Muhammad Zeeshan

Lead Security Engineer

Plot 200 Street 1, I-10/3 I 10/3 I-10
Islamabad
Pakistan
+92 (313) 0177933
muhammadzeeshan494@gmail.com

Certifications

The SecOps Group — **Certified AppSec Practitioner (CAP)** .

The SecOps Group — **Certified Network Security Practitioner (CNSP)** .

Professional Trainings

CloudGuru — **AWS solution Architect**.

CBT Nuggets — **Network Plus**.

Linux — **Linux Fundamentals**.

Cloudflare — **Rate limiting/Detection rules and Playbook creation**.

Hacking — **Website Hacking Penetration Testing & Bug Bounty Hunting**.

Professional Skills

Detection Engineering.

Gap Assessments, Threat Hunting, Threat Research, Security Hardening, Purple Teaming

Cloud Security & Assessments.

AWS, Azure Sentinel, Microsoft Defender, Cloudflare, EC2, RDS, S3, IAM, VPC, SG, CF, ES, Lambda, LB and various other services

Intrusion Analysis/SIEM Tools.

ELK Stack, Crowdstrike Falcon, Azure Sentinel, Cloudflare, Wazuh, Microsoft Defender, Qradar, Lacework, VIPRE

TCP/IP Protcols, Traffic Flow

AWS Security Tools.

Guard Duty / Security Hub / AWS Security Hub / Amazon CloudTrail

Security Tools.

Maltego, NMAP, Wireshark, Metasploit, Zscaler (policies setup etc), Azure DevOps, The Hive & Jira

Tool languages and Courses.

Kibana Query Language, Kusto Query Language, Elastic Search Query, Python, C++, C, Computer Networks, Data Structures, Objected Programming, Information Security, Operating System

Experience

Feb 2025 - Present

Lead Security Engineer, *Merik Solutions*, Islamabad.

Currently leading the internal SOC at Merik Solutions, overseeing technical operations, team development, and strategic direction. Specifically, SOC initiatives span from open source tool deployment to AI-powered security use cases for the finance sector.

Responsibilities:

- Designed and deployed a full-featured internal SOC using open-source tools including **Wazuh**, **TheHive**, and **ELK stack**, enabling real-time monitoring and incident response.
- Developed and implemented a comprehensive training roadmap for SOC analysts, including hands-on labs (e.g., buffer overflow scenarios), weekly vivas, and continuous assessments.
- Conducted technical lectures and workshops on **Python-based automation** for log parsing, alert triage, and SOAR integrations to upskill the SOC team.
- Led incident response tabletop sessions simulating real-world breaches to train the team in decision-making, escalation paths, and containment procedures.
- Building analyst rosters and shift rotations to ensure 24/7 SOC coverage and effective incident handling.
- Creating, tuning, and maintaining SIEM detection rules, including **MITRE ATT&CK**-aligned use cases and behavioral analytics.
- Mentoring and coaching team members by identifying their strengths, assigning role-based responsibilities, and guiding their technical growth paths.
- Taking active part in interviewing and hiring new SOC analysts, evaluating both technical and analytical capabilities aligned with team needs.
- Leading the development of **AI-powered cybersecurity use cases** focused on threat detection and anomaly identification for **financial institutions**.
- Conducting client meetings to assess security needs and propose tailored SOC solutions, strengthening business growth and technical trust.
- Overseeing incident response workflows, refining alert pipelines, and integrating threat intel sources to improve response times and reduce false positives.
- Continually improving internal SOC operations by identifying gaps, optimizing tooling, and aligning practices with **SANS**, **NIST**, and **MITRE** frameworks.

June 2022 - Feb 2025 **Security Engineer**, *Ebryx*, Lahore.

Working as a part of SOC Team, actively monitoring, containing and responding to known and unknown security threats by collecting the TTPs and following the effective models like SANS and NIST.

Responsibilities:

- Continuously monitor **Network/Host** in **24/7 SOC environment** using a diverse set of continuous monitoring tools and **SIEM/EDR**.
- Identification and investigation of **Logs/Events** and escalation of **security incidents**.
- Effective & efficient execution of **SOC standard operating procedures**.
- **Threat hunting**, **use-case creation**, **rate limiting**, and tuning of **SIEM** and **IDS rules** to detect potential security incidents.
- Designed, developed, and maintained **Incident Response playbooks** as part of daily operations.
- Conducted **AWS Security incident response** workshop to handle cloud-based threats.
- Led **Cloudflare incident response** workshop for crown jewel asset protection and **rate limiting** configurations.
- Developed **threat detection rules** in **ELK** and **Azure Sentinel** with automation using **Logic Apps** to enhance detection and response.
- Created multiple **rate limiting rules and playbooks** in **Cloudflare**.
- Led post-incident **remediation** and proposed actionable improvements after security incidents.
- Performed **forensic analysis** of artifacts from compromised **machines/networks**.
- Participated in and coordinated **vulnerability scanning** and **risk assessments**.
- Used **MITRE ATT&CK** to analyze APT techniques and mapped detections over **Azure Sentinel Rules**.
- Conducted deep analysis of **phishing emails** and **malware** using **static and dynamic analysis**.
- Identified and managed **IOCs**, and developed detection/blocking rules in **CrowdStrike**.
- Maintained client and team communication for tasks, changes, and delivered **weekly/monthly reports**.
- Compiled and presented **Weekly/Monthly/Quarterly Threat Reports**.
- Conducted research on latest **threats and attacks** and improved **DFIR skills** including **Windows Forensics**, **Incident Response**, **Pentesting**, and **Malware Analysis**.
- Developed multiple **automation scripts** for **Slack** and **Azure Sentinel** to accelerate escalation and detection processes.
- Set up a **VS Code Server on EC2** with **Nginx** for secure remote development.
- Created an **automated vulnerability scanner** for Windows/Linux with **buffer overflow exploitation** as part of the final year project.

Extracurricular Experience

Namal University Mianwali, *Mianwali*, .

President Cyber Security Awareness. / Head Education Wing. / Co-Head Education Wing
Responsibilities:

- Served 6 months as president of Society of Cyber Security Awareness
- Served 6 months as Head of Education wing Namal Environmental Society at Namal University Mianwali
- Served 6 months as Co-Head of Education wing Namal Society of Social Impact at Namal University Mianwali

Youth LeaderShip Camp, *Islamabad*, .

Responsibilities:

- Spent 10 days at a Youth Leadership Camp, participating in workshops on leadership, team building, and personal development.

Education

2018–2022 **BS-Computer Science**, *Namal University Mianwali*, *Final Year Project: Automated Network Penetrator*.

Awards and Achievements

Ebryx Pvt. Ltd. **Performer of the Quarterly**.

Languages

Urdu **Native**

English **Bilingual**