

# Incident response

Author: Harshitaa Ashish

## Module 1 - Introduction to incident response

### Incident response

Incident response is a method to manage security breaches and cyber threat incidents more effectively. It involves teamwork by an organization's incident response team to detect, respond and recover from cyber threats. The main goal of incident response is to minimize damage, reduce recovery time and mitigate the impact of incidents on organization's operations and reputation.

There are many phases that involve specific actions and procedures aimed at identifying, containing, and resolving the incident properly while preserving evidence for further investigation.

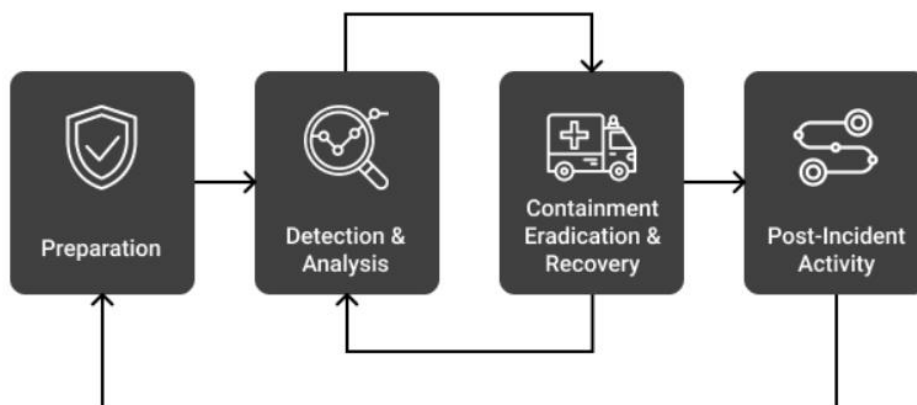
### Importance and goals of incident response

The importance of incident response involves:

- Minimizing data loss, downtime, and financial costs.
- Maintaining business data and services.
- Study about weaknesses and strengths of vulnerabilities helps to enhance security postures.
- Analyzing response identifies areas for improvement in response.
- Planning and effective response efforts showcase your commitment to cybersecurity.

Therefore, the primary objective of incident response is to promptly identify, isolate and resolve security breaches, mitigating their impact and ensuring operational stability.

### Incident response lifecycle diagram



The incident response consists of different phases:

- Preparation: defining roles and responsibilities, and following policies and procedures.
- Detection and analysis: the systems and networks are monitored and analyzed for security incidents and identifying the incident features and collecting the data.
- Containment, eradication and recovery: reacting quickly to take out data from the incident, and prevent further damage or access. And restore the services.
- Post incident analysis: performing a review of the incident to understand its root causes, evaluate response and identify the changes required.
- Improvement: correcting actions based on the post incident analysis and enhancing detection capabilities.
- Documentation and reporting: taking record of all processes, findings and reporting to the management authorities.
- Monitoring and adapting: checking for new threats and vulnerabilities, adapting incident response processes and strategies for being ready to respond to incidents.

Readings: <https://underdefense.com/blog/incident-response-life-cycle-underdefense/>

## Module 2 - Incident detection and Identification

Techniques for detecting security incidents

Network intrusion detection system NIDS, is a continuous monitoring system for network traffic to find threats and vulnerabilities. It analyzes data packets in a network and understands the patterns for attacks. NIDS works by capturing packets and analyzing them. The methods used are signature-based detection, anomaly-based detection, and heuristic based detection. When a cyber-attack is detected, NIDS alerts and notifies for a response. The alert is the information about the system events. Finally, NIDS keeps track of the logs of network activities and detects incidents for analysis and forensic purposes.

Host intrusion detection systems (HIDS) is a security tool for monitoring and analyzing cyber threat activities. It inspects system files, configuration settings and application activities to understand the patterns of incidents. HIDS also provides real time alerting and logging features for response.

