kusari

The Mythos-Ready Playbook

The Cloud Security Alliance, SANS, OWASP Gen AI, and a coalition of CISOs published a 30-page Mythos-ready security program briefing: 13 risks, 11 priority actions, and a call for a permanent Vulnerability Operations (VulnOps) function.

BE READY FOR THE NEXT WAVE

As AI accelerates vulnerability discovery and exploitation, Kusari delivers the mythos-ready response capabilities: robust dependency analysis, automated pipeline security, and machine-speed remediation across your entire software supply chain.

HOW KUSARI DELIVERS THE CSA PRIORITY ACTIONS

PA 1 · CRITICAL · THIS WEEK

Point Agents at Your Code and Pipelines

"All code — human or AI-generated — should pass LLM-driven security review before merge."

Kusari Inspector is an autonomous code security agent (native GitHub App, GitLab, CLI, IDE, & MCP). Catch transitive vulnerabilities, secrets, license issues, typosquatting, EOL components, and AI-generated code risk. Guardrails, not roadblocks.

PA 5 · CRITICAL · 45 DAYS

Prepare for Continuous Patching

"With Glasswing making Mythos available to significant vendors, prepare triage and deployment capacity for a flood of patches."

Kusari Score and Effort-to-Fix turn the incoming vulnerability storm into a ranked queue based on exploitability, reachability, dependency concentration, and remediation effort. Blast Radius Analysis answers "where is this running?" instantly across every repo.

PA 6 · CRITICAL · 45 DAYS

Update Risk Models and Reporting

"Pre-AI assumptions about patch windows, exploit scarcity, and incident frequency may no longer hold."

Kusari Executive Dashboards report MTTR, vulnerability counts, dependency health, EOL exposure, and compliance posture continuously. Track every change and your supply chain risk in real time.

PA 7 · HIGH · 90 DAYS

Inventory and Reduce Attack Surface

"Generate real SBOMs. You cannot patch, segment, or defend what you don't know exists."

Kusari SBOM Manager generates and continuously monitors SBOMs at build time. The Kusari Trust Fabric maps your software environment and normalizes SBOMs from third-party tooling into a single unified view — your source of truth for VulnOps & AppSec.

PA 9 / PA 10 · HIGH · 6–12 MO

Build Automated Response Capability

"Pre-authorized containment and response playbooks that execute at machine speed."

Kusari AutoFix traces to root cause, generates environment-specific fixes, and routes exceptions through policy. Kusari Agent answers "Are we affected? Where? What's the fix path?" in seconds. Native ticketing integrations accelerate response times.

PA 11 · CRITICAL · 12 MO

Stand Up VulnOps

"A permanent function, staffed and automated like DevOps, for autonomous vulnerability research and remediation."

The Kusari Trust Fabric is the VulnOps control plane: a living knowledge graph across your entire software estate — your own code and third-party — with Inspector at the pipeline, Agent for query, AutoFix for remediation. Engineered together from day one.

Attackers move at AI speed. Your software intelligence should too.

Know your risk instantly. Fix what matters automatically. Prove trust continuously.

kusari.dev