Axonius

AI-ready | Mythos-ready

Exposure Management

A Practical Guide to Preventative Security Operations

Security programs built for human-speed disclosure will not survive machine-speed discovery. AI is accelerating vulnerability discovery at an unprecedented rate, while foundational enrichments like the NIST NVD are pulling back.

To absorb the coming volume of vulnerabilities, your exposure management program must evolve from periodic patching to a continuous, real-time operation. Axonius provides the comprehensive asset intelligence necessary to make your security program AI-ready.

Mythos
AI-accelerated vulnerability discovery. Thousands of zero-days surfaced in a contained preview.

NIST NVD
Enrichment pullback in progress. Not every CVE will receive a CVSS score going forward.

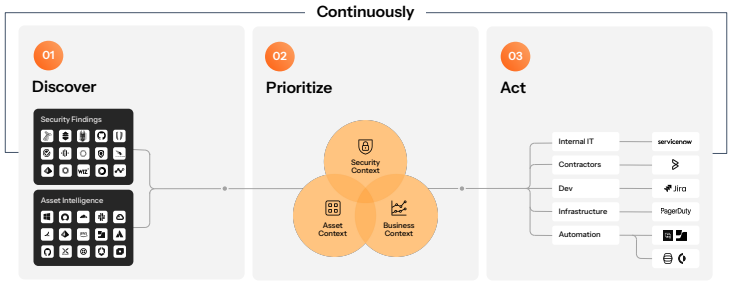
EPSS
A 30-day historical lookback — while exploitation windows compress to hours.

5 Foundational Capabilities of AI-Ready Exposure Management

With Axonius, your security team can implement a proactive, scalable approach to managing risk across your entire IT environment.

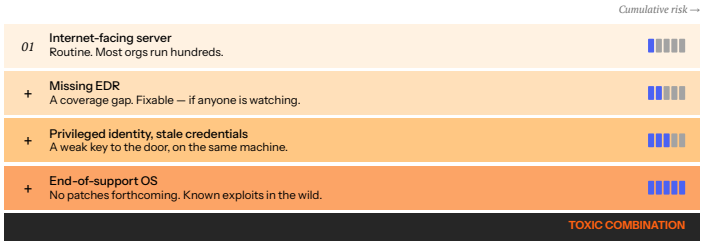
01 **Treat Exposure Management like Incident Response:** Bring the discipline of incident response to exposure management.

- **Unify Findings:** Aggregate and correlate security findings from over 150 sources (scanners, CNAPP, identity, app sec) to the specific assets they affect.
- **Define SLAs:** Establish severity tiers and response SLAs adapted for shorter exploitation windows.
- **Track in Real-Time:** Surface open findings by severity, SLA status, and aging in live operational dashboards.



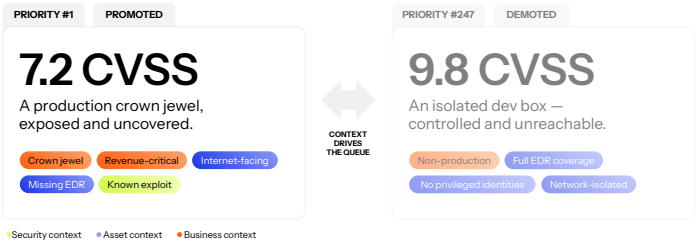
02 **Scope Exposures Beyond CVEs:** Not every exposure is a vulnerability, and not every vulnerability is an exposure.

- **Identify Toxic Combinations:** Connect the dots between missing EDR, open internet access, privileged identities, and unpatched software to uncover compound risks.
- **Holistic Prioritization:** Evaluate coverage gaps, misconfigurations, and identity risks in the same prioritized queue as scanner-reported CVEs.



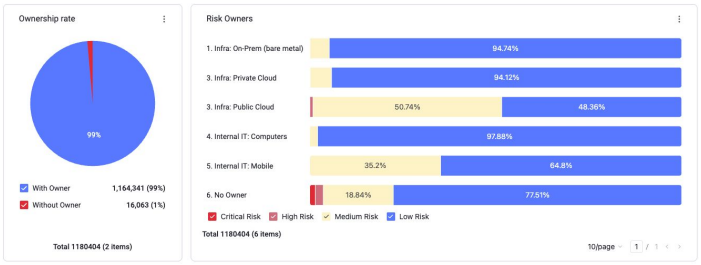
03 **Weigh Your Context to the Business:** CVSS, EPSS, and KEV are useful inputs, but they lack awareness of your specific environment.

- **Layer the Context:** Combine external security signals with internal asset and business context (e.g., ServiceNow crown jewel designations, AWS environment tags).
- **Custom Scoring:** Apply custom weights and conditional logic so a critical vulnerability on a production payment server correctly outranks the same flaw on an isolated development box.



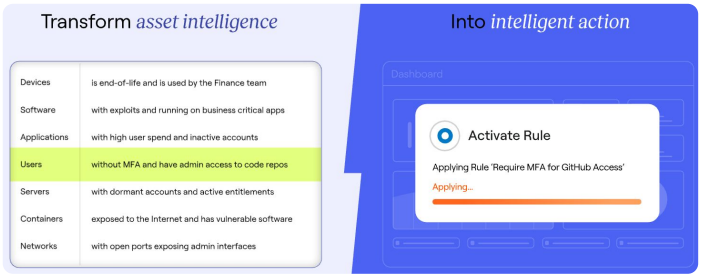
04 **4. Automate Ownership Assignment:** You cannot enforce an SLA if you cannot find the owner. Drive your Mean Time to Ownership (MTTO) to near-zero.

- **Automated Routing:** Automatically attach owners to findings the moment they surface based on business unit tags, cloud accounts, or adapter sources.
- **Granular Accountability:** Separate and track asset owners, business owners, and remediation owners independently to eliminate bottlenecks.



05 **Contain First, Remediate Next, Validate Always:** When finding volumes spike, you must contain the blast radius before you patch.

- **Scope the Impact:** Use asset relationships and Network Routes to map which systems and identities an exposure can reach.
- **Take Action:** Pre-configure automated mitigation paths for low-risk issues and generate tracked tickets with full context for complex remediations.
- **Verify the Fix:** Move beyond simple ticket closure. Axonius continuously re-evaluates assets to ensure verified remediation and flags any exposures that drift back within 30 days.



Stop Chasing Data. Start Taking Intelligent Action.

Equip your team with the automated asset intelligence required to see what's exposed, turn alert noise into prioritized action, and validate your security posture continuously.

axonius.com/demo

Axonius