Syed Mohd Hassan

syedhassan7656@gmail.com | +919792597251 | LinkedIn | Portfolio | Bengaluru, India

Seeking a cybersecurity analyst role to proactively detect, analyze, and mitigate security threats, strengthening the organization's security posture and incident response capabilities.

Education

Master's Of Computer Application Specialization In Information Security — 2024 - Present
Jain (Deemed-To-Be-University) — **Bengaluru,India**

Bachelor's Of Computer Application | CGPA: 7.8 — 2021 - 2024
Integral University Lucknow — **Lucknow,India**

Intermediate | 68% — 2020 - 2021
Central Academy — **Barabanki,India**

Skills

- **Technical Skills :** Information Security, Network Security, Incident Response, Malware Analysis, SIEM, Threat Intelligence, Log Analysis
- **Soft Skills :** Communication, Critical Thinking
- **Tools :** Splunk, Wireshark, Fiddler, Wazuh, Procmon, HxD, Regshot, Process Hacker, Shuffle, Nmap, VirusTotal, Any.run, Hybrid Analysis, REMnux, Flare VM, Kali Linux, Ubuntu

Projects

SOC Automation Project

- Developed an automated SOC workflow integrating Wazuh, Shuffle (SOAR), TheHive, and VirusTotal for threat detection and case management.
- Configured Wazuh rules to detect threats such as Mimikatz and automated enrichment using VirusTotal API, triggering TheHive case creation with analyst email alerts.

Splunk Enterprise Setup and Data Ingestion

- Set up and configured Splunk Enterprise for log analysis, monitoring, and security event detection, including custom indexes for efficient searching.
- Ingested data via CSV uploads and deployed Splunk Universal Forwarder to collect and forward logs from remote machines for threat identification and response.

Wazuh Installation and Agent Deployment Lab

- Installed and configured Wazuh for security monitoring, deploying agents in endpoints to improve threat detection.
- Integrated Wazuh Agent with Wazuh Server by generating and executing installation commands.

Malware Analysis Lab Setup

- Set up a Windows-based Malware Analysis Lab in VirtualBox, configuring a Windows 10 VM and optimizing it for malware testing.
- Installed and configured FlareVM for malware analysis and reverse engineering using PowerShell scripts.

Certifications

• Cybersecurity Professional Certificate – Google • Soc Analayst Learning Path – Letsdefend • Ethical Hacking Essentials – Eccouncil

• Fundamental Of Network Communication – University of Colorado • Splunk 101 - Splunk • Endpoint Detection and Response - Qualys