HyperionDev

Incident Response

Task

Visit our website

Introduction

In this task, you will learn about the importance of incident response in cyber security and how to develop and implement an incident response plan.

Incident response involves responding to and managing security incidents such as data breaches, cyber-attacks, or other security threats. The goal of incident response is to minimise the impact of the incident and restore normal operations as quickly as possible.

By the end of this task, you should have a solid understanding of incident response and be able to develop and implement an effective incident response plan for your organisation.

Incident response

An incident response plan is a document that outlines the steps to be taken in the event of a security incident. It includes a clear set of procedures for detecting, analysing, containing, and eradicating the threat/breach, recovering from it, and communicating with relevant stakeholders.

1. **Roles and responsibilities:** An incident response plan should clearly define the roles and responsibilities of all individuals involved in the incident response process, including the incident response team, IT staff, legal counsel, and management.

2. **Preparation:** A key component of incident response is preparation, including developing an incident response plan and training staff to implement the plan. This may also involve conducting regular drills or exercises to ensure that the incident response team is prepared to respond to a security incident.

3. **Detection:** This involves identifying the presence of a security incident, either through automated monitoring systems or through manual investigation. This may include analysing log data, network traffic, or other types of data to identify patterns of activity or anomalies that may indicate the presence of a security incident.

4. **Analysis:** This involves collecting and analysing data about the incident to determine the scope and impact of the incident and the root cause. This may include analysing log data, network traffic, or other types of data to identify patterns of activity or anomalies that may provide clues about the incident.

5. **Containment:** This involves taking steps to limit the spread of the incident and prevent further damage. This may include disconnecting affected systems from the network, shutting down affected services, or implementing other measures to isolate the incident.

6. **Eradication:** This involves identifying and removing the incident's root cause, such as by patching vulnerabilities or removing malware.

7. **Recovery:** This involves restoring normal operations after the incident has been contained and eradicated. This may include rebuilding systems, restoring data, or implementing other measures to return the organisation to its normal operational state.

8. **Communication:** This is essential in incident response, as it involves keeping relevant stakeholders informed about the incident and its progress. This may include communicating with employees, customers, regulators, and other stakeholders to provide updates and answer questions about the incident.

Extra resource

Here's a great resource that you can use as a **template incident response plan**. This template will nonetheless give you a clearer idea of the various processes and categories that could be addressed in your incident report. Please bookmark it!

The importance of incident response

Incident response is essential for several reasons, including:

1. **Financial damage:** Security incidents can result in significant financial losses, such as the cost of repairing damage or replacing lost or stolen assets and revenue due to service disruption, or handling legal costs related to data breaches.

2. **Reputational damage:** Security incidents can also damage an organisation's reputation, causing a loss of customer trust and potentially impacting the organisation's bottom line.

3. **Loss of sensitive data:** Security incidents may result in the loss of sensitive data, such as personal or financial information, which can have severe consequences for individuals and organisations.

4. **Loss of intellectual property:** Security incidents may also result in the loss of intellectual property, such as proprietary technology or confidential business information, which can blunt an organisation's competitive edge.

5. **Disruption of service:** Security incidents can disrupt the regular operation of an organisation, leading to lost productivity and potentially impacting the organisation's ability to deliver services or products to customers.

Example of a ransomware message (Meskauskas, 2022)

Extra resource

Read the SANS Institute's **fictitious example** of a phishing attack (network-based attack) that illustrates some of the details and tools used during incident response.

Programming and incident response

There are several ways that a programmer can prevent the need for incident response by employing principles such as "secure by design":

- **Use secure coding practices:** These involve writing code to minimise the risk of security vulnerabilities, such as by avoiding common coding mistakes, using appropriate input validation, and following the **principle of least privilege**.
- **Use secure frameworks and libraries:** By using specific frameworks and libraries, programmers can take advantage of specific pre-built and tested components, reducing the risk of introducing vulnerabilities into their code.
- **Follow security best practices:** There are many security best practices that programmers can follow to ensure that their code is secure, such as following the principle of least privilege, using secure communication protocols, and implementing appropriate access controls.
- **Conduct security testing:** Security testing is the process of identifying and mitigating code vulnerabilities before deployment. By conducting security testing, programmers can identify and fix vulnerabilities before they become a problem.

