Technical Quick Reference Card

SOUTHGATE TERMINAL

Technical Team Quick Reference Card

75-Minute Cyber Investigation Guide

PURPOSE

This card guides Technical Team investigation and response during the port cybersecurity incident, focusing on evidence preservation, system analysis, and threat detection without revealing specific attack details.

PHASE 1 (0-15 Minutes) - Initial Detection & Triage

EARLY WARNING INDICATORS

- **Network Anomalies**: Outbound packet queuing spikes

- **System Visibility**: AIS vessel tracking failures
- **Authentication Issues**: Service account problems emerging
- **Performance Degradation**: Routing delays to critical systems

IMMEDIATE ACTIONS CHECKLIST

1. **PRESERVE FIRST**: Hash all logs before any investigation
2. **DIVIDE TEAM**: Assign one person per affected system
3. **PRIORITIZE**: Focus on gateway and core systems first
4. **DOCUMENT**: Start incident timeline immediately

ESSENTIAL DOCUMENTS

- `VM_Specific_Investigation_Procedures.pdf` - System investigation steps
- `Evidence_Transfer_Chain_of_Custody.pdf` - Evidence handling
- `Multi_System_Failure_Coordination_Guide.pdf` - Multi-system response
- `Technical Containment Guide.pdf` - Containment procedures

CRITICAL INVESTIGATION COMMANDS

```
# Evidence Preservation (ALWAYS FIRST)
cd /var/log/ && find . -type f -name "*.log" -exec sha256sum {} \; > /tmp/initial_hashes_$(date
        +%Y%m%d_%H%M%S).txt

# Quick System Check
systemctl status --all | grep -E "failed|error"
ps aux | grep -v grep | grep -E "unusual|suspicious"
netstat -tulpn | grep ESTABLISHED

# Check for Persistence
ls -la /etc/cron.d/
crontab -l
find /tmp /opt /home -type f -name "*.sh" -mtime -1
```

SYSTEM PRIORITY ORDER

1. **vm-gateway**: External access point, highest risk
2. **vm-coretech**: Core operational systems (AIS/GPS)
3. **vm-opsnode**: Safety systems (CCTV)
4. **vm-audit**: Evidence collection system

VM-AUDIT ACCESS

```
# Login for evidence transfer
ssh audit@3.106.187.171
# Password: secure2024
```

PHASE 2 (15-35 Minutes) - Threat Identification

ESCALATING INDICATORS

- **Multiple Failures**: Scheduler anomalies detected
- **External Connections**: Unauthorised vendor access attempts
- **Service Degradation**: CCTV systems failing
- **Data Anomalies**: Configuration manipulation signs

INVESTIGATION FOCUS AREAS

1. **Authentication Logs**: Failed logins, service accounts
2. **Cron Jobs**: Unauthorised scheduled tasks
3. **Network Connections**: Unusual external communications
4. **Configuration Changes**: Modified system settings

KEY DOCUMENTS NEEDED

- `Log_Deletion_Investigation.pdf` - Finding tampered logs
- `Network_Diagnostics_SOP.pdf` - Network analysis
- `Service_Account_Authentication_Response.pdf` - Service account issues
- `AIS_Signal_Validation.pdf` - AIS system verification

ADVANCED INVESTIGATION TECHNIQUES

```
# Service Account Analysis
grep -E "svc_|service" /var/log/auth.log | grep -i "fail"
find /etc/systemd -name "*.service" -mtime -7

# Network Traffic Analysis
tcpdump -i any -n -c 1000 'not port 22' -w /tmp/capture.pcap
iftop -n -P # Real-time bandwidth by connection

# Configuration Drift Detection
find /etc -type f -mtime -1 | while read f; do
    echo "=== $f ==="
    diff "$f" "$f.bak" 2>/dev/null || echo "No backup found"
done

# Process Anomaly Detection
ps aux --sort=start_time | tail -20  # Recently started
lsof -i -P -n | grep LISTEN          # Listening services
```

TRAP DETECTION WARNINGS

DO NOT EXECUTE these if found: - Scripts in /opt/security/ or /opt/tools/ - Any script named "restore_*.sh" or "cleanup_*.sh" - Cron jobs with encoded/obfuscated commands - Scripts that delete logs or clear history

---

PHASE 3 (35-55 Minutes) - Systematic Compromise

CRITICAL ESCALATION SIGNS

- **Complete AIS Failure**: All vessel tracking lost
- **Authentication Cascade**: Multiple service accounts failing
- **Evidence Tampering**: Log deletion attempts detected
- **Coordinated Timing**: Multiple systems affected simultaneously

COMPREHENSIVE ANALYSIS

1. **Cross-System Correlation**: Match timestamps across systems
2. **Attack Vector Identification**: Entry points and methods
3. **Lateral Movement**: How attacker moved between systems
4. **Persistence Mechanisms**: Backdoors and scheduled tasks

CRITICAL DOCUMENTS

- `CCTV_Blackout_Response.pdf` - Camera system recovery
- `Authentication_Failure_Response_SOP.pdf` - Auth system analysis
- `Node Isolation Procedure.pdf` - Network isolation steps
- All previous phase documents

