SYED MUZAKKIR SHAH HAROONI

✉ muzakkir9084@gmail.com | ✆ +91-8106903190

🔗 https://linkedin.com/in/syed-muzakkir-s-harooni-148763319

PROFILE

As a Computer Science Engineer with certifications in CompTIA Security+ and ISC2 Certified in Cybersecurity (CC), I bring a strong technical foundation and a proactive approach to protecting critical systems and data. I am actively building expertise in blue team operations, including threat detection, incident response, and risk mitigation, while also developing a strategic mindset to advise organizations on enhancing their security posture. Committed to continuous learning, I stay informed about emerging threats and technologies to deliver effective and forward-thinking cybersecurity solutions.

CORE SKILLS & COMPETENCIES

- SIEM Log Monitoring & Analysis - **Splunk, QRadar**
- Security Alerts Monitoring
- Endpoint Detection and Response (EDR) – **CrowdStrike Falcon**
- Threat Intelligence & IOC Detection – **VirusTotal, OTX AlienVault, Cisco Talos**
- Phishing Analysis
- Network Packet Inspection – Wireshark, Fiddler
- Web-Attack Analysis – SQLI, XSS, CI, RFI/LFI, Shell Uploads
- Fundamental Understanding of Security Standards such as GDPR, NIST (RMF/CSF), and ISO 27001
- Malware Analysis – **Joe Sandbox/Any.run/Cuckoo**
- Hybrid Malware Analysis (Manual & Automated)
- Malicious Doc / File Analysis – Windows & REMnux (Linux)
- Reverse Engineering
- Antivirus Software Management & Installation – **(Bitdefender, CrowdStrike Falcon etc.)**
- Data Encoding/Decoding – CyberChef/Base64
- Encryption Tools – AxCrypt (file encryption), VeraCrypt (disk volume encryption)
- Vulnerability Scanning – Nessus
- AWS Cloud Technologies
- Knowledge of the **MITRE ATT&CK Framework (Techniques, Tactics, and Procedures - TTPs)**

TECHNICAL SKILLS SUMMARY

LANGUAGES	Python, SQL
OPERATING SYSTEMS, UTILITIES & VIRTUALIZATION TOOLS	Windows, Linux, Mac, iOS, Android, VMware, Oracle VM Virtual Box
COMMAND LINE SCRIPTING	Bash, PowerShell
DATA ANALYSIS	Excel, Power BI, Tableau, SQL, R

EXPERIENCE

Cybersecurity Analyst Intern - Blue Team Trainee (Sep 2024 – Mar 2025)

SkillDzire | Hyderabad, India

Engaged in security operations, gained hands-on experience using industry-standard tools for threat intelligence, malware analysis, and network security to enhance security posture.

- Monitored security alerts and analyzed log data to develop threat detection and response skills.
- Utilized Splunk to analyze security logs and craft custom queries using Search Processing Language (SPL).
- Leveraged CrowdStrike Falcon for endpoint protection and threat detection.
- Performed hybrid malware analysis with tools such as Joe Sandbox, Any.run, and PEStudio.
- Configured and managed antivirus solutions, including Bitdefender and CrowdStrike Falcon.
- Investigated network traffic using Wireshark and identified potential vulnerabilities in web applications.
- Used threat intelligence platforms like VirusTotal, OTX AlienVault, and Cisco Talos to identify Indicators of Compromise (IOCs).

AI Data Specialist – Remote (Dec 2023 – Aug 2024)

Transperfect | New York, United States

EDUCATION

Bachelor of Engineering (B.E) in Computer Science & Engineering (2020-2024)

- Osmania University | Hyderabad, India

High School

- International Indian School | Riyadh, Saudi Arabia

PROFESSIONAL CERTIFICATIONS/DEVELOPMENT

- CompTIA Security+ SY0-701 (# COMP001022696159)
- Certified in Cybersecurity (CC) – (ISC)² (#2269863)
- Google Cybersecurity Professional Certificate
- SOC Analyst & Blue Team Training – TryHackMe, Lets Defend
- Malware Analyst Training – Lets Defend
- Blue Team Junior Analyst (BTJA) – Security Blue Team

PROFESSIONAL AFFILIATIONS

- Member, (ISC)² – International Information System Security Certification Consortium

VOLUNTEERING

Cyber Security Campus Ambassador

- Promoted cybersecurity awareness and best practices among students and faculty on campus.
- Organized training awareness campaigns on topics such as phishing attacks, data privacy, and secure online behavior.
- Introduced advanced cybersecurity frameworks like the Pyramid of Pain, Cyber Kill Chain, and Unified Kill Chain & Diamond models.

RELEVANT PROJECTS

Building a SOC Lab (Home Setup)

- Designed a home-based SOC lab with tools like **pfSense**, **Active Directory**, **Sysmon**, and **CrowdSec**.
- Simulated threat detection, log analysis, and network monitoring in a virtualized environment.
- Gained hands-on experience with SOC workflows, endpoint security, and collaborative threat intelligence.

Security Information and Event Management (SIEM) Implementation (Virtual Lab)

- Deployed a SIEM solution using Splunk to simulate real-time log collection, correlation, and threat detection.
- Configured data ingestion from endpoints and network devices for security monitoring.
- Developed custom dashboards and alerts to detect anomalies and potential threats.

Building a Malware Analysis Lab

- Set up a secure malware analysis environment using **VirtualBox** and **Flare-VM**.
- Configured virtual machines for static and dynamic analysis of malicious files.
- Gained expertise in identifying malware behavior, attack vectors, and extracting IOCs.

Endpoint Detection and Response (EDR) Setup (Using CrowdStrike)

- Deployed **CrowdStrike Falcon** EDR solution on virtualized endpoints for real-time threat detection and response.
- Configured automated response actions, including isolating infected machines and blocking malicious activities.
- Gained hands-on experience with advanced endpoint monitoring, behavioral analysis, and incident response workflows.

ARTICLES

- Blue Team Insights & Activities - View Published Articles On LinkedIn