Contents

SOUTHGATE TERMINAL

## Port Operations Security Documentation

ADDITION TO: Technical Containment Guide.docx

INSERT LOCATION: Add as new section after existing containment procedures

SECTION TITLE: Log Deletion Investigation SOP

Log Deletion Investigation SOP

Purpose

This procedure provides systematic investigation steps for suspected or confirmed log deletion events, preserving evidence and determining scope of potential security compromise. Use when system logs appear missing, modified, or deliberately deleted.

When to Use

- System alerts indicating log file deletion
- Missing logs during routine security reviews
- Gaps in log timelines correlating with incidents
- Evidence of unauthorised access to log files

- System administrators reporting log anomalies

Immediate Response (First 10 minutes)

Step 1: Incident Confirmation

1. **Alert Verification**

☐ Confirm log deletion alert is genuine
☐ Identify specific log files or systems affected
☐ Note exact time of deletion detection

2. **System Status Check**

☐ Verify affected systems are still operational
☐ Check if logging services are currently functioning
☐ Assess immediate security posture

3. **Initial Scope Assessment**

☐ Determine which log types were deleted (auth, system, application)
☐ Identify time range of missing logs
☐ Check for patterns or systematic deletion

Step 2: Evidence Preservation

1. **System Isolation Assessment**

☐ Determine if affected system should be isolated
☐ Consider operational impact of isolation
☐ Document decision rationale

2. **Immediate Evidence Capture**

☐ Take system snapshots before any changes
☐ Preserve current log status and configurations
☐ Document system state with timestamps

3. **Chain of Custody Initiation**

☐ Begin forensic evidence log
☐ Assign evidence custodian
☐ Restrict system access to authorised investigators

Investigation Phase (10-45 minutes)

System Analysis

1. **Log System Configuration Review**

☐ Check log rotation settings and schedules
☐ Verify log retention policies and implementation
☐ Review recent configuration changes

2. **Access Log Analysis**

☐ Review authentication logs for unusual access
☐ Check for administrative access during deletion timeframe
☐ Identify users with log file access permissions

3. **Command History Review**

☐ Check bash/shell history for deletion commands
☐ Review sudo logs for privileged operations
☐ Analyse cron jobs or scheduled tasks

Deletion Pattern Analysis

1. **Systematic vs. Targeted Deletion**

- **Systematic:** All logs deleted = likely cover-up of extensive activity
- **Targeted:** Specific logs deleted = attempt to hide particular actions
- **Time-based:** Logs from specific period = incident-related deletion

2. **Deletion Method Analysis**

☐ Standard deletion commands (rm, del)
☐ Secure deletion tools (shred, wipe)
☐ Log rotation manipulation
☐ Service configuration changes

3. **Timeline Correlation**

☐ Compare deletion time with other security events
☐ Check correlation with system anomalies
☐ Analyse relationship to operational incidents

Technical Investigation

File System Analysis

1. **Deleted File Recovery Attempts**

☐ Check for recoverable deleted files
☐ Review system trash/recycle bins
☐ Attempt forensic file recovery if appropriate

2. **File System Metadata Analysis**

☐ Check file creation/modification timestamps

☐ Review file permission changes
☐ Analyse disk space usage patterns

3. **Backup and Archive Review**

☐ Check if deleted logs exist in backups
☐ Review archive systems for log copies
☐ Verify backup integrity and availability

Network and Remote Access Analysis

1. **Remote Access Review**

☐ Check VPN connections during deletion timeframe
☐ Review remote desktop or SSH sessions
☐ Analyze network connections to log systems

2. **External Communication**

☐ Check for data exfiltration attempts
☐ Review outbound network traffic
☐ Analyse communication to external systems

Evidence Recovery and Reconstruction

Alternative Log Sources

1. **Centralized Logging Systems**

☐ Check SIEM or centralized log servers
☐ Review log forwarding configurations
☐ Verify remote log copies

2. **Application and Service Logs**

☐ Review application-specific logs
☐ Check database audit logs
☐ Analyse service-specific logging

3. **Network Device Logs**

☐ Review firewall and router logs
☐ Check network switch logs
☐ Analyse intrusion detection system logs

Timeline Reconstruction

1. **Event Correlation**

☐ Correlate available logs with incident timeline
☐ Map user activities before deletion
☐ Identify gaps requiring investigation

2. **Activity Pattern Analysis**

☐ Analyse normal vs. anomalous activity patterns
☐ Identify unusual system or user behavior
☐ Document potential indicators of compromise

Classification and Escalation

Incident Classification

1. **Accidental Deletion**

- **Indicators:** Admin error, legitimate maintenance, single user
- **Response:** Standard incident procedures, improved controls

2. **Insider Threat**

- **Indicators:** Deliberate deletion by authorised user, selective targeting
- **Response:** HR coordination, enhanced monitoring, possible termination

3. **External Compromise**

- **Indicators:** Unauthorised access, systematic deletion, correlation with other attacks
- **Response:** Cyber team escalation, potential law enforcement, full investigation

Escalation Criteria **IMMEDIATE ESCALATION TO CYBER TEAM IF:** - [ ] Evidence of unauthorised access to log systems - [ ] Systematic deletion suggesting cover-up of extensive activity - [ ] Correlation with other confirmed security incidents - [ ] Critical security logs deleted (authentication, privileged access)

EXECUTIVE ESCALATION IF: - [ ] Evidence suggests insider threat or malicious intent - [ ] Regulatory compliance implications identified - [ ] Potential law enforcement involvement required

Recovery and Remediation

Immediate Recovery Actions

1. **Log Service Restoration**

☐ Restore logging services to full operation
☐ Implement enhanced logging if available
☐ Verify log integrity mechanisms

2. **Access Control Review**

☐ Review and restrict log file access permissions
☐ Implement enhanced monitoring for log files
☐ Consider log file immutability solutions

Long-term Improvements

1. **Enhanced Logging Strategy**

☐ Implement centralized logging with remote storage
☐ Add log integrity checking mechanisms
☐ Enhance log retention and backup procedures

2. **Monitoring and Alerting**

☐ Implement real-time log deletion monitoring
☐ Add file integrity monitoring for critical logs
☐ Enhance alerting for suspicious log access

Communication Protocols

To Technical Team "Log deletion incident confirmed on [system]. Scope: [description]. Investigation status: [in progress/completed]. Technical coordination needed for: [specific requirements]."

To Incident Coordinator "SECURITY ALERT: Log deletion detected. Classification: [accidental/insider/external]. Investigation timeline: [estimate]. Escalation requirements: [none/cyber team/executive]."

To Executive (if required) "Critical security incident: Deliberate log deletion detected. Potential implications: [regulatory/legal/operational]. Investigation underway. External assistance: [required/not required]."

Documentation Requirements

Investigation Log

☐ Timeline of all investigation activities
☐ Evidence collected and chain of custody
☐ Analysis results and conclusions
☐ Recommendations for prevention

Technical Report

☐ Detailed technical findings
☐ Recovery actions taken
☐ System configuration changes

☐ Lessons learned and improvements

Success Criteria

- Complete investigation of log deletion incident
- Maximum evidence recovery and preservation
- Accurate classification of incident type and intent
- Appropriate escalation and response actions taken
- Preventive measures implemented to reduce future risk

Related Procedures

- Use with: Breach Classification Decision Tree (for incident categorisation)
- Coordinate with: Network Diagnostics SOP (if network compromise suspected)
- Reference: Forensics Summary Template (for evidence documentation)
- Escalate to: Crisis Decision Authority Matrix (for executive decisions)