JOB DESCRIPTION

Cybersecurity Specialists are responsible for protecting an organization's computer systems and networks from information disclosure, theft, or damage. They develop and implement security measures, monitor networks for security breaches, and respond to incidents. Their role is crucial in safeguarding sensitive data and ensuring compliance with security regulations.

SALARY

€

DAILY ROUTINE

Monitoring network traffic for unusual activity, performing system vulnerability assessments, and updating security protocols. Collaborating with IT teams to enhance system security and conducting employee training on cybersecurity best practices. Staying informed about emerging threats and implementing preventive measures.

IMPACT ON PRIVATE LIFE

The position generally involves standard office hours, but may require extended hours during security incidents or emergencies. On-call duties might be necessary to address urgent threats. While the role offers a balanced work-life dynamic, certain situations may demand increased availability.

SKILLS AND COMPETENCIES

Strong knowledge of network security, encryption, penetration testing, and vulnerability assessment is required. Proficiency in firewalls, IDS/IPS, cloud security, and SIEM tools is essential. The role demands threat analysis, risk assessment, and strong problem-solving, communication, and teamwork skills.

SELECTION CRITERIA

A strong background in network security, digital forensics, and incident response is required. Proficiency in conducting penetration testing and ethical hacking is a significant advantage. Knowledge of cyber risk management, security audits, and regulatory compliance is mandatory. Candidates should demonstrate expertise in security operations, endpoint protection, malware analysis, and cyber threat intelligence. Experience in aviation cybersecurity, ATM security, or aerospace network security is highly desirable. Some roles may require security clearance due to the sensitive nature of aviation IT systems.

Engage 2

SUPPORTED BY sesar JOINT UNDERTAKING

Co-funded by the European Union

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon Europe research and innovation programme under grant agreement No 101114648.

EDUCATION

Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or related fields.

YEARS OF TRAINING REQUIRED

Around 4-6 years to qualify for this role. The process includes a bachelor's degree (3-4 years), followed by 1-2 years of experience in network security, risk assessment, and aviation cybersecurity compliance. Certifications such as CISSP or CEH can enhance qualifications.