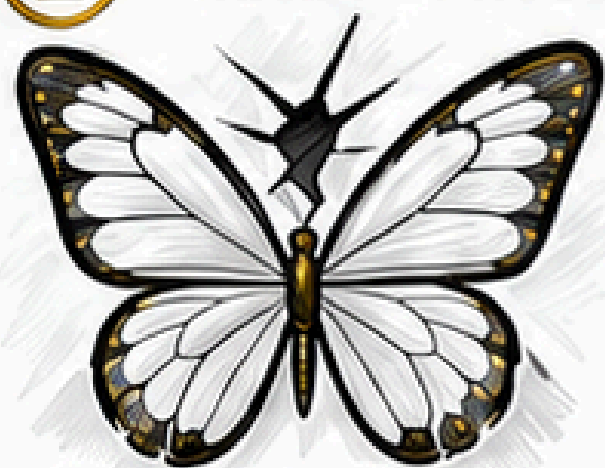


1 WHAT IS MYTHOS?

Anthropic's Mythos is an unreleased frontier AI model built for advanced coding and software reasoning. During testing, it proved unusually strong at finding, chaining, and exploiting vulnerabilities—sometimes beyond hull but the most skilled human researchers.

- Finds hidden flaws in complex codebases
- Can chain multiple small bugs into serious exploits
- Unearthed old, overlooked vulnerabilities
- Too powerful for broad public release

2 WHAT IS PROJECT GLASSWING?



Project Glasswing is a defensive, invite-only effort created to use Mythos for good: helping trusted organizations uncover and patch hidden vulnerabilities before attackers do.

- Defensive consortium
- Focused on critical software and infrastructure
- Built to reveal what has been hiding in plain sight
- A race to secure systems before offensive AI proliferates

5 THE REAL RISK ZONES



Risk now lives across ecosystems—not just inside your firewall.

THE DIRENZIC BRIEFING

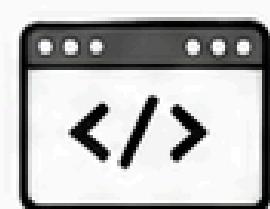
Internet Safety in the Age of AI

What Mythos & Project Glasswing Signal for Leaders Responsible for Cyber Readiness, Public Trust, and Critical Systems

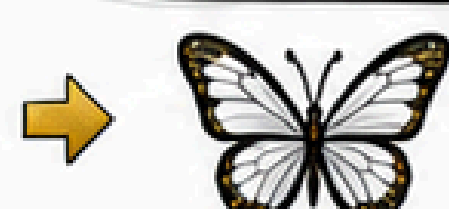
Plain-English executive briefing • No vendor pitch • No fear marketing • Live access only

WHY THIS MATTERS NOW

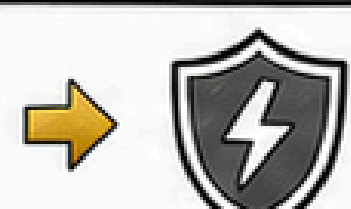
AI changed the speed of discovery, exploitation, and response. Leadership readiness can no longer lag behind technical reality.



MYTHOS



GLASSWING



INDUSTRY IMPACT



DIRENZIC BRIEFING

6 WHY DIRENZIC IS SPEARHEADING THIS EFFORT



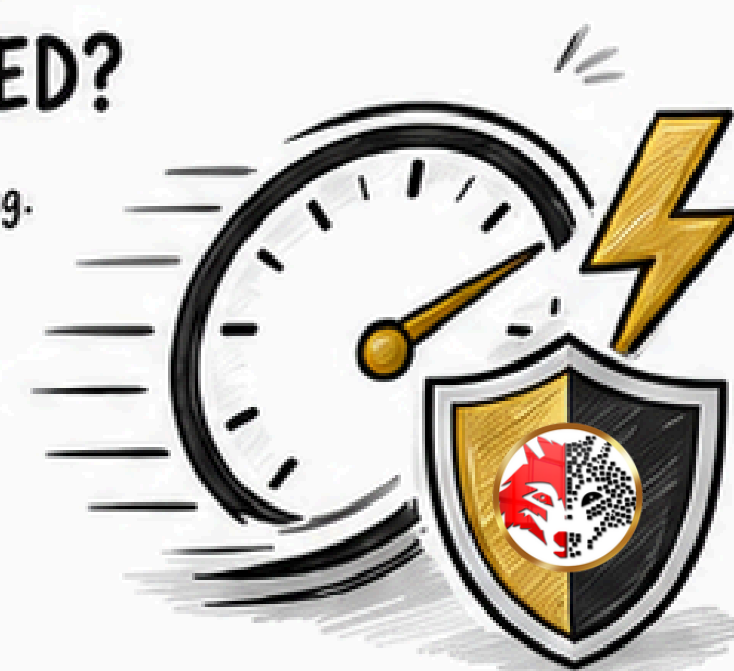
Direnzic is translating complex AI-era cyber signal into plain English leadership briefing for executives, owners, operators, and advisors. The goal is not hype—it is readiness.

