TELEMAR

Security Operations Analyst
Rome

About Telemar

For over 75 years, our maritime journey has been fuelled by expertise and innovation. We're not just a service provider; we're offering a dynamic blend of bridge electronic solutions, onboard and maintenance services.

We don't just adapt; we thrive on constant innovation. Telemar is an expert partner who supports more than 3,000 vessels, rely on our tailored services. We're not just about cutting-edge technology; we're a navigational ally, enhancing safety and operational efficiency by keeping costs down.

Role description

This is a full-time on-site role for a Security Operations Analyst at Telemar's Rome location. The Security Operations Analyst is responsible for monitoring and protecting the organization's IT infrastructure from security threats and vulnerabilities, ensuring robust defenses against potential cyber-attacks.

Main Goals

- Ensure continuous monitoring and analysis of security alerts and logs.
- Maintain the integrity and security of the organization's IT infrastructure.
- Proactively identify and remediate security vulnerabilities.

Qualification, skills & requirements

Main Tasks:
Threat Detection and Response:
- Monitor security alerts and logs to identify potential security incidents.
- Investigate and respond to security incidents promptly.
- Conduct root cause analysis and implement preventive measures.

Vulnerability Management:
- Regularly conduct vulnerability assessments and penetration testing to identify security weaknesses.
- Work with IT and development teams to prioritize and remediate vulnerabilities.
- Track and document vulnerabilities and their remediation status.

Infrastructure Security Management:
- Manage identity and access management (IAM) systems to control user access to sensitive information and systems.
- Implement and maintain security controls for servers, networks, and endpoints.
- Ensure secure configuration and management of firewalls, routers, and other network devices.

Security Operations:
- Conduct security audits.
- Respond to security related tickets raised by employees.
- Maintain KPIs related to Security Operations.

Responsibilities and Authorisation

- Monitor and analyze security alerts, logs, and reports to detect potential security incidents.
- Conduct regular vulnerability assessments and penetration tests.
- Manage identity and access management (IAM) systems.
- Collaborate with IT and development teams to prioritize and remediate identified vulnerabilities.
- Respond to security incidents, conduct investigations, and implement corrective actions.
- Stay up to date with the latest security trends, threats, and technologies.

Minimum Requirements
Necessary experience & qualifications:

- 2 to 3 years of demonstrable professional experience in the role.
- A Bachelor's Degree in Computer Science, Information Technology Cybersecurity, or a related field is required.
- Fluent in English, written and spoken.

It will be highly valued:

- A Master's Degree in Cybersecurity, Information Systems, or a related field.
- Deep knowledge of ISO27001, GDPR, NIST and MITRE Framework.
- Any of the following certifications: CEH, CISM, CompTIA, OSCP, CISA, and CISM.

Our Commitment

Our Corporate Social Responsibility approach is part of the Marlink DNA to develop our business and people operate responsibly. Marlink has incorporated and respects the Ten Principles of the UN Global Compact into our strategies to establish a culture of integrity, value, trust and innovation.

The Marlink Group is a transnational organization and considers cultural diversity as one of its greatest strengths. Additionally, we support diversity in race, gender, religion, national origin, political opinion, sexual orientation, social origins, age and physical or mental character.

In support of

WOMEN'S EMPOWERMENT PRINCIPLES

Established by UN Women and the UN Global Compact Office

WE SUPPORT

UN GLOBAL COMPACT

Interested?

Please send your CV including possible start date and location to:
pablo.sanzmoreno@marlink.com
The person of contact is:
Pablo Sanz Moreno

We look forward to receiving your job application!