

# MUHAMMAD EHTISHAM

Islamabad, Pakistan

[+92 332 9979242](#) | [connectsham95@gmail.com](mailto:connectsham95@gmail.com) | [linkedin.com/in/ehtishamcyber](https://linkedin.com/in/ehtishamcyber) | [www.ehtisham.space](http://www.ehtisham.space)

## PROFILE

Enthusiastic Final-Year Cybersecurity Student actively hunting for entry-level roles to start a career. Deeply interested in AI-driven Cyber Defense, Network Security, and Threat Hunting. Eager to apply academic knowledge and learn from experienced teams in a real-world environment.

## PROFESSIONAL EXPERIENCE

### National Aerospace Science & Technology Park (NASTP)

Islamabad, Pakistan

#### SOC Analyst Intern

July 2025 – Aug 2025

- Engaged in day-to-day SOC activities, gaining hands-on learning with various security monitoring tools.
- Performed APT tracking and threat hunting, mapping adversary behaviors against the **MITRE ATT&CK** framework.
- Contributed to the development of a Machine Learning-based **DDoS detection system** and monitoring dashboard.

### AJ Power Plant

Remote

#### Contract Project: SIEM Engineer

Dec 2024 – Jan 2025

- Hired specifically as a SIEM Engineer to troubleshoot and resolve critical configuration errors in the SCADA infrastructure.
- Successfully deployed a **Wazuh SIEM** solution, restoring network visibility and fixing data ingestion issues.
- Ensured seamless and secure integration between the critical SCADA system servers and pfSense firewalls.

### The Light Academy

Attock, Pakistan

Aug 2025 – Sept 2025

#### Freelance

Remote

#### IT & Security Support

Nov 2022 – Present

- Assisted diverse clients with troubleshooting and tool deployment, focusing on "learning while earning" to build skills.
- Solved technical problems across **Linux and Windows** domains, resolving configuration errors and deploying tools.

## TECHNICAL PROJECTS

### AI-Based Public Wi-Fi IDS (Final Year Project) | Raspberry Pi 4, Python, ML

- Developed a specialized, portable Intrusion Detection System (IDS) on **Raspberry Pi 4** for securing open networks.
- Engineered detection logic to identify and block Layer 2 threats, including **Deauth Attacks, Evil Twin, and Rogue APs**.
- Integrated a Machine Learning classifier using **Scikit-learn** to analyze packet signatures and detect anomalies in real-time.

### Honeypot on Cloud | Cloud Security, AI/ML

- Built a cloud-based deception system (Honeypot) designed to track attacker activities and analyze malicious behavior.
- Successfully recorded **1500+ daily attack attempts** from across the world, generating actionable threat intelligence.
- Utilized AI-driven insights to distinguish between automated botnets and human adversaries.

### IBM QRadar SIEM Exploration (Training Lab) | Cyber Academy, IBM QRadar

- Explored **IBM QRadar SIEM** through hands-on labs, learning log collection, normalization, and correlation.
- Practiced offense investigation and rule creation to understand real-time threat monitoring and detection.

### Deployed Wazuh SIEM on Azure Cloud | Microsoft Azure, VirusTotal

- Deployed a cloud-native SIEM architecture on Azure, configuring agents for log collection and real-time threat detection.
- Integrated **VirusTotal** and File Integrity Monitoring (FIM) within Wazuh across Windows and Linux agents to automate malware analysis and detect system or network anomalies.

## EDUCATION

### Air University

Kamra, Attock, Punjab, Pakistan

2022 – 2026

### CERTIFICATIONS & COURSES

#### (ISC)<sup>2</sup> Certified in Cybersecurity (CC) Google Cybersecurity Specialization

#### AWS Academy Cloud Security Foundations SOC & Security Assessment Bootcamp

## TECHNICAL SKILLS

**Languages:** Python (Basic), C++, Bash

**Tools:** Wazuh, QRadar, Metasploit, Nmap, Wireshark, Snort

**Cloud/OS:** Microsoft Azure, DigitalOcean, Linux (Ubuntu/Kali), Windows AD