

# CIOs 30 Day ITDR Checklist

The 30-Day ITDR Checklist acts as an essential fast-track for new CIOs to swiftly assess and reinforce their organization's Identity Threat Detection and Response (ITDR) framework, defending against the 81% of cyberattacks that exploit compromised identities and the fivefold surge in detections over the past year. Its purpose is to distill a thorough ITDR enhancement into a concise timeframe—sufficient to expose critical vulnerabilities like weak MFA or over-privileged accounts, yet urgent enough to deploy safeguards before AI-driven phishing or insider threats escalate into multimillion-dollar breaches—ultimately protecting your leadership role from security oversights. In summary, the checklist divides into six targeted phases: reviewing current IAM posture (Days 1-3), inventorying identities and access (4-7), assessing risks and vulnerabilities (8-12), implementing detection tools and monitoring (13-20), developing response plans with training and communication (21-27), and conducting a final review for go-live (28-30), leveraging Erwood Group's proven methodologies to reduce breach risks by up to 40% and foster proactive identity security.

## 1. REVIEW CURRENT IAM POSTURE

- ☐ Review IAM policies. Check MFA configs, and access logs. Password policies.
- ☐ Check basics: Is MFA enforced everywhere? Privileged accounts audited?
- ☐ Spot gaps like shadow admins or unmonitored SaaS logins, these are hacker highways.
- ☐ Create "IAM Health Check" Doc Document and flagging urgents like weak auth on critical apps.

## 2. INVENTORY IDENTITIES & ACCESS

- ☐ Catalog every user, service account, device, and API key. Use automation if available.
- ☐ User types: Employees, contractors, bots—note lifecycles (onboard/offboard).
- ☐ Access mappings: Who has what? Over-privileged devs with prod access? Flag 'em.
- ☐ External ties: Federated logins, vendor accounts, map dependencies.

## 3. ASSESS RISKS & VULNERABILITIES

- ☐ Assume compromise: Run threat modeling sessions. Simulate AI-phishing/credential stuffing.
- ☐ Threat vectors: Phishing, insider leaks, supply chain hits. What's the impact?
- ☐ Vulns scan: Weak MFA, unpatched IAM tools. Whats the impact? likelihood vs. damage.
- ☐ Behavioral baselines: Anomalous logins? What's the impact? likelihood vs. damage.

## 4. IMPLEMENT DETECTION TOOLS & MONITORING

- ☐ Are there tools currently in use for detection and monitoring?
- ☐ Roll out or tune tools: SIEM integrations for anomalies.
- ☐ Alert setups: Real-time for suspicious logins, privilege escalations.
- ☐ Integration tests: Hook IAM to EDR—simulate a phish, ensure it flags.

## 5. DEVELOP RESPONSE PLANS, TRAIN & COMMUNICATE

- ☐ Does the organization have Incident Response (IR) Plans? Are they current?
- ☐ Build IR (Incident Response) for identities: Playbooks for account lockdowns, forensics.
- ☐ Train your team: A drilled team slashes errors by 60% (per studies).
- ☐ Tiered sessions: Execs learn escalation; teams practice containment.

## 6. FINAL REVIEW & GO-LIVE

- ☐ Loop back: Validate updated ITDR against initial gaps. Are they updated properly?
- ☐ Secure sign-offs. Legal for compliance, board for buy-in.
- ☐ Schedule ongoing: Monthly reviews, bi-annual tests.
- ☐ Create "ITDR Fortress" Document. Share with team. Share summary, key points with executives.

Follow this checklist for deep insights into your company's ITDR in 30 days or less.

**Ready to accelerate without the pitfalls? Erwood Group offers an exclusive 90-Day CIO Advisory Accelerator: Personalized guidance from our veteran strategists, including weekly check-ins, custom audits, and on-demand crisis simulations. Plus, extended support into year one for seamless scaling. Valued at \$50K, yours for \$25K if you book before year's end. No fluff, just results.**