Cybersecurity Specialist

Responsabilități

Join our Cyber Defense Center as a **Security Operations Specialist** and become part of a global team dedicated to safeguarding our organization's people, systems, and data. As a member of our **Security Operations Center (SOC)**, you will investigate security alerts, respond to cyber threats, and collaborate with colleagues across IT and cybersecurity functions to strengthen our security posture. Using advanced security technologies and threat intelligence, you will perform **incident investigations**, support **threat hunting activities**, and contribute to the detection, analysis, and mitigation of security risks across our global environment.

Responsibilities

- **Investigate, validate, and respond to security incidents** escalated by CrowdStrike Falcon Complete or reported by users and other IT departments.
- Investigate security incidents using CrowdStrike Falcon, Microsoft Defender and other security tools.
- Analyze alerts and suspicious activity using endpoint telemetry, threat intelligence and SIEM logs.
- Perform **root cause analysis** of security incidents and document findings and recommendations.
- Execute **containment and remediation** actions according to established procedures.
- Conduct threat analysis and participate in **threat hunting** and proactive investigations.
- Escalate complex incidents to senior analysts or specialized response teams when required.
- Document incidents, actions taken and lessons learned for compliance and operational purposes.
- Collaborate with the Global SOC team and other IT departments to enhance the organization's security posture.
- Contribute to the development, testing, and continuous improvement of incident response playbooks and procedures.
- Stay up to date with emerging cybersecurity threats, attack techniques and security technologies.
- Identify opportunities to improve **detection capabilities** and incident response processes.
- Support **post-incident reviews** and contribute to recommendations for preventing future incidents.

Cerințe

- Bachelor's degree in Computer Science, Information Security, Cybersecurity, or a related field.

Job ID
REF99445I

Domeniul de activitate
Petaling Jaya

Nivelul de Leadership
Leading Self

Flexibilitatea programului de lucru
Onsite Job

Programul de lucru
Întreagă

Persoană juridică
Continental Tyre PJ Malaysia Sdn. Bhd.

- **1-3 years of experience** in a Security Operations Center (SOC), Incident Response, IT Security, or a related cybersecurity role. Equivalent practical experience will also be considered.
- **Hands-on experience investigating security alerts and incidents** in an enterprise environment.
- Working knowledge of security monitoring concepts, alert triage, and incident investigation methodologies.
- Familiarity with attack frameworks such as **MITRE ATT&CK** and the Cyber Kill Chain.
- Basic understanding of security frameworks and standards such as NIST, ISO 27001, and CIS Controls.
- Knowledge of Windows operating systems, Active Directory, and networking fundamentals.
- Experience using security monitoring tools such as **CrowdStrike, Microsoft Defender**, SIEM platforms, or similar technologies.
- CrowdStrike certifications such as CCFA, CCFR, or CCFH are considered an advantage.
- **Ability to analyze logs, endpoint telemetry, and security events** to determine impact and scope of incidents.
- Strong analytical and problem-solving skills.
- Strong communication and collaboration skills.
- Ability to work independently and as part of an international team.
- Passion for cybersecurity and a willingness to continuously learn and develop new skills.
- Fluent in English.

Oferta noastră

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

Despre noi

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.

Continental is a leading tire manufacturer and industry specialist. Founded in 1871, the company generated sales of €39.7 billion in 2024 and currently employs around 95,000 people in 54 countries and markets.

Tire solutions from the Tires group sector make mobility safer, smarter, and more sustainable. Its premium portfolio encompasses car, truck, bus, two-wheel, and specialty tires as well as smart solutions and services for fleets and tire retailers. Continental has been delivering top performance for more than 150 years and is one of the world's largest tire manufacturers. In fiscal 2024, the Tires group sector generated sales of 13.9 billion euros. Continental's tire division employs more than 57,000 people worldwide and has 20 production and 16 development sites.