TECHNICAL CYBERSECURITY AUDITOR. BRATISLAVA, SLOVAKIA

Join our dynamic team at Airexplore, a proud member of the Avia Solutions Group!
Embrace the opportunity to work with a leading global aviation holding, while being based in Slovakia.

The role of a Cyber Security Auditor is crucial in ensuring the integrity, confidentiality, and availability of an organization's digital assets and sensitive information.

We are expecting from Technical Cybersecurity Auditor to conduct independent reviews to assess the effectiveness of controls and the overall compliance with the organization's legal and regulatory frameworks policies. To evaluate, test, and verify cybersecurity-related controls of systems, hardware, software and services, to ensure compliance with security requirements.

TO perform technical cybersecurity audits on the company's ecosystem. To ensure compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.

Description of responsibilities:

- Develop the company's auditing cybersecurity policy, procedures, standards and guidelines.
- Establish the methodologies and practices used for systems auditing.
- Establish the target environment and manage auditing activities.
- Define audit scope, objectives, and criteria to audit against.
- Develop an audit plan describing the frameworks, standards, methodology, procedures, and auditing tests.
- Review target of evaluation, security objectives and requirements based on the risk profile.
- Audit compliance with cybersecurity-related applicable laws and regulations.
- Audit conformity with cybersecurity-related applicable standards.
- Execute the audit plan and collect evidence and measurements.
- Maintain and protect the integrity of audit records.
- Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports.

Experience:

- At least 5 years' work experience in IT security, cyber security, or information security fields.
- Bachelor's Degree in Computer Science, Engineering, or related field.
- Proven experience of developing cybersecurity audit plan and managing auditing activities, when auditing compliance with cybersecurity-related applicable laws, regulations, and applicable standards.
- Proven experience of execution of the audit plan and collecting evidence and measurements whilst maintaining and protecting the integrity of audit records.
- Experience with developing audit reports with evaluation of the security objectives and requirements based on the risk profile.

- Previous work experience with Applications, Systems, and Cloud security, SIEM, IDS, IPS.
- Knowledge of ISO27k, NIST 800-53, CSC20, ENISA Threat Landscape, and CIS benchmarks.
- Good knowledge of the infrastructure services and technologies.
- Proven experience in AD and Microsoft 365 security, ability to architect, and implement defensive security controls.
- Experience with packet analysis tools & analyzing their output (e.g. tcpdump, Wireshark) is a bonus.
- Networking knowledge and broad understanding of networking protocols and services (e.g. SFTP, HTTPS, SSH, SMB, LDAP) is a bonus.

Key skills:

- Apply cybersecurity auditing tools and techniques, scripting languages.
- Assess and review software or hardware security, as well as technical and organizational controls in relation to system hardening.
- Decompose and analyze systems to identify weaknesses and ineffective controls.
- Communicate, explain, and adapt legal and regulatory requirements and business needs.
- Collect, evaluate, maintain, and protect auditing information.
- Security event and incident risk analysis.
- Digital forensics.
- Monitoring and log management.
- Common cybersecurity tools.

Key knowledge:

- Cybersecurity controls and solutions.
- Legal, regulatory, and legislative compliance requirements, recommendations and
- best practices.
- Monitoring, testing, and evaluating cybersecurity controls' effectiveness.
- Conformity assessment standards, methodologies, and frameworks.
- Auditing standards, methodologies, and frameworks.
- Cybersecurity standards, methodologies, and frameworks.
- English (B2 or higher).
- Cybersecurity-related certifications.

What do we offer?

- MultiSport card is your key to over 2700 sports facilities in Slovakia and the Czech Republic.
- One extra day off on your birthday.
- Snack day twice a month.
- Financial benefit to support your health, sport and beauty activities and to sponsor cultural activities and entertainment.
- Referral Bonus up to 1000 EUR.
- Daily food allowance and refreshments in the office.

Salary: from 3300 € to 4000 € (brutto)

Avia Solutions Group is the world's largest ACMI (Aircraft, Crew, Maintenance, and Insurance) provider, with a fleet of 213 aircraft. The group also provides a range of aviation services including MRO (Maintenance, Repair, and Overhaul), pilot and crew training, ground handling, as well as a variety of associated services. Supported by 12,000 highly skilled aviation professionals, the group operates worldwide.