BABITHA BANAGANI – SOC Analyst

📞 8297465536   ✉ babithabanagani@gmail.com

in www.linkedin.com/in/babitha-banagani   📅 12-08-1997

TECHNICAL SKILLS

Tools

IBM QRadar	ServiceNow	Sophos
VirusTotal	Shodan.io	Qualys
Websense Triton	TrendMicro	

Skills

Incident Response	Malware Analysis
Threat Intelligence	Monitoring
Phishing Mails	Cyber Threat Analysis
Windows	Security Testing

CERTIFICATIONS

Qualys Guard Vulnerability Management

EDUCATION

2014 - 2018
Bachelor of Technology, ECE
JNTU Anantapur.

STRENGTHS

- Investigating Skills
- Communication in Detail
- Client Engagement
- Teamwork & Leadership
- Presentation Skills

PROFESSIONAL SUMMARY

Motivated IT Professional with 1.10 years of experience as SOC Analyst; Cybersecurity testing, Monitoring and system surveillance for suspicious events using IDS and SIEM tools.

- Extensive experience in Incident management and incident response.
- Perform investigating and evalutions of network traffics, read and interpret logs. Analysing of cyber attacks prone, Endpoint security.
- Monitoring security events, proxy logs, IPS/IDS events, web application Firewalls, User verification, Vulnerability scans and generating reports.
- Detection and prevention of intruder attempts. Conducting health checks, investigating, reporting daily scan activities.

WORK EXPERIENCE

SOC Analyst – Endpoint Security

HCL Technologies   *Oct 2020 – Present*

SIEM Tool : IBM QRadar

- Monitoring realtime events using SIEM tool IBM QRadar, SOC Events.
- Creating incidents for suspicious issues using ServiceNow and assigning it to concerned teams, following up till closure.
- Analysing, reporting detailed information on data loss prevention alerts using Websense Triton.
- Generating Daily, Weekly and monthly reports from IBM QRadar, IDS and IPS. Manage and apply centralized exception policies.
- Identifying and analyzing Brute force, Denial of Service (DoS), phising, ransomware, and SQL Injection attacks.
- Handling the progress to SOC team via standup calls, conducting knowledge transfer sessions to new resources and other teams.

Antivirus : Sophos Endpoint Protection

- Perform daily system monitoring, verifying the integrity and availability in accordance with standards of project/ operation requirements.
- Verifying sophos endpoint protection are online and functional, providing updation support to clients/ business teams.
- Perform AV scans to identify malicious activity occurrence on endpoints and troubleshooting the definitions, out of date issues.
- Investing incidents, remediation, tracking and following up for incident closure with concerned teams and stakeholders.

- Raised change, problem tickets, incidents, and implemented them on time. Monitoring incidents and taking immediate action.
- Responsible for providing documentation and support through creating procedural documents like SOP and drafted shift handover.