Srikanth Thota

(SOC Analyst)

Ph: +918978847556 | Gmail: srikanth87759@gmail.com

Professional Summary

SOC Analyst with over 2 years of experience in SOC Operations, Cybersecurity, and Threat Analysis. Proven expertise in SIEM tools such as Elastic and Splunk, as well as endpoint security solutions like CrowdStrike. Experienced in incident response, vulnerability assessments, and security audits. Strong technical background in implementing security controls, monitoring network traffic, and mitigating threats. Adept at collaborating with internal teams to improve security posture, developing security playbooks, and ensuring compliance with industry frameworks like NIST and ISO 27001. Committed to continuous learning and driving proactive security initiatives. Demonstrates strong skills in threat detection, forensic analysis, and reporting with a focus on improving organizational security resilience.

Professional Experience

SOC Analyst

General Logic Pvt. Ltd.–Hyderabad *2024–Present*

- Monitored and analyzed security events using Elastic, Splunk, and other SIEM tools to detect and respond to threats.
- Managed and optimized CrowdStrike endpoint security solutions to ensure proactive threat detection and mitigation.
- Conducted continuous monitoring of network traffic to identify abnormal behavior and ensure a secure environment.
- Investigated security incidents, performed detailed root cause analysis, and implemented remediation strategies.
- Conducted security audits and vulnerability assessments to identify risks and strengthen the organization's security posture.
- Developed customized security alerts, dashboards, and reports using Elastic and Splunk for improved threat visibility.
- Collaborated with IT teams to implement secure configurations for servers, endpoints, and network devices.
- Created detailed incident reports, documenting findings and recommending best practices for improved response.
- Assisted in developing and improving security playbooks for streamlined response procedures.
- Performed endpoint forensic analysis to identify malicious activity and implement containment strategies.
- Managed security configurations to ensure endpoint security tools were updated with the latest signatures and rules.
- Delivered cybersecurity awareness training to staff to mitigate security risks and improve incident response readiness.

SOC Analyst

Infomatrix Digital Solutions 2022 – 2023

- Monitored real-time security alerts using Elastic and Splunk, analyzing suspicious activities for potential threats.
- Managed endpoint security alerts using CrowdStrike and conducted malware analysis to identify and isolate threats.
- Conducted detailed phishing analysis, investigating email threats and implementing mitigation strategies.

- Performed advanced threat hunting activities to proactively identify security risks in endpoint environments.
- Conducted malware analysis to analyze infection vectors, ensuring swift remediation actions were applied.
- Collaborated with internal teams to build and maintain security runbooks and playbooks for enhanced incident response.
- Assisted in documenting security incidents, investigation findings, and recommendations for improved security policies.

Skills

- SIEM Tools: Elastic, Splunk, Microsoft Sentinel, FireEye Helix
- Endpoint Security Solutions: CrowdStrike, EDR, DLP
- Security Tools: IDS/IPS, Firewalls, Antivirus
- Incident Response & Threat Analysis
- Vulnerability Assessments & Penetration Testing
- Cyber Threat Intelligence (CTI) & Malware Analysis
- Security Automation & Scripting: Python, PowerShell, Bash
- Cloud Security Platforms: AWS, Azure, GCP
- Proficient in Security Awareness & Training Programs
- Endpoint and Server Hardening Techniques
- Strong Analytical & Problem-Solving Skills
- Excellent Communication & Collaboration Skills
- ITIL Process & Incident Management
- ServiceNow, Remedy, and Ticketing Systems

Certifications

- Network Defense Essentials by EC-Council

Education

- Bachelor of Technology (B. Tech) in Mechanical Engineering-Seshadri Rao Gudlavalleru Engineering College, Andhra Pradesh | 2020.

(**Srikanth Thota**)