

## ⚠ Mythos will flood your team with noise.

Thousands of new zero-days. More CVEs. More alerts. More dilemmas — at machine speed.

## ⚠ Mythos will flood your team with noise.

Thousands of new zero-days. More CVEs. More alerts. More dilemmas — at machine speed.

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

**<1%** of alerts are a real threat

Anthropic 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.

<b>THREAT LANDSCAPE</b>	<b>89%</b> increase in AI-enabled attacks YoY	<b>29 min</b> avg. eCrime breakout time · fastest: 27 sec	<b>72%</b> Mythos exploit success rate	<b>82%</b> of detections are malware-free attacks	<b>266%</b> rise in state-nexus cloud targeting
<b>SKYHAWK RESULTS</b>	<b>99%</b> alert noise eliminated	<b>Seconds</b> to detect & stop threat actors	<b>78%</b> faster alert promotion to action	<b>&lt;1 hr</b> to deploy; first insights in 24 hrs	<b>500K→300</b> 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 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 just what *could* go wrong with what's found, 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
<b>PA 1 · Point Agents at Code &amp; Pipelines</b> LLM-driven security review; all code passes AI review before merge	<b>Adversarial Exposure Validation</b> Continuously simulates attacker behavior and finds what will be exploited before attackers do	<b>99%</b> Alert noise eliminated 100,000+ CVEs condensed to dozens of real, weaponized attack sequences
<b>PA 4 · Defend Your Agents</b> Define blast-radius limits, human override, no new privileged agents	<b>Digital Twin Simulation</b> AI replica of your cloud runs in SaaS with zero impact to production; no new attack surface	<b>&lt;1 hr</b> To full deployment Agentless, read-only API connection gets you operational in under one hour, first insights in 24 hrs
<b>PA 9–10 · Build Deception &amp; Automated Response</b> Pre-authorized containment, machine-speed response playbooks	<b>Prepare Confident Automated Response</b> Skyhawk can train your SOC for shrinking AI timelines, closing the 29-min breakout gap	<b>Seconds</b> To detect & stop threat actors Adaptive CDR with pre-validated responses for your SOC lowering MTTR to match Mythos-speed attacks
<b>PA 6 · Update Risk Models &amp; Reporting</b> Replace pre-AI CVSS assumptions; reflect AI-accelerated timelines	<b>Weaponized Risk Prioritization</b> Vulnerabilities ranked by actual exploitability and blast radius, not a CVSS score	<b>500K→300</b> Critical findings to actionable One customer reduced 500,000 critical/high vulns to fewer than 300 real threats, a 1,000x improvement
<b>PA 11 · Stand Up VulnOps</b> Permanent autonomous vulnerability operations, staffed like DevOps	<b>Autonomous Purple Team</b> Continuous 24/7 red/blue validation replaces quarterly manual pen tests	<b>78%</b> Faster alert promotion Skyhawk AI acts like a CISO engine promoting attack sequences to high-fidelity alerts 78% faster with zero added false positives

### KEY DIFFERENTIATORS

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