CYBER SECURITY ANALYST. 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.

We offer work in R&D department, acting as an central unit for managing strategic, innovation and IT projects and programs.

Avia Solutions Group R&D department provides services to subsidiary companies related to IT Governance & Management, IT Service Delivery, IT infrastructure services, workplace support and ServiceDesk, Enterprise Applications (Digital IT Solutions, ERP), Cybersecurity and PMO.

Cyber Security Analyst plays a key role in ensuring continuous improvement of cyber security in Avia Solutions Group by taking care of system hardening, technical implementation of security controls, and conducting security assessments.

Description of responsibilities:

• Real-time security monitoring
• Network traffic analysis
• Cyber Security events and incidents analysis
• Security systems fine tuning (dashboards and detection rules creation, use cases management)
• Network, servers and endpoints intrusions finding
• Examination of security lapses to find their root source
• First-line cyber security incidents and alerts triage
• Contribute to the implementation of MITRE ATT&CK matrix to strengthen the sustainability of the organization cyber security.

Experience:

• 2 years' experience in IT or IT security
• Practical skills working with SIEM, IDS, IPS, EDR, WAF, VA
• Hands-on skills in malware analysis
• Skilled in log analysis and use case fine-tuning
• Knowledge about forensics methods
• Knowledge about Linux, Windows, Network, Cloud and Web applications security
• Common understanding of ISO27k, NIST 800-53, CSC20, Enisa Threat Landscape

Hard skills requirements:

• Security monitoring
• Incident response
• Security events and incidents analysis
• Digital forensics

- Malware analysis
- Any of scripting language (basics)
- Analytics mindset
- Troubleshooting

Soft skills requirements:

- Clear communication
- Well organized
- Self-Motivated
- Team Player
- Collaboration
- Creativity
- Detailed oriented
- English language (not less than B2)

Security Monitoring Toolkit:

- Endpoint detection and response tools
- Log management solutions
- ITSM tools
- Email security tools
- WAF solutions
- FW solutions
- Microsoft security center (AD Azure)

Additional responsibilities:

- Vulnerabilities scanning and registration
- Standard operating procedure preparation and fine tuning
- Alerts overview and management (security mailboxes)
- OSINT toolkit (Shodan and etc.)
- Communication with IT personnel in case of incident
- Risk identification and recommendation preparation (consultation, advisory)

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 2400 € 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.