CYBER SECURITY ANALYST. VILNIUS, LITHUANIA

Cyber Security Analyst

We are looking for a Cyber Security Analyst to join the Group Cybersecurity Operations team at Avia Solutions Group. You will become part of a centralized Cybersecurity Operations Center (SOC) responsible for protecting enterprise infrastructure, cloud services, endpoints, identities, and users across multiple subsidiary companies worldwide.

About the Team

The Group Cybersecurity Operations team acts as a central cybersecurity unit supporting subsidiary companies worldwide. The team is responsible for protecting the organization by monitoring, detecting, investigating, and responding to cybersecurity threats across a global environment.

Key responsibilities of the team include:

- Security monitoring and incident response
- Threat hunting and detection engineering
- Endpoint and identity protection
- Security platform administration and integrations
- Security governance and compliance support
- Cybersecurity awareness and advisory
- Continuous improvement of SOC capabilities, processes, and automation
- 24/7 SOC operations and support

Our environment includes modern enterprise security solutions such as:

- XDR / XSIAM platforms
- Microsoft Security Ecosystem
- SIEM and log management platforms
- Email security solutions
- Cloud security technologies
- Vulnerability management platforms

Key Responsibilities

- Perform real-time security monitoring and alert triage
- Investigate cyber security incidents and suspicious activity
- Conduct threat hunting across endpoints, identities, cloud, and network telemetry
- Analyze logs, endpoint events, authentication activity, and network traffic
- Support incident response, containment, and recovery activities
- Create and fine-tune detection rules, dashboards, and use cases
- Improve visibility and detection coverage using MITRE ATT&CK framework

- Participate in malware analysis and forensic investigations
- Identify vulnerabilities, misconfigurations, and security gaps
- Contribute to security automation and SOC process improvements
- Collaborate with IT teams and subsidiary companies during investigations
- Assist in preparation and improvement of SOC playbooks and standard operating procedures

Experience & Knowledge

- 2+ years of experience in IT, SOC, or Cybersecurity
- Understanding of cyber attack techniques, tactics, and procedures
- Practical experience with:
    - SIEM platforms
    - EDR/XDR technologies
    - IDS/IPS solutions
    - Email security solutions
    - Firewalls and WAF technologies
- Understanding of:
    - Windows and Linux security
    - Networking fundamentals
    - Cloud security
    - Identity Security
    - Application security
    - Incident response and forensic methodologies
- Familiarity with:
    - MITRE ATT&CK
    - ENISA Threat Landscape

Technical Skills

- Security monitoring and event analysis
- Incident investigation and response
- Threat hunting
- Log analysis and correlation
- Malware analysis fundamentals
- Digital forensics basics
- Detection engineering and alert tuning
- Basic scripting knowledge (PowerShell, Python, Bash, or similar)
- Analytical and troubleshooting mindset
- Understanding about malware behavior and indicators of compromise (IOCs)
- Understanding of network fundamentals (TCP/IP, DNS, HTTPS, etc.).

Soft Skills

Strong communication skills, attention to detail, ability to follow procedures, work independently and in a team, think critically, manage time effectively, and continuously learn and improve. English proficiency at B2 level or higher is required.

Nice to Have

Experience with SOC operations, SIEM, EDR/XDR, SOAR, IDS/IPS, threat hunting, scripting, MITRE ATT&CK, relevant security certifications, and aviation or enterprise environments.

What We Offer:

- Opportunity to work in a vibrant international and ever-growing business aviation environment;

- Opportunities for professional and personal growth; foreign language trainings;
- Remote work possibilities;
- Attractive salary and compensation package;
- Private health insurance;
- Gym, pool tables for your physical health;
- Children’s room where you can leave your kids to play with supervision;
- In-house canteen;
- Parking or public transport ticket;
- Electrical cars spots near the office;
- Discounts and special offers from various partners.
- Salary starting from 2800 EUR (including taxes), with potential ranges based on experience.

Join the multicultural environment of one of the largest aviation groups in the world and take a pivotal role in driving the financial success of an industry leader!

As part of our hiring process, the final candidate will be asked to complete a background verification in accordance with our internal procedures.

Salary: from 2800 € to 3200 € (brutto)

Avia Solutions Group, the world’s largest ACMI (Aircraft, Crew, Maintenance, and Insurance) provider, operates a fleet of 136 aircraft on 6 continents. Supported by 11,000 professionals, the group is the parent company to over 250+ subsidiaries including Avion Express, BBN Indonesia Airlines, and KlasJet. The group also provides a range of aviation services: MRO (Maintenance, Repair, and Overhaul), pilot and crew training, ground handling, as well as a variety of associated aviation.