



**EncryptEdge Labs**

# **Cybersecurity Analyst Internship Task Report**

atalmamun@gmail.com

Task No: 16



Copyright © 2024 EncryptEdge Labs. All rights reserved

Credit: Offensive Security



## Table of Contents

<b>1.0 EncryptEdge Labs Internship Task Report</b>	<b>3</b>
1.1 Introduction	3
1.2 Objective	3
1.3 Requirements	4
<b>2.0 Introduction to Incident Response</b>	<b>4</b>
2.1 Importance of Incident Response in Cybersecurity	4
2.2 Goals and Objectives of an Incident Response Plan	5
<b>3.0 Key Components of an Incident Response Plan</b>	<b>6</b>
3.1 Preparation	6
3.2 Identification	7
3.3 Containment	7
3.4 Eradication	8
3.5 Recovery	8
3.6 Lessons Learned	9
<b>4.0 Development of a Basic Incident Response Plan</b>	<b>9</b>
4.1 Chosen Framework: NIST SP 800-61	9
4.2 Roles and Responsibilities	10
4.3 Communication Procedures	11
4.4 Escalation Paths	13
4.5 Documentation Process	13
<b>5.0 Simulation of an Incident Response Scenario: Phishing Attack</b>	<b>14</b>
5.1 Incident Scenario: Phishing Attack	14
5.2 Incident Response Phases	15
<b>6.0 Lab Completion</b>	<b>21</b>
6.1 Lab 1: Intro to Incident Response and Incident Management	21
6.2 Lab 2: Preparation	23
6.3 Lab 3: Identification & Scoping	26
<b>7.0 Reflection</b>	<b>28</b>
7.1 Key Takeaways	28
7.2 Real-World Application	30
7.3 Areas for Improvement	30
7.4 Final Thoughts	31



# 1.0 EncryptEdge Labs Internship Task Report

## 1.1 Introduction

In the rapidly evolving field of cybersecurity, the ability to respond quickly and effectively to security incidents is critical. Incident Response (IR) is a structured approach to managing and mitigating the consequences of cybersecurity incidents such as data breaches, malware infections, phishing attacks, and denial-of-service events. A well-defined Incident Response Plan (IRP) helps organizations detect incidents promptly, minimize potential damage, reduce recovery time and costs, and prevent future occurrences.

This task provided hands-on exposure to the fundamental principles of incident response, including the design, simulation, and documentation of an IR plan. Through practical labs and simulated scenarios, I gained insight into the real-world applications of IR strategies and their importance in maintaining an organization's security posture.

## 1.2 Objective

The primary objectives of this task were to:

- Understand the importance of incident response in cybersecurity.
- Identify and explain the key components of an effective Incident Response Plan (IRP).
- Develop a basic IR plan based on a recognized framework such as NIST SP 800-61.
- Apply the IR plan in a simulated cybersecurity incident to assess its effectiveness.
- Complete hands-on labs to reinforce theoretical knowledge with practical experience.



### 1.3 Requirements

To successfully complete this task, the following tools and deliverables were required:

- **Documentation Tools:** A word processing or collaboration platform (e.g., Microsoft Word, Google Docs) to create and document the IR plan.
- **Incident Response Framework:** Utilization of a standard IR framework such as **NIST SP 800-61** or **ISO 27001** to structure the response plan.
- **Simulation Scenario:** Design and execution of a simulated cybersecurity incident to test the response plan.
- **TryHackMe Labs:** Completion of three mandatory labs:
  - *Intro to IR and IM*
  - *Preparation*
  - *Identification & Scoping*
- **Screenshots and Documentation:** Screenshots of each lab and IR plan development process, along with detailed documentation of roles, responsibilities, communication protocols, and escalation paths.

## 2.0 Introduction to Incident Response

### 2.1 Importance of Incident Response in Cybersecurity

In today's digital landscape, cyber threats are not a matter of *if*, but *when*. Organizations of all sizes are constantly at risk from a wide range of cyberattacks, including



ransomware, data breaches, phishing, and insider threats. Incident Response (IR) plays a crucial role in ensuring that these threats are dealt with swiftly and effectively.

