# Incident Response Fundamentals

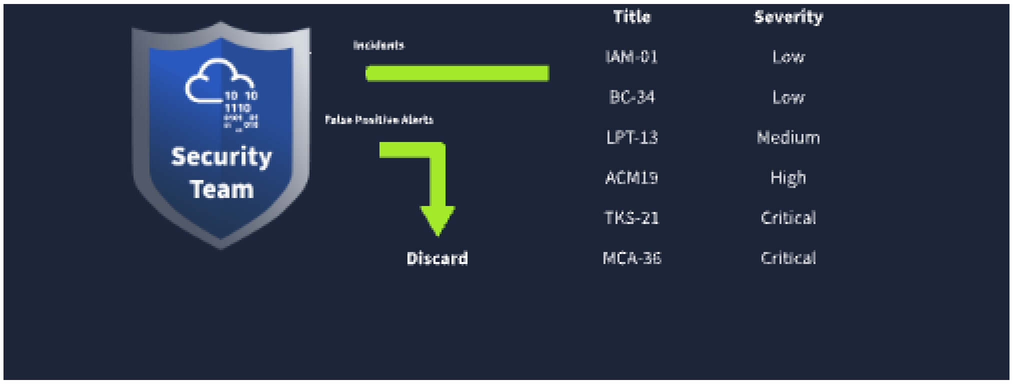
Incident Response handles an incident from its start to end. From deploying security in several areas to prevent incidents to fighting with them, and minimizing their impact, incident response is a thorough guideline.

## What are Incidents ?

when a security solution finds an event or group of events associated with a possible harmful activity, it triggers an alert. The security team then analyzes these alerts. Some of these alerts may be **False Positives**, while some would be **True Positives**.

**False positive:** A security solution raised an alert on a high amount of data being transferred from one system to an external IP address. Upon analyzing this alert, the security team found that the subject system was undergoing a backup process to a cloud storage service, which caused this. This is known as a false positive.

**True Positive:** A security solution raised an alert on a phishing attempt on one of the organization's users. Upon analyzing this alert, the security team found that the email was a phishing email sent to this user to compromise the system. This is known as a true positive.



| Title | Severity |
|---|---|
| IAM-01 | Low |
| BC-34 | Low |
| LPT-13 | Medium |
| ACM19 | High |
| TKS-21 | Critical |
| MCA-36 | Critical |

## Types of Incidents

**Malware Infections**: Malware is a malicious program that can damage a system, network, or application.

**Security Breaches:** Security Breaches arise when an unauthorized person gets access to confidential data (something we don't want them to see or have).

**Data Leaks:** Data leaks are incidents in which confidential information of an individual or an organization is exposed to unauthorised entities.

**Insider Attacks:** Incidents from within an organization are known as insider attacks.

**Denial Of Service Attacks:** Denial of Service attacks, or DoS attacks, are incidents where the attacker floods a system/network/application with false requests, eventually making it unavailable to legitimate users.

