Anzen Technologies Pvt. Ltd.

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

Job title: SOC Level 2 Engineer

Location: Mumbai

Number of Vacancies: 2

Educational Qualifications: BE-IT / B Tech /Comps / MCA

Certifications: CEH or equivalent and minimum one product certification such as Checkpoint, Juniper, Cisco etc.

Experience: Min. 2-4 years

Essential Duties and Responsibilities:

- Perform Administration, Maintenance and Management of security devices and tools such as Firewall, IPS, URL Content Filtering, Proxy, Mail Gateways, SIEM, DLP, DAM etc.
- Perform configuration of security devices such as backup, networking, time sync, user roles, Domain Integration, email configuration etc.
- Policy Management and fine tuning
- Perform checklists and health monitoring activities
- Troubleshooting of issues observed in security tools
- Co-ordination with OEM support
- Co-ordination with client and other stakeholders with respect to device management
- 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 2 analysis of the alerts to identify the criticality, source, type of incident etc.
- Follow-up with stakeholders for incident remediation and ticket closures
- Assist Level 3 engineers with required information and tasks during incident response
- Generate Reports and Dashboards based on request
- Adhere to agreed SLAs and escalation procedures
- Perform tuning of use cases, reducing false positives, new device integration in SIEM, increase monitoring efficiency
- Assist Level 3 engineer in streamlining of procedures & process workflows
- Create required documentation
- Manage L1 engineers & act as next level of escalation for their queries.
- Follow shift hygiene and discipline in line with customer requirements.

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.

- Experience in generating reports and dashboards as per client requirements
- 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
- Experience in working & managing operations at customer locations.
- Good communication and collaboration skills
- Good Analytical and Problem solving skills
- Working knowledge and experience with MS office.