Log analysis and monitoring involves the studying of the system and network logs for identifying security threats and other events in the system. Endpoint security solutions protect devices and systems from cyber-attacks. The solutions consist of antivirus softwares, firewalls and IDS/IPS systems. They monitor endpoint activities, detect and prevent threats. It also provides features like encryption, remote device management and device control to protect the network infrastructure.

Common indicators of compromise (IOCs)

Unusual network traffic patterns are a sign for cyber threats. It consists of sudden spikes or drops of data flow, and strange movements of data across networks.

Repeated failed logins could show that someone could also be trying to get into the network or system by unauthorized access methods.

It is also necessary to keep track of who is making changes to the files and the changes do not seem suspicious.

Also keeping track of the programs that are running in the system and watching any strange programs which should not be starting up.

#### Incident classification and prioritization

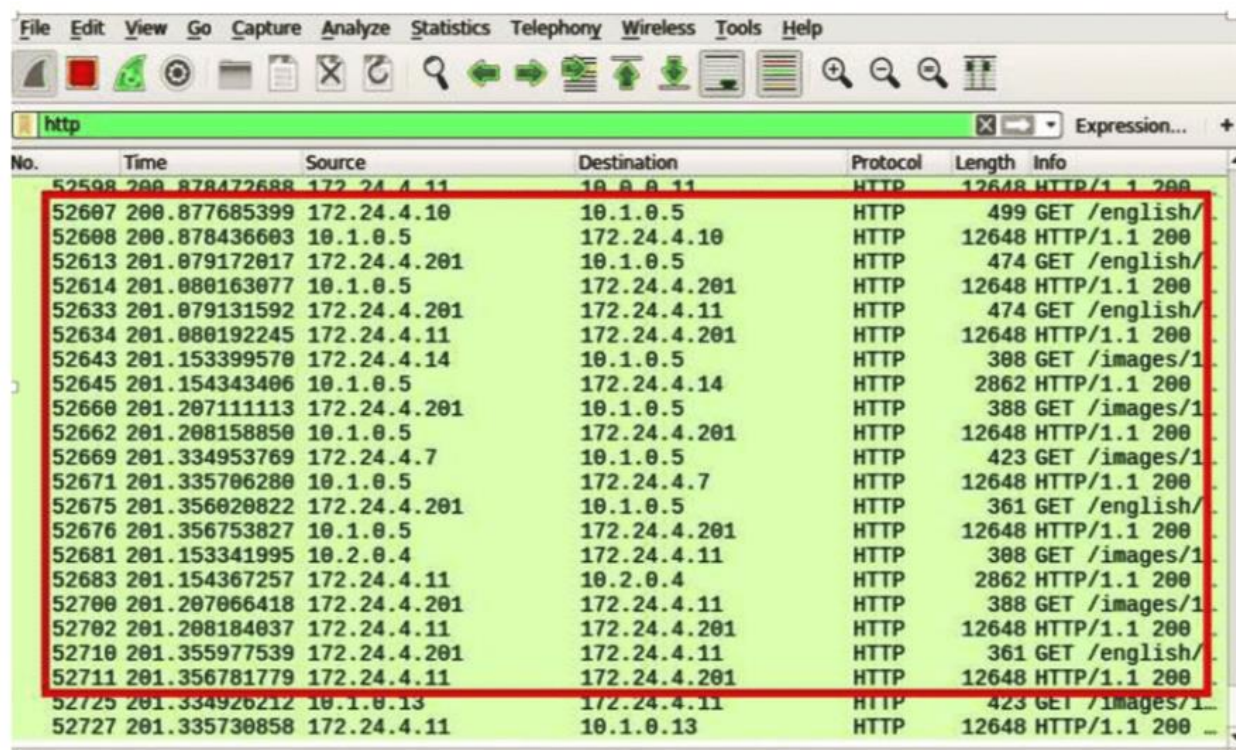
When an incident occurs, the severity is understood by factors like impact, sensitivity and potential the threat can cause to the organization. The impact of the incident involves calculating the extent of disruption it causes to the business, service, and data. The incidents are also classified based on the levels of risk they pose. The risks are data breaches, system downtime, financial loss, reputational damage, etc.

