Anzen Technologies Pvt. Ltd.

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

Job title: SOC Level 1 Engineer

Location: Mumbai

Division/Department: SOC

Number of Vacancies: 1

Educational Qualifications: BE-IT / B Tech /Comps

Certifications: CEH or equivalent

Experience: Min. 0-2 years

Essential Duties and Responsibilities:

- Continuous Monitoring of real time security alerts generated from SIEM and monitoring consoles
- Correlation of security alerts with threat intelligence and other sources of information
- Level 1 analysis of the alerts to identify the criticality, source, type of incident etc.
- Identifying the right stakeholders for assigning the incident for further investigations
- Creating a security incident ticket in ticket management system for analysis and recording
- Follow-up with stakeholders for incident remediation and ticket closures
- Identify and highlight false positives
- Assist Level 2 and Level 3 engineers with required information and tasks during incident response
- Perform basic administration activities of various security tools such as SIEM, IPS, Firewall etc.
- Perform daily maintenance checklists
- Assist the Level 2 engineers in implementation and upgradation activities
- Assist Level 2 engineers in configuration management of devices, taking backups and health monitoring
- Assist in Policy Management
- Generate Reports and Dashboards based on request
- Adhere to agreed SLAs and escalation procedures
- Provide necessary inputs to Level 2 and Level 3 engineers for tuning use cases, reducing false positives, increase monitoring efficiency and streamlining procedures & process workflows
- Validation of alerts and event received after new device integration
- Follow shift hygiene and discipline

Education and/or Work Experience Requirements:

- Knowledge of Incident Monitoring, Management and Response
- Experience in real time security alert monitoring, ticket management, incident investigation and analysis
- Experience working on various security tools such as SIEM, Firewall, IPS, Proxy, URL Content Filtering, Mail Gateways etc. is preferred

- Experience in generating reports and dashboards as per client requirements in SIEM
- Knowledge of security concepts such as cyber-attacks and techniques, threat vectors, risk management, incident management etc.
- Experience in threat management
- Knowledge of applications, databases, middleware to address security threats against the same is preferred.
- Experience in preparation of reports, dashboards and documentation in Excel, Word and PowerPoint
- Good communication and collaboration skills
- Good Analytical and Problem solving skills
- Working knowledge and experience with MS office.