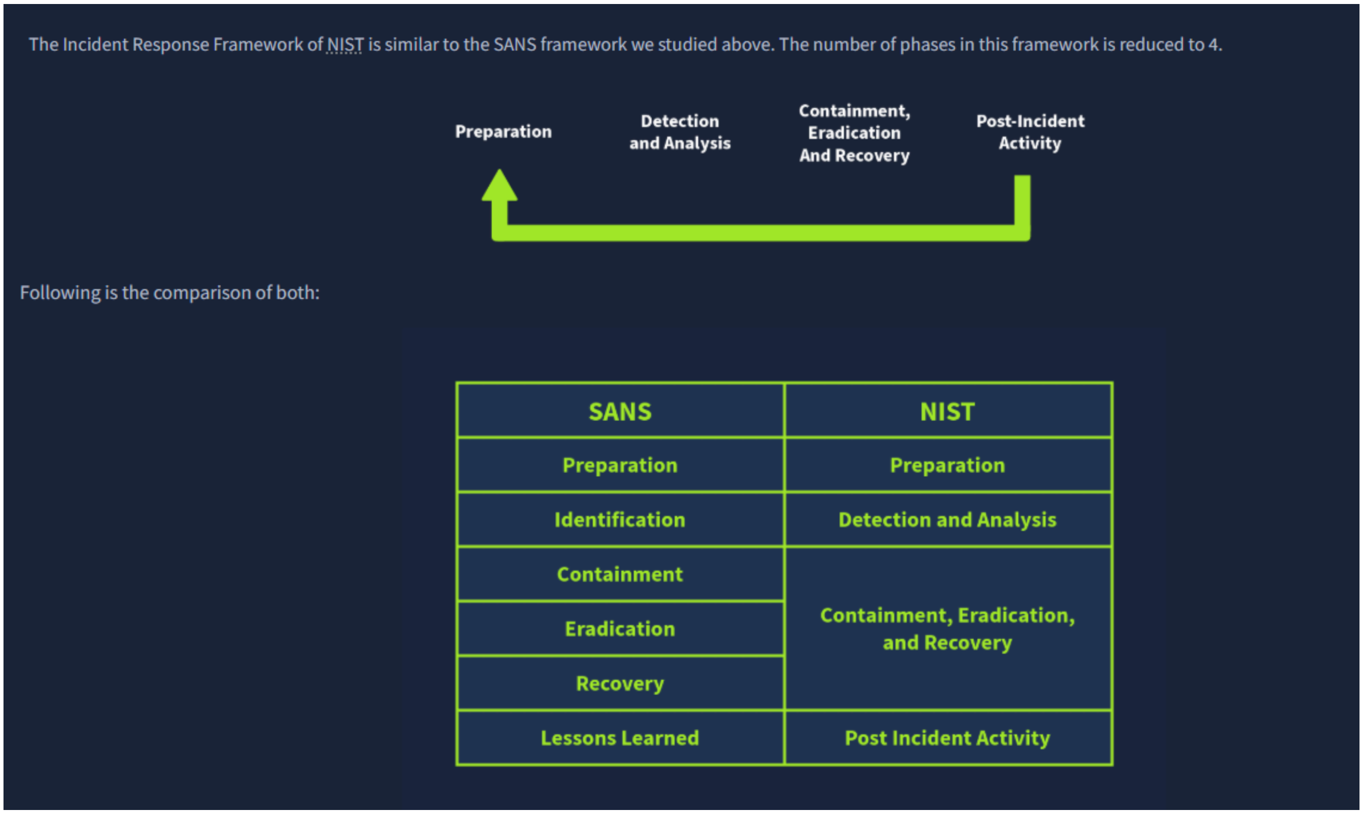
## Incident Response Process

SANS and NIST are popular organizations contributing to cyber security. SANS has offered various courses and certifications in cyber security, and NIST played its role in developing standards and guidelines for cyber security.

The SANS incident Response framework has 6 phases, which can be called 'PICERL' to remember them easily.

| Phase | Explanation | Example |
|---|---|---|
| Preparation | This is the first phase. The preparation phase includes building the necessary resources to handle an incident. These resources include developing incident response teams, having a proper incident response plan in place, and deploying necessary security solutions to combat the incidents. | Conducting awareness training for employees<br>on phishing emails. Phishing emails are fraudulent emails sent by malicious attackers that can trick you into performing actions that can lead you to an incident. |
| Identification | The identification phase refers to looking for any abnormal behavior that may indicate an incident. This involves using various security solutions and techniques to monitor abnormal events. | The security team notices a huge amount of data being sent out from one of the hosts. Upon analysis, it was found to be compromised after a malicious file was downloaded from a phishing email attachment. |
| Containment | Once an incident has been identified, the next step should be to contain it. This means minimizing the impact of the attack. This is usually done by isolating the victim machine, disabling the compromised user accounts, etc. | The Security team isolates the host from the network to minimize the impact and not allow the attacker to jump to other systems, leveraging the compromised host. |
| Eradication | This phase, as its name suggests, involves removing | A deep malware scan was executed on the system to remove the malicious software |

| Phase | Explanation | Example |
|---|---|---|
| | the threat from the attacked environment. The threat may be of any kind. The eradication phase will ensure the subject environment is clean, and now we can move to the recovery phase. | from the host. |
| Recovery | The recovery phase is very important in this chain. It involves recovering the affected systems from backup or rebuilding them. The recovered systems are then tested and are ready to use. | The compromised host was re-configured, and the exfiltrated data was restored from the backup. |
| Lessons Learned | This is also an important part of the incident response lifecycle. Gaps in the detection and analysis of the incident are identified and documented, helping to improve the overall process in future incidents. | Conducting a post-incident review meeting to analyze the incident's root cause and improve the security to prevent future attacks. |



The Incident Response Framework of NIST is similar to the SANS framework we studied above. The number of phases in this framework is reduced to 4.