FORENSIC INVESTIGATION COMMANDS

```
# Timeline Reconstruction
find /var/log -type f -name "*.log" -exec grep -H "ERROR\|FAIL\|WARN" {} \; | sort -t: -k2,2 >
        /tmp/timeline.txt

# Backdoor Detection
find / -type f \( -perm -4000 -o -perm -2000 \) -exec ls -l {} \; 2>/dev/null
find /tmp /var/tmp -type f -executable -mtime -7

# Deleted File Recovery
grep -a "DELETE\|unlink\|removed" /var/log/* 2>/dev/null
ls -la /proc/*/fd/ 2>/dev/null | grep deleted

# Memory Analysis
ps aux | sort -nrk 3,3 | head -10  # CPU usage
ps aux | sort -nrk 4,4 | head -10  # Memory usage
cat /proc/meminfo | grep -E "^Mem|^Swap"
```

EVIDENCE PACKAGING

1. Create forensic copies with hashes
2. Document chain of custody
3. Prepare for transfer to vm-audit
4. Brief incident coordinator on findings

Transfer to Audit System:

```
# Login: ssh audit@3.106.187.171 (password: secure2024)
scp /tmp/evidence_* audit@3.106.187.171:/incident/archive/$(hostname)/
```

PHASE 4 (55-75 Minutes) - Containment & Recovery

FINAL PHASE CHALLENGES

- **Active Exfiltration**: Data leaving the network
- **Persistent Access**: Cron jobs maintaining access
- **Safety Systems**: Critical infrastructure at risk
- **Evidence Requirements**: Legal and regulatory needs

CONTAINMENT DECISIONS

1. **Isolation vs Monitoring**: Block or observe?
2. **Service Restoration**: What can be safely restored?
3. **Evidence Preservation**: What must be kept intact?
4. **Communication**: What to report to other teams?

ESSENTIAL FINAL DOCUMENTS

- `Manual_Override_Authorisation.pdf` - System override procedures
- `Forensics Summary Template.pdf` - Investigation summary
- `Ops After-Action Checklist.pdf` - Technical debrief
- All previous documents remain relevant

CONTAINMENT PROCEDURES

```
# Network Isolation (COORDINATE WITH OPS FIRST)
iptables -I INPUT -s <suspicious_ip> -j DROP
iptables -I OUTPUT -d <suspicious_ip> -j DROP

# Service Isolation
systemctl stop <compromised_service>
systemctl disable <compromised_service>
chmod 000 /path/to/suspicious/binary

# Cron Job Neutralisation
chmod 000 /etc/cron.d/suspicious_job
mv /etc/cron.d/suspicious_job /evidence/

# Log Preservation
rsync -av /var/log/ /evidence/logs_$(date +%Y%m%d_%H%M%S)/
```

RECOVERY PRIORITIES

1. **Safety Systems**: CCTV and monitoring
2. **Core Operations**: AIS and navigation
3. **Business Systems**: Scheduling and routing
4. **Support Systems**: Non-critical services

SYSTEM-SPECIFIC INVESTIGATION GUIDES

VM-GATEWAY INVESTIGATION

```
# Check vendor access logs
grep -E "vendor|temp_session|ghost" /var/log/gateway/*.log
# Look for privilege escalation
grep -E "sudo|su -|root" /var/log/auth.log
# Check for trap scripts
ls -la /opt/security/
```

VM-CORETECH INVESTIGATION

```
# AIS system checks
tail -f /var/log/sim/ais_feed.log
grep -i "filter\|coordinate" /etc/ais-tracker/config.conf
# Container routing
grep "CON4489[12]" /var/log/container/scheduler.log
```

VM-OPSNODE INVESTIGATION

```
# CCTV system analysis
tail -100 /var/log/cctv/stream.log
find /var/cctv/archive -name "*.ts" -mtime -1
# RF interference patterns
grep -i "interference\|jitter" /var/log/cctv/*.log
```

COORDINATION & REPORTING

INFORMATION TO SHARE

With Operations: - System availability status - Safety system integrity - Recovery time estimates

With Legal: - Evidence preservation status - Regulatory compliance data - Incident timeline

With Executive: - Technical summary (non-technical language) - Business impact assessment - Recovery recommendations

With Incident Coordinator: - Complete technical timeline - System interdependencies - Resource requirements

REPORTING TEMPLATES

```
SYSTEM STATUS REPORT
Time: [timestamp]
System: [name]
Status: [Operational/Degraded/Failed]
Evidence: [Preserved/At Risk]
Recovery: [Immediate/Hours/Days]
Notes: [Key findings]
```

CRITICAL WARNINGS & REMINDERS

DO NOT

- Execute unknown scripts found during investigation
- Delete or modify evidence
- Restart services without coordination
- Share passwords or access credentials
- Speculate on attribution

ALWAYS

- Preserve evidence before investigation
- Document every action with timestamps

- Coordinate with Operations on isolation
- Report trap scripts to all teams
- Maintain chain of custody

ESCALATION TRIGGERS

- Safety system compromise
- Active data exfiltration
- Evidence deletion attempts
- Multiple system coordination
- Regulatory notification requirements

QUICK COMMAND REFERENCE

Evidence Commands

```
sha256sum [file] > hash.txt          # Generate hash
tar czf evidence.tar.gz /path/       # Archive evidence
dd if=/dev/sda of=disk.img           # Disk image
```

Analysis Commands

```
strings [binary] | less              # Extract text
ldd [binary]                         # Check dependencies
strace -p [pid]                      # System call trace
```

Network Commands

```
netstat -tulpn                       # Network connections
ss -tulpn                            # Socket statistics
iptables -L -n                       # Firewall rules
```

Remember: Your primary mission is to preserve evidence, identify threats, and support safe system recovery. When in doubt, preserve evidence and coordinate with other teams.