pairview™

endless possibilities

Incident Response, Forensics and Vulnerability Management

Bukunmi OJO

TRAINER

Cybersecurity Engineer with 3+ Years experience in development, implementation and maintenance of security processes,

Course Prerequisite

Basic Knowledge of the following will be a good starting point:

- Cybersecurity concepts
- Specific security threats and mitigation

About this course

In this course, attendees will learn:

- The fundamentals of Incident response, cycles of incident response, etc.
- Forensics
- Vulnerability management techniques and procedure

Benefit to Learners

By the end of this course, you will be able to understand what incident response is, best approach to incident response, forensics, vulnerability management and how it contributes towards overall organization security program.

Module 1: Introduction to Incident Response

Module Overview

- What is incident response
- Need for incident response
- Steps in Incident Response

What is Incident Response ?

Incident response is the process of managing and responding to security incidents that may affect an organization's information systems.

- This is often a structured process with steps to identify, contain and resolve incident.
- A dedicated team of professionals including security analysts, forensic analysts, etc are involved in this cycle.

Why Incident Response

There are several reasons why incident response is prepared for and done. Some of them are:

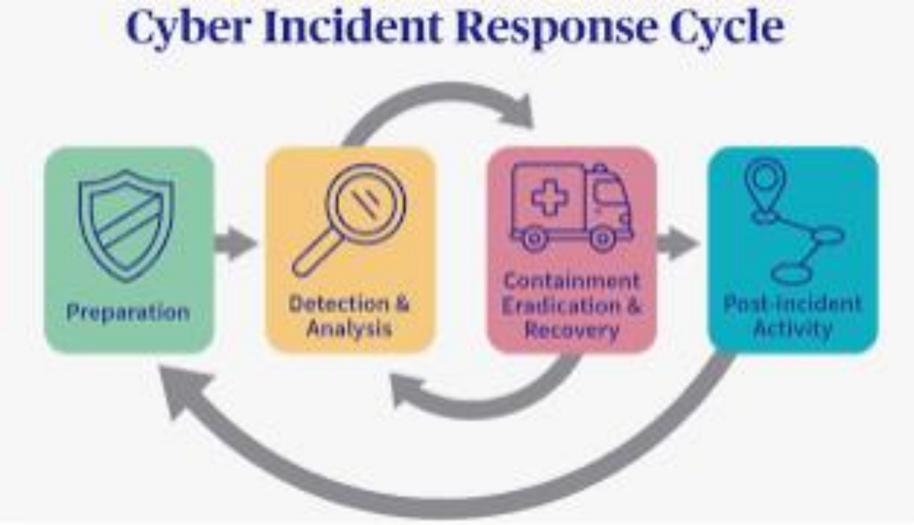
- **Minimizing damage:** This is the primary goal of incident response. By quickly identifying and containing incidents, impact of damage can be reduced
- **Protecting sensitive information:** Incident response also helps to protect customers' data, intellectual property, etc. from compromise during incidents
- **Compliance:** Incident response plans are required by regulatory compliance bodies
- **Learning and improvement:** Incident response provides insights into security posture, causes of incidents and improvement procedures and controls
- **Reputation protection:** How an incident is handled contributes largely to customer and public perception and overall reputational health

Incident Response Cycle

Just as every technology process, incident response has a predefined cycle of activities from start to finish.

According to NIST (National Institute of Science and Technology), there are 4 stages in a typical IR cycle.

- **Preparation:** This phase contains the creation of incident response plans (playbook), training of personnel, establishing right tools, procedures, and resources and active prevention of incidents.
- **Detection and analysis:** This phase identifies incidents, gathering information about it and further conducting investigation and impact evaluation. (this is most difficult part of IR).


Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

Incident Response Cycle (cont’d)

- **Containment, eradication and recovery:** This phase focuses on keeping the impact of verified incidents minimal, removing the cause of the incident, and restoring systems to their normal operating state
- **Post-Incident activity:** In this phase, the incident, response activities and outcomes are analyzed, lessons are drawn to prevent future occurrence, and improve future incident response activities.

