Test Corp
Incident Response Plan

Computer Security Incident Handling Guide

Inspired by the recommendations of the
National Institute of Standards and Technology
(NIST SP 800-61)

Organization:	Test Corp
Industry:	Technology
Generated Date:	2026-01-31
Version:	1.0

Table of Contents

Appendices

1. Introduction

1.1 Context

Cyber security relates to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat.

It is commonly recognized that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through the alignment of people, processes and tools.

This document supports **Test Corp** in managing contemporary cyber threats and incidents. The application of this document will support the organization in reducing the scope, impact and severity of cyber incidents.

1.2 Purpose and Scope

This publication seeks to assist Test Corp in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program, with the primary focus on detecting, analyzing, prioritizing, and handling incidents.

1.3 Audience

This document has been created for:

- Computer Security Incident Response Teams (CSIRTs)
- System and Network Administrators
- Security Staff
- Technical Support Staff
- Chief Information Security Officers (CISOs)
- Chief Information Officers (CIOs)
- Computer Security Program Managers

1.4 Infrastructure Environment

Primary Infrastructure: AWS

The organization primarily operates on Amazon Web Services (AWS) cloud infrastructure. Incident response procedures should account for AWS-specific services, logging (CloudTrail, CloudWatch), and remediation tools.

2. Organizing a Computer Security Incident Response Capability

2.1 What is a Computer Security Incident?

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents include:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
- Users are tricked into opening malware disguised as a "quarterly report" sent via email
- An attacker obtains sensitive data and threatens to release it publicly unless a ransom is paid
- A user provides or exposes sensitive information through peer-to-peer file sharing services
- Unauthorized access to systems or data
- Denial of Service (DoS) attacks
- Malware infections

2.2 Need for Incident Response

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. Benefits of having an incident response capability include:

- Systematic response following a consistent incident handling methodology
- Minimized loss or theft of information
- Reduced disruption of services
- Maintained stakeholder confidence
- Compliance with regulatory requirements

2.3 Incident Response Team Structure

2.3.1 Team Leadership

Incident Commander: John Doe

The Incident Commander is responsible for:

- Overall coordination of incident response activities
- Making critical decisions during incidents
- Communicating with executive leadership
- Ensuring proper resource allocation

2.3.2 SOC Analysts

The following personnel are responsible for security monitoring and initial incident analysis:

Jane Smith

2.3.3 Infrastructure & Cloud Remediation

Remediation Owner: Bob Wilson

Responsible for:

- Implementing containment measures
- Executing eradication procedures
- Coordinating system recovery
- Infrastructure-level security changes

2.3.4 Legal & Compliance Coordination

Legal/Compliance Owner: Alice Brown

Responsible for:

- Regulatory notification requirements
- Legal implications assessment
- Evidence preservation for potential litigation
- Compliance documentation

2.4 Incident Response Team Services

The incident response team provides the following services:

- **Intrusion Detection:** Monitoring for and analyzing potential security incidents

- **Advisory Distribution:** Disseminating information about new vulnerabilities and threats
- **Education and Awareness:** Training users on security best practices
- **Information Sharing:** Participating in threat intelligence sharing groups

3. Handling an Incident

The incident response process consists of several phases: **Preparation**, **Detection and Analysis**, **Containment, Eradication, and Recovery**, and **Post-Incident Activity**.

3.1 Preparation

Preparation involves establishing an incident response capability and preventing incidents through proper security controls.

3.1.1 Incident Handler Communications and Facilities

- Contact information for team members and external parties
- On-call information and escalation procedures
- Incident reporting mechanisms (phone, email, online forms)
- Issue tracking system for incident management
- Secure communication channels (encrypted messaging)
- War room or virtual collaboration space
- Secure evidence storage facility

3.1.2 Incident Analysis Hardware and Software

- Digital forensic workstations and backup devices
- Laptops for data analysis and report writing
- Spare workstations, servers, and networking equipment
- Packet sniffers and protocol analyzers
- Digital forensic software
- Evidence gathering accessories

3.1.3 Preventing Incidents

- **Risk Assessments:** Periodic assessment of threats and vulnerabilities
- **Host Security:** System hardening using standard configurations
- **Network Security:** Perimeter configured to deny unauthorized activity

- **Malware Prevention:** Anti-malware deployed at host and network levels
- **User Awareness and Training:** Regular security awareness training