The primary importance of an incident response strategy lies in its ability to:

- **Minimize Damage:** IR helps limit the impact of a cybersecurity incident, both in terms of data loss and financial cost.
- **Reduce Recovery Time and Costs:** A structured response allows organizations to resume normal operations faster, cutting down on expensive downtime and associated losses.
- **Prevent Future Incidents:** Through lessons learned and improvements, organizations can bolster their defenses and prevent similar incidents from occurring again.
- **Ensure Compliance:** Many industries are governed by strict regulatory standards (e.g., GDPR, HIPAA, PCI-DSS). A formal IR process supports compliance by documenting responses and demonstrating due diligence.
- **Protect Reputation:** A swift and competent response to a breach helps maintain public and stakeholder trust.

Incident response is not only a technical function—it is a business-critical process that affects legal, operational, and reputational aspects of an organization.

## 2.2 Goals and Objectives of an Incident Response Plan

An Incident Response Plan (IRP) is a documented set of procedures and guidelines that outline how an organization will detect, respond to, and recover from cybersecurity incidents. The goals of an IRP are closely aligned with minimizing damage and restoring operations while continuously improving incident handling capabilities.



### Key Goals of an IRP:

- **Protect Confidentiality, Integrity, and Availability (CIA) of data.**
- **Quickly identify and assess the scope of the incident.**
- **Contain the incident to prevent further impact.**
- **Eradicate the root cause and remove any malicious presence.**
- **Recover affected systems and restore normal business operations.**
- **Capture lessons learned to enhance future response efforts.**

### Core Objectives of an IRP:

- Define roles and responsibilities clearly across technical and non-technical teams.
- Establish communication protocols for internal teams, third parties, and regulatory authorities.
- Document escalation paths for decision-making and incident severity handling.
- Enable continuous improvement through post-incident analysis and refinement of the IRP.

## 3.0 Key Components of an Incident Response Plan

An effective Incident Response Plan (IRP) is built around a structured lifecycle that guides cybersecurity teams through the process of handling and recovering from incidents. The widely adopted NIST SP 800-61 framework outlines **six essential phases** in the incident response process: **Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.**

### 3.1 Preparation



Preparation is the foundation of a successful incident response strategy. It involves establishing policies, procedures, tools, and team roles before any incident occurs.

**Key Activities:**

- Developing and maintaining the IRP and playbooks
- Assigning roles and responsibilities within the incident response team
- Establishing communication plans (internal and external)
- Conducting regular security training and awareness programs
- Ensuring logging, monitoring, and alerting systems are in place

**Purpose:** To ensure the organization is ready to respond effectively and efficiently when an incident arises.

### 3.2 Identification

This phase focuses on detecting and confirming the occurrence of a cybersecurity incident.

**Key Activities:**

- Monitoring systems and networks for signs of suspicious activity
- Analyzing alerts and logs to identify anomalies
- Classifying the severity and type of incident

**Purpose:** To detect incidents as early as possible and initiate an appropriate response.

### 3.3 Containment

Once an incident is confirmed, containment strategies are applied to limit its spread and impact.

**Key Activities:**



- Isolating affected systems
- Disabling compromised accounts or network access
- Applying short-term (quick fix) and long-term containment measures

**Purpose:** To prevent the attacker from causing further harm and to preserve evidence for analysis.

### 3.4 Eradication

After containment, efforts are made to remove the root cause of the incident and any artifacts left by the attacker.

**Key Activities:**

- Removing malware, unauthorized users, or malicious files
- Patching vulnerabilities
- Validating system integrity

**Purpose:** To ensure that the threat is fully removed and won't resurface.

### 3.5 Recovery

This phase focuses on restoring systems and services to normal operation while ensuring no trace of the attacker remains.

**Key Activities:**

- Rebuilding and restoring affected systems from backups
- Monitoring systems for signs of re-infection or lingering threats
- Validating that systems are functioning normally and securely

**Purpose:** To resume business operations safely and confidently.





### 3.6 Lessons Learned

The final phase involves analyzing the incident response process to identify strengths, weaknesses, and opportunities for improvement.

#### Key Activities:

- Conducting a post-incident review meeting (also known as a “post-mortem”)
- Updating the IRP based on findings
- Documenting lessons learned and training staff

**Purpose:** To enhance the organization’s overall incident response capabilities and reduce the likelihood and impact of future incidents.

