CYBER THREAT INTELLIGENCE & HUNTING

Threat Hunting Checklist

A repeatable, hypothesis-driven hunting loop for small security teams. Use with MITRE ATT&CK, Sigma rules, and the free Nexus CTI Hunt Loop Kit on GitHub.

Prepare

- [ ] Pick a hypothesis tied to a real threat (e.g., 'Attackers abuse remote monitoring tools in our environment')
- [ ] Map it to MITRE ATT&CK techniques
- [ ] Confirm the data you need exists: endpoint, identity, DNS, proxy, cloud logs
- [ ] Define scope, time window, and what 'found' looks like

Execute

- [ ] Run queries (Sigma, KQL, SPL) and baseline normal behavior
- [ ] Pivot on anomalies: users, hosts, parent-child processes, rare destinations
- [ ] Document findings, false positives, and data gaps as you go
- [ ] Escalate confirmed malicious activity to incident response immediately

Act with knowledge

- [ ] Turn useful queries into detections and alerts
- [ ] Fix logging gaps you discovered
- [ ] Share indicators and lessons with your ISAC or peers where appropriate
- [ ] Record hunt metrics: hypotheses tested, detections created, gaps closed
- [ ] Feed results back into your threat intelligence priorities

General guidance for training and planning, not legal advice. Adapt to your environment, contracts, and regulators.