ManageEngine Log360

Translating AD weak spots into business-ready metrics

Understanding Active Directory (AD) vulnerabilities goes beyond IT ; it's a strategic risk that demands board-level attention. CISOs need to communicate risk posture, security performance, and compliance risk exposure through clear, measurable indicators. That's where SIEM and IAM bridge the gap between real-time threat detection and executive-level clarity.

Below are key boardroom metrics mapped to the five AD vulnerabilities covered on this page:

Excessive privileges and over-provisioning

1

What the board needs to know:

- How many privileged users exist and whether they actually need those rights.
- Trends in privilege misuse or escalations.

Metrics to report:

- *Number of users with Domain Admin rights*
- *Count of unauthorized privilege elevation attempts*
- *Average time to detect privilege misuse (MTTD)*

Tools in Action:

- **SIEM:** Tracks suspicious privilege escalations and correlates them with abnormal activity (e.g., rare hours, rare devices).
- **IAM:** Reports on over-privileged users, inactive admins, and implements just-in-time access workflows.

Stale, Orphaned, and Dormant Accounts

2

What the board needs to know:

- Are unused accounts increasing attack surface?
- Are we cleaning them up promptly?

Metrics to report:

- *Stale account cleanup rate*
- *Average account dormancy duration before deactivation*
- *Failed login attempts on orphaned accounts*

Tools in Action:

- **SIEM:** Automates stale user detection and scheduled deprovisioning.
- **IAM:** Flags login attempts on decommissioned or expired accounts in real time.

Misconfigured group policies and insecure defaults

3

What the board needs to know:

- Are misconfigurations leaving gaps in security?
- How fast are they being identified and fixed?

Metrics to report:

- *Number of high-risk GPO changes detected per month*
- *GPO compliance deviation score*
- *Average time to revert misconfigurations*

Tools in Action:

- **SIEM:** Audits and compares GPO settings to secure baselines.
- **IAM:** Detects policy changes in critical OU paths and correlates with login anomalies.

Weak or exposed authentication mechanisms

4

What the board needs to know:

- Are password policies and authentication methods strong enough?
- How often are brute-force or pass-the-hash attempts happening?

Metrics to report:

- *Multi-factor authentication (MFA) coverage rate*
- *Volume of failed login attempts per account*
- *Successful logins using legacy authentication protocols*

Tools in Action:

- **SIEM:** Enforces MFA and tracks authentication policy compliance.
- **IAM:** Detects brute-force attempts, legacy protocol usage, and correlates with attacker TTPs.

Insecure delegation and ACL misconfigurations

5

What the board needs to know:

- Are access control rules exposing sensitive assets?
- Are delegated permissions being abused?

Metrics to report:

- *Delegated admin role changes per quarter*
- *Count of ACL anomalies on critical AD objects*
- *Time taken to detect and revoke risky delegation*

Tools in Action:

- **SIEM:** Audits ACLs and highlights overly permissive delegations.
- **IAM:** Alerts on suspicious object access or modifications by non-owner users.

Why these metrics matter to leadership?

Business objective	Supporting metric	Outcome
Reduce breach risk	Dormant accounts removed in 30 days	Smaller attack surface
Ensure compliance	Audit trail coverage of GPO and privilege changes	Regulatory alignment (SOX, GDPR)
Improve resilience	Time to detect privilege escalation (MTTD)	Faster incident containment
Optimize operations	Number of auto-deprovisioned stale users	Fewer manual errors and delays