VENKATESH C

Cybersecurity Analyst

Bengaluru, India

+91 7353609734

cvenkatesh208208@gmail.com

https://www.linkedin.com/in/venkatesh-c-414124233/

SUMMARY

Experienced SOC Analyst with 2 years in threat detection, incident response, and security monitoring. Skilled in SIEM tools, malware analysis, phishing investigations, and log analysis. Expertise in threat mitigation and enhancements to organizational security posture, focusing on incident management and security metrics analysis. Passionate about threat intelligence and proactive threat hunting to enhance cybersecurity defenses.

SKILLS

- Incident Response & Management
- Threat Detection and Analysis
- SIEM tools expertise
- Network and System Monitoring
- Malware analysis
- Collaboration & Escalation
- Incident automation
- Security Tools and Technologies
- Log Analysis and Monitoring
- Use case fine-tuning
- Cloudflare alert & Log Analysis
- Windows, Linux
- MITRE ATT&CK Framework
- Security audits and compliance
- Threat Hunting & Intelligence

CERTIFICATIONS

- Qualys: Endpoint Detection and Response ABC of Malware | SOC Experts
- Aviatrix Certified Engineer: Multi cloud Network Associate
- Qualys: Basic concept of Vulnerability Management.
- Fortinet: NSE1 and NSE2

HANDS ON KNOWLEDGE ON TOOLS

- SIEM- Proact, Splunk, IBM Qradar
- Threat Intelligence (OSINT)
- DDoS-Cloudflare
- Virus Total, MX Toolbox, Abuse IPDB, IBM X-force exchange
- EDR-Microsoft Defender, TrendMicro Vision One, CrowdStrike
- Sandbox- Any Run, Wireshark
- Microsoft O365 defender
- VPN- Fortinet, Sophos

EXPERIENCE

CYBERSECURITY ANALYST, 03/2023 - Current
SISA Information Security PVT. LTD., Bangalore, India

- Monitor security events and alerts using the Proact SIEM tool (an in-house built tool based on ELK) to identify potential threats and vulnerabilities across multiple client environments.
- Investigate security incidents and alerts, conduct root cause analysis, and escalate incidents to clients.
- Conduct thorough forensic analysis, including log reviews, to determine impact of security incidents.
- Support major security incidents, identify indicators of compromise (IOCs), and assist in containment and remediation activities.
- Implement and fine-tune detection rules and dashboards within SIEM to improve event correlation and reduce false positives by 20% to 30%.
- Prepare daily, weekly SOC reports, DDoS reports.
- Collaborate with the Integration team to drive key activities.
- Skilled in log monitoring and threat hunting using raw logs.
- Collaborate with internal teams and clients to ensure timely response and resolution of security incidents.
- Perform threat hunting and vulnerability assessments to proactively identify potential weaknesses.
- Research solutions and implementations to meet client requirements.
- Provide daily firewall traffic reports, IDS/IPS alerts, open tickets status, and prepare weekly & monthly KPI reports
- Ensured adherence to security policies, compliance standards, and industry best practices while analyzing and responding to security incidents.

EDUCATION

Jain Institute of Technology (VTU)
B.E: Electrical and Electronics Engineering

ACCOMPLISHMENT

- Recognized for developing creative automation solutions that improved security workflows.
- Awarded by SISA Infosec for exceptional handling of Multiple CAT-A client relationships.
- Recognized for consistently Exceeding client expectations and providing outstanding service to CAT-A clients, with availability 24/7 to offer assistance whenever required.
- Recognized by SISA Infosec for successfully conducting Proof of Concept (POC) on Splunk and ProAct SIEM tools.