INTERNEE.PK

Cyber Security Internship Program

BATCH 2026

INCIDENT RESPONSE PLAN

Ransomware Simulation & Defense Protocols

PREPARED BY:
Muhammad Hamza Hayat
Cyber Security Intern

SUBMITTED TO:
Internee.pk Management
Security Operations Center (SOC)

Date: February 25, 2026
Version: 1.0

COMPLIANCE STATEMENT

his document adheres to **NIST SP 800-61 Rev. 2** standards for Computer Security Incident Handling.

1.0 Executive Summary

The purpose of this **Cyber Incident Response Plan (CIRP)** is to provide a structured framework for handling cybersecurity incidents at **Internee.pk**. By defining clear roles and pre-approved procedures, we aim to reduce the *Mean Time to Respond (MTTR)* and minimize the impact of security incidents on business operations.

2.0 Scope of Applicability

This plan applies to all systems, networks, and data owned or operated by the organization.

- **Infrastructure:** Workstations, Servers (Windows/Linux), and Network Devices.
- **Cloud Assets:** AWS Instances, S3 Buckets, and Hosted Databases.
- **Users:** All employees, contractors, and interns with network access.

3.0 Incident Response Team (IRT)

A clearly defined chain of command is critical during a crisis. The following roles constitute the authorized IRT.

ROLE	RESPONSIBILITIES
Incident Commander	Highest authority. Coordinates response, approves containment strategies, and manages stakeholder communication.
Lead Security Analyst	Technical Lead. Investigates logs (SIEM/Wazuh), identifies root causes, and determines breach scope.
IT Operations Lead	Execution. Performs system isolation, password resets, firewall blocking, and backup restoration.

Authority to Act

The **Incident Commander** is authorized to sever network connections to the internet without prior approval if a critical threat is detected spreading laterally.

4.0 Incident Severity Matrix

To ensure efficient resource allocation, all incidents must be classified upon detection. This matrix determines the urgency and escalation path.

SEVERITY	CRITERIA	RESPONSE
CRITICAL	Widespread Ransomware, Data Breach of PII, or Total Service Outage.	Immediate (24/7)
HIGH	Targeted malware on a server or unauthorized admin access.	Within 1 Hour
MEDIUM	Isolated virus on a workstation or suspicious login attempts.	Within 4 Hours
LOW	Spam, Adware, or minor policy violations.	Next Business Day

5.0 Detection & Analysis Procedures

The goal of this phase is to confirm whether a security event is a true incident or a false positive.

5.1 Detection Sources

Internee.pk utilizes the following sources for initial detection:

- **SIEM Alerts:** Monitoring Wazuh agents for file integrity and log anomalies.
- **Endpoint Security:** Antivirus and EDR alerts on workstations.
- **User Reporting:** Employees reporting suspicious emails or system behavior.

5.2 Verification Steps

Upon receiving an alert, the Lead Security Analyst must:

1. **Analyze:** Review timestamps, source IPs, and user accounts involved.
2. **Correlate:** Check if other systems are showing similar anomalies.
3. **Validate:** Determine if the activity is authorized (e.g., scheduled maintenance).

Pro Tip

Always assume a "Critical" severity for any alert involving multiple encrypted files until proven otherwise.

6.0 Ransomware Simulation Playbook

This section simulates a response to a high-impact ransomware attack. This playbook is designed to be executed immediately upon the detection of encryption artifacts.

6.1 Scenario Overview

- **Trigger:** A Wazuh File Integrity Monitor (FIM) alert detects rapid file extension changes (.crypt) on the Finance Server.
- **Initial Assessment:** 25% of files are encrypted; a ransom note is present on the desktop.

6.2 Phase 1: Containment (Stop the Spread)

1. **Network Isolation:** The IT Operations Lead must immediately disable the switch port or disconnect the virtual NIC of the infected server.
2. **Lateral Movement Check:** Block all SMB (Port 445) and RDP (Port 3389) traffic internally to prevent the ransomware from spreading.
3. **Endpoint Lockdown:** Force a global password reset for all Domain Admin accounts to prevent credential harvesting.

6.3 Phase 2: Eradication & Investigation

- **Root Cause Analysis:** Use Wazuh logs to identify the "Patient Zero" (the first machine infected).
- **Malware Removal:** Perform a full disk scan using offline tools. If the infection is deep, the system must be wiped and re-installed from a "Golden Image."

6.4 Phase 3: Recovery & Restoration

POLICY: RANSOM NON-PAYMENT

Internee.pk maintains a strict policy against paying ransoms. This prevents funding criminal activity and does not guarantee data recovery.

1. **Backup Validation:** Verify the integrity of the most recent offline backup (Veeam/AWS Snapshots).
2. **Incremental Restore:** Restore data to a "Clean Room" environment first to ensure no malware is hidden.
3. **Production Re-entry:** Gradually bring services back online while keeping monitoring levels at "Maximum" for 72 hours.

Note: All actions taken during this simulation must be logged in the Incident Chronology for post-mortem analysis.

7.0 Staff Training & Awareness

Human error is the leading cause of initial compromise. To support this IRP, **Internee.pk** shall conduct the following training modules for all staff.

7.1 Phishing Simulation

- **Frequency:** Quarterly unannounced simulations.
- **Objective:** Train users to identify suspicious senders, mismatched URLs, and urgent/threatening language.
- **Reporting:** Users are instructed to use the "Report Phishing" button rather than deleting the email.

7.2 Incident Reporting Protocol

In the event of suspicious system behavior (slow performance, disappearing files, or pop-ups), staff must:

1. **Stop:** Cease all activity on the device.
2. **Report:** Call the IT Helpdesk immediately.
3. **Do Not Shutdown:** Leave the machine on but disconnect the Ethernet cable (to preserve RAM artifacts for forensics).

8.0 Emergency Contact List

In a "Critical" severity incident, the following contacts are to be used for immediate escalation.

DEPARTMENT	PRIMARY CONTACT	PHONE / EXT
IT Security (SOC)	Lead Security Analyst	+92-XXX-XXXXXXX
Management	Incident Commander	+92-XXX-XXXXXXX
Cloud Provider	AWS Support (24/7)	1-800-AWS-HELP
Law Enforcement	FIA Cybercrime Wing	1991

END OF DOCUMENT

This plan shall be reviewed and updated annually or after any major security incident.

9.0 Post-Incident Report Template

This document must be completed within 72 hours of incident resolution. The goal is to identify root causes and improve future response capabilities.

9.1 Incident Summary

Describe the timeline, the systems affected, and the initial point of entry (e.g., Phishing, Unpatched Vulnerability).

9.2 Resolution & Recovery Actions

- **Containment Method:** _____
- **Backup Success:** [ ] Yes [ ] No (If no, why?)
- **Data Loss Status:** _____

9.3 Lessons Learned & Improvements

What went well?	What could be improved?

9.4 Corrective Action Plan

1. **Immediate Task:** _____
2. **Security Patching:** _____
3. **Staff Retraining Required:** [ ] Yes [ ] No

_____

Incident Commander Signature

Date: _____

References & Frameworks

- **MITRE ATT&CK:** Techniques T1486 (Data Encrypted for Impact) and T1566 (Phishing) were used to model the Ransomware Simulation.
- **NIST SP 800-61 Rev. 2:** Followed for the Incident Handling Lifecycle standards.
- **Internee.pk Internship Tasks:** Aligned with Wazuh deployment and secure cloud infrastructure projects.