The CISO Mythos Readiness Checklist

The patches are coming. Before they land, your board, legal team, and regulators will have questions.

1 Exposure & Asset Visibility

"What is our exposure, and do we have an accurate asset inventory?"

- [ ] Refresh your asset inventory so it reflects your current production environment.
- [ ] Confirm continuous scanning is live across production environments.
- [ ] Re-rank vulnerabilities using risk-based prioritisation, not raw CVE count.
- [ ] Prepare a one-page exposure brief ready for leadership on demand.

2 Patch Velocity & Production Safety

"Can we patch fast enough, at scale, without breaking production?"

- [ ] Audit current patch cycle cadence against the disclosure-to-weaponisation window.
- [ ] Rank assets by criticality before the wave hits, not during it.
- [ ] Codify a change management protocol with named owners and rollback paths.
- [ ] Run a tabletop on a high-velocity patch deployment scenario to pressure test decision paths and rollback readiness.

3 Supply Chain & Open-Source Exposure

"What's hiding in our open-source and third-party software?"

- [ ] Generate or refresh your Software Bill of Materials (SBOM).
- [ ] Inventory third-party integrations inherited through acquisitions.
- [ ] Stand up continuous scanning of open-source library dependencies.
- [ ] Identify supplier patch SLAs and contact points before disclosure lands.

4 Engineering Capacity

"Do we have the engineering capacity to remediate our own backlog?"

- [ ] Estimate remediation hours against your team's current commitments.
- [ ] Triage the backlog to focus internal teams on highest-risk items only.
- [ ] Line up external engineering resources before you need them.
- [ ] Build secure-by-default practices into ongoing development now.

5 Detection & Containment

"If a patch lags, can we detect and contain the exploit?"

- [ ] Confirm 24/7 SOC monitoring is live across critical environments.
- [ ] Define a target mean time to triage and isolate (minutes, not hours).
- [ ] Run proactive threat hunts focused on Mythos exposure surfaces.
- [ ] Validate your assume-breach playbook through a recent exercise or simulation.

Executive Readiness Check

Before you brief leadership:

- [ ] Identify which of these answers you can defend today, and which ones require executive alignment or air cover.

If you're deciding how to cover these gaps:

Some organisations build these capabilities in-house. Others partner to accelerate coverage or supplement constrained teams. **Insight Managed Exposure Defence** is an integrated approach that spans all five areas above – built and operated internally first, then extended to clients facing the same questions.

Learn more on se.insight.com