Security Incident Reporting:

Link to challenge: https://academy.hackthebox.com/module/238/

(log in required)

Class: Tier I | Easy | General

Introduction to Security Incident Reporting:

Question: Name the type of an incident involving an attempt of infiltration through an email.

Answer: Phishing

Method: "Fraudulent endeavors to exfiltrate sensitive information, predominantly via email."

The Incident Reporting Process:

Question: Name the step responsible for writing down every information that could be used and be classified as important. (2 words)

Answer: Incident Logging

Method: "Every facet, action, and observation related to the security incident should be meticulously logged using an established system."

Elements of a Proper Incident Report:

Question: Name the type of a diagram that provides an overview of the attack path and the methods used by an attacker. (3 words)

Answer: Attack Vector Diagram

Method: "utilize arrows, nodes, and annotations to trace the attacker's navigation and (post-)exploitation activities through our defenses visually."