



Senior Expert Cyber Security (DFIR) (f/m/div)*

Job description

Your heart is beating for cyber security? Taking responsibility and the ability to apply strategic guidance are part of your personal profile? If you see yourself in this area we have the perfect job to offer for you.

In your new role you will:

- Perform **advanced incident response for cyber security incidents** across the Infineon global networks.
- Incident detection through **proactive threat hunting and data analysis** of cybersecurity-relevant data sets.
- Incident **investigation using SIEM, EDR, Log Management and big data technology** based on data such as event graphs, annotations, cases and reports.
- Integrate and work with **tactical cyber threat intelligence** to enhance incident response.
- Ensure adequate documentation of cybersecurity incidents.
- Operate, maintain and enhance **tools for forensic analysis and malware analysis**.
- **Provide host and network forensics, malware analysis** during security incident response.
- **Act as the subject matter expert** for the services, processes and procedures of one of the service areas offered by our team.
- **Manage projects** of global scale in the area of incident response, digital forensics and malware analysis.
- Participate in **product evaluations** and **joint projects with the IT department** for applications and platforms of own area.
- **Mentoring and coaching** other team members and perform other duties as assigned.
- Closely work with Senior Experts of other functional areas in the team to support overall department goals.
- Join projects of other functional areas to provide support and expertise.

This position can be filled at our sites in **Munich or Klagenfurt**.

Profile

You have in-depth knowledge about fundamental concepts of networking, host security technologies and operating systems. You bring knowledge about the (Cyber) Security Incident Lifecycle / Process and corresponding standards.

You are best equipped for this task if you have:

- **Education** in the area of **computer science, IT** or a **degree in computer science, IT security** or any comparable education or degree (alternatively relevant direct experiences).

At a glance

Location: **Munich**
Job ID: **309444**
Start date: **immediately**
Entry level: **3-5 years**
Type: **Full time**
Contract: **Permanent**

Apply to this position online by following the URL and entering the Job ID in our job search:

Job ID: **309444**
www.infineon.com/jobs

Contact

Christian Miller
Talent Attraction Manager



- Direct **experience in the line of SOC/CDC/CERT** work (e.g., security monitoring and detection, incident response, network event analysis, threat analysis, threat intelligence or malware analysis).
- Direct experience with incident response, digital forensics and malware analysis.
- Direct experience with software and standard formats for digital forensics and malware analysis.
- Experience with typical **active or passive security solutions** are preferable (e.g. IDS/IPS, firewall, web-filters, malware sandboxes, EDR).
- Experience in **offensive security, pentetration testing, red teaming** (advantageous).
- Experience in **automation / scripting** (advantageous).
- Knowledge about the (Cyber) **Security Incident Lifecycle** / Process and corresponding standards.
- In depth knowledge about **fundamental concepts of networking** and **operating systems**.
- Ability to acquire **in-depth knowledge of network and host security** technologies, and continuously improve these skills.
- Possess one of the following certifications (or similar) would be an advantage: **GIAC Certified Intrusion Analyst (GCIA)**, **GIAC Certified Incident Handler (GCIH)**, **GIAC Certified, Forensic Analyst (GCFE)**, **GIAC Certified Reverse Engineering Malware (GREM)** or other **GIAC certifications**.
- Experience in technical writing and communication of technical details to various audience groups.
- Fluent English language skills (German is a plus) in speaking and writing.
- **Hands-on attitude** and **self-disciplined approach** to problem solving.
- **Taking responsibility** of own area and the ability to apply strategic guidance for own area of responsibility.

