flare

Identity Security Quick-Start Checklist: Tiered Action Plan for Practitioners

Step 0. Know if You are Already Compromised

Before hardening anything, confirm whether your credentials are already circulating. Subscribe to an external identity exposure monitoring service (infostealer log feeds, credential breach databases, technical exposure data) and cross-reference exposed credentials against your directory immediately. If compromised accounts exist, remediate them first. Once that is done, work through the four tiers below:

Step 1. Reduce Credential Value

Goal: Stolen artifacts should expire before attackers can use them.

- [ ] Audit accounts with non-expiring passwords. Prioritize service accounts with admin-like privileges.
- [ ] Enforce MFA on every IdP admin account. No exceptions without hardware keys.
- [ ] Shorten OAuth access token lifetimes to ≤1 hour for sensitive apps. Rotate API keys older than 90 days.

Step 2. Reduce Artifact Reuse

Goal: A credential from one context should be worthless in another.

- [ ] Block admin sign-ins from unmanaged devices via Conditional Access / Authentication Policies.
- [ ] Require device compliance for your top five sensitive SaaS applications.
- [ ] Enable Continuous Access Evaluation (CAE) so sessions revoke in near-real-time on risk signal changes.

Step 3. Harden Trust Boundaries

Goal: Protect the infrastructure that issues and validates identity.

- [ ] List every federated domain and external IdP trust. Investigate any you don't recognize.
- [ ] Restrict OAuth app registration and admin consent grants to approved administrators only.
- [ ] Inventory all non-human identities (service principals, API keys, CI/CD tokens, package registry tokens). Assign a living owner to each.

Step 4. Detect Identity-Plane Drift

Goal: The gap between what the audit says and what is actually true is where breaches live.

- [ ] Enable alerting on new admin role assignments, Conditional Access changes, federated domain additions, and high-privilege OAuth app registrations.
- [ ] Run BloodHound/AzureHound. Count users with a path to Tier 0. That's your baseline.
- [ ] Establish a monthly identity posture review: dormant privileged accounts, unrotated NHI credentials, attack path trends, OAuth permission drift.

The identity plane is now the highest-value collection target, both for adversaries and for defenders. Securing your organization with these steps will be crucial in staying ahead of threat actors in this era of “logging in, instead of hacking in.”