Incident prioritization involves assessing the danger and urgency of cyber incidents to allocate the resources, addressing high priority issues based on the potential impact and risk.

Prioritization helps establish response timeframes for addressing incidents. It requires continuous monitoring of the threats and systems for the response.

#### Simulation with Wireshark for incident detection:

Given the scenario, we are using Wireshark, and the network traffic is flooded with HTTP, which shows suspicious activities. Hence giving us the idea that it could be a DDoS attack due to the analysis and study of the features.



The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of network packets. The filter bar at the top of the packet list is set to 'http'. The packet list is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
52508	200.878472688	172.24.4.11	10.1.0.11	HTTP	12648	HTTP/1.1 200
52607	200.877685399	172.24.4.10	10.1.0.5	HTTP	499	GET /english/
52608	200.878436603	10.1.0.5	172.24.4.10	HTTP	12648	HTTP/1.1 200
52613	201.079172017	172.24.4.201	10.1.0.5	HTTP	474	GET /english/
52614	201.080163077	10.1.0.5	172.24.4.201	HTTP	12648	HTTP/1.1 200
52633	201.079131592	172.24.4.201	172.24.4.11	HTTP	474	GET /english/
52634	201.080192245	172.24.4.11	172.24.4.201	HTTP	12648	HTTP/1.1 200
52643	201.153399570	172.24.4.14	10.1.0.5	HTTP	388	GET /images/1
52645	201.154343406	10.1.0.5	172.24.4.14	HTTP	2862	HTTP/1.1 200
52660	201.207111113	172.24.4.201	10.1.0.5	HTTP	388	GET /images/1
52662	201.208158850	10.1.0.5	172.24.4.201	HTTP	12648	HTTP/1.1 200
52669	201.334953769	172.24.4.7	10.1.0.5	HTTP	423	GET /images/1
52671	201.335706280	10.1.0.5	172.24.4.7	HTTP	12648	HTTP/1.1 200
52675	201.356020822	172.24.4.201	10.1.0.5	HTTP	361	GET /english/
52676	201.356753827	10.1.0.5	172.24.4.201	HTTP	12648	HTTP/1.1 200
52681	201.153341995	10.2.0.4	172.24.4.11	HTTP	388	GET /images/1
52683	201.154367257	172.24.4.11	10.2.0.4	HTTP	2862	HTTP/1.1 200
52700	201.207066418	172.24.4.201	172.24.4.11	HTTP	388	GET /images/1
52702	201.208184037	172.24.4.11	172.24.4.201	HTTP	12648	HTTP/1.1 200
52710	201.355977539	172.24.4.201	172.24.4.11	HTTP	361	GET /english/
52711	201.356781779	172.24.4.11	172.24.4.201	HTTP	12648	HTTP/1.1 200
52725	201.334926212	10.1.0.13	172.24.4.11	HTTP	423	GET /images/1
52727	201.335730858	172.24.4.11	10.1.0.13	HTTP	12648	HTTP/1.1 200

### Case study: Suspicious File Access

At a medium-sized company, the IT team noticed unusual activity on one of the file servers. Multiple failed login attempts have been recorded for an employee's account outside of regular working hours. Additionally, the server logs show that several sensitive files were accessed and copied to an external USB drive. The incident response team is tasked with investigating this suspicious activity and determining if it constitutes a security breach.

- Incident detection: suspicious activity is detected on file server logs.
- IOCs: many failed logins, unauthorized access and file copying to devices
- Classification: potential data damage due to sensitivity of accessed files.
- Prioritization: investigation started due to sensitivity of accessed files.
- Response: the employee account is disabled and investigated
- Resolution: the affected files are restored and security measures are implemented.
- Communication: the organization owners are informed about the incident.
- Review: More efficient protocols are implemented and data access controls are reinforced.

