Harshitha Chenna

SOC Analyst | Security Operations Analyst

☎ +91-6309091241 | ✉ harshithachenna01@gmail.com | harshitha-chenna | harshi-cyber | Portfolio

Professional Summary

Entry-level Cybersecurity professional with hands-on SOC lab experience in SIEM monitoring, alert triage, and incident analysis. Skilled in log and phishing investigations using Splunk and Wazuh, with a strong foundation in networking and security fundamentals. Willing to work 24/7 rotational shifts and ready for a SOC Analyst L1 role.

Skills

SOC Operations : SIEM Monitoring, Alert Triage, Incident Response, SOC Playbooks, Ticketing
Security Tools : Splunk, Wazuh, Microsoft Sentinel, Wireshark, Nessus, VirusTotal
Threat Analysis : Log Analysis, Phishing Analysis, IOC Analysis, MITRE ATT&CK
Networking : TCP/IP, OSI Model, HTTP/HTTPS, Firewalls, IDS/IPS
Operating Systems : Windows security events, Linux
Cloud & Security frameworks: Azure Basics, IAM, MFA, CIA Triad, NIST CSF
Vulnerability Management : Nessus Scanning, Risk & Severity Analysis, OWASP Top 10

Experience

SOC Analyst – Virtual Lab Experience (LetsDefend) Remote — Self-paced *Aug –Sep 2025*

- Investigated security alerts using **SIEM workflows** and SOC analyst methodologies
- Scrutinized **logs, email, network, and endpoint activity** to identify true positives vs false positives
- Created and managed incident tickets, documented findings, followed **SOC playbooks for incident handling**
- Gained hands-on exposure to **EDR, SOAR**, and **threat intelligence, case management** concepts

Projects-Home labs

SOC Log Analysis | *Splunk*

- Analyzed **150+ Windows, Linux, firewall, and Apache logs** using Splunk
- Used SPL queries to detect abnormal authentication and access anomalies
- Basic **dashboards** built to visualize log trends and system activity

Phishing Email Analysis | *MXToolbox, VirusTotal, WHOISLookup*

- Performed phishing email analysis using **SPF, DKIM, and DMARC validation**
- Investigated malicious URLs, spoofed domains, and sender anomalies
- Validated **IOCs using VirusTotal and MXToolbox** and mapped to MITRE ATTCK

Vulnerability Assessment | *Nessus Tenable, Windows VM*

- Conducted vulnerability scans on **Windows VM using Nessus**
- Identified exposed services, outdated software, and misconfigurations
- Reviewed findings to understand **severity, risk impact, and remediation prioritization**

Certifications & Training

- **Google Cybersecurity Certificate** - Coursera (2025): Completed training in SOC fundamentals, SIEM log analysis, incident detection and response, networking basics, Linux, NIST, SQL, and risk management.
- **Cybersecurity Awareness Program** – Infosec Train:Common cyber scams, risk indicators safe online practices

Extracurricular Activities -Virtual Internships

- Mastercard Cybersecurity – Identified phishing threats and suggested security-awareness strategies.
- Deloitte Cybersecurity – Analyzed web activity logs and supported breach investigation efforts.

Education

- Bachelor's degree – Community Science | College of Community Science, Hyderabad | Graduated - 2024