

Security Operations and Architecture Principal

Description

The Security Operations and Architecture Principal is responsible for leading and managing the security operations and architecture team within the organization. This hands-on leadership role involves leading the execution of 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

- 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

Functional Competencies:

- Experience leading and building Information Systems delivery organizations.
- Demonstrated leadership qualities communicating and reporting at the business and IT executive level.
- 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

Hiring organization

PulseHrm

Job Location

Porvorim, Goa

Working Hours

3.30 pm to 11.30 pm IST

Date posted

June 18, 2024

Valid through

18.07.2024

- 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 and architecture, with at least 4 years of experience in a managerial or leadership role.
- 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

It's not expected that any single candidate would have expertise across all of these areas. If you believe you meet a majority and are excited to learn what you do not already know, Please Apply!

"We are an equal opportunity employer. All applicants will be considered for employment without attention to race, color, religion, sex, sexual orientation, gender identity, national origin, veteran or disability status."