

123456

## Security Operations Centre Level 1 Operator (f/m)

Engineering with respect to electromagnetic effects on military A/C at system and equipment level considering EMC / EMI:

### Your responsibilities:

- Monitor alerts, information security events and incidents identified through security event management sensors and tools
- Leverages standard supporting tools to perform initial triage of incidents identified through security event management tools and providing defined first reactions with a high quality and correctness
- Differentiates false positives from true attack attempts or dangerous or suspicious behaviours following provided instructions
- Collects information to support of the Level 2 analysts to perform deep analyses
- Escalates alarms to Level 2 analysts or administrators whenever it is needed
- Opens, tracks, and closes tracking tickets resulting from triage and investigation in the ticketing tool to provide high quality action documentation as well as reporting and metrics
- Communicates with users while fully respecting agreed communication rules, corporate identity and given mandates as well as quality requirements
- Documents any requests to the Security Operations Centre respecting customer service levels to provide a seamless and consisting documentation of ongoing activities
- Provides performance reports defined for supporting service management activities
- Create reports and visualizations of security attacks on an ad-hoc basis using defined tools and procedures
- Performs 1st Level troubleshooting with provided procedures to act within Service Level Agreements on sensor failures or IT issues encountered and communicates with the on call specialists
- Actively investigates the latest in security vulnerabilities, advisories, incidents, and penetration techniques and responsible of the customer's notification when appropriate
- Possess with an Information Security and operational oriented mindset
- Provides feedback for the development of future goals and objectives for the department and services and raises ideas for improvements within the own activity perimeter
- Participates in knowledge sharing with other operators and coordinates or participates in individual projects or team projects
- Participates in the permanent improvement and development of procedures, manuals and documentation and checks usability of these supports. Writes technical articles for internal knowledge base

### Your profile:

- A recent graduate in information technologies (IT) is a "nice to have" but not a "must have"
- Basic knowledge of information technology components networks and beginner knowledge in the field of remote service delivery and IT operations is required
- Experience in network and systems Monitoring is required
- Knowledge of information technology concepts and Technologies is required
- Experience in IT Service Desk is helpful
- Fluent English and fluent German
- Due the nature of Security Operations Centre operations, operators will be required to work in alternate shifts including nights and weekends

- The Level 1 Operator will be required to accommodate flexible working hours and shifts work over a 24\*7\*365 rotation
- Strong interest and a good background of Cyber Defence field
- Successful experience of a mission where following process and knowledge sharing within a team spirit were key points
- An active interest in cyber defence and secure information system and system security architecture
- Rigorous and respectful usage and application of procedures and first reaction instruction
- Strong attention to detail, correct and coherent documentation, correct orthography application
- Strong time management skills with the ability to multitask
- Understanding of Information Security relating to the Confidentiality, Integrity and Availability of information
- The Level 1 Operator will be required to accommodate flexible working hours and shifts work over a 24\*7\*365 rotation

**Willingness for shifts work is absolutely necessary**

Location: Taufkirchen

**What to expect from us:**

- An interesting and diversified job
- Cordial cooperation in a great team
- Individual working models
- An above-average salary and benefits

We are looking forward to your application. Please refer to the reference number in the job description. Thank you.

Please send your application to: [bewerber@scengineering.de](mailto:bewerber@scengineering.de)

For further questions please contact Ulrike Kogel (08442-67932-15).