By following principles such as "secure by design" and adopting secure coding practices, programmers can significantly reduce the risk of security incidents and the need for incident response.

Potential career options

Here are some potential career options for someone with programming and incident response skills:

1. **Cyber security analyst:** Responsible for protecting an organisation’s networks and systems from cyber threats. This may involve using programming skills to develop custom tools and scripts for analysing data from various sources, such as log files, network traffic, and mobile devices.
2. **Digital forensics analyst:** Responsible for collecting, analysing, and presenting digital evidence supporting criminal investigations or other legal proceedings. This may involve using programming skills to automate the collection and analysis of digital evidence or developing custom tools and scripts for specific tasks.
3. **Security engineer:** Responsible for designing, building, and maintaining secure systems and networks. This may involve using programming skills to develop

custom security tools and scripts or to integrate security measures into existing systems and applications.

4. **Information security manager:** Responsible for developing and implementing security policies and procedures for an organisation. This may involve programming skills to build custom tools and scripts for monitoring and enforcing security policies.

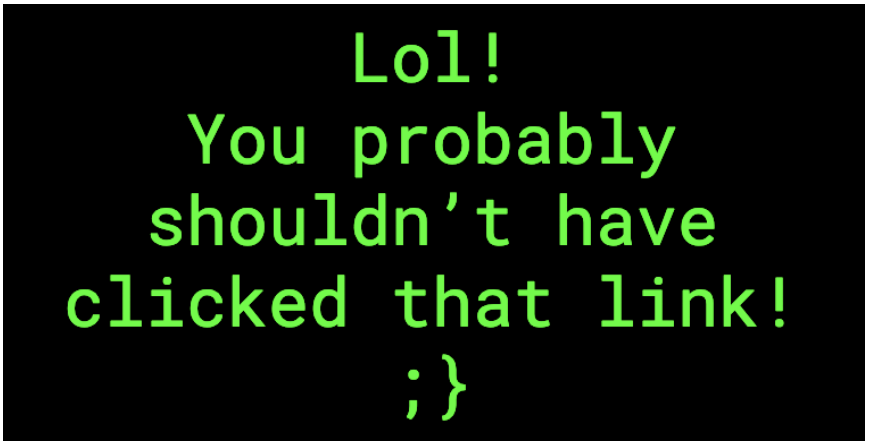
5. **Computer forensic specialist:** Responsible for collecting, analysing, and presenting digital evidence supporting criminal investigations or other legal proceedings. This may involve using programming skills to develop custom tools and scripts for analysing data from various sources, such as hard drives, mobile devices, and cloud storage.

Practical task

Imagine the following cyber attack scenario:

You work as a cyber security analyst for a medical insurance company. As such, your company is responsible for safeguarding highly sensitive personal records and ensuring compliance with national data protection legislation.

A colleague requests your urgent attention to a problem with her personal device. Her screen reveals the following image:



You are the first line of defence against a possible security breach.

Develop a simple but thorough incident plan using the components introduced in this task for responding to this network intrusion.

The plan should:

- outline the steps to be taken to detect, analyse, contain, and eradicate the security breach incident,
- specify the roles and responsibilities of the incident response team members, and
- appropriately ensure your plan reflects the severity of the risk.

Your plan does not need to be longer than 400 words. Aim to be concise and clear. And remember, you don't have much time. Valuable data is potentially at risk!

When you're done, save your plan as a PDF file titled **incident_plan.pdf** and upload it to your folder for this task.

Important: Be sure to upload all files required for the task submission inside your task folder and then click "Request review" on your dashboard.

Share your thoughts

Please take some time to complete this short feedback **form** to help us ensure we provide you with the best possible learning experience.

Reference list

Meskauskas, T. (2022, December 9). *How to remove text ransomware*. PCrisk. **https://www.pcrisk.com/removal-guides/20109-text-ransomware**