Muhammad Zaim Akhtar Threat Hunter | SOC Analyst

✉ zaimakhtar@outlook.com | in linkedin.com/in/zaim-akhtar

pin-z.github.io/Cyberfolio/ | tryhackme.com/p/Pin309

PROFILE

Threat Hunter and SOC Analyst with proven success in reducing adversary dwell time by 35% through optimized SIEM alerts, custom detection rules, and proactive threat intelligence integration. Specialized in identifying and responding to advanced threats (APT, ransomware, lateral movement). Experienced in rapid incident triage, response, and resolution within a Security Operations Center (SOC) environment. Proficient in hardening defenses via Splunk, EDR, and MITRE ATT&CK-driven hunting.

EDUCATION

BS (Hons) in Cyber Security, *Air University Islamabad* 2021 – 2025 | CGPA: 3.25

CERTIFICATES AND COURSES

- **eLearning Security Certified Threat Hunting Professsional (eCTHPv2) - INE**
- **Practical Ethical Hacking,** *TCM Security*
- **Practical Web Application Security and Testing,** *TCM Security*
- **Google IT Support**
- **Backend Development and APIs,** *Freecodecamp*

COMPETITIONS & ACHIEVEMENTS

- **Qualified , Black Hat MEA 2024** | Riyadh, KSA
- **Participant, Digital Pakistan Cybersecurity Hackathon (by Ignite)** | 2023 and 2024
- **Finalist,** Pakistan Cybersecurity Challenge **CTF (by Airoverflow)** | 2024

PROFESSIONAL EXPERIENCE

Cyber Security Intern, *TISS (Trillium Information Security Systems)* 05/2024 – 09/2024 | Islambad

- Detected **5+ suspicious lateral movement attempts** via Splunk correlation searches, leading to **improved detection rules**.
- Reduced false positives by **30%** by tuning SIEM alerts for brute-force attacks.
- **Authored 10+ Sigma rules** for TTPs like credential dumping (T1003) and DLL hijacking (T1574), adopted org-wide.
- Conducted log analysis on **CloudTrail & VPC Flow Logs**, identifying anomalous behavior.
- Participated in the incident response process, analyzing and containing potential security events.

Secure Backend Development Intern, *Internee.pk* 09/2023 – 11/2023 | Remote, Pakistan

- **Reduced API abuse by 20%** by implementing rate-limiting (OWASP API8) and input sanitization against SQLi/XSS.
- Enhanced security in backend systems by integrating **OWASP best practices**.

PROJECTS

Disk Tracer, *Forensics analysis tool*

DiskTracer is designed to provide thorough scanning of disk images so that security personnel can evaluate trends and changes in the system.

- **comparing disk images** to detect malicious changes post-infection.
- Integrated the MITRE ATT&CK framework to automatically correlate discovered IOCs with adversary TTPs.
- Utilizes STIX/TAXII for ingesting threat intelligence feeds to contextualize findings against known threat actors.

AWS Threat Detection Simulator

- Built a lab environment to **simulate AWS-based attacks** (e.g., IAM privilege escalation, S3 bucket breaches).
- Analyzed **CloudTrail logs** to develop detection rules for GuardDuty & Splunk.

Gmail Phishing Application

- Developed a mock phishing platform and conducted a phishing campaign to study attack techniques and enhance email security awareness.

SKILLS

- **Threat Hunting:** SIEM (Splunk, ELK Stack), EDR (CrowdStrike, SentinelOne), Threat Intelligence (MISP, OpenCTI), Digital Forensics (Autopsy, FTK), Memory Analysis (Volatility), Malware Analysis.
- **Security Tools:** IDS/IPS (Snort), Wireshark, Burp Suite, OWASP ZAP, Metasploit, nmap, Nessus, aircrack-ng.
- **Programming/Scripting:** Python (Pandas, Volatility), PowerShell, Bash, JavaScript.
- **Frameworks:** MITRE ATT&CK, NIST CSF, Cyber Kill Chain.
- **Manual Exploitation:** Privilege Escalation, Reverse Shells, DLL Hijacking.