Muhammad Zain Din

Entry-level SOC Analyst with hands-on experience triaging alerts, tuning detection rules, and analyzing logs across Windows and Linux environments. Trained in Tier 1 SOC workflows through in MITRE ATT&CK mapping, threat detection, and log correlation, with a solid foundation in both offensive (eJPT, eWPT) and defensive techniques.

✉ muhzaindin03@gmail.com ☎ +48 730 745 313 Gdańsk, Poland | Online - relocate
https://www.linkedin.com/in/muhammad-zaindin/

WORK EXPERIENCE

University of Extremadura

Cybersecurity Intern April 2025 – Present

- Built and tuned custom detection rules in Splunk/ELK for simulated brute-force, privilege escalation, and lateral movement techniques
- Triaged 30+ simulated alerts using MITRE ATT&CK logic
- Correlated logs across systems (auditd, Windows, Sysmon) to reconstruct attacker path

Hackerone

Vulnerability Researcher Jan 2025 - April 2025

- Reported 6 real-world web app vulnerabilities, including CORS misconfigs and account lockout bypasses
- Used attacker TTPs to improve SOC alert correlation and web threat detection
- Leveraged OSINT and manual recon to simulate attacker behavior for blue team analysis

Certifications

- SOC Analyst Learning Path Certification (LetsDefend, 2025)
- eWPT - Web App Penetration Tester (INE, 2025)
- eJPT - Junior Penetration Tester (INE, 2024)
- CCNAv7: Introduction to Networks – Cisco Networking Academy (2024)

PROJECT

Security Log Monitoring Dashboard - Splunk March 2025

- Simulated Tier 1 SOC using log data from Linux/Windows machines.
- Built MITRE-aligned detection rules for T1486 (Data Encryption), T1078 (Valid Accounts), and T1110 (Brute Force).
- Demonstrated detection and triage workflow, from alert generation to initial investigation.
- https://github.com/Barbarossa01/Security-Log-Monitoring-Analysis

Wazuh SIEM Detection & Response Lab May 2025

- Lab-based SIEM simulation project mimicking real SOC alerts for brute-force and lateral movement
- Mapped detection rules to MITRE ATT&CK framework to enhance threat visibility and categorization
- Demonstrated triaging of alerts, log analysis, and correlation of events in a SOC context
- Showcased vulnerability detection, filtering, and severity assessment using Wazuh
- https://github.com/Barbarossa01/Wazuh-SIEM-Detection-Response-Lab

SKILLS

- SIEM & Detection Tools: Splunk, ELK Stack, Wazuh
- Log Analysis & Alert Triage: Windows Event Logs, Sysmon, auditd, MITRE ATT&CK mapping
- Threat Detection & Response: Brute-force, privilege escalation, session hijacking patterns
- Network & Security Tools: Wireshark, Nmap, Burp Suite, OSSEC
- Operating Systems & Environments: Linux (Debian), Windows (Admin), VirtualBox

- Lab & Deployment Setup: Docker, custom SOC simulations, GitHub project workflows

EDUCATION

Gdynia Maritime University

B.Eng. in Information Technology Oct 2022 - Mar 2026

- Specialization: Internet and Mobile Applications
- Erasmus+ Exchange Program (Cybersecurity focus) at University of Extremadura, Spain - Spring 2025