babithabanagani@gmail.com
8297465536

BABITHA BANAGANI

CAREER OBJECTIVE

Result-oriented professional with 1.7+ years of experience in Information technology and Proven knowledge of Information security. Aiming to leverage my skills to successfully fill the SOC Analyst role at your company.

PROFESSIONAL SUMMARY

- Having 1.7+ years relevant experience in Information Security and currently working as Security Analyst (SOC Team)
- Working in Security Operation Center (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Experience on SIEM (Security Information and Event Management) tools like Monitoring real-time events using IBM QRadar tool.
- Responding to various security alerts for client and scanning for vulnerabilities.
- Experience on performing log analysis and analyzing the crucial alerts at immediate basis.
- Experience in generating Daily, Weekly & Monthly Reports from IBM QRadar and DLP.
- Preparing reports as per client request, preparing knowledge base and use cases.
- Monitoring incidents and taking the immediate action in Sophos.
- Troubleshooting the definitions, out-of-date and other AV related issues.
- Filling the Daily health checklist and status of Security Devices and Connectors.
- Manage and apply policies such as centralized exception policies

SKILLS & Tools

- Malware Analysis
- Incident Response
- Threat Intelligence

- SIEM Tool: IBM QRadar
- Endpoint security: Sophos.
- Email Security: TrendMicro cloudapp tool.
- Ticketing Tool: ServiceNow.
- Operating Systems: Windows.
- Analysis Tools: VIRUS TOTAL, SHODAN.IO
- Work environment: Cyber Threat Analysis, Monitoring, Phishing Mails, incident response.

EDUCATION

- B. Tech in ECE from JNTU Anantapur

WORK EXPERIENCE

Currently working as Security Analyst in HCL Technologies, Chennai from January 2021 to Till Date

PROFESSIONAL EXPERIENCE

Project - Security Operation Center(SOC). Endpoint Security
Role – SOC Analyst

SIEM TOOL: IBM QRADAR

- Monitoring real-time events using SIEM tool IBM QRadar.
- Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Investigating and reporting on daily scan activities.
- Creating incidents for suspicious issues using ServiceNow ticketing tool and assign it to concerned teams for further investigation on incidents.
- Analysing and reporting detailed information related on the Data Loss Prevention alerts using the tools like Websense Triton.
- Managing the Incident reports from IBM QRadar and ServiceNow ticketing tool.
- Generating the Daily, Weekly, Monthly reports from IBM QRadar, IPS and IDS.
- Identifying and analysing Brute Force, DOS(Denial Of Service), Ransomware, SQL Injection & Phishing attacks.
- At the end of shift passing the shift handover report with all encountered issues and follow-ups will be submitted to next shift guys.

ANTIVIRUS: SOPHOS ENDPOINT PROTECTION

- Perform daily System monitoring, verifying the integrity and availability in accordance with standards and project/operation requirements.
- Verify Sophos Endpoint Protection clients are online and functional.
- Used to perform the AV scans on endpoints which we identify malicious activity detect on endpoints.
- Investigating incidents, remediation, tracking and follow up for incident closure with concerned teams and stakeholders.
- Helped in providing documentation and support through creating procedural documents like SOP.
- Raised Change, Problem tickets and incidents – Implemented the changes and provided the resolution on time.
- Given KT related to different topics as a part of Shift-Left approach.
- Draft Shift Handover.

CERTIFICATIONS

- Qualys Guard Vulnerability Management

PLACE:
DATE:

BABITHA BANAGANI