You’re an important part of our future. Hopefully, we're also a part of your future! At B. Braun, we protect and improve the health of people worldwide. You support this vision, bringing expertise and sharing innovation, efficiency and sustainability as values. That’s why we would like to keep developing our company with you. Keeping your future in mind, we’re making a joint contribution to health care worldwide, with trust, transparency and appreciation. That's Sharing Expertise.

Security Analyst (CDC Department)

Reference Code ES-SBL-DLO-87433

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
- Monitor security events and alerts using our SIEM (Security Information and Event Management) system.
- Investigate and analyze suspicious activities, anomalies, and potential threats.
- Collaborate with the incident response team to address security incidents promptly.
- Threat Hunting / Purple Team
- Conduct proactive threat hunting exercises to identify potential vulnerabilities and attack vectors.
- Collaborate with the red team (offensive security) to simulate real-world attacks and assess our defenses.
- Provide actionable insights to improve our security controls based on purple team findings.
- Security Incidents
- Respond to security incidents promptly and effectively.
- Coordinate incident handling, containment, eradication, and recovery efforts.
- Document incident details and lessons learned for continuous improvement.
- Incident Response
- Develop and maintain incident response playbooks and procedures.
- Participate in tabletop exercises and real-time incident simulations.
- Work closely with other teams (network, IT-Security, system administrators, etc.) during incident resolution.
- Penetration Testing
- Collaborate with external penetration testers or conduct internal penetration tests.
- Identify vulnerabilities in our systems, applications, and network infrastructure.
- Provide actionable recommendations to remediate identified weaknesses.
- Vulnerability Management
- Regularly assess and prioritize vulnerabilities across our environment.
- Coordinate vulnerability scanning and patch management efforts.
- Ensure timely remediation of critical vulnerabilities.
- KPI / Compliance Monitoring
- Define and track key performance indicators (KPIs) related to security operations.
- Monitor compliance with security policies, standards, and regulations.
- Generate reports and metrics for management and stakeholders.

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.
- 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

- Strong analytical skills and attention to detail.
- Residence in Barcelona

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.

Closing date

30.06.2025

Your next step

Contact us!

Contact: B. Braun Medical S.A. | Soledad Barragan | 935866200