Senior Cybersecurity Specialist

あなたの仕事内容

Join our Cyber Defense Center as a **Senior 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 **lead the investigation and response** to complex cyber threats, drive continuous improvement of detection and response capabilities, and act as a **senior escalation point** for the SOC team. Using advanced security technologies, threat intelligence, and proactive threat hunting techniques, you will play a key role in protecting our global environment against sophisticated adversaries.

Responsibilities

- Investigate, validate, and respond to **complex security incidents** escalated by CrowdStrike Falcon Complete MDR Service, SOC analysts, users, and other IT departments.
- Lead investigations of **advanced security incidents** using CrowdStrike Falcon, Microsoft Defender, SIEM platforms, and other security technologies.
- Analyze alerts, suspicious activity, attack patterns, and threat actor behavior using endpoint telemetry, threat intelligence, cloud telemetry, and SIEM data.
- Perform advanced **root cause analysis**, determine attack scope and impact, and provide detailed findings and recommendations.
- Lead **containment, eradication, and recovery** activities for major security incidents.
- Conduct proactive **threat hunting** activities and initiate investigations based on intelligence, emerging threats, and hypothesis-driven analysis.
- Coordinate with Incident Response, Infrastructure, Cloud, Identity, and Business teams during major cyber incidents.
- Produce high-quality incident reports, executive summaries, lessons learned, and technical documentation.
- Collaborate with the Global SOC team and cybersecurity stakeholders to strengthen operational effectiveness and security monitoring maturity.
- Lead the development, optimization, and maintenance of incident response playbooks, use cases, and operating procedures.
- Stay up to date with emerging cybersecurity threats, attack techniques, adversary tradecraft, and security technologies.
- Develop and tune **detection rules**, analytics, and correlation logic to improve SOC visibility and effectiveness.
- Perform advanced threat modeling and map detections to the **MITRE ATT&CK** framework.
- **Mentor junior and mid-level SOC analysts** and provide technical guidance during investigations.
- Act as a senior escalation point for high-severity incidents and provide

ジョブID
REF99446J

勤務地
プタリン・ジャヤ

リーダーシップレベル
Leading Self

勤務に関する柔軟性
Onsite Job

勤務時間
フルタイム

法的事項
Continental Tyre PJ Malaysia Sdn. Bhd.

incident leadership during major cyber events.
- **Identify security gaps**, recommend strategic improvements, and drive implementation of detection and response enhancements.
- Support purple-team exercises, tabletop exercises, and adversary emulation activities to validate security controls.

あなたのプロフィール

- Bachelor's degree in Computer Science, Information Security, Cybersecurity, or a related field.
- **5+ years of experience** in Security Operations, Incident Response, Threat Hunting, or a related cybersecurity role.
- Proven experience investigating and managing complex cyber incidents in enterprise environments.
- Strong hands-on experience security monitoring operations, incident investigation, and enterprise detection technologies.
- Strong understanding of attack frameworks such as MITRE ATT&CK and the Cyber Kill Chain.
- Strong understanding of security frameworks and standards such as NIST, ISO 27001, CIS Controls, and incident response best practices.
- Advanced knowledge of Windows operating systems, Active Directory, **Entra ID**, networking, and enterprise security architectures.
- Extensive experience with **CrowdStrike**, **Microsoft Defender**, **SIEM** planforms, **EDR/XDR** solutions and cloud security technologies.
- Experience developing detection logic, threat hunting hypotheses, and security monitoring use cases.
- Experience performing malware triage, attack chain analysis, and forensic investigations.
- Understanding of cloud security concepts across Microsoft **Azure**, **AWS** and Microsoft 365 environments.
- Experience with scripting or automation using PowerShell, Python, KQL, or similar technologies.
- CrowdStrike certifications such as CCFA, CCFR, or CCFH are considered an advantage.
- Advanced cybersecurity certifications such as GCIA, GCIH, GCFA, GCFE, CISSP, SC-200, or equivalent are considered an advantage.
- Strong analytical and problem-solving skills.
- Strong communication and collaboration skills.
- Ability to work independently and as part of an international team.
- Demonstrated ability to lead technical investigations and drive cross-functional collaboration during major security incidents.
- Passion for cybersecurity and a willingness to continuously learn and develop new skills.
- Fluent in English.

オファー

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

会社概要

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.