Following is the comparison of both:

| SANS | NIST |
|---|---|
| Preparation | Preparation |
| Identification | Detection and Analysis |
| Containment | Containment, Eradication, and Recovery |
| Eradication | |
| Recovery | |
| Lessons Learned | Post Incident Activity |

## Incident Response Techniques

- **SIEM:** The Security Information and Event Management Solution (SIEM) collects all important logs in one centralized location and correlates them to identify incidents.
- **AV:** Antivirus (AV) detects known malicious programs in a system and regularly scans your system for these.
- **EDR:** Endpoint Detection and Response (EDR) is deployed on every system, protecting it against some advanced-level threats. This solution can also contain and eradicate the threat.

Playbooks are the guidelines for a comprehensive incident response.

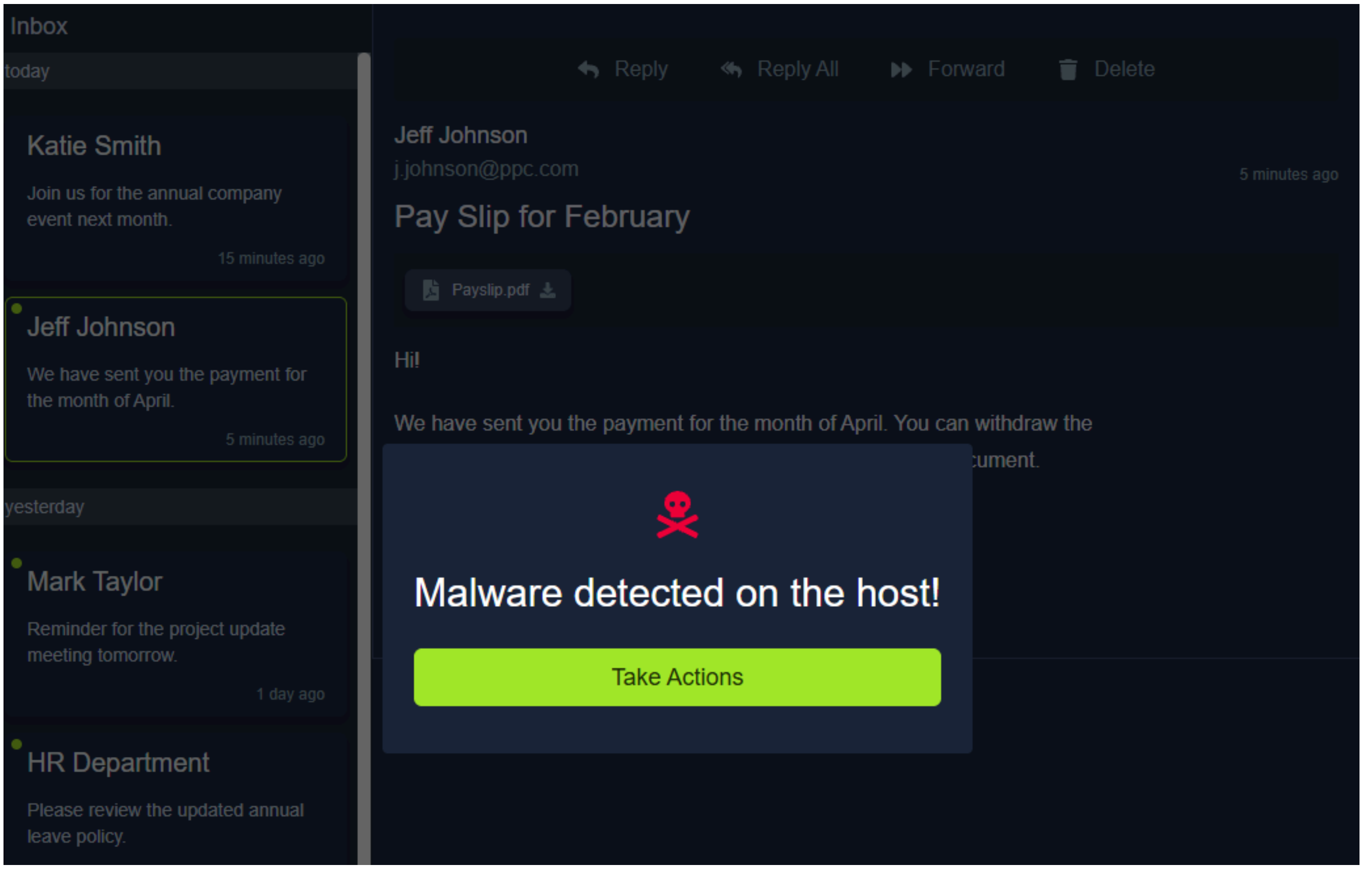
Following is an example of a **Playbook** for an incident: Phishing Email

1. Notify all the stakeholders of the phishing email incident
2. Determine if the email was malicious by conducting header and body analysis of the email
3. Look for any attachments with the email and analyze them
4. Determine if anybody opened the attachments
5. Isolate the infected systems from the network
6. Block the email sender

**Runbooks**, on the other hand, are the detailed, step-by-step execution of specific steps during different incidents. These steps may vary depending on the resources available for investigation.

