Mahesh Babu Pentapati

SOC Analyst | Cybersecurity Professional | Threat Hunter

Profile Summary

SOC Analyst with 2+ years of hands-on experience in identifying and mitigating security threats. Seeking a challenging role in a dynamic organization where I can leverage my expertise in threat detection, incident response, and security best practices to enhance the cybersecurity posture. Committed to continuous learning and professional growth to stay at the forefront of evolving security challenges and technologies while contributing to the organization's security goals.

• 2+ years of IT & SOC experience in securing the network environment.
• Expertise in Information Security with emphasis on incident management, intrusion detection, and SIEM analysis.
• Experienced in SIEM tools: Splunk, QRadar, FortiSIEM, and Azure Sentinel.
• Skilled in monitoring & investigating incoming events, log analysis, and handling critical alerts.
• Hands-on with CrowdStrike EDR, Symantec Endpoint Protection, and malware triage.
• Exposure to phishing/spam email analysis and global threat monitoring.
• Strong knowledge of Incident Management lifecycle and use of ServiceNow ticketing.
• Adept at team coordination, reporting (daily/weekly/monthly), and communication.

Professional Experience

SOC Analyst & Cybersecurity Threat Hunter — TechOwl

06/2025 – Present | Surat, Gujarat, India

• Designed and deployed FortiSIEM correlation rules for SQL Injection, XSS, brute-force, and privilege escalation.
• Built custom parsers for Trend Micro, Imperva, FortiWeb, FortiGate, and Windows DNS logs.
• Conducted proactive threat hunts leveraging Sysmon data and MITRE ATT&CK framework.
• Automated incident workflows using FortiSOAR playbooks, reducing MTTR.
• Developed severity dashboards for EPS tuning, RBI compliance, and SOC KPIs.
• Led incident triage and collaborated with client teams for continuous SOC improvements.

SOC Analyst — Mastercard

09/2022 – 06/2025 | Pune, Maharashtra, India

• Monitored global Mastercard infrastructure using Splunk and QRadar SIEM.
• Analysed and responded to alerts from Proxy, Anti-Virus, and EDR sources.
• Conducted phishing and spam email analysis and malware investigations.
• Performed deep-dive investigations using CrowdStrike Falcon EDR.
• Created ad hoc/customized reports and scheduled reports for various event sources.
• Investigated suspicious activities from network device logs and prepared incident reports.
• Supported vulnerability monitoring, incident response, and root cause analysis.
• Participated in purple team exercises to strengthen detection and response capabilities.

Education

• B.Tech in Computer Science — Kakinada Institute Of Engineering & Technology, Korangi (2022)

• Intermediate (MPC) — Aditya Junior College, Kakinada (2018)

• SSC — ZP High School, Kakinada (2016)

Certifications

• Fortinet Certified Associate in Cybersecurity — Issued Jul 2025, Expires Jul 2027, Credential ID 2072677544MP
• Fortinet Network Security Expert Level 1: Certified Associate — Issued Jul 2025
• Cyber Threat Hunting (CTH), Threat & Vulnerability Management

Strengths

• Quick learner with ability to adapt to new technologies.
• Strong analytical and problem-solving skills.
• Effective communication and collaboration across teams.
• Dedication to continuous learning and professional growth.

Personal Details

• Name: Mahesh Babu Pentapati
• Date of Birth: 29/06/2001
• Gender: Male
• Nationality: Indian
• Languages Known: English, Telugu, Hindi

• Address: Kakinada, Andhra Pradesh, India

Declaration

I hereby declare that the above-mentioned details are true to the best of my knowledge.

(Mahesh Babu Pentapati)