Anzen Technologies Pvt. Ltd.

Phone: +91-9052577661
Email: contact@anzentech.com
Website: www.anzentech.com

Job title: Senior Consultant

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 SIEM domain as mentioned below or equivalent.
SIEM Analyst
SIEM Administrator
Network and Security tools
OSCP will be preferred.

Experience: Min. 5-8 years

Essential Duties and Responsibilities:

- Implementation, administration, maintenance and troubleshooting of SIEM
- Creation of new content consisting of rules, dashboards, reports etc.
- Design and implement use cases
- Create content based on provided use cases
- Perform integration of new device logs in SIEM
- Perform SIEM capacity assessments and planning
- Co-ordinate with SOC team and assist them in SIEM related activities
- Perform system health assessments and fix issues
- Preform new installations, updates, upgrades and configuration changes in SIEM
- Fine tuning of SIEM alerts
- Develop custom log collection agents
- Co-ordinate with SIEM support team

Required Skills:

- Excellent knowledge and hands-on comprehensive experience working on SIEM tool(s) on administrative level
- Expertise on developing correlation rules and creation of Dashboards, Reports and Documents as per

customer requirement
- In depth knowledge of SIEM functioning
- Knowledge of various operating system flavors including but not limited to Windows, Linux, Unix
- Excellent communication skills, with a view of interacting with various vendors as well as stakeholders and articulating customer requirements
- Good Analytical skills, Problem solving and Interpersonal skills
- In-depth knowledge of security concepts such as cyber-attacks and techniques, threat vectors, incident management etc.
- Knowledge of applications, databases, middleware to address security threats against the same.
- Experience in security device management and security tools
- Experience in threat management
- Experience in Incident Management and Response