Muhammad Ehtisham

Islamabad, Pakistan
+92 332 9979242 | connectsham95@gmail.com | linkedin.com/in/ehtishamcyber | www.shamtech.online

Profile

Results-driven Security Engineer specializing in SIEM architecture, continuous infrastructure optimization, and advanced threat detection. Proven expertise in centralizing enterprise-wide visibility (EDR, firewalls, servers) and developing high-fidelity correlation rules within IBM QRadar. Adept at reducing alert noise, empowering analyst teams with streamlined data, and proactively hardening the enterprise security posture.

Professional Experience

Trillium Infosec Systems (Deployed at FBR Headquarter) — Islamabad, Pakistan
SOC Engineer — *June 2026 – Present*
- Drive daily SOC engineering operations by architecting and tuning custom detection use cases within **IBM QRadar** to minimize false positives and enhance real-time alerting.
- Elevate the security posture by continuously centralizing network visibility, seamlessly onboarding and parsing logs from EDR platforms, perimeter firewalls, Active Directory, and critical servers.
- Coordinate closely with tier-1/tier-2 SOC Analysts to streamline incident triage workflows, providing advanced engineering support for complex threat investigations.

National Aerospace Science & Technology Park (NASTP) — Islamabad, Pakistan
SOC Analyst Intern — *July 2025 – Aug 2025*
- Conducted active threat hunting and log analysis within a fast-paced SOC environment to identify network anomalies.
- Profiled adversary behaviors and mapped tactical indicators to the **MITRE ATT&CK** framework.
- Collaborated on a machine learning-driven DDoS detection dashboard to streamline volumetric traffic monitoring.

AJ Power Plant — Remote
Contract Project: SIEM Engineer — *Dec 2024 – June 2026*
- Engineered log management pipelines to resolve persistent data ingestion failures across critical SCADA infrastructure.
- Architected and deployed a **Wazuh SIEM** solution, restoring vital system visibility and centralized event tracking.
- Secured endpoint integrations between SCADA host architectures and localized pfSense firewalls.

Technical Projects

AI-Based Public Wi-Fi IDS | *Raspberry Pi 4, Python, Scikit-learn*
- Engineered a portable Intrusion Detection System (IDS) on **Raspberry Pi 4** to secure and monitor open networks.
- Configured precise detection logic for Layer 2 threats, including Deauthentication attacks and Evil Twins.
- Integrated a Machine Learning classifier to analyze packet signatures and detect real-time behavioral anomalies.

Cloud Deception Architecture (Honeypot) | *Cloud Security, Threat Intel*
- Deployed a cloud deception environment designed to capture unauthorized connections and trace methodologies.
- Ingested and cataloged over **1500+ daily log events**, leveraging analytics to categorize automated botnet scans.

Wazuh SIEM Deployment on Azure | *Microsoft Azure, VirusTotal API*
- Provisioned cloud infrastructure using Azure virtual machines to host and manage centralized log ingestion pipelines.
- Automated malware analysis and file integrity monitoring by linking the **VirusTotal API** with Wazuh agents.

Education

Air University — Kamra, Attock, Punjab, Pakistan
Bachelor of Science in Cyber Security — *2022 – 2026*

Certifications & Courses

(ISC)² Certified in Cybersecurity (CC)
AWS Academy Cloud Security Foundations
Google Cybersecurity Specialization
SOC & Security Assessment Bootcamp

Technical Skills

Core Domains: SIEM Administration, Log Analysis, Incident Triage, Use-Case Engineering, Threat Hunting
Tools: QRadar, CrowdStrike, Wazuh, Metasploit, Nmap, Wireshark, Snort
Platforms/OS: Microsoft Azure, DigitalOcean, Linux (Ubuntu/Kali), Windows AD