MUHAMMAD QASEEM

Punjab, Pakistan

• qaseem.infosec@gmail.com • linkedin.com/in/muhammad-qaseem • +92-3347896514

EDUCATION

Bachelor of Science in Computer Science Sep 2020 – Jul 2024 (Graduated)
Pak-Austria Fachhochschule: IAST, Haripur, Pakistan

EXPERIENCE

Security Engineer Jul 2024 – Present (11+ months)
Cydea Tech (Pvt) Limited Rawalpindi, Pakistan

- Deployed and maintained **DFIR IRIS** to centralize threat intel and automate case management.
- Co-developed an **Attack Surface Monitoring** pipeline to track external assets and their Attack Surface Score.
- Automated security incident response using **Shuffle**, **Wazuh**, **Velociraptor** and **SIEM** integrations.
- Developed playbooks to reduce triage time and integrate alert enrichment workflows.

Hive Sentinel Developer May 2023 – Jun 2024 (14 months)
CydeaTech (Pvt) Limited, Rawalpindi, Pakistan (in collaboration with Pak-Austria Fachhochschule: IAST, Haripur, Pakistan)

- Designed a deception framework for automated deployment of **Gen 2 industrial honeypots**.
- Integrated event collection, **MITRE ATT&CK mapping**, and alert pipelines.
- Conducted controlled attack simulations and validated event detection accuracy.
- Utilized **Elastic Stack**, **Wazuh**, **Terraform**, **ESXi Hypervisor**, **Proxmox**, and **Ansible**.

Product Analyst and Development Team Intern Jul 2022 – Sep 2022 (3 months)
Cydea Tech (Pvt) Limited Rawalpindi, Pakistan

- Evaluated and deployed honeypot platforms like **T-Pot**, **Dionaea**, and **Cowrie**.
- Performed attack simulation, data capture, and detection tuning.
- Created proof-of-concept detections mapped to **MITRE ATT&CK** framework.
- Explored alerting and correlation pipelines using **Snort** and **Suricata**.

SKILLS

Technical Skills	Penetration Testing, Security Operations, DFIR, SIEM, SOAR, OSINT, Deception, Detection Engineering
Security Tools	Wazuh, Suricata, Snort, Elastic Security, DFIR IRIS, Shuffle, Velociraptor, T-Pot, Cowrie
Scripting	Python, Bash

PROJECTS

- **Hive Sentinel: The Hacker Confine** – Project focused on designing a scalable deception-based defense framework that automates deployment of high-interaction Gen 2 industrial honeypots across hypervisors like ESXi and Proxmox. Integrated centralized event logging, MITRE ATT&CK technique mapping, and real-time alerting via Elastic Stack and Wazuh. Conducted multiple simulated attacks to validate detection accuracy and operational effectiveness for SOC use cases in industrial environments.
- **Open Source SIEM Deployment** – Architected and deployed a centralized SIEM environment using Wazuh to collect, correlate, and analyze security logs from distributed Linux and Windows nodes. Fine-tuned detection rules to reduce false positives and enhance actionable alerting. Developed custom dashboards for security visibility and ran adversary emulation exercises to validate log integrity and alert fidelity under real-world threat scenarios.

CERTIFICATIONS & TRAININGS

• **Certified Ethical Hacker (Master), EC-Council**	Issued: Mar 2025 to Apr 2028
• **Certified Ethical Hacker (Practical), EC-Council**	Issued: Mar 2025 to Apr 2028
• **Certified Ethical Hacker (CEH), EC-Council**	Issued: Aug 2024 to Aug 2027
• **Certified Associate Penetration Tester (CAPT), Hackviser**	Issued: May 2025
• **FullHouse Mini ProLab, Hack The Box**	Issued: Oct 2024
• **Zephyr ProLab, Hack The Box**	Issued: Jun 2024
• **Dante ProLab, Hack The Box**	Issued: Mar 2024
• **Detection Engineering Certification, LetsDefend**	Issued: Mar 2024
• **Malware Analysis Certification, LetsDefend**	Issued: Mar 2024
• **Incident Responder Certification, LetsDefend**	Issued: Feb 2024

AWARDS & HONORS

• **1st Place - Cyber Hackathon '23 (Online + KP Regional Qualifiers)**	Ignite National Technology Fund, 2023
• **runZero Coin Challenge Solver**	runZero, Texas, 2023
• **Best Final Year Project Award in School of Computing Sciences**	PAF-IAST FYP Exhibition, 2024
• **FYP Funded by NGIRI**	Ignite National Technology Fund, 2024