# Lab Work Incident Response

after downloading a file from an email there is an alert saying malware detected



today

Katie Smith
Join us for the annual company event next month.
15 minutes ago

Jeff Johnson
We have sent you the payment for the month of April.
5 minutes ago

yesterday

Mark Taylor
Reminder for the project update meeting tomorrow.
1 day ago

HR Department
Please review the updated annual leave policy.

Jeff Johnson
j.johnson@ppc.com
5 minutes ago

Pay Slip for February

Hi!

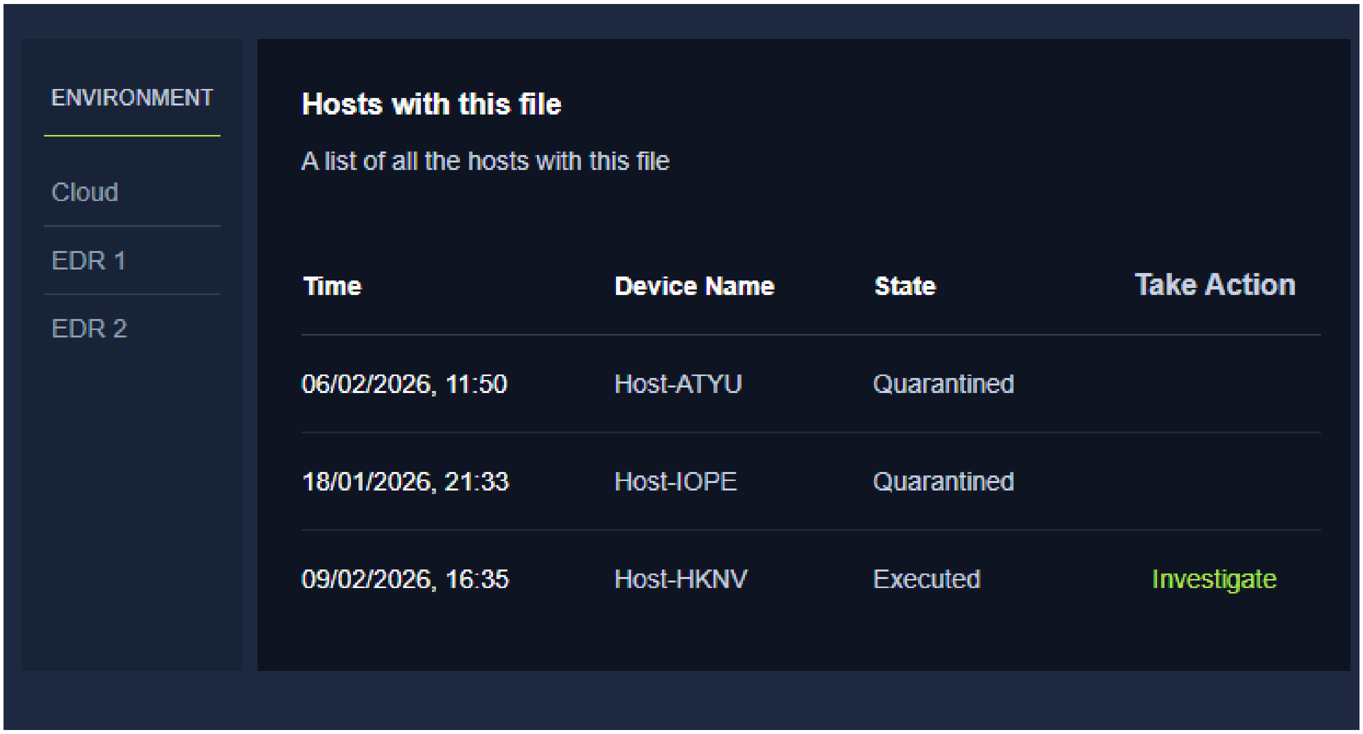
We have sent you the payment for the month of April. You can withdraw the

cument.

