# Phase 3 Facilitator Guide – Technical / Cyber Team

## Phase Overview: Full Crisis Realised (T+60 to T+90)

In Phase 3, compromise is confirmed and operational impact is unavoidable. The Technical team must act on anomalous behaviour, including crane system failures and possible system overrides. Escalation to Executive is no longer optional — clear containment and impact articulation is required.

This phase tests:

* Critical infrastructure troubleshooting
* Attack vector confirmation and containment
* Communication of risks to Exec and Ops

## Injects Relevant to Technical

### P3-1 (T+60 to T+70)

**INJ010A:** Network gateway logs show scan from vendor subnet (follow-up to earlier anomalies)

**Facilitator Notes (P3-1)**

* Technical should now confirm compromise or clear false positives
* Should notify Ops and escalate to Exec
* Prompt:
  + "Have you confirmed the scanning activity source?"
  + "What systems are at risk based on this subnet’s reach?"

### P3-2 (T+70 to T+80)

**INJ011D:** Crane system partially unresponsive, field unit logs show override attempts

**Facilitator Notes (P3-2)**

* This is a critical failure — Technical must respond fast
* Coordination with Ops essential
* Prompt:
  + "Are you isolating the affected crane systems?"
  + "Is this being treated as an active attack?"

### P3-3 (T+80 to T+90)

**INJ012A:** Log review shows deletion of past alert records

**Facilitator Notes (P3-3)**

* Log tampering confirmed — high confidence in compromise
* Must prepare report for Exec and recommend next steps
* Prompt:
  + "Have you documented this breach?"
  + "What are your recommendations to contain or mitigate further loss?"

## Technical Role Expectations

* Identify and confirm system-level compromise
* Coordinate with Ops on affected systems
* Escalate detailed findings to Executive with logs

**Key Policy References:**

* Incident Response Plan §4.4
* Critical Infrastructure Cyber Threat Checklist

## Technical Decision Point – Phase 3

**Decision: Formally Declare Critical System Compromise?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Description** | **Implication** | **Score** |
| ✅ Confirm compromise, document, and notify Exec | Accurate & timely | Enables informed response, aids recovery | +10 |
| ⚠️ Delay pending more evidence | Conservative | Risks delayed containment | +2 |
| ❌ Downplay issue or reclassify | Dangerous | Undermines response, potential legal risk | -8 |

## End-of-Phase Checkpoint Prompt

At or near **T+90**, facilitator should ask:

"Technical team — have you confirmed the source and scope of the system compromise? Has this been escalated to Executive with clear impact and next-step recommendations?"

Ensure log details and response actions are recorded.

## Tip for Facilitator

If Tech team hesitates:

* Highlight INJ011D (crane override) and INJ012A (log deletion)
* Ask whether logs were shared with Ops or Exec
* Confirm use of Incident Response Plan

#### End of Phase 3 – Technical / Cyber Team Facilitator Guide