SASI VARDHAN REDDY NIMMAKAYALA

Information Security Analyst

Thalapanur (V), Kadapa (Dist.), Andhra Pradesh-516339, India. ✉ yourssasivardhan@gmail.com ☎ +91 9375008008

PROFILE SUMMARY:

An experienced ***Information security Analyst*** with a demonstrated history of working in the Networking Security, Ethical Hacking, and Cybersecurity with an overall experience of ***3.0 years*** in an IT Security and SOC team. Performing Real-time monitoring, investigation, Incident Management, analysis, reporting and escalating Security events with SEIM Tools like Splunk and QRadar.

ROLES AND RESPONSIBILITIES:

- Provide Cyber Security Operations Center support on a 24x7x365 basis by shift work with rotation.
- Monitoring and investigation of security incidents using SIEM tools like **QRadar, and Splunk.**
- Creation of Dashboard & Report based on various log sources.
- Performing analysis of Spam, Phishing mails and notify it with remediation.
- Handling Alert on SIEM Dashboard by creating tickets.
- Investigating and creating case for the security threats and forwarding it to Onsite SOC team for further investigation and action.
- Experience on performing log analysis and analyzing the crucial alerts at immediate basis.
- Recognizing attacks based on their signatures.
- Monitoring and carrying out second level analysis incidents.
- Escalating the security incidents based on the client's **Service Level Agreements (SLAs)** and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.
- Co-ordinate extensively with networking teams to maintain and establish communication to remote QRadar Collectors/Processors.
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Monitoring real-time events using SEIM tools like IBM Qradar, and Splunk.
- Ad hoc report for various event sources customized reports and scheduled reports as per requirements.
- Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
- Preparing daily, weekly, and monthly report as per client requirement.
- Reporting weekly / monthly dashboards to customer.

TECHNICAL SKILLS:

- Network concepts: OSI model, TCP/IP protocols.
- Ports and protocols in Networking.
- Good understanding on Three-way handshake protocol.
- Security concepts such as CIA, AAA, and VPN
- Good knowledge on different types of servers such as DNS, DHCP, and AD.
- Security operation center process & it’s functions.
- Alert analysis-Phishing alert, Brute force, DOS attack, SQL injection, Blacklisted IP.
- Creating Repots and dashboards in SIEM.
- Knowledge on Vulnerability assessment, and OWASP Top10 Vulnerability.

- SIEM (Security Information and Event Management) Tool: ArcSight, QRadar, and Splunk.
- Knowledge on different types of cyber-attacks like malware, phishing mails, Man in middle attack and its mitigation.
- Phishing Email Analysis and hands on experience on Nmap, Hping3, theHarvester, Burp Suite, OWASP Zap, and SQL Map tools.
- Ticketing tool: ServiceNow, BMC Remedy
- Sound knowledge in Metasploit Framework and Social Engineering.

WORK EXPERIENCE:

Role: Information Security Analyst **Company: Tech Mahindra** **June'2019 - Present**

- Working in Security Operation Center (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Monitoring the customer network using SIEM tools: IBM Qradar, and Splunk.
- Work closely with business units to ensure that they know what and how to feed data into QRadar and to create network hierarchy, classify Log Sources within the Qradar SIEM.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Maintain keen understanding of evolving internet threats to ensure the security of client networks.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.
- Co-ordinate extensively with networking teams to maintain and establish communication to remote Qradar Collectors/Processors.
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Ad hoc report for various event sources customized reports and scheduled reports as per requirements.
- Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
- Responsible to preparing the root cause analysis reports based on the analysis.
- Analyzing daily, weekly, and monthly reports.
- Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
- Creating the tickets in ticketing tool.

CERTIFICATIONS:

- **Certified Ethical Hacker_V11 (CEH V_11).**
- Splunk SIEM Security Training from Intellipaat Institute.
- Security Operation Center – SOC Training from Sai acuity institute.

EDUCATION:

Bachler of science (BSc) – Computer Science Sarvepalli Radhakrishnan University. From 2016 - 2019

- Completed BSc in computer science in 2019 from Sarvepalli Radhakrishnan University, Bhopal, Madhya Pradesh, India.

LANGUAGES

- English
- Telugu
- Hindi
- Tamil