You’re an important part of our future. Hopefully, we're also a part of yours! At B. Braun, we protect and improve the health of people worldwide. This is also our vision for research and development. You see complexity as an opportunity – and quality and sustainability are important criteria for your work. We would like to work with you on tomorrow’s solutions. That’s how we work to create sustainable healthcare – locally, in regions, countries and worldwide. Together. That's Sharing Expertise.

Security Analyst

Reference Code PL-KW 0098-86426

As a Security Analyst in our CDC (Cyber Defense Center) Department, you will play a crucial role in safeguarding our organization’s digital assets. Your responsibilities will span various aspects of cybersecurity, including threat detection, incident response, and vulnerability management. You’ll collaborate with cross-functional teams to enhance our security posture and ensure compliance with industry standards.

Duties and responsibilities

- Security Monitoring (monitoring security events and alerts using our SIEM system, investigating and analyzing suspicious activities, collaborating with the incident response team)
- Threat Hunting / Purple Team (conducting proactive threat hunting exercises, collaborating with the red team, providing actionable insights to improve our security controls)
- Security Incidents (responding to security incidents, coordinating incident handling, containment, eradication, and documenting the recovery efforts)
- Incident Response (developing and maintaining incident response playbooks and procedures, participating in tabletop exercises and real-time incident simulations)
- Penetration Testing (collaborating with external penetration testers or conducting internal penetration tests, identifying vulnerabilities in our systems, applications, and network infrastructure.
- Vulnerability Management (coordinating vulnerability scanning and patching management efforts, ensuring timely remediation of critical vulnerabilities)
- KPI / Compliance Monitoring (defining and tracking key performance indicators (KPIs) related to security operations, monitoring compliance with security policies, standards, and regulations)

Professional competencies

- Bachelor’s degree in Computer Science, Information Security, or a related field (or equivalent experience).
- Relevant certifications (e.g., CISSP, CEH, CompTIA Security+, etc.) are highly desirable.
- Strong analytical skills and attention to detail.
- Experience with security tools, such as SIEM platforms, vulnerability scanners, and penetration testing frameworks.
- Knowledge of industry standards (ISO 27001, NIST, CIS Controls, etc.).

Personal competencies

- passionate about cybersecurity
- willing to learn attitude is required

What we offer

Become part of a corporate culture that actively promotes constructive exchanges between colleagues, customers and partners. Work with us to improve people's lives in the long term. We can offer you interesting, varied tasks and excellent opportunities for advancement, as well as an attractive salary with extensive benefits, all within a dynamic family-owned company.

Benefits

- Active participation in challenging developmental projects
- Open communication at all levels of the hierarchy
- Personal and professional development
- Stable work in a friendly team
- Flexible working hours
- Free foreign language courses

- Training and integration events
- Private medical care
- Group Insurance
- Multisport card

Closing date

31.05.2024

Your next step

Contact us!

Contact: B. BRAUN BUSINESS SERVICES POLAND SP. Z | Katarzyna Wiercińska | +48 728-965-202