- Executive-focused, not overly technical
- Built for leaders responsible for critical systems
- Connects cyber readiness to governance, trust, and continuity
- Helps organizations understand what to assess, document, and defend next

3 WHAT CHANGED?

The old cyber timeline is shrinking. AI can accelerate vulnerability discovery and attack preparation, which means annual assessments and slow governance cycles may no longer be enough.

- Discovery is faster
- Exposure spreads faster
- Patch windows feel smaller
- Governance must move faster too

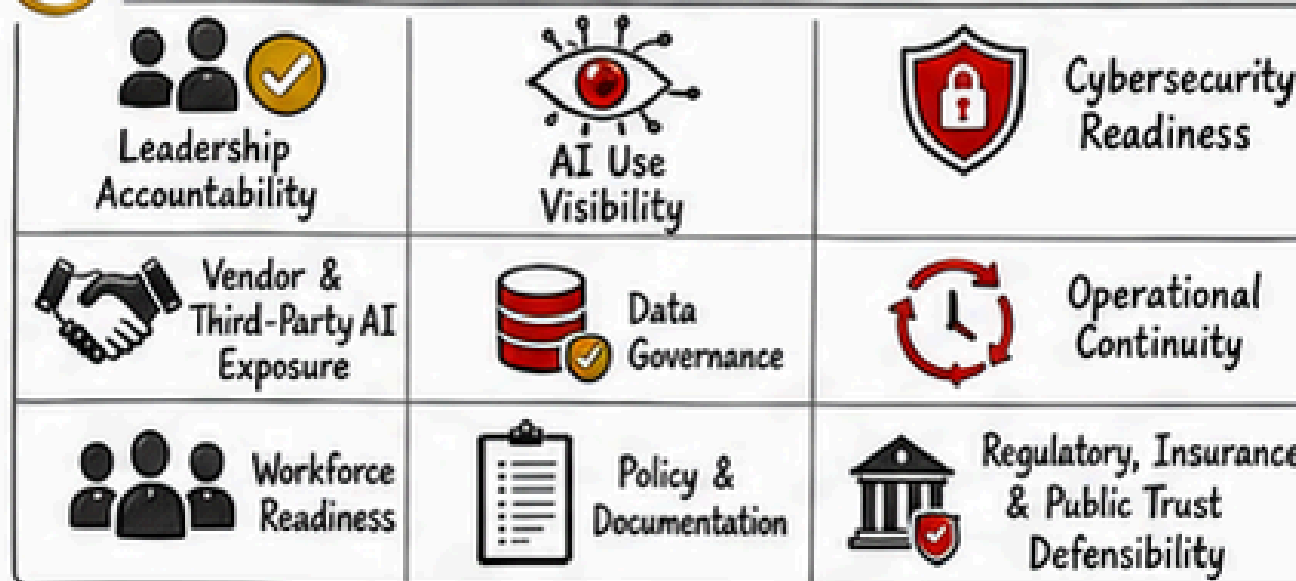


4 WHO COULD BE IMPACTED?



If your systems support people, operations, or public trust, this conversation belongs to you.

7 THE DIRENZIC READINESS LENS



Readiness has a structure. It can be assessed, documented, and defended.

WHAT LEADERS WILL LEAVE WITH

- ✓ A plain-English understanding of the Glasswing signal
- ✓ Better questions about AI governance ownership
- ✓ A clearer view of AI-era cyber exposure
- ✓ Practical next steps for assessment and defensibility
- ✓ A structured path forward instead of guesswork

9 JOIN THE BRIEFING

THE DIRENZIC BRIEFING

Internet Safety in the Age of AI

- 📅 WEDNESDAY, JUNE 24, 2026
- 🕒 11:30 AM ET / 12:30 PM ET
- 🕒 90-MINUTE LIVE EXECUTIVE BRIEFING
- 🎟️ COMPLIMENTARY • REGISTRATION REQUIRED

If you will be expected to answer what your organization can and cannot defend a year from now, this is where the work begins.

