# Phase 2 Facilitator Guide – Technical / Cyber Team

## Phase Overview: Public & Internal Chaos (T+30 to T+60)

In Phase 2, the Technical team faces active service impacts and worsening data integrity. They must interpret logs, make calls on isolation/containment, and communicate effectively with Ops and Executive. Evidence of compromise becomes more visible and persistent.

This phase tests:

* Log analysis and threat identification
* Effective cross-team escalation
* Service impact mapping and decision making

## Injects Relevant to Technical

### P2-1 (T+30 to T+40)

**INJ004A:** SSH logs show repeat logins from unusual source  
**INJ004B:** Vendor unable to connect through gateway

**Facilitator Notes (P2-1)**

* Technical should begin immediate log review and flag source IP.
* Possible network segmentation or gateway isolation should be raised.
* Prompt:
  + "Have you triaged the vendor issue and SSH logs?"
  + "Are you considering containment at the gateway?"

### P2-2 (T+40 to T+50)

**INJ005A:** Vendor technical contact reports their session was terminated abnormally (follow-on to INJ004B)

**Facilitator Notes (P2-2)**

* Technical now has evidence of session disruption — attack or misconfiguration?
* Should escalate findings to Executive.
* Prompt:
  + "What’s your assessment of the cause?"
  + "Have you informed other teams of potential gateway compromise?"

### P2-3 (T+50 to T+60)

**INJ006A:** Log extract shows alert suppressed by local cron job (Technical only)

**Facilitator Notes (P2-3)**

* Strong indicator of compromise.
* Technical should immediately raise alarm and request deeper access if needed.
* Prompt:
  + "Have you reviewed who placed the cron job?"
  + "Is this being escalated as active compromise?"

## Technical Role Expectations

* Analyse logs (SSH, cron)
* Identify signs of active compromise
* Escalate confirmed incidents to Exec

**Key Policy References:**

* Technical Containment SOP – Section 4.2
* Log Review Checklist

## Technical Decision Point – Phase 2

**Decision: Escalate Confirmed Gateway Compromise?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Description** | **Implication** | **Score** |
| ✅ Escalate with evidence to Exec and isolate affected systems | Proactive | Protects broader network, supports containment | +10 |
| ⚠️ Monitor further before acting | Conservative | May delay critical response | +1 |
| ❌ Ignore anomaly as false positive | Risky | Service risk and post-incident exposure | -8 |

## End-of-Phase Checkpoint Prompt

At or near **T+60**, facilitator should ask:

"Technical team — have you confirmed any compromise? What are your next actions? Has this been raised with Executive or Ops yet?"

Ensure logs, access, and recommendations are captured.

## Tip for Facilitator

If Tech is unclear:

* Refer them to INJ006A (cron job suppression)
* Ask if SSH logs have been cross-checked
* Confirm use of containment and logging protocols

#### End of Phase 2 – Technical / Cyber Team Facilitator Guide