# Phase 1 Facilitator Guide – Technical / Cyber Team

## Phase Overview: Disruption Emerges (T+0 to T+30)

This phase introduces subtle technical disruptions, including packet delays, AIS anomalies, and low-level system warnings. The Technical team plays a key role in detecting and interpreting early signals, and coordinating containment actions with Executive and Ops.

This phase tests:

* Detection of subtle but coordinated anomalies
* Correct use of containment policy
* Coordination with Executive and Ops

## Injects Relevant to Technical

### P1-1 (T+0 to T+10)

**INJ001A:** Delayed packet routing to ship manifest system  
**INJ001B:** Packet queue spike at Node-04  
**INJ001D (Noise):** Low battery warning on container sensor 12B

**Facilitator Notes (P1-1)**

* Tech should start investigating Node-04.
* They may coordinate with Ops or flag to Executive.
* Prompt:
  + "Have you started logging anomalies from Node-04?"
  + "Any sign of coordinated failure or early containment?"

### P1-2 (T+10 to T+20)

**INJ002A:** AIS dashboard hides Ship\_Alpha  
**INJ002E (Noise):** Email delivery failure to admin@port

**Facilitator Notes (P1-2)**

* Tech should correlate AIS and network issues.
* This is a key moment to brief Exec on the growing pattern.
* Prompt:
  + "Are you escalating Ship\_Alpha’s disappearance?"
  + "Is Node-04 linked to AIS or isolated?"

### P1-3 (T+20 to T+30)

**INJ003A:** CCTV blackout triggered on dashboard  
**INJ003G:** Email from Harjit Mann suggesting Node-04 isolation

**Facilitator Notes (P1-3)**

* Harjit’s email is a containment trigger.
* Tech should now consider isolating Node-04.
* Prompt:
  + "Are you acting on Harjit’s recommendation?"
  + "Have you updated the Exec team on containment status?"

## Technical Role Expectations

* Investigate anomalies (AIS, network)
* Identify compromised systems
* Notify Executive of containment or risk recommendations
* Maintain log of actions and indicators

**Key Policy References:**

* Technical Containment Guide – Sections 2.1, 3.0

## Technical Decision Point – Phase 1

**Decision: Isolate Node-04 to Contain Risk?**

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Isolate Node-04, notify Ops/Exec | Preventive | Limits compromise, preserves diagnostics | +9 |
| ⚠️ Monitor without action | Passive | Delays response, risk of spread | +3 |
| ❌ Take no action, assume false positive | Risky | Misses containment window | -7 |

## End-of-Phase Checkpoint Prompt

At or near **T+30**, facilitator should ask:

"Technical team — have you isolated any systems or logged major anomalies? What’s your recommendation to the Executive team?"

Ensure that logs and actions are recorded.

## Tip for Facilitator

If Tech is not reacting:

* Reference INJ001B (Node-04 anomaly) and INJ002A (AIS disappearance)
* Ask if they’ve run the Containment Guide or initiated logging
* Encourage coordination with Ops and Executive

#### End of Phase 1 – Technical / Cyber Team Facilitator Guide