Incident Handling Process – SOC Analyst Cheat Sheet

Incident Handling Process Summary Table

Stage	Goal	Key Actions	Tools / Notes
Stage	Goal	Key Actions	Tools / Notes
Preparation	Be ready before an incident hits	- Build response team - Create playbooks - Train staff - Harden systems (EDR, MFA, etc.)	- Jump bag - Baselines - External comms - Purple teaming
Detection & Analysis	Identify what, where, and how	- Multi-layer detection - Build timeline - Collect IOCs - Classify severity	- SIEM, EDR, AV - Timeline logs - IOC search tools
Containment	Stop the spread quietly	- Short-term: isolate, redirect DNS - Long-term: patch, change creds	- VLAN, DNS sinkhole - Business coordination
Eradication	Remove threat and close access	- Remove malware - Rebuild systems - Harden network	- Patch tools - System hardening guides
Recovery	Restore operations safely	- Restore from backup - Test systems - Monitor heavily	- Log everything - Watch for reinfection
Post-Incident	Learn and improve	- Write report - Post-mortem meeting - Train juniors - Update tools/playbooks	- Final report - Lessons learned docs

Critical Concepts Summary Table

Concept	What It Means	Why It Matters
IOC	Indicators like file hash, IP, domain	Tracks attacker movement
Chain of Custody	Who accessed what and when	Ensures legal admissibility
Memory Forensics	RAM analysis for hidden threats	Essential for advanced threats
PsExec Behavior	With creds = caches / Without = safer	Know tool impact
Confidentiality	Limit info access on incidents	Avoid internal threat escalation