Malware detected on the host!

from here i then had to go to the EDR

which showed hosts within a file that had been executed and not executed

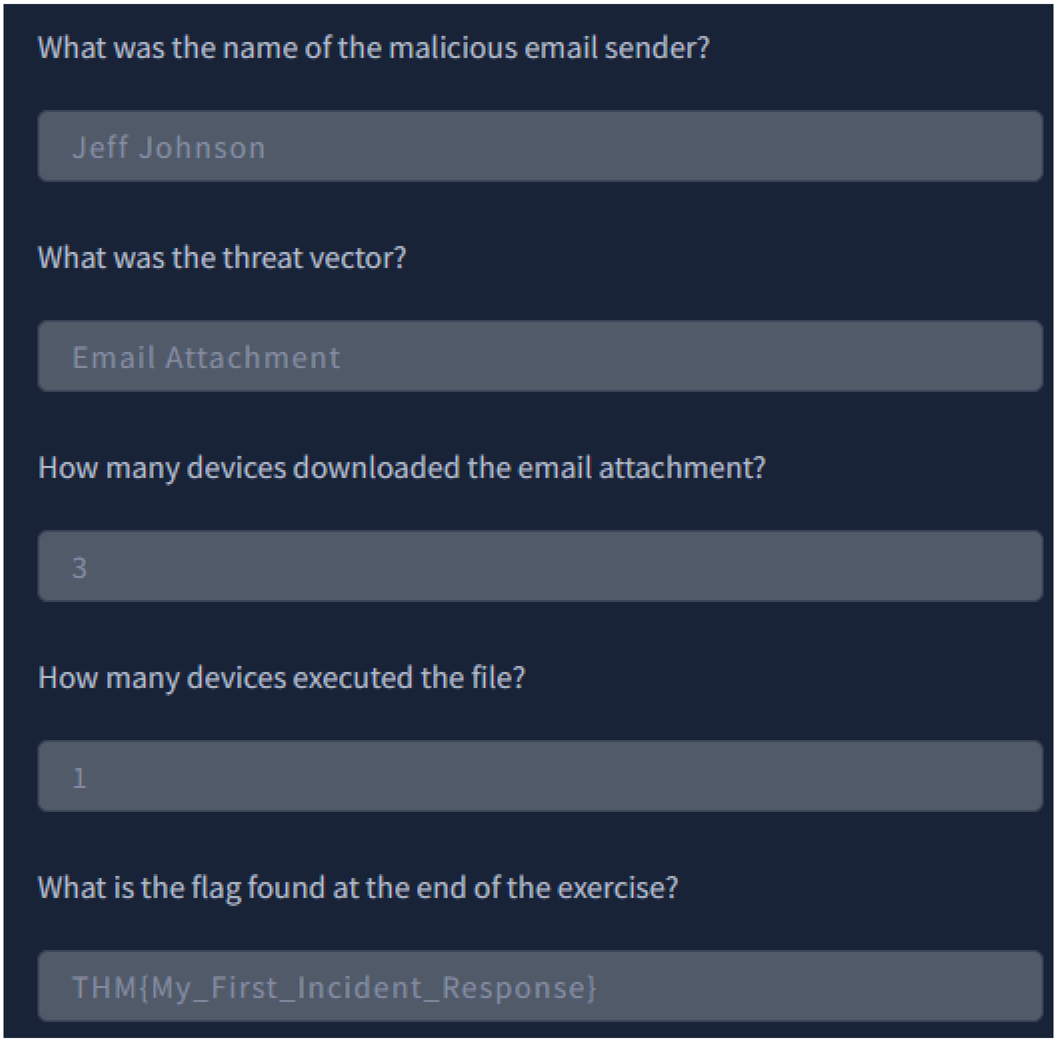


Hosts with this file

A list of all the hosts with this file

| Time | Device Name | State | Take Action |
|---|---|---|---|
| 06/02/2026, 11:50 | Host-ATYU | Quarantined | |
| 18/01/2026, 21:33 | Host-IOPE | Quarantined | |
| 09/02/2026, 16:35 | Host-HKNV | Executed | Investigate |

I had to quarantine the non executed files and investigate the executed file
when investigating I isolated the host that had executed the file and stopped the malware.



What was the name of the malicious email sender?

Jeff Johnson

What was the threat vector?

Email Attachment

How many devices downloaded the email attachment?

3

How many devices executed the file?

1

What is the flag found at the end of the exercise?

THM{My_First_Incident_Response}