AUDAX CYBERSECURITY
OFFENSIVE SECURITY · CTEM

SOC / SIEM / EDR Effectiveness — Checklist

Ένα SOC αξίζει όσο αυτά που πραγματικά ανιχνεύει. Δείτε αν το SOC/SIEM/EDR σας πιάνει πραγματικές επιθέσεις — και πώς η Audax το επικυρώνει.

ΚΆΛΥΨΗ ΤΗΛΕΜΕΤΡΊΑΣ

- [ ] **Πλήρες logging κρίσιμων πηγών (endpoints, identity, cloud, network)**
- [ ] **Κενά ορατότητας (blind spots)**

ΚΆΛΥΨΗ ΑΝΊΧΝΕΥΣΗΣ

- [ ] **Detection rules αντιστοιχισμένα σε ATT&CK**
- [ ] **Δοκιμή απέναντι σε πραγματικές τεχνικές** — πώς: **Audax: adversary validation**

ΛΕΙΤΟΥΡΓΙΚΉ ΑΠΌΔΟΣΗ

- [ ] **Triage, tuning & μείωση false positives**
- [ ] **Μετρήσεις MTTD / MTTR**

EDR EFFICACY

- [ ] **Το EDR μπλοκάρει/ανιχνεύει bypass techniques;**
- [ ] **Συνεχής επανα-επικύρωση**

Ζητήστε SOC effectiveness assessment;
Επικοινωνήστε με την Audax — τεχνική απόδειξη, τεκμηρίωση για διοίκηση & αποκατάσταση.
✉ info@audax.gr · ☎ +30 210 9839367 · 🌐 www.audax.gr/services/adversary-validation-services/soc-siem-edr-effectiveness/