EC-Council Certified Incident Handler

Module 01 : Introduction to Incident Handling and Response

Eng. Mohammad Khreesha
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha

https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*

Information Security Policies

Security policies are the foundation of the security infrastructure that defines the basic security requirements and rules necessary to protect and secure an organization's information systems.

- The following are the goals of security policies:
  - To maintain an outline for the management and administration of network security.
  - To protect an organization's computing resources.
  - To eliminate legal liabilities arising from workers or third parties.
  - To prevent wastage of company's computing resources.
  - To prevent unauthorized modifications of the data.
  - To scale back risks caused by illegal use of the system resource.
  - To differentiate the user's access rights.
  - To protect confidential, proprietary data from theft, misuse, and unauthorized disclosure.

Threats and Threat Actors

A threat is an undesired event that attempts to access, exfiltrate, manipulate, or damage the integrity, confidentiality, security, and availability of an organization's resources.

- A threat actor or malicious actor is a person or entity that is responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity.
- Types of Threat Actors :
  - Script Kiddies.
  - Organized Hackers.
  - Hacktivities.
  - State-sponsored Attackers.
  - Insider Threat.
  - Cyber Terrorists.
  - Recreational Hackers.
  - Suicide Hackers.
  - Industrial Spies.

Incident Management

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent further recurrence of the incident.

- Incident management includes the following:
  - Vulnerability analysis
  - Artifact analysis
  - Security awareness training
  - Intrusion detection
  - Public or technology monitoring

Vulnerability Assessment

It is a process that defines, identifies, and classifies the security holes in a computer, network, or communications infrastructure.

- In addition, it can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.
- Types of Vulnerability Assessment:
  - Active Assessment
  - Passive Assessment
  - Internal Assessment
  - External Assessment
  - Application Assessment
  - Host-Based Assessment
  - Network Assessment
  - Wireless Network Assessment

https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*