Security Operations Center Specialist

Náplň práce

As a Security Operations Specialist at our Cyber Defense Center, you will become part of our global SOC dedicated to ensuring the cybersecurity and integrity of our systems. The Team is responsible for monitoring, analyzing, and responding to security incidents using advanced tools and methodologies. Your expertise in Cybersecurity Frameworks, Standards and Operations is crucial in defending our company.

Responsibilities:

- Monitor and analyze security events and alerts generated by CrowdStrike MDR and SIEM services.
- Respond to security incidents and perform root cause analysis.
- Conduct threat hunting and proactive investigations with CrowdStrike Falcon Insight and SIEM analytics.
- Define, review and finetune Cybersecurity settings of the Falcon Agents.
- Develop, configure, and optimize SIEM solutions to enhance our threat detection capabilities (SIEM Engineering).
- Collaborate with Global SOC Team and other IT Departments to enhance security posture.
- Develop and maintain incident response plans and procedures.
- Stay updated on the latest Cybersecurity Threats and Technologies.
- Ensure compliance with industry standards and regulations.

Profil kandidáta

- Bachelor's degree in Computer Science, Information Security, or related field.
- 3+ years of relevant work experience with EDR in SOC environment.
- Experience with CrowdStrike Falcon incident response and threat hunting.
- CrowdStrike certifications such as CCFA (Certified Falcon Administrator), CCFR (Certified Falcon Responder), or CCFH (Certified Falcon Hunter) preferred.
- Familiarity with attack frameworks (MITRE ATT&CK, Cyber Kill Chain) and threat hunting methodologies.
- Knowledge of security frameworks and standards (e.g., NIST, ISO 27001, CIS Controls)
- Strong analytical and problem-solving skills.
- Strong communication and collaboration skills.
- Ability to work independently and as part of an international team
- Fluent in English

Čo ponúkame

Ready to drive with Continental? Take the first step and fill in the online application.

ID pozície
REF80016A

Miesto práce
Petaling Jaya

Úroveň vedenia ľudí
Leading Self

Flexibilita
Hybrid Job

Právnická osoba
Continental Tyre PJ Malaysia Sdn. Bhd.

O nás

Continental's digital capabilities are growing every day. Our Tires Manufacturing change accordingly IT Competence Center drives the digitization of our tire plant's processes – and we want you to join us!

We analyze business requirements and transform them into the latest digital processes and systems. This enables Continental's Tire business to continuously improve production performance and quality results in order to meet customer requirements.