MUHAMMAD ABDUL HADI

Cybersecurity | SOC Operations | Threat Detection

Islamabad, Pakistan | 0321-6863431 | haadi.baloch.2004@gmail.com | linkedin.com/in/haadibalouch | github.com/Haadi-Balouch

SUMMARY

CompTIA Security+ certified Computer Science student specialising in blue-team security: SIEM and SOAR pipelines, custom detection rules mapped to MITRE ATT&CK, and log and network traffic analysis. Completed a Security and Detection internship at Arzens and the TryHackMe SOC Level 1 path; active CTF competitor. Seeking SOC analyst and security roles.

EXPERIENCE

Security and Detection Intern, Arzens Jul 2026 - Sep 2026

- Triaged SIEM alerts, separating real incidents from noise and documenting each investigation with supporting evidence.
- Wrote and tuned detection rules for behaviour the default rulesets missed, mapped to MITRE ATT&CK and tested against simulated attacks.
- Analysed endpoint and authentication logs to trace suspicious activity, and helped automate the routing of high-severity alerts to analysts.

CYBERSECURITY PROJECTS

Wazuh x Shuffle SOAR: SSH Brute-Force Detection and Response 2026

Wazuh, Shuffle SOAR, Azure VM, Docker, MITRE ATT&CK

- Built a SIEM-SOAR pipeline on Azure where Wazuh detects a live SSH attack, Shuffle triages it by severity, and an analyst is emailed within about 5 seconds; all 7 end-to-end checks passed.
- Routed only level 10+ alerts to prevent alert fatigue, raising SSH rule 5710 through a local override (T1110.001, T1021.004) instead of lowering the threshold.
- Wrote 3 custom Linux privilege-escalation rules (sudo brute force, sudo group addition, unauthorized sudo use) mapped to T1548.003 and T1098, each verified against a simulated attack.

ThreatCast PK: Crowdsourced Threat Intelligence Platform 2026

SignalR, Azure App Service, Google OAuth, AbuseIPDB API, GreyNoise API

- Developed the frontend, backend and database of a live threat intelligence platform for Pakistan: threat map, analytics, sector-risk panel and real-time SignalR and email alerts, with live threat feeds.
- Implemented role-based access, a moderation queue fed by a teammate's Isolation Forest model that flags coordinated campaigns, email verification, new-login alerts and an admin audit log.

Cerberus: Vulnerability Assessment Framework 2026

Python, Flask, Socket.IO, React, NIST NVD API, ReportLab

- Built a Python framework chaining host discovery, 50-thread port scanning, service fingerprinting and live NIST NVD CVE lookups with correct version-range matching.
- Added web checks (security headers, 20+ XSS payloads, SQL injection, directory enumeration) and scored PDF reports (0-100 risk, Critical to Low) from a CLI or web GUI.

TRAINING AND CTFS

- TryHackMe SOC Level 1 path, top 15% globally: SIEM, alert triage, phishing analysis, network traffic analysis, incident workflows.
- CTFs: picoCTF 2025 and 2026, TJCTF 2026, DAM CTF 2026 (forensics, web exploitation, cryptography); 9 write-ups published on GitHub.
- Home security lab: Kali Linux and Splunk against Metasploitable 2 on an isolated host-only network.

EDUCATION

BS Computer Science, Air University, Islamabad Sep 2024 - Jun 2028 (expected)

- CGPA: 3.71 / 4.00. Relevant coursework: Operating Systems, Computer Networks, Information Security.

CERTIFICATIONS

- CompTIA Security+ (SY0-701), Oct 2026
- Google Cybersecurity Professional Certificate (Google, Coursera), Apr 2026
- SOC Level 1 Learning Path (TryHackMe), May 2026
- Python for Everybody Specialization (University of Michigan), Jul 2026
- AWS Cloud Technical Essentials (Amazon Web Services), Aug 2026

SKILLS

Security: SIEM (Wazuh, Splunk, Elastic), SOAR (Shuffle), detection engineering, MITRE ATT&CK, incident response, threat hunting, log analysis, alert triage, phishing analysis, vulnerability assessment, malware analysis

Tools: Wireshark, tcpdump, Nmap, Burp Suite, Nessus, Snort, Metasploit, NetworkMiner, Brim, SysmonView, CyberChef

Platforms: Linux (Ubuntu, Kali), Docker, Microsoft Azure, AWS, VirtualBox, Git

Programming: Python, C++, Java, C#, SQL, JavaScript

Languages: English (fluent), Urdu (native)