

# Muhammad Mubashir

## SOC Analyst & Security Engineer

Karachi, Pakistan    mubashirwasi7@gmail.com    LinkedIn (linkedin.com/in/muhd-mubashir)  
GitHub (github.com/Muhd-Mubi)    muhd-mubi.github.io

---

### Summary

SOC Analyst and Security Engineer working across security monitoring, incident investigation and response, and IBM QRadar administration. Hands-on with log source integration, parsing and normalization, SIEM troubleshooting, and the cloud and virtual infrastructure underneath security operations, including an in-progress QRadar migration from AWS to GCP. ISC2 Certified in Cybersecurity (CC); preparing for CCNA.

### Experience

#### SOCByte

##### Jr. Security Engineer & Engineering Team Lead

April 2026 – Present

- Responded to a compromise of internet-exposed production servers running at 100% CPU, where host isolation and service termination were constrained by uptime requirements. Identified malware masquerading as Realtek audio services running from a temp directory instead of System32 by baselining process behaviour against a known-good host.
- Deployed CrowdStrike to affected hosts, validated extracted binary hashes against VirusTotal, terminated malicious services via PowerShell, and removed registry Run-key persistence. Blocked confirmed hashes and the wider threat-group IOC set sourced from Group-IB and CTM360.
- Cut active C2 communication and XMRig crypto-mining traffic with a host-based firewall using default-deny egress and an explicit allow-list of business-required ports, chosen over enabling Microsoft Defender, which would have blocked legitimate production processes. The underlying access vector was then remediated.
- Led a SIEM audit for a microfinance bank: corrected log source parsers and DSM/event mappings that were sending traffic from 50+ assets into SIM Generic, cutting unknown/unparsed events by 80% and restoring accurate normalization for rules, offenses, and reporting.
- Identified 190 unintegrated assets in the same environment and remediated their log source integrations to forward the relevant event IDs, bringing previously unmonitored systems into monitoring coverage.
- Root-caused a recurring IBM QRadar instability (an hourly, roughly one-minute service crash) to expired internal certificates; renewed the internal certificate chain, eliminating the outage window and stabilizing event collection.
- Configured the QRadar mail server and automated scheduled daily reporting to stakeholders.
- Deployed and maintained VMware ESXi infrastructure on on-premises servers, provisioning virtual machines and supporting system stability.
- Supported SOC platform operations: user management, monitoring workflows, and incident investigation and response.

##### SOC Analyst Trainee

February 2026 – April 2026

- Investigated a quarantined email that had passed SPF/DKIM authentication and sandbox detonation and carried no links or attachments. Pivoted on sender alias, source IP, and subject line to uncover a 90-day, multi-domain campaign sending rotating proverb-based lures through an abused relay in a European datacenter; every sending IP and domain scored clean on VirusTotal.
- Identified the campaign as a reply-bait / conversation-hijack precursor (payload delivered only after a victim replies). Ran a retro-hunt sweep across the tenant, blocked the follow-on infrastructure, initiated targeted user awareness, and submitted the analysis to Trend Micro Email Security as a detection-gap report.
- Performed L1 monitoring and alert triage across SIEM/XDR/NDR platforms (Wazuh, QRadar, Rapid7 InsightIDR, Trend Micro Vision One, Vectra AI) and EDR (CrowdStrike), escalating confirmed incidents per playbooks.
- Monitored WAF events and HTTP logs for common web attacks such as SQL injection patterns, validating findings and recommending blocks.
- Operationalized threat intelligence by curating and blocking IOCs (URLs, domains, hashes) in MISP, based on Group-IB and CTM360 feeds and reports.
- Investigated active alerts by validating evidence (process and user activity, network indicators, timelines) to support accurate escalation.

Pakistan Petroleum Limited

Information Technology Intern

February 2025 – April 2025

- Supported office network design and implementation across switching, routing, firewalls, and server connectivity; assisted with baseline hardening and access requirements.
- Assisted with cybersecurity and compliance work, including an ISO 27001 control review, vulnerability scanning with Rapid7 InsightVM, and SIEM exposure (LogRhythm).

Devtects

Junior Software Developer

May 2024 – July 2024

- Developed and deployed websites using Django, MySQL, cPanel, and Vercel.
- Built and maintained web applications with attention to security and performance.

Selected projects

IBM QRadar migration from AWS to GCP

In progress

Professional project: preparing the destination environment, configuration restoration, historical Ariel data transfer, collector connectivity and routing, and licensing and cutover dependencies. Historical data transfer milestone reported complete; production cutover not yet confirmed.

Wazuh SIEM deployment and security monitoring

October 2025

Deployed a Wazuh SIEM stack, enrolled Windows and Linux endpoints, configured perimeter controls (firewall policy, NAT/PAT, port forwarding) and DDNS for remote monitoring with least-privilege exposure.

Multi-cipher cryptography application

July 2025

GUI/CLI tool implementing AES, DES, RSA, Caesar, Vigenère, Playfair and other ciphers for encryption and decryption workflows.

Skills

|                           |                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| SIEM administration       | IBM QRadar (administration, log source onboarding, DSM and event mapping, AQL searches and reports), Wazuh, LogRhythm (internship exposure) |
| Monitoring and response   | CrowdStrike, Trend Micro Vision One, Rapid7 InsightIDR, Vectra AI, WAF and HTTP log review                                                  |
| Threat intelligence       | MISP, Group-IB and CTM360 feeds, VirusTotal                                                                                                 |
| Infrastructure            | Linux, Windows, VMware ESXi, AWS, GCP, PowerShell                                                                                           |
| Vulnerability management  | Rapid7 InsightVM                                                                                                                            |
| SIEM (lab)                | Wazuh standalone and two-node cluster, Agent onboarding, Syslog ingestion, Load testing around 5–6K EPS                                     |
| Systems and network (lab) | Ubuntu, TLS, Firewall policy, NAT/PAT, port forwarding, DDNS, Server hardening with scan-and-verify loops                                   |
| Code (lab)                | Python, Bash, SQL, Django (earlier development work)                                                                                        |
| Networking (learning)     | CCNA preparation: routing, switching, secure network design                                                                                 |
| Cloud security (learning) | GCP and AWS security, through migration work                                                                                                |
| Familiarity (learning)    | Splunk, Wireshark, Nmap                                                                                                                     |

Education and certifications

BS Computer Science, University of Karachi (UBIT), 2022 – 2026

- Certified in Cybersecurity (CC), ISC2, January 2026
- IBM & ISC2 Cybersecurity Professional Certificate, IBM & ISC2, June 2025
- Google Cybersecurity Professional Certificate, Google, May 2025
- Palo Alto Networks Cybersecurity Professional Certificate, Palo Alto Networks, May 2025

Involvement

- Board Member, UNDP, June 2022 – August 2024
- Chapter Lead, KidsRights, January 2020 – January 2022