SOUTHGATE TERMINAL

Port Operations Security Documentation

Technical / Ops Procedures – Node Isolation Procedure

Purpose:
To provide step-by-step instructions for isolating compromised or anomalous nodes (VMs or containers) within the Southgate Maritime environment. This procedure ensures threats are contained without triggering unnecessary operational outages.

When to Use

- Suspicious activity or compromise is confirmed or strongly suspected on a system
- Persistence mechanisms (e.g. hidden cron jobs, altered binaries) are found
- Lateral movement or unauthorised access between VMs is detected

Pre-Isolation Checklist

- Confirm isolation need with Technical Lead or Incident Coordinator
- Identify system owner and assess operational impact
- Capture key logs and evidence before action:
- cp /var/log/syslog /var/log/evidence/syslog-$(date +%F-%H%M).log
- tar -czf /var/log/evidence/service-logs.tar.gz /opt/app/logs/
- sha256sum /var/log/evidence/*.log
- Alert Coordinator and update team log

Isolation Techniques

1. Container Isolation
   - Stop individual containers:
   - docker ps
   - docker stop [container_id]
   - docker export [container_id] > /var/log/evidence/container-[id].tar
   - Remove from auto-restart:
   - docker update --restart=no [container_id]
2. Service-Level Isolation
   - Stop suspicious service:

- systemctl stop [servicename]
- systemctl disable [servicename]
- Prevent restart (masking):
- systemctl mask [servicename]

3. VM Network Isolation
   - Disconnect VM network interface (requires elevated rights):
   - sudo ip link set eth0 down
   - # or
   - sudo nmcli connection down ”Wired connection 1”
   - Confirm interface state:
   - ip a | grep DOWN
   - Optional: block outbound traffic using UFW
   - sudo ufw deny out from any to any

Post-Isolation Actions

- Log all actions in incident log with timestamps
- Notify relevant stakeholder group (e.g. vendor, legal)
- Continue passive monitoring:
  - Watch syslog, cron, container state
  - Use journalctl -f, docker logs, or auditctl if enabled

Do Not:

- Delete any binaries, logs, or user data
- Wipe systems without Legal authorisation
- Restart isolated systems without group consensus

Network Diagnostics and Investigation SOP

Purpose

This procedure provides step-by-step guidance for investigating network anomalies, packet routing delays, and suspected malicious activity. Use when receiving reports of network performance issues or unusual traffic patterns.

When to Use

- Delayed packet routing to critical systems (e.g., ship manifest system)
- Packet queue spikes or unusual traffic patterns
- Cross-system timing anomalies that may indicate network issues
- Suspected external interference or malicious connections

Investigation Steps

Phase 1: Initial Assessment (First 5 minutes)

1. Identify Scope
   - ☐ Note specific systems affected (manifest, AIS, CCTV, etc.)
   - ☐ Record time of initial report
   - ☐ Identify reporting source and reliability
2. Quick System Check
   - ☐ Check Node-04 traffic status and packet queues
   - ☐ Review recent configuration changes
   - ☐ Verify external gateway connectivity
3. Document Initial Findings
   - ☐ Record baseline metrics before investigation
   - ☐ Note any obvious patterns or anomalies

Phase 2: Detailed Investigation (Next 10 minutes)

1. Traffic Analysis
   - ☐ Analyze packet queue origins and destinations
   - ☐ Check for unusual connection patterns
   - ☐ Review bandwidth utilization trends
   - ☐ Identify any automated traffic spikes
2. Cross-System Correlation
   - ☐ Compare network event timing with AIS anomalies
   - ☐ Check correlation with CCTV or operational disruptions
   - ☐ Review vendor system access logs
3. External Gateway Diagnostics
   - ☐ Test external connectivity and latency
   - ☐ Review firewall and security logs
   - ☐ Check for blocked or suspicious connections

Phase 3: Analysis and Decision (Final 5 minutes)

1. Pattern Analysis
   - ☐ Determine if issue is isolated to local switch
   - ☐ Assess potential for upstream network degradation
   - ☐ Evaluate signs of external interference
2. Impact Assessment
   - ☐ Document affected systems and operations

☐ Estimate operational impact if network isolation required
☐ Consider safety implications

Decision Matrix: Escalation vs. Continued Investigation

CONTINUE LOCAL INVESTIGATION IF:

- Issue appears isolated to local network
- Clear technical cause identified
- Low operational impact
- Recent configuration changes may be cause

ESCALATE TO CYBER TEAM IF:

- Evidence of external interference
- Multiple unrelated systems affected
- Unusual or sophisticated attack patterns
- Cannot identify clear technical cause within 20 minutes

COORDINATE WITH OPERATIONS BEFORE:

- Isolating any nodes that affect operations
- Making changes that could impact CCTV or AIS
- Implementing network restrictions

Required Communications

To Operations Team:

- “Network investigation underway. [System] may need isolation - operational impact: [description]”
- “Network issue appears [local/external]. Recommend [continue operations/prepare for manual mode]”

To Incident Coordinator:

- “Network investigation status: [findings]. Escalation [required/not required]. Timeline: [estimate]”

To Executive/Legal (if external threat suspected):

- “Network anomalies suggest potential external factor. Recommend legal review of vendor relationships and contracts”

Investigation Tools and Commands

- Network monitoring dashboard
- Packet capture tools
- Traffic analysis utilities
- External connectivity tests
- Security log review tools

Documentation Requirements

- Incident Log Entry: All investigation steps and findings
- Timeline: Correlation with other system events
- Evidence: Packet captures if malicious activity suspected
- Decisions: Rationale for escalation or continued local response

Success Criteria

- Clear determination of network issue scope and cause
- Informed decision about escalation to cyber specialists
- Other teams briefed on network status and potential impacts
- Documentation complete for post-incident analysis

Related Procedures

- Use with: Signal Anomaly Response (for AIS correlation)
- Coordinate with: Manual Ops SOP (if network isolation required)
- Escalate to: Technical Containment Guide (if cyber threat confirmed)

Owner: Technical Lead
Reference: TECH-03
Version: 1.0
Approved by: Cyber-Ops Coordination Cell