Incident Response Quick-Start

A one-page playbook for the first hours of a suspected security incident.

First 15 minutes — stay calm, confirm

- [ ] Confirm it's a real incident (not a false alarm or test)
- [ ] Note the time, who reported it, and what was observed
- [ ] Start an incident timeline document and keep it updated
- [ ] Assign an incident lead to coordinate

Contain

- [ ] Isolate affected systems (disconnect, don't power off if forensics needed)
- [ ] Revoke compromised credentials, tokens, and sessions
- [ ] Block malicious IPs/domains and disable affected accounts
- [ ] Preserve evidence: snapshots, logs, memory where possible

Assess

- [ ] Determine what was accessed, changed, or exfiltrated
- [ ] Identify the entry point and scope of impact
- [ ] Decide severity and whether to escalate

Communicate

- [ ] Notify internal stakeholders and decision-makers
- [ ] Assess legal/regulatory notification obligations
- [ ] Prepare clear, factual updates; avoid speculation

Recover & learn

- [ ] Eradicate the cause and rebuild from known-good state
- [ ] Restore from clean backups; reset all relevant secrets
- [ ] Monitor closely for recurrence
- [ ] Run a blameless post-incident review and fix root causes

guardioninfosec@gmail.com