AUDAX CYBERSECURITY
OFFENSIVE SECURITY · CTEM

Active Directory & Identity Security — Hardening Checklist

Το Active Directory είναι ο #1 στόχος σε σχεδόν κάθε breach. Χρησιμοποιήστε το checklist για να εντοπίσετε τα πιο κρίσιμα κενά — και πώς η Audax τα **αποδεικνύει τεχνικά** μέσα από Active Directory & Cloud assessment και red teaming.

PRIVILEGED ACCESS & TIERING

- [ ] **Tier 0/1/2 model — απομόνωση Domain Admins & κρίσιμων assets** — πώς: **Audax: attack path analysis**
- [ ] **Ελάχιστα μέλη σε privileged groups (DA/EA/Schema Admins)· καθαρισμός stale admins**

CREDENTIAL HYGIENE

- [ ] **Καμία cleartext/reversible password· LAPS για local admin passwords**
- [ ] **Προστασία από credential theft: LSASS dumping, pass-the-hash, pass-the-ticket**

KERBEROS & AUTHENTICATION

- [ ] **Έλεγχος για Kerberoastable SPNs & AS-REP roasting· ισχυρά service-account passwords** — πώς: **Audax: AD assessment**
- [ ] **Έλεγχος delegation (unconstrained/constrained/RBCD)· απενεργοποίηση NTLM όπου γίνεται**

ATTACK PATHS & LATERAL MOVEMENT

- [ ] **Χαρτογράφηση attack paths προς Domain Admin (BloodHound-style)** — πώς: **Audax: red teaming**
- [ ] **Έλεγχος ACL misconfigurations & shadow admin rights**

DETECTION & MONITORING

- [ ] **Logging κρίσιμων events· ανίχνευση DCSync, Golden/Silver Ticket, DCShadow**
- [ ] **Έλεγχος αν το SOC/EDR βλέπει AD επιθέσεις σε πραγματικό χρόνο** — πώς: **Audax: detection validation**

HYBRID & CLOUD IDENTITY (ENTRA ID / M365)

- [ ] **Ασφάλεια Entra Connect / sync· conditional access & MFA παντού**
- [ ] **Έλεγχος hybrid attack paths (on-prem → cloud) & privileged cloud roles** — πώς: **Audax: cloud assessment**

Πόσο γρήγορα φτάνει ένας αντίπαλος στον Domain Admin σας;

Ζητήστε Active Directory security assessment από την Audax — χαρτογράφηση attack paths, επικύρωση με πραγματικές τεχνικές & τεκμηρίωση για διοίκηση και αποκατάσταση.

✉ info@audax.gr · ☎ +30 210 9839367 · 🌐 www.audax.gr/services/offensive-security-services/active-directory-cloud-assessment/