SOUTHGATE TERMINAL

Port Operations Security Documentation

Technical / Ops Procedures – Forensics Summary Template

Purpose:
To provide a structured template for capturing technical forensic evidence following an incident. This document assists in investigation, reporting, and supporting legal or policy decisions.

When to Use

- Post-containment, during incident investigation
- As part of closure reporting or lessons learned
- When evidence must be retained for legal, insurer, or audit purposes

Forensics Summary Header

Field	Entry
Incident Reference ID	[e.g. INC-2025-042]
Date of Evidence Collection	[YYYY-MM-DD]
Systems Investigated	[List VMs or Containers]
Lead Analyst / Team	[Name or Role]
Purpose of Review	[Containment / Attribution / Audit]

Section 1: Initial Indicators

Document what triggered the investigation, including:

- Unexpected system behaviour (e.g. service crash, restart loop)
- GPS/AIS signal anomalies (phantom vessels, location drift)
- Suspicious cron jobs or unknown binaries
- Repeated authentication failures or logins from unusual IPs
- CPU spikes or memory drain in containers or host system
- Alert from coordinator, dashboard discrepancy, or manual report

Section 2: Collected Artifacts

Artifact Type	Location or Hash	Notes
Log File	/var/log/syslog	[Lines extracted]
Application Log	/opt/app/logs/planner.log	[Key errors noted]

Artifact Type	Location or Hash	Notes
Network Capture	/var/log/evidence/ais-signal.pcap	[Timeframe captured]
Container Image	/var/log/evidence/container-ab123.tar	[Tool used: docker export]
Modified Binary	/usr/bin/ssh – sha256sum: abcd...1234	[Mismatch found]

Section 3: Timeline Reconstruction

- Chronological summary of indicators and actions
- Include timestamps from logs, alerts, and human response

Section 4: Attribution Assessment (Optional)

- Indicators of compromise (e.g. known IPs, signatures)
- Potential attacker behaviour (if identifiable)
- Related previous incidents (if any)

Section 5: Containment & Recommendations

- What actions were taken, and when
- Summary of stability post-isolation
- Recommendations for:
  - System hardening
  - Patch application
  - Future detection improvements

Submission:
Attach to the final incident log archive and submit to Technical Lead + Legal. Retain hash of this file.

Owner: Technical Lead
Reference: TECH-04
Version: 1.0
Approved by: Cyber-Ops Coordination Cell