Sr. Security Operations Engineer

Hiring organization
PulseHRM

Employment Type
Full-time

Job Location
Porvorim, Goa
Remote work possible

Working Hours
6:30pm – 2:30am IST

Date posted
August 6, 2024

Valid through
31.08.2025

Description

The Sr. Security Operations Engineer is responsible for executing the design, implementation, and maintenance of security systems, processes, and controls to protect the organization's IT infrastructure, data assets, and information systems. The role will collaborate with cross-functional teams to develop and execute security strategies, policies, and initiatives to mitigate security risks and ensure compliance with industry standards and regulatory requirements.

Responsibilities

- Ability to execute simultaneous projects to successful delivery.
- Ability to communicate (verbally and in writing) effectively with stakeholders and senior business leadership of departments and customers participating in this project.
- Ability to organize and work effectively with project teams made up of internal staff and/or external parties.
- Demonstrated experience and relevant expertise in the configuration and deployment of Information Systems business solutions.
- Strong technology skills with the ability to synthesize relevant information and make key decisions.
- Strong analytical skills to relate security requirements to appropriate security controls including sensitive data management.
- Strong project management skills and experience in creating and managing project plans, including budgeting and resource allocation.
- Excellent communication abilities and relationship building skills.
- Written, verbal, and presentation skills with the ability to effectively interact with internal and external business partners.

Qualifications

- Minimum of 5 years of progressive experience in security operations, with demonstrated expertise in threat detection, incident response, and implementing security frameworks in enterprise environments.
- Bachelor's degree in Computer Science, Information Security, or related field; Master's degree or relevant certifications (e.g., CISSP, CISM, CEH) preferred.
- Proven experience in security operations.
- In-depth knowledge of security technologies, tools, and practices, including threat detection, incident response, encryption, network security, and security frameworks.
- Demonstrated experience in leading teams, including day-to-day prioritization of work, reviewing system changes and approving all work going into Production.
- Preferably proven experience in building relationships with business partners to align and deliver on common objectives for the company.
- Excellent verbal and written communication skills in English, with the ability to convey complex technical concepts clearly to both technical and non-technical stakeholders.
- Preferred MSP experience.
- Experience with Active Directory, AWS, Oracle, Azure/Entra, and other Cloud technologies.

- Experience with Linux access control.
- Experience with secure authentication strategies.
- Knowledge of and experience with cloud architecture deployments and SaaS, PaaS and IaaS solutions.
- PowerShell scripting.
- In Depth understanding of Network Security.
- In Depth knowledge of security tools such as, endpoint security tools, network monitoring tools, SIEM, Phishing Simulation tools, Vulnerability Management & App Code Analysis tools, Web Application Firewalls tools, Email Security Platforms.