Muhammad Hamza Sattar

Punjab, Pakistan mhamzasattar03@gmail.com 0309 6523350

Summary

Cybersecurity Analyst with practical experience in SOC operations, incident management, threat intelligence, and security monitoring. Proficient in security event analysis, alert investigation, log correlation, and incident response support across enterprise environments. Skilled in SIEM operations, threat hunting, IOC analysis, vulnerability assessment, firewall monitoring, and intrusion detection with a strong foundation in network security and cyber defense principles. Experienced in identifying suspicious activities, correlating security events, and contributing to proactive threat detection and effective security operations. Committed to continuous learning and strengthening organizational security through analytical problem-solving and security-focused practices.

Skills

Security Operations: • Security Monitoring • Incident Management • Incident Response • Threat Intelligence • Threat Hunting • Alert Triage • Security Event Analysis • Log Analysis & Event Correlation • Vulnerability Assessment • MITRE ATT&CK Framework

SIEM & Security Tools: • Wazuh SIEM • Suricata IDS • Wireshark • Pfsense • Nmap • Burp Suite • Metasploit • VirusTotal

Networking & Systems: • TCP/IP • DNS • HTTP/HTTPS • OSI Model • Windows • Linux (Kali Linux, Ubuntu)

Security Technologies: • Firewall Configuration & Monitoring • Intrusion Detection Systems (IDS) • Threat Detection • Security Alert Investigation

Programming & Scripting: • Python, • PowerShell • Bash • HTML,CSS,JavaScript

Experience

National Telecommunication Corporation, SOC Internee — Islamabad, Pakistan
Apr 2026 – present
3 months

- Contributed to cybersecurity operations by supporting security monitoring, threat detection, and protection of enterprise network infrastructure.
- Configured and managed Wazuh SIEM, including agent deployment, log collection, alert monitoring, and security event analysis across monitored systems.
- Developed and optimized custom Wazuh detection rules while performing alert triage, log analysis, and event correlation to identify potential security threats.
- Deployed and configured Suricata IDS and managed pfSense firewall policies to monitor network activity, strengthen security controls, and support threat detection efforts.
- Supported incident management and threat intelligence activities through IOC analysis, threat hunting, security investigations, and incident documentation.
- Analyzed Windows Event Logs, Sysmon logs, and Procmon activity to investigate suspicious behavior, conduct vulnerability assessments, and improve overall security posture.

Cybersecurity Intern, DevelopersHub Corporation (Remote) — Apr 2026 – May 2026
2 months

- Assisted in SOC and blue team activities, including security monitoring, alert investigation, and analysis of security events across simulated environments.
- Performed vulnerability assessments, log analysis, and threat investigations to identify potential security risks and strengthen overall security posture.
- Applied threat intelligence and incident response concepts while working with cybersecurity tools and security best practices for threat detection and analysis.

Burton and Burton Solicitors, IT & Network Support Assistant — Islamabad, Pakistan
May 2024 – Nov 2024
7 months

- Managed and monitored network infrastructure ensuring stable connectivity and optimal performance across the organization.
- Worked hands-on with TCP/IP, DNS, VLANs, and core network protocols in a live production environment.
- Assisted in identifying, troubleshooting, and resolving network faults and connectivity issues in a timely manner.
- Supported configuration and basic management of network devices, gaining practical exposure to network operations.
- Coordinated with team members to ensure smooth and uninterrupted IT service delivery across the organization.

Education

BS **National University of Modern Languages**, Software Engineering — Islamabad, Pakistan
Feb 2020 – Jan 2024

Projects

Cybersecurity Monitoring Lab

- Built and configured a cybersecurity lab environment using virtual machines to simulate real-world security monitoring scenarios.
- Deployed and managed Wazuh SIEM, Suricata IDS, and pfSense firewall for log collection, threat detection, and network security monitoring.
- Performed alert investigation, log analysis, threat hunting, and IOC analysis to identify and respond to simulated security incidents.

SOC Operations and Incident Analysis Lab (TryHackMe)

- Completed TryHackMe SOC Level 1 Path, gaining experience in alert triage and incident investigation.
- Practiced SIEM operations, correlating security events, and investigating Windows Event Logs.
- Developed skills in threat intelligence, IOC tracking, and phishing email analysis.

Certifications

- Google Cybersecurity Certificate – Coursera
- Self-Learning / Practical Tools Training (YouTube and Labs)
- NSE1,NSE2

Additional Professional Experience

Worked as a WordPress Developer at Digitechway from November 2024 to December 2025, developing and maintaining WordPress websites for clients across various industries. Gained experience in website customization, troubleshooting, performance optimization, and client communication while delivering technical solutions based on business requirements.