MAJETI SIVA RAM

Cyber Security Analyst

[](mailto:saichandra1206@gmail.com) **majetisivaram485@gmail.com**

 +91 9666813823

 Hyderabad, India



**TECHNICAL SKILLS**

# SIEM :

Splunk , Azure Sentinel & Qradar

## EDR : Falcon Crowdstrike TICKETING TOOL

Service now

# DLP

Forcepoint

# AI & ML Tools (LLM Models)

## Phishing Email analysis Security Incident Management Email Security

Microsoft Defender

# XDR

Trend Micro

## Vulnerability Scanner

Nessus

## Firewall

Palo Alto

## Antivirus

Trend Micro Apex One

## Scripting

Power Shell

## Firewall

Sophos

Results-driven Cyber security Professional with over 3+ years of experience as a Associate Cyber Security Analyst, specializing in threat detection, incident response, and security operations. Proficient in leveraging SIEM tools, EDR solutions, and vulnerability management to safeguard enterprise assets against evolving cyber threats. Seeking to contribute my expertise in security monitoring and risk mitigation to a dynamic cyber security team, enhancing organizational resilience and defense strategies.



**CAREER OBJECTIVE**

Passionate about continuous learning and implementing innovative security solutions to strengthen cyber security posture.



**WORK EXPERIENCE**

 Proactively monitored security alerts from **Splunk** and **Azure Sentinel SIEM** to detect potential security threats.

 Assessed and prioritized alerts based on severity, impact, and risk level to ensure efficient incident handling.

 Performed initial triage and validation of security alerts, escalating incidents as required for deeper investigation.

 Worked closely with L2 and L3 analysts, contributing to in-depth security investigations and remediation efforts.

 Documented and maintained detailed incident logs, ensuring accuracy in tracking response activities.

 Engaged with the threat intelligence team to stay updated on evolving cyber threats and improve threat detection strategies.

 Utilized ITSM tools (Jira/ManageEngine) to track incidents, manage escalations, and ensure timely resolution.

 Actively participated in incident response procedures, adhering to structured Incident Response Plans (IRPs).

 Followed and improved Standard Operating Procedures (SOPs) for security alert handling and escalation workflows.

 Expertise in identifying and mitigating phishing attacks, spam, malware, and impersonation attempts.

 Familiar with implementing email filtering technologies and DMARC, DKIM, SPF protocols to ensure email authenticity.

 Proficient in managing and troubleshooting email security solutions like Microsoft Defender for Office 365 & Trend Micro XDR.

 Hands-on experience in identifying, analyzing, and mitigating threats using Trend Micro XDR's extended detection and response capabilities.



**EDUCATION**

## Bachelor of Technology (B.Tech)

JNTUK



**DECLARATION**

I do here by confirm that the information given in this form is true to do the best of my knowledge and belief.

# MAJETI SIVARAM

Experience with SIEM tools like Splunk and IBM QRadar, conducting in-depth log analysis, correlation, and threat hunting.

Strong exposure to vulnerability management using Nessus, ensuring compliance with security best practices.

Experience with ticketing tools like ServiceNow, creating and managing incidents for effective resolution.

Investigate and mitigate phishing email threats by leveraging Microsoft Defender for Office 365 tools. Manage IDS/IPS alerts, firewall traffic (Sophos), and security logs to detect and respond to anomalies.

Hands-on experience in endpoint security solutions like Falcon CrowdStrike EDR for threat detection, analysis, and response.

Monitor and analyze Data Loss Prevention (DLP) incidents using Forcepoint, ensuring data security compliance.

Perform threat intelligence gathering and analysis using Recorded Future to enhance proactive threat detection.

Conduct forensic analysis and deep-dive investigations to identify and respond to security breaches.

Utilize PowerShell scripting to automate security tasks, analyze logs, and improve SOC efficiency. Perform proactive threat hunting using SIEM, and EDR tools to detect and mitigate potential security risks.

## HCLTECH (Hyderabad)



**ORGANIZATIONS**

Security Analyst

05/2023 – present | Hyderabad

## MANAS SOLUTIONS

SOC Analyst

11/2021 – 05/2023 | Pune