Sameel Ahmad Junaid

sameelahmad9876@gmail.com | sameelahmad | sameel01 | Islamabad, Pakistan | +923046097333

Profile

Cyber Security graduate with a strong motivation to protect data and mitigate risks. competent in applying controls to satisfy industry standards, conducting security audits, and scanning for vulnerabilities.

Professional Experience

SOC Analyst & SIEM Engineer (ITSOLERA) — Apr 2024 – present, Islamabad, Pakistan

I specialize in designing and implementing custom rules, tunning, integrating with Atlassian, and alert monitoring within SIEM. My responsibilities extend to managing alerts, documentation, and ticket automation as well as monitoring and handling alerts on CrowdStrike. Additionally, I am actively engaged in working on SOAR (n8n) to automate and enhance our security operations and incident response capabilities.

Network Administration Intern (PHDEC) — Aug 2023 – Oct 2023, Islamabad, Pakistan

At PHDEC, my responsibilities included managing and the organization's network infrastructure. This involved tasks such as troubleshooting to ensure seamless connectivity within the network

Malware Analyst Intern (Protect Lab) — Jun 2023 – Jul 2023, Islamabad, Pakistan

Completed a summer internship as a Malware Analyst, focusing on exploring static and dynamic malware analysis techniques and tools i.e IDA pro, Ghidra, YarGen,CFF Explorer, Frida and Objection.

Education

Bachelors of Science in Cyber Security — 2020 – 2024

FAST NUCES — Islamabad, Pakistan

Projects

ParaDefense

Designed a GUI-based advanced Intrusion Detection System (IDS) using a parallel approach, enabling real-time detection of DOS/DDOS attacks in network traffic with alert generation. Implemented SDLC to properly alerting alert and log storage in Elasticsearch, (database) facilitating report generation and analysis.

Governance Guard

Implemented Governance, Risk, and Compliance (GRC) framework, specifically ISO 27001, conducting comprehensive risk assessments, developing contiguency plans, contingency plans, and performing threat analysis to ensure proactive organizational governance

TriNet Traverse: Routing Trio in Cisco

Implemented network architecture featuring routing protocols NAT, EIGRP, OSPF, RIP, and DHCP using CISCO Packet Tracer.

E2EE Chat Application

Developed a client-server console-based secure chat application using Python, incorporating advanced encryption protocols including AES, RSA, Diffie-Hellman, and X.509 certificates for enhanced security measures.

Privilege Escalation

Exploited eternalblue vulnerability in windows and got reverse shell of the victim's system

Malware Analysis

Conducted static and dynamic malware analysis utilizing various tools and techniques within Flare VM.

OWASP Juice Shop

Exploit the OWASP Top 10 vulnerabilities that exist in OWASP Juice Shop (a vulnerable website)

Skills

Python | Firewall Rule Writing | SIEM (ELK Stack) | SOAR (n8n) | Threat Hunting | Malware Analysis | IDS | Network Security | ISO 27001 | Linux | Shell scripting | AWS | Vulnerability Assessment | Networking

Certificates

- AWS Academy Cloud Security Builder
- API Security Fundamentals