RANKSECURE

Take Control.

Where Trust Meets Technology

How NeoCISO Battles Different Hacker Attacks - Matrix

Attack Type	What are we up against? *(Goal & signals)*	How does NeoCISO know? *(Detection & context)*	How does it decide? *(Decision & priority)*	What does it do? *(Automated actions)*	How is closure proven? *(Verification & KPIs)*	How do we prevent recurrence? *(Hardening next steps)*
Phishing / BEC	Credential theft & wire fraud; lookalike domains, mailbox rule changes, vendor bank detail updates, MFA fatigue patterns.	Correlates email/identity logs, payment workflow changes, and communication graph anomalies to build a BEC narrative.	Prioritizes by business impact (e.g., finance/exec targets, payment-change attempts), policy risk appetite.	Quarantines messages, invalidates sessions, enforces step-up auth/reset MFA, removes rogue rules, opens tracked ticket.	No new campaign deliveries; clean mailbox rules; user re-auth; tokens rotated; attempted transfers blocked.	Tighten DMARC/DKIM/SPF; enforce payment verification playbooks; train flagged users; vendor callback verification.
Ransomware	Disruption & extortion; rapid file renames, SMB spikes, shadow copy deletion, suspicious tooling, new C2 beacons.	Fuses EDR, network, and identity to detect staging and lateral prep; ties to business-critical shares/systems.	High severity when crown-jewel data or OT lines at risk; weighs blast radius and dwell time.	Isolates hosts, disables compromised accounts, blocks hashes, snapshots/isolate shares, enforces EDR containment.	Encryption halted; no further rename bursts; backups validated; access paths sealed; credential hygiene confirmed.	Segmentation, least privilege, immutable backups, patch hygiene, EDR tamper protection, restore drills.

Credential Stuffing / ATO	Account takeover; high login failures, odd ASN/geo, device churn, unusual OAuth grants/sessions.	Correlates IdP logs, geo-velocity, device/app fingerprinting, token reuse to confirm ATO patterns.	Elevates risk for privileged users and sensitive apps; evaluates downstream data access potential.	Rate-limit/deny, require MFA reset, revoke tokens/grants, challenge with step-up auth, notify owners.	Failed attempts fall; session inventory clean; no anomalous grants; user confirms legitimate access restored.	Universal MFA, password hygiene, bot/anti-automation controls, conditional access, token lifetime policy.
Lateral Movement / Privilege Escalation	Spread & escalate; pass-the-hash, Kerberoasting, admin share access, sudden role elevation, RDP/SMB bursts.	Combines AD changes, EDR telemetry, east-west flows to build a privilege-chain narrative and DA path mapping.	High when privileged paths are viable or domain-wide impact is likely; time-sensitive containment.	Kill active sessions, revoke elevation, isolate endpoints, block RDP/SMB, rotate keys/secrets, purge golden tickets.	No new admin events; DA paths broken; stabilized lateral traffic baselines; tamper attempts drop.	Tiered admin model, JIT/JEA access, PAM rollout, service account scoping, host-based firewalling, LDAP hardening.
Supply Chain / Third-Party Compromise	Compromise via vendor or pipeline; odd package versions, signing anomalies, vendor portal changes, build drift.	Correlates SBOM/asset inventory with CI/CD and connector logs; flags anomalous provenance and trust breaks.	Prioritizes by dependency criticality and distribution reach; considers customer impact exposure.	Quarantines artifacts, blocks deployment, rotates credentials, disables suspicious connectors, notifies vendor.	Clean rebuilds pass integrity; no downstream propagation; connectors audited; secrets rotated.	Version pinning, verified signed builds, least-privileged connectors, continuous vendor posture monitoring.
Cloud Misconfig / Public Exposure	Data exposure/takeover; public buckets, permissive IAM, open admin ports, weak control plane protections.	Contextualizes CSPM findings with data classification, external reachability, and identity paths.	Ranks by sensitivity of exposed data and exploitability of access paths; applies compliance guardrails.	Auto-remediates policies, restricts ACLs, closes ports, attaches guardrails/SCPs, creates change record.	Drift monitors stay green; external scans show closed; no anomalous access post-fix.	IaC policy-as-code, SCP guardrails, least privilege IAM, continuous compliance & drift controls.

Data Exfiltration / Insider Threat	Theft of crown jewels; large egress, unusual file access, off-hours downloads, USB usage, long-lived tokens.	Correlates DLP, identity, and network egress with data classification to form an exfil narrative.	Severity set by data classification (PII/IP/regulated) and recipient risk; legal/regulatory impact considered.	Block egress, revoke tokens, suspend/offboard account, legal hold, rotate API keys, snapshot evidence.	Egress baselines normalize; access revoked; chain of custody recorded; regulator-ready artifacts captured.	Data classification program, least privilege, token hygiene, DLP tuning, anomaly alerts on crown-jewel stores.
ICS/OT Process Manipulation	Operational disruption/safety risk; unscheduled PLC changes, atypical commands, IT/OT bridge activity.	Merges OT telemetry with IT identity and network paths; maps to process impact and safety envelopes.	Safety-first triage; elevated priority for lines impacting uptime, quality, or safety systems.	Isolate cell/zone, move to fail-safe states, revoke OT creds, block routes across Purdue layers, restore configs.	Process parameters stable; alarms cleared; engineering change logs reconciled; controlled restart validated.	Purdue segmentation, command allowlists, secured remote access, golden config backups, strict change control.
DDoS / Service Exhaustion	Availability impact; volumetric spikes, app-layer floods, sudden error rate increases.	Correlates CDN/WAF metrics with infra telemetry and user journey degradation for business impact.	Prioritizes by customer-facing impact, SLA risk, and cascade to dependencies.	Orchestrates WAF/CDN rules, rate-limits, traffic scrubbing, autoscaling signals, circuit breakers.	Error rates and latency return to baseline; customer SLOs restored; attack attribution logged.	Pre-baked WAF runbooks, autoscaling policies, bot mitigation, resilient fallbacks and circuit-breakers.