3.2 Detection and Analysis

3.2.1 Attack Vectors

Common attack vectors include:

Attack Vector	Description
External/Removable Media	Attacks from USB drives or peripheral devices
Attrition	Brute force attacks, DDoS
Web	Attacks via websites or web applications
Email	Phishing, malicious attachments
Impersonation	Spoofing, man-in-the-middle attacks
Improper Usage	Policy violations by authorized users
Loss/Theft	Lost or stolen devices or media

3.2.2 Signs of an Incident

Indicators that may suggest an incident:

- Network intrusion detection alerts
- Antivirus alerts
- Unusual filenames or system changes
- Unauthorized configuration changes
- Multiple failed login attempts
- Suspicious email activity
- Unusual network traffic patterns

3.2.3 Incident Analysis Recommendations

- Profile networks and systems to identify deviations
- Understand normal behavior patterns
- Create and follow a log retention policy
- Perform event correlation across multiple sources
- Keep all host clocks synchronized (NTP)
- Maintain a knowledge base of information
- Use search engines for research
- Run packet sniffers when additional data is needed

3.2.4 Incident Prioritization

Test Corp uses the following incident severity levels:

Priority	Level	Description	Response Time
P1	**Critical**	Severe business impact, critical systems affected	Immediate (15-30 min)
P2	**High**	Significant business impact, multiple systems	Within 1-2 hours

Severity Determination Criteria:

Based on impact

3.2.5 Incident Notification

Escalation Matrix:

P1 goes to CTO

Communication Channels:

The following channels are used during incident response:

- Email
- Slack

Critical Incident Notification List:

CEO, CTO

3.3 Containment, Eradication, and Recovery

3.3.1 Choosing a Containment Strategy

Containment is critical before an incident overwhelms resources or increases damage. Criteria for selecting a containment strategy:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability requirements
- Time and resources needed to implement
- Effectiveness of the strategy
- Duration of the solution

3.3.2 Evidence Gathering and Handling

Test Corp maintains forensic evidence during security incidents.

Evidence Storage Location: Secure vault

Evidence handling requirements:

- Document how all evidence is preserved
- Collect evidence according to procedures meeting applicable laws
- Maintain chain of custody documentation
- Keep detailed evidence logs including:
    - Identifying information (serial numbers, IP addresses, hostnames)
    - Name and contact of each individual handling evidence
    - Time and date of each evidence handling occurrence
    - Storage locations

3.3.3 Identifying the Attacking Hosts

Activities for attacking host identification:

- Validating the attacking host's IP address

- Researching the attacking host through search engines
- Using incident databases and threat intelligence
- Monitoring possible attacker communication channels

3.3.4 Eradication and Recovery

Eradication involves eliminating incident components:

- Deleting malware
- Disabling breached user accounts
- Identifying and mitigating exploited vulnerabilities
- Identifying all affected hosts for remediation

Recovery involves restoring systems to normal operation:

- Restoring systems from clean backups
- Rebuilding systems from scratch if necessary
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security
- Implementing enhanced monitoring

3.4 Post-Incident Activity

3.4.1 Lessons Learned

Test Corp conducts post-incident reviews after security incidents.

A lessons learned meeting should be held within several days of incident closure to address:

- What exactly happened and at what times?
- How well did staff and management perform?
- Were documented procedures followed?
- Were the procedures adequate?
- What information was needed sooner?

- Were any steps or actions taken that might have inhibited recovery?
- What would staff and management do differently next time?
- How could information sharing with other organizations be improved?
- What corrective actions can prevent similar incidents?
- What precursors or indicators should be watched for in the future?
- What additional tools or resources are needed?

3.4.2 Using Collected Incident Data

Metrics for incident-related data:

- Number of incidents handled
- Time per incident (detection, containment, recovery)
- Objective analysis of incident handling effectiveness
- Subjective assessment by team members

3.4.3 Evidence Retention

Factors for evidence retention policy:

- Potential for prosecution
- Data retention requirements
- Storage costs
- Regulatory requirements

