Adarsh V S

Soc Analyst

Actively looking for SOC analyst role in a quality driven environment where i can contribute to the Company with my technical skills and also enhance my technical knowledge, which will be utilized to grow constantly along with the company.

Contact

☎ +91 9108695114

✉ adarshsheelavantar1@gmail.com

https://www.linkedin.com/in/ adarsh-sheelavantar-998658248/

Education

Bachelors of computer applications(BCA)

From: KLS gogte college of commerce, Belagavi

Year of passing: 2022

TOOLS & TECHNOLOGIES

- Security information and event management (SIEM)
- Splunk
- IBM Qradar
- Analysis tools: IPVOID, Virus Total, URL void, AbuseIPDB.
- Vulnerability assessment
- Rapid7 Nexpose
- Tenable Nessus
- Putty

CERTIFICATIONS

- Fortinet NSE1 & NSE2
- Splunk E-learning
- SOC Analyst training SOC Experts
- Qualys Vulnerability Management

Languages

- **English, Kannada, Hindi**

TECHNICAL SKILLS

- Good knowledge on Networking concepts: OSI model, TCP/IP model, IP, NAT, PAT, networking devices, TCP three way handshake.
- Knowledge on security concepts: CIA, AAA, MFA, Defense in Depth, VPN.
- Knowledge onCyber kill chain, MITRE attack framework.
- Understanding of servers: DNS, DHCP
- Security solutions: Firewall, IPS, IDS, VPN, Proxy.
- Understanding of Cyber attacks, types of attacks and phases of attack.
- Knowledge on OWASP top 10, Threat Intelligence, vulnerability assessment and management, raw logs.
- Understanding of SIEM technology and hands on experience on Splunk,
- Monitoring logs & triggered alerts.
- Log analysis, Malware analysis, alert analysis, Email analysis and threat intelligence.
- Creating Alerts, Reports and dashboards.
- Creating Sites and deletion of sites in Insight VM
- Adding assets and deleting assets
- Performing VA Scans
- Generating Reports
- Performing Compliance Scans
- Editing Scans templates
- Excluding parameters and vulnerabilities
- Good knowledge on open source terminal emulator (Putty)

SOC ANALYST SKILLSET

- Monitoring and analyzing the logs & triggered alerts 24*7.
- Acknowledging and closing false positive alters and raising tickets for validated incidents.
- Assisting IR team/ System team in remediation's by providing supporting data and recommendations.
- Monitoring and troubleshooting silent log sources.
- Drafting shift handovers.