-MUHAMMAD RAFAY ALI-

CYBER SECURITY ANALYST

☎ +92 300 9817 567 | ✉ muhammad.rafayali@outlook.com | 🌐 LinkedIn | 📍 Wah Cantt, Pakistan

Cyber Security Analyst with over **1 year of hands-on experience in SOC operations, SIEM engineering, threat detection, and incident response.** Experienced in optimizing detection infrastructure, reducing false positives, and building scalable, **compliance-aligned detection frameworks**. Skilled in integrating and tuning SIEM tools such as **Threat Hawk** and **Wazuh,** with expertise in crafting custom detection rules mapped to **MITRE ATT&CK techniques** and regulatory standards including, **ISO 27001, NCA-ECC,** and **SAMA.**

PROFESSIONAL EXPERIENCE

CYBER SECURITY ANALYST

Cyber Silo | Islamabad | Remote FEB 2025 – JULY 2025

- Designed and implemented **custom SIEM detection rules and parsers**, increasing detection fidelity by **40%** across critical systems.
- Automated compliance mapping in SIEM by correlating **ISO 27001, NCA-ECC,** and **SAMA** controls with **global standards** using **Excel-based matrices** and **scripting**, improving rule tagging consistency and reducing manual alignment efforts by 60%.
- Integrated **MITRE ATT&CK techniques via Atomic Red Team**, simulating real-world threats to validate detection accuracy and coverage.
- Debugged and resolved SIEM data flow issues by correcting **agent misconfigurations and log parsing errors**, improving log integrity by **99%**.
- Developed **YAML-based** CIS hardening templates and **audit automation scripts** for FortiGate, Cisco, and pfSense firewalls, simulating secure baseline enforcement using **CIS Benchmarks** and .conf execution files.

SOC ANALYST - Allama Iqbal Open University

Cyber Silo | Islamabad | Hybrid FEB 2024 – FEB 2025

- Spearheaded SIEM deployment and integration across 30+ servers, network devices, and endpoints, enhancing visibility and reducing detection blind spots by 35%.
- Identified exposed assets via **OSINT tools** such as **Google Dorking** and **WHOIS-based reconnaissance**.
- Reduced **false positives by 45%** through rule optimization and logic alignment with threat intel sources and attacker TTPs.
- Designed and implemented **incident response playbooks** for containment, remediation, and escalation, cutting average response time from **30+ minutes to under 10.**
- Troubleshot and remediate **SIEM integration errors**, ensuring 24/7 uptime and uninterrupted log ingestion for **critical assets**.

EDUCATION

Hamdard University – Islamabad

BS Computer Science (2023) **CGPA: 3.01**

SKILLS

- Security Engineer
- Wazuh
- Threat Hawk
- Rule Parsing
- Alert Tuning
- Incident Documentation & Reporting
- Incident Responder
- Threat Hunting
- Cyber Threat Intelligence
- IOC Analysis
- MITRE ATT&CK
- OSINT
- API Integration
- VAPT
- Linux Hardening
- Nmap
- Metasploit
- Burp Suite
- Python Scripts
- PowerShell Scripting
- ISO 27001
- NCA ECC
- SAMA
- ADHICS
- Azure Cloud
- VMware
- Active Directory

CERTIFICATIONS

- **SIEM XPERT**
  Certified SOC Analyst Foundation
- **Google**
  Cybersecurity Specialization
- **UDEMY**
  Ethical Hacking & Penetration Testing
  Kali Linux OS Mastery
- **MASTERMIND**
  ISO 27001:2022 Lead Auditor
- **IBM**
  Security Analyst Fundamentals
- **SKILLFRONT**
  ISO/IEC 27001:2022 Associate

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 three domain-connected hosts for red team validation.
- 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**, identifying and **remediating 50+ misconfigurations**. Verified hardening effectiveness via **Wazuh dashboards**, resulting in an **80%** increase in **benchmark compliance** and improved endpoint resilience.

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

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

- Developed an IoT-based home/office security solution using **ESP32, motion/gas/fire sensors**, and **ESP32-CAM** for live 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%.
- Produced for **low-cost deployment**, achieving **real-time alerting** with high scalability for smart environments.