adaface

Cyber Security Analyst Job Description template

Cyber Security Analyst Job Description Template/Brief

We are looking for a Cybersecurity Analyst responsible for defending IT infrastructure (including networks, hardware, and software) against a variety of criminal activities. You will monitor networks and systems, discover security risks ('events,' analyse and assess alerts, and report on threats, intrusion attempts, and false alarms, resolving or escalating them based on severity.

In general, you will work on:

- Consultation, providing advisory services to clients
- Maintain the security of the organisation

Cyber Security Analyst Job Profile

Cybersecurity Analysts defend computer networks from cyberattacks and unwanted access. They are in charge of safeguarding your company's hardware, software, and networks from theft, loss, or unwanted access. They accomplish this by attempting to predict and protect against cyber threats and responding to security breaches when they occur.

Reports To

- Chief Technology Officer (CTO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)

Cyber Security Analyst Responsibilities

- Keep a close eye on network traffic for security problems and occurrences
- Conduct real-time investigations and respond to situations
- Create comprehensive incident response reports
- Set up and maintain firewalls, encryption software, and other security tools
- Address security flaws
- Create and disseminate best practices for information security
- Conduct threat analysis
- Conduct risk assessments and penetration testing regularly

Cyber Security Analyst Requirements & Skills

- A bachelor's degree in computer science or a comparable subject
- Strong interest in IT and a passion for cyber security
- Strong information technology abilities, including understanding of computer networks, operating systems, software, hardware, and security
- Awareness of the cyber security hazards connected with various technologies, as well as methods for mitigating them
- Solid understanding of various security technologies such as network and application firewalls, host intrusion prevention systems, and anti-virus software
- Analytical and problem-solving abilities to recognise and analyse risks, hazards, patterns, and trends
- Collaboration abilities to cooperate with team members and clients verbal communication skills, including presentation skills, with the ability to communicate with a diverse spectrum of technical and non-technical team members and other relevant persons
- Written communication abilities, such as writing technical reports
- Time-management and organisational abilities are required
- Capacity to multitask and prioritise your workload