## Module 3 - Incident investigation and analysis

### Gathering evidence and forensic data collection

The data is gathered from various resources like logs, network traffic and screenshot records from the system. The exact copy of the storage devices are used to preserve the evidence integrity. A document is also maintained to keep the record of who accessed the evidence.

### Post incident analysis and root cause analysis

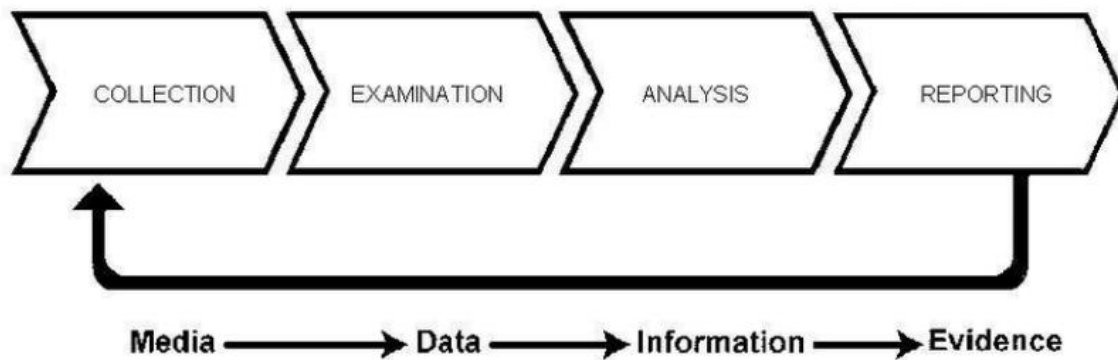
To understand the incident, we need to understand the events and its sequence from the collected evidence. Underlying factors like vulnerabilities and human error can also be determined, which gives us the root cause. To prevent similar incidents in future, implementing corrective actions are required.

### Tools and techniques for incident investigation

Various tools and techniques are used for incident investigation as following:

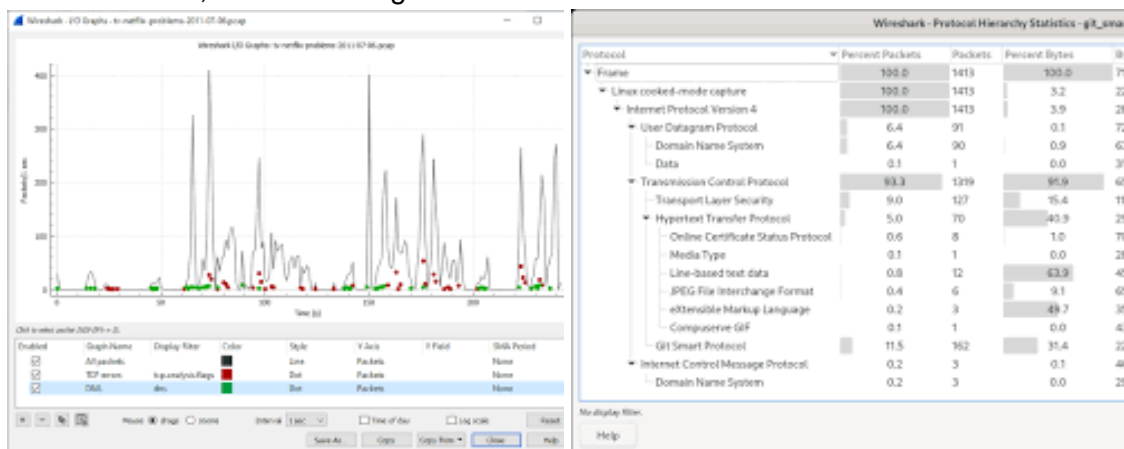
- Forensic analysis: Autopsy, encase.  
The tools are used for digital evidence.
- Network analysis: Wireshark  
The tool is used for analyzing network traffic.
- Memory forensics: is used to analyze volatile memory for evidence.

