GIAC Certified Incident Handler (GCIH) Quick Summary

Fast 3-5 minute refresh for the handler mindset, comparisons, and common incident-response traps.

Best for	Focus	Use with
Ultra-fast memory refresh	Definitions, priorities, and handler shortcuts	Use with cheat sheet for deeper review

1. Fast refresh

GCIH focus	Detect, respond, and resolve security incidents.
Think attacker + defender	Understand how attacks work so you can investigate them faster.
Correlate evidence	One alert is rarely enough.
Contain with purpose	Stop spread without losing critical evidence.

2. Common traps

IOC vs IOA	Indicators of compromise differ from behavioral indicators of attack.
Detection vs confirmation	An alert suggests risk; it does not prove scope or root cause.
Containment vs eradication	Stopping spread is not the same as removing persistence.
Noise vs signal	High event volume does not equal high confidence.

3. Handler shortcuts

Build a timeline	Do it early.
Check scope	Always ask how far it spread.
Reset credentials wisely	Good move when compromise touches auth paths.
Document live	Do not rely on memory later.

4. Exam traps

DNS matters	Attackers use it for resolution, tunneling, and command channels.
SMB/RDP matter	Lateral movement often lives here.
Packet truth	When logs conflict, packets can clarify behavior.
Recovery needs monitoring	Do not declare victory too early.