Senior Staff Specialist Cyber Security (DFIR)

Job description

In your new role you will:

- **Perform advanced incident response for cybersecurity incidents** across the Infineon global networks.
- **Perform cybersecurity incident detection** through **proactive 'threat hunting'** and **data analysis of cybersecurity-relevant data sets.**
- **Perform cybersecurity incident investigations** 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 cybersecurity incident response.
- **Perform host and network forensics techniques** as well as **malware analysis** during cybersecurity incident response.
- **Ensure adequate documentation of cybersecurity incidents.**
- **Operate, maintain** and **enhance toolset** in help of cybersecurity incident response (e.g. digital forensic and malware analysis tools)
- **Manage projects** and **provide necessary expertise in the areas of cybersecurity incident response**, **threat hunting, digital forensics** and **malware analysis.**
- P **articipate in product evaluations** and **joint projects** with the IT department for applications and platforms of own area.
- **Team working** and **coaching other team members** as well as **perform other duties** as assigned.
- **Work closely with members from other functional areas** in the team to support overall department goals.

Profile

You are best equipped for this task if you have:

- Bachelor Degree in Computer Science, Information Technology, IT Security or any equivalent course.
- **Experience with cybersecurity incident response.** Direct experience in the fields of **digital forensics, malware analysis, threat hunting** is a strong advantage.
- **Experience as security incident analyst** or similar in the line of SOC/CDC/CERT work (e.g. security monitoring and detection, host and network security event analysis, threat analysis, threat intelligence etc.)
- **Experience with typical active or passive security solutions** is preferable (e.g. IDS /IPS, firewall, web-filters, SIEM, EDR, SOAR, etc.).
- Knowledge about the **(Cyber) Security Incident Lifecycle / Process**
- Knowledge about **fundamental concepts of networking** and **operating systems** and ability for continuous improvement.

At a glance

Location:	**Melaka**
Job ID:	**305215**
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: 305215
www.infineon.com/jobs

- **Skills in programming/scripting languages** which allows automation for incident response purposes (e.g. Python) is a plus.
- **Possession of cybersecurity incident response / analyst** related certification is a plus (e.g. GIAC based or similar certification).
- **Experience in technical writing** and **communication of technical details** to various audience groups.
- **Hands-on attitude** and **self-disciplined** approach to problem solving.