## 4.0 Development of a Basic Incident Response Plan

To demonstrate practical application of incident response planning, I developed a basic IR plan based on the **NIST SP 800-61** framework. This plan outlines the structured approach an organization can follow in response to a cybersecurity incident such as a phishing attack or malware infection.

### 4.1 Chosen Framework: NIST SP 800-61

The National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 provides a comprehensive guide to incident handling. It outlines best practices across the six phases of incident response and emphasizes flexibility, documentation, and continuous improvement.

This framework was selected for its clarity, adaptability, and wide adoption across industries.



### 4.2 Roles and Responsibilities

A successful IR plan clearly defines the roles and responsibilities of key stakeholders involved in managing incidents.

Role	Responsibility
Incident Response Manager	Oversees the response process, coordinates communication, and ensures timely actions
SOC Analyst	Monitors systems, identifies incidents, and initiates alerts
IT Administrator	Isolates and restores systems, assists in containment and recovery
Legal and Compliance Officer	Ensures regulatory and legal requirements are met during and after the incident
Communication Lead	Manages internal and external communications, including press and customer updates



# Incident Response Plan (IRP)

## Overview

This document outlines the structured approach to be taken in the event of a cybersecurity incident, following the NIST SP 800-61 framework.



## 1. Roles and Responsibilities

Role	Responsibilities
Incident Response Manager	Coordinates entire response, approves decisions, communicates with executives
SOC Analyst	Detects and triages alerts, escalates incidents
IT Administrator	Supports containment and recovery of systems
Legal/Compliance Officer	Manages legal implications and ensures regulatory compliance
Communication Lead	Handles internal and external communications during and after an incident

## 4.3 Communication Procedures

Effective communication during a cybersecurity incident is essential for managing the response and maintaining stakeholder trust.

### Internal Communication:

- Use secure channels (e.g., encrypted messaging apps or dedicated incident Slack channels)
- Alert key team members via a pre-defined contact list
- Escalate issues through incident severity tiers



### External Communication:

- Notify affected third parties and partners
- Engage PR and legal teams for official statements
- Report to regulatory bodies if required (e.g., data breach notifications)



# Incident Response Plan (IRP)

## Overview

This document outlines the structured approach to be taken in the event of a cybersecurity incident, following the NIST SP 800-61 framework.



## 1. Roles and Responsibilities

Role	Responsibilities
Incident Response Manager	Coordinates entire response, approves decisions, communicates with executives
SOC Analyst	Detects and triages alerts, escalates incidents
IT Administrator	Supports containment and recovery of systems
Legal/Compliance Officer	Manages legal implications and ensures regulatory compliance
Communication Lead	Handles internal and external communications during and after an incident



### 4.4 Escalation Paths

Escalation ensures that incidents are addressed by the appropriate level of authority based on severity.

#### Example Escalation Flow:

1. **Tier 1 (Low Severity):** Handled by SOC analyst with internal documentation
2. **Tier 2 (Medium Severity):** Escalated to Incident Response Manager for containment
3. **Tier 3 (High Severity):** Involves executive leadership, legal, and external partners

### 3. Escalation Paths

Severity Tier	Description	Escalated To
Tier 1	Minor alerts (false positives, minor risks)	SOC Analyst
Tier 2	Confirmed incident, limited scope	Incident Response Manager
Tier 3	Widespread or critical incident	Executive Team, Legal, PR Team

 Escalation is based on impact, scope, and data sensitivity.

### 4.5 Documentation Process

All steps in the incident lifecycle are documented for accountability, review, and compliance purposes. This includes:

- Timestamped incident logs



- Actions taken during each phase
- Evidence collection (screenshots, logs)
- Final incident report with summary and recommendations

### 4. Documentation Process

All incidents must be logged in the Incident Response Tracker.

