 6 · Update Risk Models & Reporting Replace pre-AI CVSS assumptions; reflect AI-accelerated timelines	**Weaponized Risk Prioritization** Vulnerabilities ranked by actual exploitability and blast radius — not CVSS score	**500K→300** critical findings to actionable One customer reduced 500,000 critical/high vulns to fewer than 300 real threats — a 1,000× improvement
PA 11 · Stand Up VulnOps Permanent autonomous vulnerability operations, staffed like DevOps	**Autonomous Purple Team** Continuous 24/7 red/blue validation — replaces 4× annual manual pen tests	**78%** faster alert promotion Gen AI CISO engine promotes attack sequences to high-fidelity alerts 78% faster — zero added false positives

KEY DIFFERENTIATORS

01 Adversarial Exposure Validation **80%** analyst productivity gain	**02 Weaponized Risk Prioritization** **Top 0.1%** of findings that truly threaten crown jewels	**03 Autonomous Purple Team** **4×/yr → 24/7** pen test frequency improvement
04 Confident Automated Response **Seconds** mean time to contain	**05 Digital Twin Simulation** **<1 hr** agentless deployment	**06 Agentless & Cloud-Native** **24 hrs** to first validated attack path

Skyhawk Security © 2026