Diagram: forensic data collection process



### Simulation:

To get experience with network analysis, troubleshooting, and security monitoring approaches, Wireshark simulation entails building network scenarios to generate traffic, collecting packets with Wireshark, and evaluating data.



Readings: <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>

## Module 4 - Incident containment and eradication

### Strategies for containing security incidents

The affected systems or networks are isolated to prevent further spread of the incident. Suspicious activities or connections are suspended to limit damage. Security patches are applied to vulnerable systems and updated consistently.

### Eradicating the root cause of incidents

Identifying and addressing underlying security vulnerabilities that are exploited in the incident. Utilizing an antivirus software or by manual methods to remove malicious softwares from the affected systems.

Minimizing impact and preventing further damage

The data is restored to minimize the data loss. And different methods are used to monitor and detect mechanisms to identify security incidents.

Case study:

- Incident description: suspicious activity is detected.
- Containment: affected systems are isolated from the network systems.
- Root cause analysis: all the systems and networks are investigated to understand the security vulnerability or affected system by the attacker.
- Remediation: the software patches are applied and anti-malware softwares are installed and finally the affected systems are restored from backup.

## Module 5 - Incident response communication and coordination

Internal communication channels and protocols

It is very important to spread the awareness and inform everyone in the organization about the incident related information through emails and messaging platforms. Automated internal notification alerts can also be used to notify relevant people in the organization about the security incident.

Cross functional collaboration in incident response

The incident response team consists of the IT, security, legal and communications personnel. Regular meetings should be conducted to facilitate the collaboration and decision making between the team members during the incident response.

Engaging with law enforcement and regulatory agencies

Designated organization wonders will have to coordinate with law enforcement and other legal systems. This ensures that the incident response activities align with legal and regulatory obligations.

Reading: <https://medium.com/@mkumar9009/measurability-of-incident-management-process-94e0645690a4>

Case study:

Incident Description: A data breach is discovered in a large retail company, potentially compromising customer payment information.

- Internal communication: the incident response team notifies the departments through email and conducts meetings for the discussion to conduct response efforts.
- Cross functional collaboration: The incident team collaborates to contain the breach, assess impacts, and communicate with organization owners.
- Engaging with law enforcement: for the investigation the legal department collaborated with the law enforcement agencies.

## Module 6 - Recovery and remediation

### Recovery strategies and procedures

To reduce downtime and quickly resume operations following an incident, recovery tactics include redundancy measures, backup systems, and quick restoration techniques. The main goals of business planning and disaster recovery are to identify key functions, create recovery strategies, and guarantee business continuity. Post-event evaluations determine the efficacy of the response, point out lessons learnt, and guide future developments. When combined, these procedures seek to reduce incident impact, maintain business continuity, and strengthen organizational resilience.

### Conducting post incident reviews (PIR)

Evaluating the reaction to security issues is part of conducting post-incident reviews, or PIRs. It comprises documenting lessons learned, identifying areas for improvement, and evaluating how effective incident handling processes are. PIR assists companies in improving security procedures, strengthening incident response teams, and averting future recurrence of the same problems. To improve overall security posture, critical components include evaluating incident response actions, recording results, and putting remedial measures into place.

Reading: <https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/>

## Module 7 - Conclusion

Trends in incident response include cloud-native security solutions, automation, and AI-driven threat identification. Sophisticated technology simplifies incident handling, such as SOAR tools and threat intelligence platforms. Workflows for incident response are shown in diagrams. Simulated experiences that provide hands-on practice improve team readiness. Comprehensive analysis and improvement initiatives are among the post-event actions. In summary, developing trends and technology combined with real-world experience fuel ongoing enhancements to incident response capacities, strengthening an organization's defenses against new threats.

Readings: <https://www.sciencedirect.com/science/article/abs/pii/S0167404812000624>