**Careers in Cyber (Tryhackme)**

**Assignment 3**

link : https://tryhackme.com/r/room/careersincyber

**Security analyst**

Security analysts are integral to constructing security measures across organisations to protect the company from attacks.

Analysts explore and evaluate company networks to uncover actionable data and recommendations for engineers to develop preventative measures

**Responsibilities**

- Working with various stakeholders to analyse the cyber security throughout the company

- Compile ongoing reports about the safety of networks, documenting security issues and measures taken in response

- Develop security plans, incorporating research on new attack tools and trends, and measures needed across teams to maintain data security.

**Security engineer**

Security engineers develop and implement security solutions using threats and vulnerability data - often sourced from members of the security workforce. The ultimate goal is to retain and adopt security measures to mitigate the risk of attack and data loss.

**Responsibilities**

- Testing and screening security measures across software

- Monitor networks and reports to update systems and mitigate vulnerabilities

- Identify and implement systems needed for optimal security

**Incident responders**

Incident responders respond productively and efficiently to security breaches. The aim is to achieve a swift and effective response, retain financial standing and avoid negative breach implications. Ultimately, incident responders protect the company's data, reputation, and financial standing from cyber attacks.

**Responsibilities**

- Developing and adopting a thorough, actionable incident response plan

- Maintaining strong security best practices and supporting incident response measures

- Post-incident reporting and preparation for future attacks, considering learnings and adaptations to take from incidents

**Digital Forensics Examiner**

if your work falls under defending a company's network, you will be using your forensic skills to analyse incidents, such as policy violations.

**Responsibilities**

- Collect digital evidence while observing legal procedures

- Analyse digital evidence to find answers related to the case

- Document your findings and report on the case

**Malware Analyst**

A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings. The ultimate goal is to learn about all the activities that a malicious program carries out, find out how to detect it and report it.

**Responsibilities**

- Carry out static analysis of malicious programs, which entails reverse-engineering

- Conduct dynamic analysis of malware samples by observing their activities in a controlled environment

- Document and report all the findings

**Penetration Tester**

A penetration tester's job role is to test the security of the systems and software within a company - this is achieved through attempts to uncover flaws and vulnerabilities through systemised hacking. Penetration testers exploit these vulnerabilities to evaluate the risk in each instance. The company can then take these insights to rectify issues to prevent a real-world cyberattack.

**Responsibilities**

- Conduct tests on computer systems, networks, and web-based applications

- Perform security assessments, audits, and analyse policies

- Evaluate and report on insights, recommending actions for attack prevention

**Red Teamers**

Red teamers are enacted to test the company's detection and response capabilities. This job role requires imitating cyber criminals' actions, emulating malicious attacks, retaining access, and avoiding detection. They are often best suited to organisations with mature security programs in place.

**Responsibilities**

- Emulate the role of a threat actor to uncover exploitable vulnerabilities, maintain access and avoid detection

- Assess organisations' security controls, threat intelligence, and incident response procedures

- Evaluate and report on insights, with actionable data for companies to avoid real-world instances