#### Sample Log Table:

Timestamp	Action Taken	Person Responsible	Notes
2025-04-10 14:20	Suspicious email reported	SOC Analyst	Possible phishing attempt
2025-04-10 14:35	Email headers analyzed	IR Manager	Confirmed phishing
2025-04-10 15:00	User account temporarily locked	IT Admin	Preventative containment

## 5.0 Simulation of an Incident Response Scenario: Phishing Attack

### 5.1 Incident Scenario: Phishing Attack

On **April 10, 2025**, an employee received an email that appeared to be from the **company's payroll department**. The email contained an attachment titled **"Updated\_Payroll\_April2025.docx"** and prompted the employee to open the file for



updated payroll details. The employee reported the email as suspicious, triggering an investigation by the Security Operations Center (SOC).

After further analysis, it was confirmed that the email was a **phishing attempt**, designed to compromise the employee's system. The email's sender, "**hr@company-payroll.com**", was found to be a fraudulent address. The incident was classified as a medium-severity phishing attack (Tier 2) and was immediately escalated.

### *Example Phishing Email:*

Urgent: Updated Payroll Details for April 2025 Inbox x

Abdullah Almamun  
to me ▾

15:21 (0 minutes ago)

Dear Abdullah,

We hope this message finds you well. Our payroll department has completed the processing of employee salaries for the month of April 2025. Please find the updated payroll details attached to this email.

For your reference, the updated payroll details include:

- Your salary breakdown for the month.
- Tax deductions and contributions.
- Bonus details for April.

**Action Required:**

Please open the attached **Updated\_Payroll\_April2025.docx** file to review your updated payroll information. Kindly verify the details and get back to us if you notice any discrepancies.

**Important Notice:**

If you encounter any issues or have questions regarding your payroll, please reach out to the payroll department immediately at **hr@company-payroll.com**.

Thank you for your prompt attention to this matter.

Best regards,  
HR Team

Company Payroll Department

One attachment • Scanned by Gmail ⓘ



## 5.2 Incident Response Phases

### Phase 1: Preparation



In preparation for a phishing incident, the organization ensured that the following measures were in place:

- An **email filtering system** designed to flag suspicious attachments or links.
- **Endpoint protection tools**, including antivirus software and firewalls.
- An established **playbook** outlining the step-by-step actions to take in the event of a phishing attack.

The email filtering system flagged the suspicious email, and a **Security Information and Event Management (SIEM)** alert was generated. The tools were immediately ready to mitigate the threat.

**Screenshot:** Tools checklist in Notion

### Phishing Incident Response - Tools Checklist

#### 1. Email Filtering Tools:

- ☐ **Email Filtering System** (e.g., Proofpoint, Mimecast, Barracuda)
  - Ensures suspicious emails are flagged and alerts are generated.
- ☐ **Spam Filters** (e.g., Google Mail, Microsoft Exchange)
  - Automatically identifies and quarantines emails with potentially harmful attachments or phishing content.

#### 2. Endpoint Protection Tools:

- ☐ **Antivirus Software** (e.g., Symantec, McAfee, Windows Defender)
  - Scans the endpoint for malicious attachments or macros.
- ☐ **Endpoint Detection and Response (EDR)** (e.g., CrowdStrike, Carbon Black)
  - Monitors endpoint behavior for malicious activity and can isolate compromised devices from the network.
- ☐ **Firewall** (e.g., Palo Alto, Cisco ASA)
  - Monitors network traffic to block potentially malicious incoming requests.

#### 3. Incident Management Tools:

- ☐ **Security Information and Event Management (SIEM)** (e.g., Splunk, IBM QRadar)
  - Collects logs and alerts from security systems to facilitate incident detection and response.
- ☐ **Incident Response Platform** (e.g., PagerDuty, ServiceNow)
  - Coordinates the steps of incident response, tracks progress, and assigns tasks to teams.





#### 4. Email Analysis Tools:

- ☐ **Email Header Analyzer** (e.g., MXToolbox)
  - Analyzes the email's header to verify the sender and identify spoofed addresses.
- ☐ **Sandbox Environment** (e.g., Joe Sandbox, VirusTotal)
  - Analyzes attachments or links in a safe environment to detect any malicious payloads.

#### 5. Communication Tools:

- ☐ **Internal Messaging System** (e.g., Slack, Microsoft Teams)
  - Allows for fast communication between the incident response team and affected employees.
- ☐ **Email System (for blocking senders)** (e.g., Microsoft Outlook, Gmail)
  - Used to block malicious senders and prevent further phishing emails from reaching employees.