3.4.4 Incident Handling Checklist

Phase	Action	Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	□
1.1	Analyze precursors and indicators	□
1.2	Look for correlating information	□
1.3	Perform research	□
1.4	Begin documenting investigation and gathering evidence	□
2.	Prioritize handling based on relevant factors	□
3.	Report to appropriate personnel and organizations	□
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	□
5.	Contain the incident	□
6.	Eradicate the incident	□
6.1	Identify and mitigate exploited vulnerabilities	□
6.2	Remove malware and inappropriate materials	□
6.3	Repeat detection steps if additional affected hosts discovered	□
7.	Recover from the incident	□
7.1	Return systems to operationally ready state	□
7.2	Confirm systems are functioning normally	□

Phase	Action	Completed
7.3	Implement additional monitoring if necessary	□
Post-Incident Activity		
8.	Create a follow-up report	□
9.	Hold a lessons learned meeting	□

4. Coordination and Information Sharing

4.1 Coordination

The incident response team may need to interact with:

- Other incident response teams within the organization
- Law enforcement agencies
- Internet service providers
- External vendors and partners
- Industry-specific ISACs (Information Sharing and Analysis Centers)

4.2 Information Sharing Techniques

4.2.1 Ad Hoc

Traditional information sharing through email, instant messaging, and phone calls using established relationships with peers.

4.2.2 Partially Automated

Where possible, automate information sharing while maintaining human oversight for sensitive decisions.

4.2.3 Security Considerations

- Designate who can see which pieces of incident information
- Perform data sanitization to remove sensitive information
- Protect information shared by other organizations

4.3 Granular Information Sharing

4.3.1 Business Impact Information

Share business impact information only with parties that have interest in the organization's mission (typically coordinating teams).

4.3.2 Technical Information

Technical indicators include:

- Hostnames and IP addresses of attacking hosts
- Malware samples
- Indicators of compromise (IOCs)
- Vulnerability information

Appendix A: Situation Update Template

Field	Value
Date of Entry	
Time of Entry	
Author	
Date/Time Incident Detected	
Current Status	New / In Progress / Resolved
Incident Type	
Incident Classification	Incident / Significant Incident / Emergency
Scope	(affected networks, systems, applications)
Impact	(affected stakeholders)
Severity	
Notifications Actioned/Pending	
Additional Notes	
Incident Manager Contact	
Next Update	

Appendix B: Resolution Action Plan Template

Date/ Time	Category	Action	Owner	Status
	Contain / Eradicate / Recover / Communications			Unallocated / In Progress / Closed

Appendix C: Evidence Register Template

Date, Time, Location of Collection	Collected By	Item Details	Storage Location	Access Log
	(name, title, contact, phone)	(quantity, serial number, model, hostname, MAC, IP)	(location, label number)	(date, time, person, rationale)

Appendix D: Assets and Key Contacts

Site Information

Category	Details
IP Subnet	
DHCP Scope	
Core Router IP	
DNS Servers (Internal)	
DNS Name / Logs & Location	

Internet Connection / Communications

Category	Details
Internet Service Provider	
Network Provider	
VoIP/PABX Phone System	
Fixed Line Services	
Mobile Data Services	

Firewall & Security

Category	Details
Firewall Software/Hardware	
Wired Network	
Wireless Network	

Key Contacts

Role	Name	Contact
Incident Commander	John Doe	
Cloud/Infrastructure Remediation	Bob Wilson	
Legal/Compliance	Alice Brown	

Appendix E: Glossary

Term	Definition
Baselining	Monitoring resources to determine typical utilization patterns so that significant deviations can be detected
CSIRT	Computer Security Incident Response Team - a capability set up for assisting in responding to computer security-related incidents
Event	Any observable occurrence in a network or system
False Positive	An alert that incorrectly indicates that malicious activity is occurring
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Incident Handling	The mitigation of violations of security policies and recommended practices
Indicator	A sign that an incident may have occurred or may be currently occurring
IDPS	Intrusion Detection and Prevention System - software that monitors events for signs of possible incidents
Malware	A virus, worm, Trojan horse, or other code-based malicious entity
Precursor	A sign that an attacker may be preparing to cause an incident
Profiling	Measuring the characteristics of expected activity so that changes can be more easily identified
Signature	A recognizable, distinguishing pattern associated with an attack
Social Engineering	An attempt to trick someone into revealing information
Threat	The potential source of an adverse event
Vulnerability	

Term	Definition
	A weakness in a system, application, or network that is subject to exploitation or misuse

This document was generated by ResponseForge on 2026-01-31 at 13:04:44.

Based on NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide