# Muhammad Mohsin Ashraf

Email: m.mohsinashraf11@gmail.com
LinkedIn: linkedin.com/in/mmohsinashraf
Mobile: +923086060088
Address: Islamabad, Pakistan

## Skills Summary

- **Cyber Security**: SOC Analyst, CrowdStrike Falcon EDR, Elastic Security (Elasticsearch, Kibana, Logstash, Beats, ECS, KQL, Detection Engineering), Wazuh, Defender, SOAR, The Hive, Cortex, N8N, Dfir-Iris, Vulnerability Assessment, Networking, Cryptography, OpenVAS, OSINT, Kali Linux, Nmap, Wireshark, Hydra, Nikto
- **Programming**: Automation Scripting (Python & Bash)
- **Soft Skills**: Leadership, Event Management, Public Speaking, Teamwork, Critical Thinking

## Experience

- **IOTA Solutions** — Pakistan
  *Senior Security Expert - Team Lead* — *February 2025 - Present*
  - **Responsibilities**:
    - Lead and manage the security operations team, assigning priorities, reviewing investigations, and ensuring effective handling of security incidents across environments.
    - Design, develop, and deploy SIEM and XDR solutions, building detection capabilities that provide real-time visibility and actionable security monitoring.
    - Manage security operations for multiple customers, ensuring consistent monitoring, incident response, and service delivery aligned with agreed security requirements.
    - Lead in-house development of security platforms, including architecture planning, implementation, configuration, and operational handover.
    - Analyze security events and incidents generated by SIEM, XDR, and network security tools, producing clear reports outlining impact, root cause, and remediation actions.
    - Oversee endpoint security operations, including management of EDR alerts, investigation workflows, and continuous improvement of response procedures.
    - Conduct incident response and triage activities, validating alerts, assessing severity, coordinating containment efforts, and guiding teams through resolution.
    - Develop and fine-tune detection rules, correlation logic, and parsing mechanisms to improve threat detection accuracy and reduce operational noise.
    - Build and maintain dashboards and reporting views that provide meaningful security insights for both technical teams and management stakeholders.
    - Perform vulnerability assessments and risk evaluations, tracking remediation efforts and advising customers on mitigation strategies.
    - Evaluate and introduce new security tools and technologies to enhance SOC capabilities and improve operational efficiency.
    - Work closely with infrastructure and client teams to strengthen security posture, resolve production security challenges, and maintain stable, secure deployments.
- **Etika Info Sdn Bhd** — Malaysia
  *Cybersecurity Engineer* — *July 2023 - February 2025*
  - **Responsibilities**:
    - Analyze security events and incidents generated by SIEM and XDR solutions, producing comprehensive reports on nature, impact, and resolution.
    - Manage and operationalize CrowdStrike EDR alerts, including resolving incidents, creating workflows, and ensuring effective response to endpoint threats. Develop and refine procedures for efficient alert handling and incident resolution, integrating EDR insights with broader security operations.
    - Conduct incident response and triage when security incidents are detected, assessing severity and coordinating response plans with relevant teams.
    - Implement and configure SIEM and XDR solutions to collect and analyze security data from various sources, ensuring real-time visibility and response capabilities.
    - Fine-tune rules and decoders to optimize performance and accuracy in detecting and prioritizing security threats.
    - Create custom dashboards and visualizations for displaying actionable security information according to different scenarios.
    - Conduct vulnerability assessments using security tools, producing reports on identified risks, vulnerabilities, and proposed mitigation strategies.

    - Conducted research and testing of new security tools and products, making recommendations for implementation in the security operations center environment.
    - Innovated new solutions to solve existing production security issues and improve overall security posture.

- **IOTA Solutions** Pakistan
  *Consultant SecOps* *August 2021 - December 2023*
    - **Responsibilities**:
        - Provided strategic cybersecurity recommendations to senior leadership based on comprehensive threat and vulnerability assessments, ensuring the protection of critical assets, products, and services from potential security breaches.
        - Led or contributed to security risk assessments that identified key threats, consequences, and vulnerabilities to assets, products, and services.
        - Demonstrated a user-focused approach to handling security incidents, minimizing user impact, and ensuring clear articulation of the situation to all stakeholders.
        - Expertly tuned and administered SIEM solutions, including firewall appliances, intrusion prevention systems, data loss prevention systems, analysis tools, and log aggregation tools.
        - Possessed a solid understanding of network defense principles, common attack vectors, and techniques used by attackers.
        - Analyzed network flow data for anomalies and swiftly detected and mitigated malicious activity.
        - Conducted research and testing of new security tools and products, making recommendations for implementation in the security operations center environment.
        - Innovated new solutions to solve existing production security issues and improve overall security posture.

- **SOFTAGICS**
  *Internship* *May 2020 - August 2020*
    - **Web Development**: Company's Website design, PSD To HTML, Graphic design, JavaScript, and JQuery Event Calls
    - **Networking**: Key activities include setting up and configuring of firewall and its applications in network security

## Projects

- **Ministry of Transport, Malaysia – SOC Support with SIEM & XDR Deployment**: Designed and deployed a complete SIEM & XDR platform with ongoing SOC support for the Ministry of Transport, onboarding Windows, Linux, network, and firewall log sources with MITRE ATT&CK–mapped detection rules and analyst dashboards.
- **Visa & Immigration, Malaysia – SOC Support with SIEM & XDR Deployment**: Implemented an end-to-end SIEM & XDR solution with continuous SOC support for a national visa and immigration environment, rolling out managed endpoint agents, tuning custom detection rules, and standing up monitoring and incident-response workflows.
- **University of Malaya – SIEM Deployment**: Deployed a complete SIEM solution for the University of Malaya, building ingest pipelines to normalize logs and authoring detection rules and role-based dashboards for continuous security monitoring.
- **Optiva, Saudi Arabia – SIEM & XDR Deployment**: Delivered a full SIEM & XDR deployment for Optiva, integrating endpoint and network telemetry with automated alert triage and enrichment across the environment.
- **Depth Defense, UAE – XDR & SOAR Deployment**: Delivered an XDR deployment integrated with SOAR, configuring endpoint protection and automated response workflows to accelerate containment.
- **Redtone Telecom, Pakistan – SOC Support with SIEM & XDR Deployment**: Provided SOC support alongside SIEM & XDR deployment for a national telecom operator, delivering continuous monitoring, incident response, and detection engineering across critical infrastructure.
- **NUSHkia Tech, UAE – SIEM Deployment**: Deployed a SIEM solution for NUSHkia Tech, onboarding log sources, tuning detection rules, and building operational dashboards for security visibility.

## Education

- **National University of Sciences and Technology - NUST**
  *Master's Information Security — CGPA: 3.5/4* *September 2021 - December 2024*

  ***Courses:*** *Information Security Management, Computer Security, Network Security, Advanced Cryptography, Cloud Security, Vulnerability Exploitation and Defense, Computer Forensics, Advanced Topics in Information Security*

  ***Thesis Title:*** *Investigation of security-related routing issues in IoT Networks*

- **Bahauddin Zakariya University Multan**
  *BS Computer Systems Engineering — CGPA: 3.85/4* *August 2017 - July 2021*
  ***Courses:*** *Computer Security, Operating Systems, Networking, Data Structures, Cloud Computing, Project Management, Microprocessors, Communication Systems*

- **Academic Projects**:
  - Vulnerability Assessment Using OpenVAS
  - Vulnerability Assessment of Web Server Using Nikto
  - OS Fingerprinting Using Wireshark
  - Network Scanning Using Nmap
  - Web Server Password Cracking Using Hydra
  - Gesture Control Reboot – Final Year Project
  - Smart Parking using Arduino

## Awards and Certifications

- Certified Ethical Hacker v13 (CEH) (**EC-Council**)
- Oracle Certified Associate (**OCI**)
- ISO/IEC 27001:2022 Lead Auditor (**Mastermind**)
- AWS Certified Cloud Practitioner (**AWS**)
- Certified in Cybersecurity (**ISC2**)
- Certified Network Security Practitioner (**CNSP**)
- CrowdStrike Certified Falcon Hunter
- Crash Course on Python (**Google**)
- Using Python to Interact with the Operating System (**Google**)
- Foundations of Cybersecurity (**Google**)
- Barracuda Web Application Firewall - Foundation: **WAF01**
- CISCO Introduction to Cybersecurity
- CISCO Introduction to Packet Tracer
- Best Performance Award: IOTA Solutions

## Training

- AWS Cloud Practitioner Certification (**LearnKartS**)
- Elasticsearch Engineer (On-Demand) Training (**Elastic**)
- Linux Training (**Alnafi**)
- Elastic Security Fundamentals: SIEM
- Elastic Observability Fundamentals

## Positions of Responsibility

- **IEEE Conference** January 2020
  *Conducted online technical & soft-skills training impacting over 500 students*