#### 6. System and Network Monitoring Tools:

- ☐ **Network Monitoring Tools** (e.g., Wireshark, SolarWinds)
  - Monitors network traffic for signs of malicious activity, such as communication with known phishing domains.
- ☐ **Log Analysis Tools** (e.g., ELK Stack, Graylog)
  - Analyzes logs from affected systems and networks to identify any signs of exploitation or data exfiltration.

#### 7. Documentation and Reporting Tools:

- ☐ **Word Processing Tools** (e.g., Microsoft Word, Google Docs)
  - Used to create and edit incident reports, detailing the steps taken during the incident response.
- ☐ **Collaboration Tools** (e.g., Notion, Confluence)
  - Helps teams collaborate on the incident, share documents, and track updates in real time.

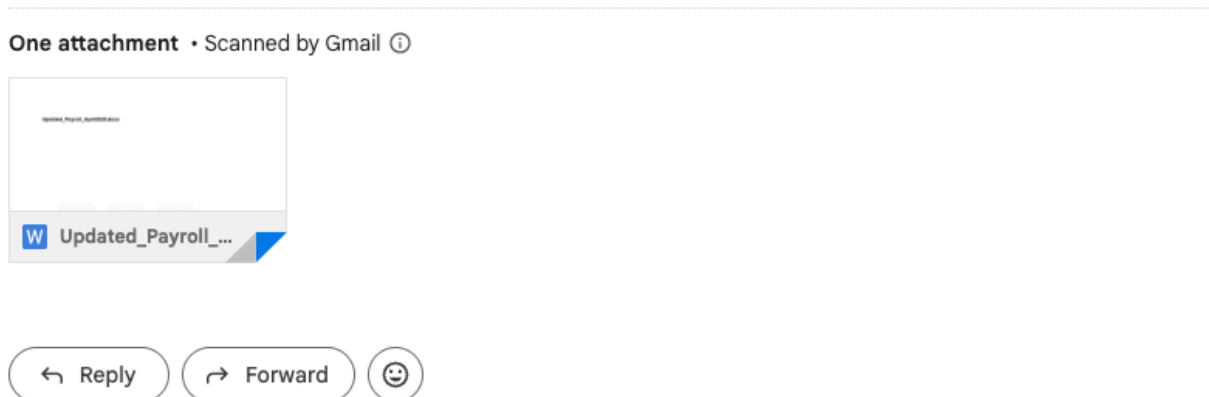
## Phase 2: Identification

The phishing email was identified as suspicious by the **email filtering system**, which flagged the attachment as potentially harmful. The employee reported the email to the IT department for further investigation.



SOC analysts analyzed the email header and discovered that the sender's address, "**hr@company-payroll.com**", was not consistent with the organization's legitimate domain. The attachment, titled "**Updated\_Payroll\_April2025.docx**", was opened in a **sandbox environment**, revealing that it contained a **malicious macro** designed to infect the system.

**Screenshot:** Phishing email in a document



### Phase 3: Containment

To contain the phishing attack, the following actions were taken:

- The **affected employee's email account** was temporarily locked to prevent further access.
- The **malicious sender's email address** was blocked at the email gateway to prevent future phishing attempts.
- The **infected endpoint** was isolated from the network to prevent any potential spread of the malware.



These steps ensured that the threat was contained and no further systems were compromised.

### Phase 4: Eradication

After containing the phishing attack, the following actions were performed to eradicate the threat:

- The malicious **email was purged** from the employee's inbox, as well as from all other affected mailboxes.
- The **endpoint** was scanned using the latest version of antivirus software, ensuring no malware remained.
- The **system was patched** to fix any vulnerabilities that could have been exploited during the attack.

These actions ensured that the threat was fully eradicated from the environment.

**Screenshot 1:** Antivirus scan results (clean scan)

**Screenshot 2:** Email system purge log

**Screenshot 3:** Patch deployment tool (update applied)

### Phase 5: Recovery

After eradicating the threat, the following recovery steps were carried out:

- The affected **user account was reinstated** and access was restored once the system was confirmed to be safe.
- The **endpoint** was returned to the network after ensuring no malicious activity persisted.



