1 ROLE RESPONSIBILITIES

Injects, phone, flex support, coordinating the team. Rarely fixes anything directly. Makes sure every fix has an owner and nothing falls through.

2 ORDER OF OPERATIONS

Round start: Confirm every role staffed. Confirm shared log/template open.

Inject arrives: Read fully. Note deadline. Assign owner immediately.

Foothold reported: Get host, time, symptom. Assign loop: threat hunter continues user/hole, SIEM lead checks other hosts, engineer stages fix.

Findings converge: Confirm engineer has what they need. Confirm scope logged before eviction.

Verified fixed: Log closed, timestamped, with confirmer. Move to next item.

3 THINK LIKE RED TEAM

- Weigh a fix by how much of red team's playbook it disables, not just whether it closes today's hole.
- Push the engineer toward removals that cost red team more than blue team or the scored service: unused interpreters, unused remote-management protocols, reused local admin passwords.
- A quiet stretch can mean red team is regrouping around tooling you removed, not that they've given up.

4 TRIAGE PRIORITY

- Severity first: scoring/safety impact now, or can it wait.
- Effort second: 5-minute fix ahead of a 30-minute one, all else equal.
- An owner, always. Untracked work does not happen.
- A visible queue. Everyone sees what is pending, not just you.

5 THE TRACKING TEMPLATE

Keep running the entire round, not reconstructed after.

- Time detected, reported by, host(s) affected
- User/account involved, entry vector (the hole)
- Lateral movement: yes/no, where
- Exfiltration: yes/no, what
- Owner assigned, actions taken (timestamped)
- Verified closed: time, by whom

6 HANDLING INJECTS

- Read the whole queue before assigning from it.
- Schedule injects alongside technical work, not after it.
- Do not pull a threat hunter or engineer off active eviction for a routine inject. Use flex, or handle it yourself.
- Keep a standard inject response template ready: restate the ask, list what was done, note timestamps. Saves time under a deadline.

7 RUNNING THE COMMS CHANNEL

- One channel for status updates, separate from casual chat, if your tool allows it.
- Pin the tracking template link and the current priority list.
- Use short, structured updates: role, host, status, next step. Not paragraphs.
- A 60-second radio check every 15-20 minutes catches silent blockers early.

8 YOUR OWN CHECKS

Things you can verify yourself without pulling a specialist off task.

- `ping [host]` / `Test-Connection`: is it even up.
- `curl -I [url]` or a browser: is the scored service responding.
- `ssh [host]` or RDP: can you still get in at all.
- `whoami`: confirm you did not just get logged in as someone unexpected.

9 DELEGATION MAP

- *Domain Admin:* Anything AD-specific.
- *Threat hunters:* Detect, find user, find hole, assess scope, per OS.
- *Engineer(s):* Evict and patch, after handoff.
- *SIEM lead:* Scope across every host. Watches for return.

10 FLEX BRIEFING: DOMAIN ADMIN

Enough to cover if nobody else can.

- Baseline: `Get-ADUser -Filter *`, `Get-ADGroupMember "Domain Admins"`.
- Health: `dcdiag`, `repadmin /replsummary`.
- Policy: `Get-GPO -All`, `gpresult /r` to confirm it applied.
- Red flag: a new Domain Admin, or unusual Kerberos ticket activity.
- Reset: `Set-ADAccountPassword`, or `Disable-ADAccount` if unsure.

11 FLEX BRIEFING: THREAT HUNTER

- Who's logged in: `w`/`who` (Linux), `query user` (Windows).
- Who logged in recently: `last` (Linux), Event ID 4624/4625 (Windows).
- Trace a process: `ps -o user,pid,ppid,cmd -p [PID]` (Linux), `Get-CimInstance Win32_Process` for parent PID (Windows).
- Find the hole: check auth logs for the login window around the suspicious timestamp.
- Scope: `ss -tunp` / `Get-NetTCPConnection` for unfamiliar connections.

12 FLEX BRIEFING: ENGINEER

- Kill it: `kill -9 [PID]` (Linux), `Stop-Process -Id [PID] -Force` (Windows).
- Remove persistence: cron/`/etc/cron.d` (Linux), Task Scheduler/Run keys (Windows).
- Patch the actual vulnerability, not just the symptom. Rotate anything possibly exposed.
- Protect a fix: `chattr +i` on Linux, tighter `icacls` on Windows.
- Confirm the scored service is still up after any change.
- If time allows: strip unused interpreters (Python, Perl), disable unused WinRM/PSRemoting.

13 FLEX BRIEFING: SIEM LEAD

- Health: `so-status`. Access: `so-allow` if the web UI refuses you.
- Use Hunt for ad-hoc queries, not just the prebuilt Alerts view.
- Lateral movement: `event.dataset:conn` filtered to the host in question.
- Other hosts: search Suricata alerts by the same signature across every sensor.
- If Wazuh is deployed, File Integrity Monitoring alerts confirm a specific file changed fast.

14 SCOREBOARD

- Points typically split between service uptime (checked on an interval) and injects (graded on submission quality and timeliness).
- Uptime is scored automatically and continuously; a service down for ten minutes costs more than one incident report submitted five minutes late.
- Know which services are actually scored vs. which are just present. Do not spend a scarce engineer on a box that earns nothing.
- Ask White Team early if scoring criteria for an inject are ambiguous. A clarifying question costs less than a wrong guess.

15 SIMULTANEOUS INCIDENTS

- Rank by scored-service impact first, safety second, everything else after.
- Do not let a loud, obvious problem eclipse a quiet one on a more valuable host. Check the full host list, not just what people are shouting about.
- Assign a distinct owner per incident even if hands are shared across them; the tracking template still needs one line per incident, not one merged mess.
- If truly overloaded, tell the team explicitly what is being deprioritized and why, out loud, not silently.

16 WORKING WITH WHITE TEAM / JUDGES

- Report an outage or scoring dispute the moment it is noticed, not after trying to fix it quietly first.
- Keep language factual: what you observed, when, what you believe caused it. Save the argument for after the round.
- A formal timeout or scoring pause exists for a reason. Use it for a genuine platform issue, not as a stalling

tactic.

- Written communication (chat, ticket) beats verbal when a dispute might need to be revisited later.

17 DEBRIEF

- Walk the timeline from the template, not memory.
- Find what slowed the loop, not who to blame.
- Ask where a handoff was slow or unclear. That is usually the real fix.