Ahmed Sajid Butt

SOC Analyst L1 / Security Analyst

+923151461971 | ahmedsajid_bw@proton.me | Lahore, Pakistan | GitHub | LinkedIn

SUMMARY

Recent Computer Science graduate with a strong foundation in threat detection and Security Operations Center (SOC) workflows, built through hands on lab work with Microsoft Defender XDR, Microsoft Sentinel, KQL, and the ELK Stack.

Experienced in endpoint security administration, simulating adversary techniques with Atomic Red Team, and building custom SIEM detection content mapped to MITRE ATT&CK. Strong documentation and communication skills, with a continued willingness to learn new cybersecurity tools.

Former OWASP BULC Chapter Lead and published IEEE coauthor. Seeking an entry level SOC, security analyst, or detection engineering role to apply and grow these skills in a live environment.

EXPERIENCE

Threat Detection & SOC Research Intern (Cybersecurity Intern) | CNS Engineering, Lahore Jan 2026 to Jun 2026

- Conducted hands on Microsoft Defender XDR research in a self built Microsoft 365 E5 lab environment, covering endpoint detection, threat simulation, and incident investigation workflows.
- Investigated a high severity incident correlating 14 alerts and 13 pieces of forensic evidence, cross referencing file hashes against VirusTotal to confirm malicious payloads and trace the attack chain to root cause.
- Ran a full ransomware attack simulation from Kali Linux and traced the resulting incident end to end in Microsoft Defender XDR to assess detection and alerting gaps.
- Executed 7 MITRE ATT&CK techniques via Atomic Red Team and Kali Linux, confirming Defender blocked 3 techniques outright, including Mimikatz credential dumping, while detecting 3 others, such as scheduled task persistence, through behavioral analysis alone.
- Wrote 3 KQL queries in Microsoft Sentinel and Advanced Hunting across a 2 hour telemetry window, surfacing 5 findings mapped to 6 MITRE ATT&CK techniques.
- Documented Microsoft Defender's Automated Investigation and Response (AIR) capability during a Priority 100 incident with 6 correlated alerts, including automatic account containment and evidence collection.
- Simulated phishing attacks using Attack Simulation Training, measuring a 20 percent credential compromise rate with credential entry occurring in under 2 minutes of email delivery.
- Authored a 6 phase Phishing Response Playbook aligned to NIST SP 800-61, mapping containment, eradication, and recovery actions to 7 MITRE ATT&CK techniques.
- Provided endpoint security administration by onboarding 4 endpoints to Microsoft Defender for Endpoint across GPO and Microsoft Intune deployment methods, troubleshooting and resolving silent onboarding failures and EDR policy conflicts.
- Authored formal SOC deliverables, including a Threat Hunt Report, Incident Forensics Report, and Ransomware Investigation Runbook, translating technical findings into actionable documentation.

EDUCATION

BS Computer Science | Bahria University, Lahore Oct 2021 to July 2025

PROJECTS

Vigil: SOC Detection Lab and Incident Response Jul 2026 to Aug 2026

- Built a self built SOC detection lab simulating a four stage web application compromise, from initial access through destructive impact, with each stage independently detected and escalated for investigation.
- Deployed a full SIEM stack from scratch using Wazuh and OpenSearch on Docker, closing a log visibility gap by adding an Nginx reverse proxy for web layer request logging.
- Wrote custom Wazuh detection rules using signature matching and frequency based behavioral correlation, mapping each detected technique to MITRE ATT&CK (T1190, T1059.007, T1213, T1486).
- Integrated Wazuh with TheHive for automated alert to case escalation, then ran the full analyst workflow of detection, triage, investigation, and formal case closure with a written verdict.

- Documented the entire build and investigation in a public GitHub repository as a cybersecurity portfolio project, including detection rule logic and a complete evidence trail.

Sentinel Forge: SOC Home Lab, SIEM Deployment and Incident Triage Oct 2025 to Nov 2025

- Built a cloud based security lab on Vultr using the ELK Stack for centralized log collection and analysis.
- Deployed Sysmon on Windows endpoints to capture system activity and network connection telemetry.
- Created custom Kibana detection rules to identify threats including brute force attacks.
- Simulated adversary activity using Mythic C2 to test and validate detection coverage.
- Integrated Kibana alerts with OS Ticket to automate incident ticket creation.

Federated Learning IDS for IoT Healthcare, Final Year Project (Team Lead) June 2024 to May 2025

- Led a team to design a CNN, BiLSTM, and GRU based intrusion detection model for IoT enabled healthcare systems, achieving 99.8% detection accuracy and an overall Grade A evaluation.
- Coauthored “Leveraging AI for Real-Time Intrusion Detection in IoT-Enabled Healthcare Systems,” published in IEEE Xplore (ieeexplore.ieee.org/document/11523932), and delivered a virtual oral presentation at the DataSciMI 2026 conference hosted at Bahria University.

TECHNICAL SKILLS

Microsoft Defender XDR | Microsoft Defender for Endpoint (MDE) | Endpoint Security Administration | Microsoft Sentinel (SIEM) | Kusto Query Language (KQL) | Wazuh SIEM | TheHive Case Management | ELK Stack (Elasticsearch, Logstash, Kibana) | OpenSearch | Sysmon | Log Analysis | Incident Triage | Threat Hunting | Active Directory | Microsoft Intune | Docker | Mythic C2 | Linux (Ubuntu, Kali Linux) | Windows Server | Troubleshooting

CERTIFICATIONS AND TRAINING

- KC7 Security Analyst I, 2026
- KC7 Security Analyst II, 2026
- TryHackMe, 2025
- ISO 27001 Associate, SkillFront, 2024
- Google Cybersecurity, Coursera, 2023

LEADERSHIP

OWASP BULC (Bahria University Lahore Campus), Chapter Lead, May 2024 to June 2025.