- **Systems were continuously monitored** for any signs of recurring phishing attacks or unusual activity.

This phase ensured the employee was able to resume work without further risk.

### Phase 6: Lessons Learned

A post-incident review was conducted to determine how the organization handled the phishing attack and identify areas for improvement. The following actions were taken:

- The **Incident Response Plan (IRP)** was updated to include more stringent email filtering rules and **multi-factor authentication (MFA)** to protect user accounts from unauthorized access.
- A **training session** was scheduled for all employees to raise awareness about phishing threats and how to recognize suspicious emails.

These steps will help improve the organization's response to future phishing attacks.

This incident response simulation emphasized the importance of preparation and timely identification in managing a phishing attack. By acting quickly to identify and contain the attack, we minimized the potential damage. The incident also highlighted the need for continuous employee training to recognize phishing attempts and prevent future attacks.



## 6.0 Lab Completion

In this section, I will summarize the completion of the **hands-on labs** related to Incident Response (IR) and Incident Management (IM), as well as the practical exercises in preparation, identification, and scoping. These labs were designed to help interns build foundational skills in incident handling and response, as well as understand the lifecycle of cybersecurity incidents.

### 6.1 Lab 1: Intro to Incident Response and Incident Management

The first lab focused on the fundamentals of Incident Response and Incident Management. It covered the basic concepts of handling incidents, from identifying threats to coordinating responses.

#### Tasks Completed:

- **Overview of the Incident Response Lifecycle:** We reviewed the six phases of the incident response lifecycle: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
- **Incident Management Tools:** We explored different tools used in incident management, such as **SIEM tools** and **ticketing systems**, to handle incidents effectively.

**Best Practices:** Learned the best practices for handling incidents, including **evidence collection**, **incident classification**, and **communication protocols**.



## Screenshots:

TryHackMe Dashboard Learn Compete Other

Learn > Intro to IR and IM

### Intro to IR and IM

An introduction to Incident Response and Incident Management.

Easy 120 min

Share your achievement Help Save Room 513 Options

Room completed (100%)

- Task 1 Introduction
- Task 2 What is Incident Response and Management
- Task 3 The Different Roles During an Incident
- Task 4 The Process of Incident Management
- Task 5 Common Pitfalls During an Incident
- Task 6 Conclusion

Room completed (100%)

- Containment - Actions taken to "stop the bleed". These are actions meant to stop the incident from growing larger.
- Eradication - Actions taken to eradicate the threat actor from the estate.
- Recovery - Actions taken to recover the environment allow the organisation to go back to Business as Usual (BAU).

The reason these are split into three phases is because their order matters. If you start eradication or recovery before containment, the threat actor will be able to persist. For example, if the threat actor compromised Active Directory and we simply changed each account's password (eradication action), the threat actor could simply leverage their current permissions to recover the credentials again. We would first have to ensure that we have closed-off access to the threat actor before taking other actions.

As you will note in the diagram, phases 2 and 3 are cyclic. This is because when we start to deal with the incident, we will not understand the full scope. However, we also simply can't wait to understand the full scope before we start to take any action. Therefore, as the investigation is ongoing, we already start to take some actions and note the effect that they have on the incident. Only once we can return to BAU do we stop this process.

### Post-Incident Activity

Once an incident has been closed, that isn't the end of the incident management process. As a last step, we want to evaluate what happened during the incident in order to learn lessons and improve how we deal with incidents in the future. As such, we learn from these incidents to better prepare ourselves to deal with the next one.

Open and complete the static site to show you understand the incident management process!

Answer the questions below

What is the value of the flag you receive after correctly matching the steps of the incident management process?

THM[Preparation.is.Key.for.Incident.Management]

Correct Answer

- Task 5 Common Pitfalls During an Incident
- Task 6 Conclusion



# EncryptEdge Labs

## 6.2 Lab 2: Preparation

This lab focused on the **preparation phase** of incident response. We learned how to develop playbooks, create communication protocols, and maintain necessary tools for incident management.

