TECHNICAL_TEAM_QUESTIONS

SOUTHGATE TERMINAL

Facilitator Questions - TECHNICAL TEAM

75-Minute Cyber Crisis Exercise

PURPOSE

These questions help facilitators guide and assess the Technical Team's investigation, threat detection, and system recovery efforts throughout the exercise.

TIMING OPTIONS

- **Option A**: Ask questions every 10 minutes for continuous assessment
- **Option B**: Ask at phase transitions (T+30, T+60, T+90)
- **Option C**: Ask after major technical discoveries

PHASE 1: Initial Detection & Triage (T+0 to T+30)

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

Question: "Have you started investigating the Node-04 packet anomalies? What have you found?"

Look for: - Evidence preservation first - Systematic investigation approach - Initial threat indicators

Notes: _____ _____ _____ _____

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

Question: "What diagnostic outcomes have you logged regarding the AIS disappearance? Did Operations provide sufficient details?"

Look for: - Log analysis completion - Cross-team information gathering - Pattern recognition

Notes: _____ _____ _____ _____

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

Question: "Have you compiled your AIS diagnostic summary for the Incident Coordinator? Are further diagnostic tools required?"

Look for: - Documentation quality - Tool utilisation - Investigation completeness

Notes: _____ _____ _____ _____

PHASE 2: Threat Identification (T+30 to T+60)

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

Question: "Have you identified the root cause of the scheduler anomalies? Are isolation measures needed?"

Look for: - Root cause analysis - Threat vector identification - Containment recommendations

Notes: _____ _____ _____ _____

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

Question: "Have further technical anomalies been validated? Is there evidence of malicious activity?"

Look for: - Multiple system correlation - Malicious vs technical failure - Evidence collection

Notes: _____ _____ _____ _____

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

Question: "Have system isolation decisions been confirmed? Are forensic actions clearly documented?"

Look for: - Isolation coordination - Forensic methodology - Chain of custody

Notes: _____ _____ _____ _____

PHASE 3: Systematic Compromise Response (T+60 to T+70)

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

Question: "Are container routing manipulations forensically validated and documented?"

Look for: - Advanced threat detection - Attack timeline construction - Evidence packaging

Notes: _____ _____ _____ _____

PHASE 4: Containment & Recovery (T+90 to T+120)

P4-1 Questions (T+90 to T+100)

Question: "Have all teams consolidated and verified their documentation? Are final reports accurate?"

Look for: - Technical report completeness - Evidence transfer status - Recovery recommendations

Notes: _____ _____ _____ _____

P4-2 Questions (T+100 to T+110)

Question: "Have final reports been validated for alignment and accuracy? Any outstanding concerns?"

Look for: - Technical accuracy - Unresolved threats - Future security recommendations

Notes: _____ _____ _____ _____

P4-3 Questions (T+110 to T+120)

Question: "Are final forensic and operational reports clearly documented and submitted?"

Look for: - Forensic report quality - Technical recommendations - Lessons learned capture

Notes: _____ _____ _____ _____

OVERALL ASSESSMENT CRITERIA

Investigation Quality

- [ ] Evidence preserved before analysis
- [ ] Systematic investigation approach
- [ ] Cross-system correlation completed
- [ ] Root cause identified

Threat Detection

- [ ] Threat indicators recognised
- [ ] Attack vectors identified

- [ ] Persistence mechanisms found
- [ ] Timeline reconstructed

Technical Response

- [ ] Appropriate containment measures
- [ ] Coordination with Operations
- [ ] Documentation standards met
- [ ] Recovery path defined

GENERAL OBSERVATIONS

Technical Competency: _____
_____ _____

Key Findings: _____
_____ _____

Investigation Strengths: _____
_____ _____

Technical Gaps: _____
_____ _____

Facilitator: _____ **Date:** _____ **Exercise ID:** _____