Network Security Incident Response

Overview

This document provides comprehensive procedures for identifying, containing, and resolving network security incidents to protect organizational assets and data.

Purpose

- Rapidly identify and respond to security threats
- Minimize impact and damage from security incidents
- Preserve evidence for forensic analysis
- Ensure compliance with regulatory requirements
- Maintain business continuity during incidents

Incident Classification

Severity Levels

Level	Description	Response Time	Examples
Critical	Immediate threat to business operations	15 minutes	Data breach, ransomware, critical system compromise
High	Significant security risk	1 hour	Malware outbreak, unauthorized access, DDoS attack
Medium	Moderate security concern	4 hours	Suspicious network activity, policy violations
Low	Minor security issue	24 hours	Failed login attempts, minor policy violations

Response Process

1. Detection and Analysis (0-30 minutes)

- **Initial Alert**: Security tools, user reports, or monitoring systems
- **Triage Assessment**: Determine incident severity and classification
- **Evidence Collection**: Preserve logs, screenshots, and system states
- **Impact Assessment**: Evaluate affected systems and potential data exposure

Detection Sources

- SIEM alerts and monitoring tools
- Antivirus and endpoint detection systems
- Network intrusion detection systems (IDS)
- User reports and help desk tickets
- Automated security scanning tools

2. Containment (30 minutes - 2 hours)

- **Immediate Actions**:
  - Isolate affected systems from network
  - Disable compromised user accounts
  - Block malicious IP addresses and domains
  - Preserve system images for forensic analysis

Short-term Containment

- Network segmentation and traffic blocking
- System isolation and quarantine
- Account lockouts and password resets
- Temporary workarounds for business continuity

Long-term Containment

- System patching and security updates
- Enhanced monitoring and logging
- Additional access controls and restrictions
- Temporary security measures implementation

3. Eradication (2-8 hours)

- **Threat Removal**:
  - Remove malware and malicious files
  - Close security vulnerabilities
  - Apply security patches and updates
  - Strengthen security configurations
- **System Hardening**:
  - Update security policies and procedures
  - Implement additional security controls
  - Enhance monitoring and detection capabilities
  - Review and update access permissions

4. Recovery (4-24 hours)

- **System Restoration**:
  - Restore systems from clean backups
  - Rebuild compromised systems
  - Implement security improvements
  - Gradual return to normal operations
- **Validation Steps**:
  - Security testing and validation
  - Functionality verification
  - Performance monitoring
  - User access testing

5. Lessons Learned (1-2 weeks post-incident)

- **Post-Incident Review**:
  - Timeline analysis and documentation
  - Response effectiveness evaluation
  - Process improvement recommendations
  - Training and awareness updates

Incident Response Team

Core Team Members

Role	Responsibilities	Contact
Incident Commander	Overall response coordination	security-lead@company.com
Security Analyst	Technical analysis and investigation	security-team@company.com
Network Engineer	Network isolation and containment	network-team@company.com
System Administrator	System recovery and restoration	sysadmin@company.com
Legal Counsel	Regulatory compliance and notifications	legal@company.com
Communications Lead	Internal and external communications	comms@company.com

Escalation Contacts

- **CISO**: +1-800-SEC-EXEC
- **IT Director**: +1-800-IT-LEAD
- **Legal**: +1-800-LEGAL-01
- **External Security Firm**: +1-800-SEC-HELP

Communication Procedures

Internal Communications

- **Immediate**: Security team and incident commander
- **30 minutes**: IT leadership and affected department heads
- **1 hour**: Executive leadership and legal team
- **2 hours**: All staff (if organization-wide impact)

External Communications

- **Regulatory Bodies**: Within 72 hours (GDPR requirement)
- **Law Enforcement**: If criminal activity suspected
- **Customers/Partners**: As required by contracts and regulations
- **Media**: Only through designated spokesperson

Tools and Resources

Security Tools

- **SIEM Platform**: Splunk, IBM QRadar, or Microsoft Sentinel
- **Endpoint Detection**: CrowdStrike, Carbon Black, or Microsoft Defender
- **Network Monitoring**: Wireshark, SolarWinds, or PRTG
- **Forensic Tools**: EnCase, FTK, or Volatility
- **Communication**: Microsoft Teams or Slack for coordination

Documentation Templates

- Incident tracking spreadsheet
- Evidence collection forms
- Timeline documentation template
- Post-incident report template
- Regulatory notification templates

Compliance and Reporting

Regulatory Requirements

- **GDPR**: Data breach notification within 72 hours
- **HIPAA**: Security incident documentation and reporting
- **SOX**: Financial system security incident reporting
- **PCI DSS**: Payment card data security incident procedures

Documentation Requirements

- Detailed incident timeline
- Evidence collection and chain of custody
- Response actions taken
- Impact assessment and damages
- Lessons learned and improvements

Training and Preparedness

Regular Activities

- **Monthly**: Security awareness training
- **Quarterly**: Incident response tabletop exercises
- **Annually**: Full-scale incident response simulation
- **Ongoing**: Security tool training and certification

Knowledge Areas

- Threat landscape and attack vectors
- Security tool operation and management
- Forensic analysis techniques
- Legal and regulatory requirements
- Communication and coordination skills

Best Practices

1. **Prepare in Advance**: Maintain updated contact lists and procedures
2. **Act Quickly**: Time is critical in security incident response
3. **Document Everything**: Maintain detailed logs and evidence
4. **Communicate Clearly**: Keep stakeholders informed appropriately
5. **Learn and Improve**: Use incidents to strengthen security posture

---

Last Updated: September 2025
Document Owner: Information Security Team