KOMAL GORE

• komalgore713@gmail.com
• +91 8007503589
• Mumbai, Maharashtra.
• www.linkedin.com/in/komal-475503213/

SUMMARY

Accomplished Knowledge in Information Security and handling wide Gamut of Security functions as an Information Security (SIEM), Security Monitoring and SOC Professional.

PROFESSIONAL EXPERIENCE

Designation : SOC Analyst L1 at SysTools Software Pvt. Ltd., Pune.
[JUL 2022 - APR 2024 (1 Year 9 months)]

- Dashboard Monitoring
- Event log analysis
- Incident Response & Reporting.
- Hands on Experience on SIEM tool (AlienVault), Scanning tools (Nmap, Nessus), Kali Linux, Cisco packet tracer.

SKILLS

- Approx. 2 years of experience in Cyber Security Specialization in SOC, SIEM, Incident Response.
- Daily health check Monitoring and Reporting.
- Managing day to day SIEM operation.
- Aggregating and Correlating the Logs and Configuring Reports, Queries, Rules, Filters, Dashboards, Real Time Alerts.
- Monitoring Dashboards for any malicious activity checks.
- Understanding of SOAR product.
- Daily reports and alerts analysis, and checking if any false positive or true positive.
- Threat analysis and Preparation of Incident report.
- Raising true positive incidents to respective stack holders and taking appropriate actions.
- Experience Service now ticketing tool.
- Pulling and analysing logs for the investigation cases.
- Creating monthly reports and sending them to stakeholders for audit purposes.
- Understanding of the MITRE ATT&CK framework.

EDUCATION

SGBA University, Maharashtra. 2020
B.E in Computer Science, GPA: 9

CERTIFICATIONS

- CEH (Certified Ethical Hacker v11) JAN-2023
- Training of CCNA (Cisco Certified Network Associate)
- MSCIT (Maharashtra state Certificate in Information Technology)