# - M U H A M M A D  R A F A Y  A L I -

## CYBER SECURITY ENGINEER

+92 300 9817 567 | muhammad.rafayali@outlook.com | LinkedIn | Portfolio | Wah Cantt, Pakistan

## SUMMARY

**Cyber Security Engineer** with **2+ years** of hands-on experience in **SOC operations, SIEM engineering, threat detection, incident response,** and **security hardening**. Deployed and tuned security platforms across multi-server enterprise environments, cutting undetected threat windows by **35%** and false positive rates by **45%,** with expertise in **ISO 27001, NCA-ECC, SAMA CSF, CIS Benchmark audits,** and **MITRE ATT&CK** frameworks. Supplemented by independent security consultancy and continuous lab-based research on **TryHackMe**. Seeking to deliver managed security excellence in **SOC/MSSP environments**.

## PROFESSIONAL EXPERIENCE

### CYBER SECURITY ENGINEER

Encbit | Lahore, Pakistan | Full-Time | Hybrid — JUL 2025 – PRESENT

- Managed **Wazuh SIEM** deployments across **5+ client environments** handling **agent integrations**, log source onboarding, **rule tuning**, and ongoing platform maintenance for **50+ monitored assets**.
- Authored **15+ tailored detection rules** and **decoders** for new device types, resolving **parsing issues** and improving **log ingestion accuracy** by **30%** across monitored assets.
- Conducted **OSINT-driven attack surface analysis** using **Google Dorking**, **WHOIS reconnaissance**, and **Shodan**, identifying **10+ exposed assets** and misconfigurations for remediation.
- Monitored **200+ daily security events**, triaging incidents, investigating anomalies, and coordinating fixes across **endpoint and network layers**.
- Maintained active hands-on research via **TryHackMe** labs practicing offensive and defensive techniques grounded in **MITRE ATT&CK TTPs**.

### CYBER SECURITY ANALYST

Cyber Silo | Islamabad, Pakistan | Full-Time | Hybrid — FEB 2025 – JUL 2025

- Engineered and deployed **custom SIEM detection rules and log parsers** using **Wazuh** and **Threat Hawk**, increasing detection fidelity by **40%** across critical systems.
- Automated compliance mapping workflows in SIEM by correlating **ISO 27001, NCA-ECC,** and **SAMA** controls with **global standards** via **Excel-based matrices** and **Python scripting**, cutting manual alignment effort by **60%**.
- Validated threat detection coverage by integrating **MITRE ATT&CK techniques via Atomic Red Team**, simulating **20+ real-world attack scenarios** to verify rule accuracy and identify coverage gaps.
- Resolved SIEM data flow issues by correcting **agent misconfigurations and log parsing errors**, restoring **99% log integrity** across monitored assets.
- Built **YAML-based CIS hardening templates** and **audit automation scripts** for FortiGate, Cisco, and pfSense firewalls, enforcing secure baseline configurations per **CIS Benchmarks**.

### SOC ANALYST (CLIENT: ALLAMA IQBAL OPEN UNIVERSITY)

Cyber Silo | Islamabad, Pakistan | Full-Time | Hybrid — FEB 2024 – FEB 2025

- Spearheaded **SIEM deployment and integration** across **30+ servers, network devices,** and **endpoints**, expanding threat visibility and closing **35%** of previously unmonitored attack surfaces.
- Reduced **false positives by 45%** through systematic rule optimization, logic refinement, and alignment with curated **threat intelligence feeds** and attacker TTPs.
- Designed and implemented **incident response playbooks** for containment, remediation, and escalation workflows, cutting MTTR from **30+ minutes to under 10 minutes**.
- Monitored and triaged security alerts in real time, performing **IOC analysis, log correlation,** and root cause analysis across **endpoint and network telemetry** sources.
- Managed **endpoint security monitoring** using **Wazuh**, detecting and containing threats across **30+ endpoints** with **MITRE ATT&CK**-mapped detection rules.

## SKILLS

- **SIEM & SOAR:** Wazuh, Threat Hawk, QRadar, Microsoft Sentinel, Rule Parsing, Incident Response
- **Vulnerability Management:** Metasploit, Burp Suite, Nmap, Virus Total, Threat Hunting, Atomic Red Team
- **GRC Frameworks:** ISO 27001:2022, NCA-ECC, SAMA CSF, MITRE ATT&CK, CIS Benchmark's
- **Scripting & Automation:** Python, PowerShell, Bash, API Integration
- **Cloud & DevSecOps:** Azure, Docker, VMware, Vercel
- **Identity & Access:** IAM, Active Directory

## EDUCATION

### Bachelor of Science in Computer Science

**Hamdard University | Islamabad, Pakistan**

## CERTIFICATIONS

- **SIEM XPERT**

**Certified SOC Analyst Foundation**

- **Google**

**Cybersecurity Specialization**

- **ISC2**

**Certified in Cybersecurity (CC)**

- **SkillFront**

**ISO/IEC 27001:2022 Associate**

- **TryHackMe**

**Active profile; continuous lab-based practice in red/blue team techniques (tryhackme.com/p/0xRafuSec)**

- **MASTERMIND**

**ISO 27001:2022 Lead Auditor**

- **IBM**

**Security Analyst Fundamentals**

- **Udemy**

**Ethical Hacking & Penetration Testing**

- **TCM Security**

**Linux 100**

## TECHNICAL PROJECTS

### Active Directory Attack Simulation & Endpoint Hardening (Lab Project)

**Cyber Silo** | Github.com/0xRafuSec/Active-Directory-Attack-Simulation-and-Hardening-Lab

- Emulated post-exploitation techniques in a **Windows AD lab** using **Atomic Red Team, PowerShell, Python,** and **Mimikatz**, simulating credential theft and lateral movement across **3 domain-connected hosts**.
- Analyzed telemetry from **Event Viewer** and **Sysmon**, integrating **Wazuh SIEM** to alert on **20+ MITRE-mapped TTPs**, improving detection fidelity and expanding endpoint visibility across **5 lab systems**.
- Performed **CIS-based Security Configuration Assessments (SCA)** on **Windows/Linux endpoints**, remediating **50+ misconfigurations** and achieving an **80% increase in benchmark compliance** verified via **Threat Hawk dashboards**.

### Multi-Sensor Automation & Intrusion Detection IoT (Final-Year Project)

**Hamdard University** | Github.com/0xRafuSec/Multi-Sensor-Intrusion-Detection-IOT

- Designed an IoT-based security solution using **ESP32, motion/gas/fire sensors,** and **ESP32-CAM** for real-time threat detection and monitoring.
- Engineered a mobile application using **Flutter and Firebase** to deliver real-time **alert notifications** for **fire, gas leaks,** and **intrusions**, improving user **response time** by **60%**.