### Tasks Completed:

- **Creating Incident Response Playbooks:** Developed a template for incident response playbooks, ensuring all actions were documented for various types of incidents.
- **Communication Plan:** Set up communication procedures for notifying internal teams and stakeholders during a security incident.



**EncryptEdge Labs**

- **Maintaining Tools:** Ensured that systems like firewalls, antivirus tools, and logging systems were ready and configured for use during an incident.

## Screenshots:

Woop woop! Your answer is correct

Congratulations on completing Preparation!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
80	6	Walkthrough	Medium	39

Leave Feedback

Next






# EncryptEdge Labs

tryhackme.com/room/preparation

TryHackMe Dashboard Learn Compete Other Access Machines 39

Learn > Preparation

 **Preparation**  
A look into the Preparation phase of the Incident Response.  
Medium 60 min


Share your achievement Start AttackBox Help Save Room 319 Options

Room completed (100%)

- Task 1 Introduction
- Task 2 Incident Response Capability
- Task 3 People and Documentation Preparation
- Task 4 Technology Preparation
- Task 5 Visibility
- Task 6 Conclusion

tryhackme.com/room/preparation

Learn > Preparation

 **Preparation**  
A look into the Preparation phase of the Incident Response.  
Medium 60 min

Share your achievement Start AttackBox Help Save Room 319 Options

Room completed (100%)

- Task 1 Introduction
- Task 2 Incident Response Capability
- Task 3 People and Documentation Preparation
- Task 4 Technology Preparation
- Task 5 Visibility
- Task 6 Conclusion

How likely are you to recommend this room to others?



### 6.3 Lab 3: Identification & Scoping

The focus of this lab was on **identifying incidents** and **scoping** the attack to understand its breadth. We covered the procedures for detecting threats and assessing their impact.

#### Tasks Completed:

- **Incident Detection:** We simulated scenarios to identify incidents through **SIEM alerts, intrusion detection systems (IDS), and manual reporting.**
- **Evidence Collection:** We practiced collecting logs and other forensic data necessary for identifying the root cause and scope of an incident.
- **Scope Assessment:** We used tools to assess the impact and determine how widespread the incident was, identifying all potentially affected systems and users.


#### Screenshots:



# EncryptEdge Labs

tryhackme.com/room/identificationandscoping

Woop woop! Your answer is correct



## Congratulations on completing Identification & Scoping!!! 🎉

Points earned 80	Completed tasks 5	Room type Walkthrough	Difficulty Medium	Streak 39
---------------------	----------------------	--------------------------	----------------------	--------------

Leave Feedback

Next

tryhackme.com/room/identificationandscoping

TryHackMe Dashboard Learn Compete Other Access Machines 39

Learn > Identification & Scoping

## Identification & Scoping

A look into the second phase of the Incident Response Framework, Identification & Scoping.  
Medium 60 min

Share your achievement Start AttackBox Help Save Room 221 Options

Room completed (100%)

- Task 1 Introduction
- Task 2 Identification: Unearthing the Existence of a Security Incident
- Task 3 Scoping: Understanding the Extent of a Security Incident
- Task 4 Identification and Scoping Feedback Loop: An Intelligence-Driven Incident Response Process
- Task 5 Conclusion



Room completed (100%)

Scoping involves grasping the extent of the incident, including which systems are affected, what data is at risk, and how the incident impacts the organisation.

The transition from identification to scoping is crucial in the Incident Response Process, demanding clear communication, effective collaboration, and a well-defined process. The insights gained from the identification phase will prove instrumental in facilitating this transition and strengthening the effectiveness of the incident response process.

Answer the questions below

What is the Subject of Ticket#2023012398704232?

Weird Error in Outlook ✓ Correct Answer

According to your colleague John, the issue outlined on Ticket#2023012398704232 could be related to what?

SPF, DKIM & DMARC records ✓ Correct Answer

Your colleague requested what kind of data pertaining to the machine WKSTN-02?

Web Proxy logs ✓ Correct Answer

Task 3 ✓ Scoping: Understanding the Extent of a Security Incident

Task 4 ✓ Identification and Scoping Feedback Loop: An Intelligence-Driven Incident Response Process

Task 5 ✓ Conclusion

How likely are you to recommend this room to others?