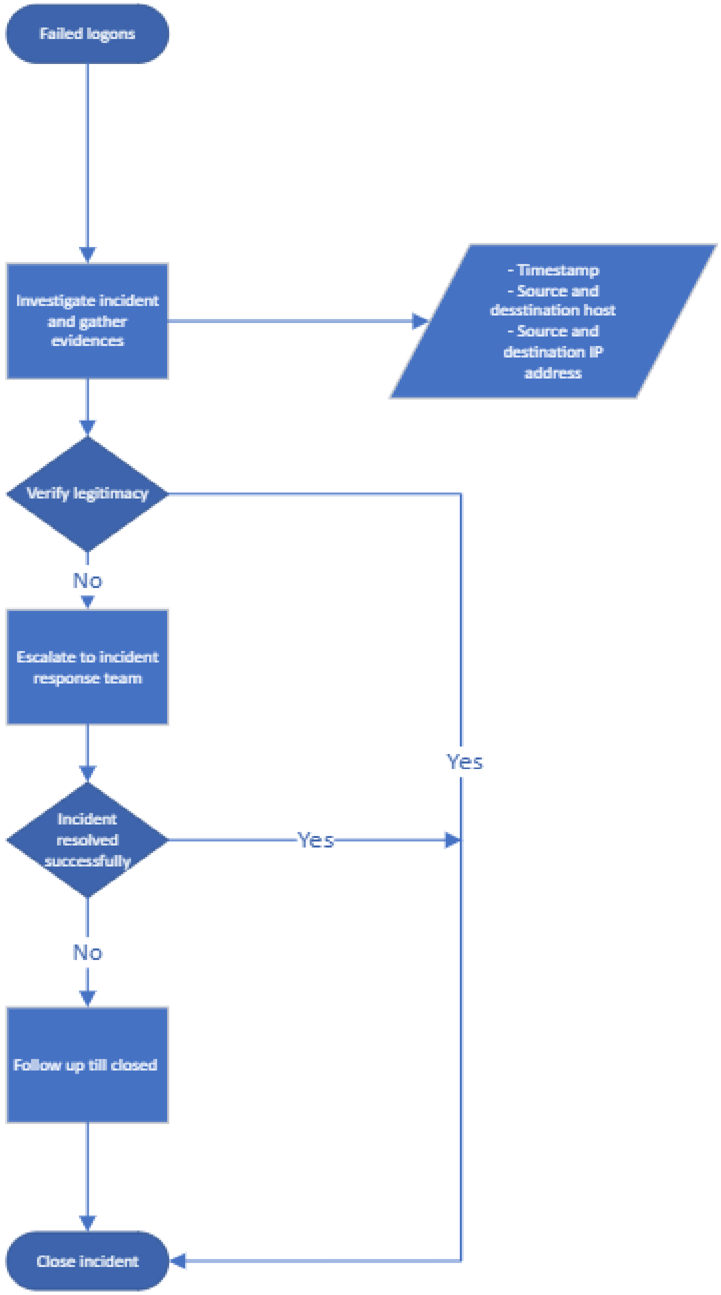
Important Incident Response Concepts

- **Incident response plan:** This is a document that outlines different types of incidents and steps to be taken to resolve them
- **Incident classification:** low, medium, high and critical
- **Incident response communication:** a communication plan that outlines all communication channels during an incident
- **Incident analysis:** conducting analysis to determine the cause, scope and impact of the incident
- **Incident response team:** Trained professionals that handle incidents depending on severity level. They include IR manager, security analyst triage analyst, forensic analyst, threat researcher

Typical Incident Response Scenarios

We will consider some common scenarios and IR procedures

- Failed logon: Information is gathered about the failed logon and decisions are made based on data in the flowchart
- Malware scenario
- Ransomware scenario



Failed logons

Investigate incident and gather evidences

- Timestamp
- Source and desstination host
- Source and destination IP address

Verify legitimacy

No

Yes

Escalate to incident response team

Incident resolved successfully

Yes

No

Follow up till closed

Close incident

Creating an IR Playbook

In creating an incident response playbook, the following should be considered/ put in place

- Definition of incidents:
- Establish designated roles
- Define certain processes and workflow for each incident
- Put in place checklists to work with
- Outline recovery path

Module Summary

- Incident response plan is a very important aspect of an organization's security strategy
- Lessons learnt should be adequately documented to prevent similar occurrences

Module 2: Forensics

Module Overview

- We will discuss forensics, what it entails, processes and tools.

