CHECKLIST · 21-POINT READINESS AUDIT

Mythos-Ready Application Security Checklist

Claude Mythos showed that AI can read source code and find exploitable weaknesses faster than any human team. Use this checklist to confirm your application security program is ready for an AI-accelerated threat environment, before your next penetration test.

- Most teams start with a penetration test, then add secure code review as their program matures.
- **21 controls** across 3 phases: before, during, and after your engagement.
- Check off items, tally your total, and match it to the **scoring key** below.

1 Before the Engagement

7 controls

- [ ] 01 Asset inventory complete
  All cloud, SaaS, infra & AI agent surfaces documented. SBOMs generated for all builds.
- [ ] 02 Dependency audit done
  Third-party libraries reviewed. Known high-severity CVEs in open-source dependencies flagged.
- [ ] 03 Scope includes AI surfaces
  MCP servers, LLM integrations, agentic workflows added to scope, not just traditional endpoints.
- [ ] 04 Patch velocity baselined
  Current mean time to patch critical vulnerabilities documented. Target: under 24 hrs for critical, internet-facing issues.
- [ ] 05 IR playbooks reviewed
  Incident response plans updated for multi-vector, AI-assisted attack scenarios, not just single-CVE events.
- [ ] 06 Access hygiene verified
  Phishing-resistant MFA enforced, least-privilege access confirmed, secrets rotation current, extended to repos and git history: branch protection, mandatory PR review, and no leaked credentials in history.
- [ ] 07 AI coding assistant policy set
  Clear policy for what proprietary source code can be shared with AI coding tools. Vendor data-retention terms reviewed.

2 During the Engagement

6 controls

- [ ] 08 Exploit chain simulation
  Tester maps multi-step attack paths across identity, app, infra, not isolated vulnerabilities.
- [ ] 09 AI-assisted discovery used
  Engagement uses AI tooling to surface vuln classes automated scanners and humans miss.
- [ ] 10 Detection speed tested
  Mean time to detect (MTTD) and contain (MTTC) actively measured during simulated attack sequences.
- [ ] 11 Glasswing patches checked
  Project Glasswing vendor patches reviewed. Confirm your stack has absorbed the latest disclosure wave.
- [ ] 12 Egress filtering probed
  Outbound traffic controls tested. Data exfiltration paths mapped and validated.
- [ ] 13 Sandbox escape tested
  If AI agents or LLM pipelines are in scope, tested for unsanctioned actions and privilege escalation.

3 After the Engagement

8 controls

- [ ] 14 Vulnerabilities ranked by attack path
  Vulnerabilities prioritised by exploitability and chain potential, not just CVSS score in isolation.
- [ ] 15 Remediation SLAs set
  Critical, internet-facing: patch within 24 hrs. High: 7 days. No quarterly maintenance-window exceptions.
- [ ] 16 MTTD / MTTC benchmarked
  Detection and containment times documented. Used to update board-level risk metrics going forward.
- [ ] 17 Open-source deps patched
  All flagged third-party library vulnerabilities triaged and patched. SBOMs updated to reflect current state.
- [ ] 18 Secure code review completed
  The natural next step after your first pentest: a dedicated secure code review, not just automated scanning, for hardcoded secrets, injection flaws, and business-logic gaps.
- [ ] 19 Source code vulnerabilities retested
  Secure code review vulnerabilities remediated and revalidated. Confirms fixes hold before the next engagement cycle.
- [ ] 20 IR playbooks updated
  Playbooks revised based on attack paths found. Multi-simultaneous zero-day scenarios explicitly covered.
- [ ] 21 Next engagement scheduled
  Continuous cadence confirmed. Point-in-time testing is insufficient in an AI-accelerated threat environment.

SCORING KEY

18–21	★★★★★	You're well prepared for a Mythos-ready penetration test.
13–17	★★★★☆	Strong foundation with a few areas to improve.
7–12	★★★☆☆	Several important security capabilities should be strengthened before testing.
0–6	★★☆☆☆	Start with foundational application security improvements before scheduling a comprehensive engagement.

Not sure where you stand? Book a consultation. We'll help you scope the right mix of penetration testing and secure code review for where your program is today.

Book a Consultation →

Sources: Anthropic, Project Glasswing (Apr 2026) · Mandiant M-Trends 2026 · CSA/SANS/OWASP, "The AI Vulnerability Storm: Building a Mythos-Ready Security Program" (Apr 2026) · UK AI Security Institute, Mythos Preview cyber evaluation (Apr 2026)