

Anzen Technologies Pvt. Ltd.

Phone: +91-9052577661

Email: contact@anzentech.com

Website: www.anzentech.com

Job title: SOC Manager

Location: Mumbai

Division/Department: SOC

Number of Vacancies: 1

Educational Qualifications: BE-IT / B Tech /Comps

Certifications: CEH or equivalent

Additionally, one more certification in information security domain as mentioned below or equivalent.

CISSP

PMP

GCIH

GSEC

Experience: Min. 8-10 years

Essential Duties and Responsibilities:

- Lead and Manage Security Operations Centre
- Primarily responsible for security event monitoring, management and response
- Ensure incident identification, assessment, quantification, reporting, communication, mitigation and monitoring
- Ensure compliance to SLA, process adherence and process improvisation to achieve operational objectives
- Revise and develop processes to strengthen the Security Operations framework, Review policies and highlight the challenges in managing SLAs.
- Responsible for team management, overall use of resources and initiation of corrective action where required for Security Operations Centre.
- Management, administration & maintenance of security devices under the purview of SOC which consists of state-of-the art technologies.
- Perform threat management, threat modeling, identify threat vectors and develop use cases for security monitoring
- Responsible for integration of standard and non-standard logs in SIEM
- Creation of reports, dashboards, metrics for SOC operations and presentation to Sr. Mgmt.
- Co-ordination with stakeholders, build and maintain positive working relationships with them

Education and/or Work Experience Requirements:

- Proficient in Incident Management and Response
- Experience in security device management and SIEM

- In-depth knowledge of security concepts such as cyber-attacks and techniques, threat vectors, risk management, incident management etc.
- Experience in threat management,
- Knowledge of various operating system flavors including but not limited to Windows, Linux, Unix
- Knowledge of applications, databases, middleware to address security threats against the same.
- Proficient in preparation of reports, dashboards and documentation
- Excellent communication and leadership skills
- Experience in performing vendor management
- Ability to handle high pressure situations with key stakeholders
- Good Analytical skills, Problem solving and Interpersonal skills
- Working knowledge and experience with MS office with proficiency in Excel.