Introduction to Forensics

Forensics is the practice of using scientific and analytical methods to collect, preserve, and analyze digital or physical evidence in with the purpose or intention of using it in a court of law. Digital forensics involves the analysis of digital devices and data to investigate and prevent cybercrime and other associated digital offenses:

- **Identification:** The first step in the forensic process is identifying the digital devices and data sources that may contain relevant evidence.
- **Preservation:** The next step is to preserve the integrity of the evidence by creating an exact copy of the data and storing it in a secure manner.

Introduction to Forensics (cont'd)

- **Collection:** Once the data is preserved, forensic experts can collect it using specialized tools and techniques.
- **Analysis:** The collected data is then analyzed to identify any relevant information, such as the origin and purpose of the data, its metadata, and its relationships to other data.
- **Reporting:** The final step in the process is to document the findings in a report that is admissible in a court of law.

Data Collection Procedure

There are procedures and best practices to follow in a typical forensic activity

- Capture and hash system images
- Analyze data with tools
- Capture screenshots
- Review network traffic and logs
- Capture video
- Consider Order of Volatility
- Take statements
- Review documentation

Module Summary

- Forensics is a very important aspect of security incident response.

Module 3: Vulnerability Management

Module Overview

- Fundamentals of vulnerability management
- Cycles and processes of vulnerability management

Vulnerability Management

Vulnerability management is the process of identifying, assessing, prioritizing, and mitigating vulnerabilities in computer systems, software, and networks before it is used to compromise the system.

It is very important, as it helps organizations to reduce the risk of security breaches and data loss by identifying and addressing potential weaknesses before they can be exploited by attackers.

Three important things to ask during vulnerability management

- The value of the information obtained
- The threat to your system
- Possible mitigation methods

Vulnerability Management (cont'd)

- Vulnerability management is a continuous process.
- Common tools used in vulnerability assessments are Nessus, Qualys, Alienvault
- Vulnerability management can either be automated or manual
- Risk assessment also plays a major role in vulnerability management
- Healthy vulnerability management is a major contributor to compliance

External references: https://youtu.be/l5At5WDj7v0, (for setting up qualys scanner)

https://youtu.be/7kcqDy7aeGg?si=W1na9U11CPawUmmR (To set up VMware Workstation)

Vulnerability Management Process

As Incident response, there is a dedicated approach to vulnerability management.

- **Discovery and Scoping:** This involves identifying all the devices, applications, and IT systems that are within an organization's network. This can be achieved by automated scanning tools, network mapping, or manual inventory checks.
- **Assessment:** this is the phase where the systems are assessed for vulnerabilities. This involves using vulnerability scanners, penetration testing, or manual.
- **Prioritization:** In this phase, discovered vulnerabilities will be prioritized based on their severity and the potential impact they could have on the organization. Vulnerabilities that pose a high risk should be addressed immediately, followed by the less risky ones.

Vulnerability Management Process (cont’d)

- **Remediation:** Vulnerabilities that have been identified and prioritized need to be fixed through patching, configuration changes, or other recommended methods. Remediation actions should first be deployed in a test environment to ensure smooth operations.
- **Verification:** After remediation efforts, the system are to be tested again to ensure that the identified vulnerabilities have been properly fixed and closed.
- **Monitoring:** Vulnerability management is a continuous process, and there is a need to continuously monitor systems for new vulnerabilities and reassess the risk posed by remaining unfixed vulnerabilities.

Knowledge Check

- What are a few common vulnerabilities you have come across in recent times

Module Summary

- Vulnerability management is a continuous process and should be taken with utmost importance

Questions