GIAC Certified Incident Handler (GCIH) Cheat Sheet

One-page cram sheet for incident handling, attacker techniques, detection, containment, recovery, and practical workflow.

Best for Last review before drills or course revision	**Focus** Attacker-informed defense + evidence correlation + response flow	**Use with** Use with ports sheet and commands sheet

1. Incident handler mindset

Offense informs defense	GCIH expects you to understand attacker tools and techniques so you can detect and respond effectively.
Triage first	Prioritize alerts by scope, impact, confidence, and current business risk.
Containment tradeoffs	Stop spread while preserving evidence and maintaining critical operations where possible.
Verification	Do not trust one alert or one signature; correlate logs, host data, and network evidence.

2. Attack techniques and vectors

Initial access	Phishing, exposed services, weak auth, vulnerable apps, and misconfigurations are common entry paths.
Command and control	Beaconing patterns, unusual ports, DNS abuse, and encrypted tunnels are recurring themes.
Credential abuse	Password reuse, spraying, Kerberos abuse, and token misuse matter as much as malware.
Lateral movement	SMB, RDP, remote execution, and trust-path abuse often reveal the real incident scope.

3. Detection and analysis

Logs + packets + endpoint	Use all three to distinguish noise from real compromise.
Indicators vs behavior	Static IOCs are useful, but behavior often survives tool or hash changes.
Timeline building	Good timelines expose persistence, spread, and missed controls.
Threat intel	Use context to enrich findings, not to replace validation.

4. Response and recovery

Containment	Isolation, blocking, credential reset, and segmentation can all be valid depending on impact.

Eradication	Remove persistence, patch root cause, and close the entry path.
Recovery	Restore safely, monitor for recurrence, and verify control effectiveness.
Lessons learned	Feed the incident back into playbooks, detections, and architecture decisions.

5. Practical handling

Evidence discipline	Document commands, timestamps, hostnames, hashes, and decisions as you work.
Communication	Executives need impact; responders need exact scope and next actions.
Tools are helpers	IDS, SIEM, EDR, packet capture, and scripts support judgment; they do not replace it.
Hands-on orientation	This track rewards practical reasoning more than memorized buzzwords.