## 7.0 Reflection

In this section, I will reflect on the overall experience of completing the **Incident Response (IR) Simulation** and the **mandatory labs**. The purpose of this reflection is to examine how the skills learned in this task apply to real-world scenarios, identify areas for improvement, and understand the importance of effective incident management in cybersecurity.

### 7.1 Key Takeaways

#### Understanding the Incident Response Lifecycle



The **Incident Response Lifecycle**—including preparation, identification, containment, eradication, recovery, and lessons learned—was crucial to successfully managing the simulated phishing attack. Each phase of the lifecycle highlighted the importance of well-prepared tools and processes in mitigating potential damage from security incidents.

Through the labs and simulation, I gained practical knowledge of the essential steps involved in handling an incident. By learning how to **contain** the threat, **eradicate** any malicious files, and **recover** systems to normal operations, I now understand the critical role these steps play in minimizing the impact of an incident.

### Incident Detection and Scoping

The **Identification & Scoping Lab** was particularly valuable in teaching me how to identify incidents using tools like **SIEM** systems and **intrusion detection systems (IDS)**. I learned how to analyze logs and assess the scope of an incident, which is a crucial skill in determining the extent of damage and deciding the appropriate course of action. The hands-on experience allowed me to understand how to **contain** the threat by isolating compromised systems and preventing further damage.

### Phishing Attack Simulation

The phishing attack scenario emphasized the importance of **user awareness** and **early detection** in combating such threats. The ability to quickly identify and contain the phishing email and its associated malware was key to preventing a breach. By following the IR plan and utilizing the response tools effectively, I was able to contain the attack before it caused significant damage. This experience reinforced the importance of ongoing **employee training** on phishing threats and the need for an effective **incident response plan**.



### 7.2 Real-World Application

The skills learned during this task are directly applicable to real-world situations. Incident response and management are critical in minimizing the damage caused by cybersecurity incidents. As an intern aiming to become proficient in **cybersecurity**, I recognize that:

- **Preparation:** Having the right tools and procedures in place before an attack occurs is essential. **Playbooks** and **incident response templates** help speed up the process of managing incidents and reduce the risk of human error.
- **Identification:** Early detection is key to stopping incidents before they escalate. Tools like **SIEM** and **IDS** are invaluable for identifying anomalies and intrusions.
- **Scoping:** Properly assessing the impact of an incident ensures that resources are allocated appropriately, and the right actions are taken to mitigate further damage.
- **Containment and Eradication:** After identifying an incident, it's crucial to act quickly to **contain** it and remove any malware or malicious files from the system.
- **Recovery and Lessons Learned:** Ensuring systems are restored to normal operations, and documenting the response process for future reference, helps strengthen the organization's security posture.

### 7.3 Areas for Improvement

While the simulation was successful, there are areas where I could improve:

- **Speed and Efficiency:** During the incident simulation, I noticed that some steps could have been executed more quickly. In a real-world scenario, time is of the essence, so improving the speed and accuracy of response is essential.



- **Communication:** Although the communication plan was in place, I could improve my efficiency in notifying stakeholders and coordinating with teams during an active incident. Clear and concise communication is critical to effective incident management.
- **Automation:** I learned that while manual incident response actions are important, integrating automation into the incident response process can significantly improve efficiency, especially during repetitive tasks like isolating compromised systems or applying patches.

### 7.4 Final Thoughts

The **Incident Response Simulation** and **hands-on labs** have provided me with the skills necessary to effectively handle cybersecurity incidents, from detection to recovery. These experiences have helped me understand the **importance of preparation** and **training** in ensuring an organization is ready to respond to security threats.

As I continue my internship, I aim to further refine my incident response skills by practicing more complex scenarios, improving my speed in decision-making, and collaborating more effectively with teams during incidents. I also plan to stay updated on the latest trends in cybersecurity incidents to ensure I am always prepared for emerging threats.

In conclusion, this experience has been invaluable in shaping my understanding of the importance of incident response in cybersecurity, and it has provided me with the tools and knowledge necessary to manage and mitigate security incidents effectively.



**EncryptEdge Labs**

**This Internship Task report was developed on [April, 10, 2025]**

**By:**

**atalmamun@gmail.com**