

# Waqar Ahmed

Mobile: +92-3072568434 | Email: waqarahmed\_72@hotmail.com | Karachi - 75300, PK

I do what needs to be done

I am a seasoned professional with 10+ years' experience in IT, mainly with Information Security and Consulting. Over the years I have worked with many technologies and have served clients across diverse industries.

---

## Professional Experience

### Senior Information Security Engineer

**Feb 2021 - Present | Afiniti Ltd. - Karachi Office, PK**

- Perform network architecture and design reviews including Corp, Prod and cloud environments (Azure and AWS) with security recommendations to the internal teams to secure the overall network architecture along with systems and applications.
- Evaluate the potential exposure to security risks and threats based on industry security frameworks (PCI-DSS and ISO27001), identify control gaps for remediation and recommend appropriate mitigation.
- Work closely with other teams to review alerts, correlate events and investigate security incidents. Prepare reports in timely manner and share with relevant teams and management.
- Perform threat hunting and threat analysis by performing network traffic and log analysis using Sophos EDR, QRadar SIEM, Firemon and outputs from other available tools.
- Vulnerability assessments of internal and external assets using Nexpose, Nessus and Acunetix, and provide support to remediate vulnerabilities such as patching, implementing controls to mitigate risk
- Document SOC playbooks using Mitre ATT&CK, configuration guides, and secure standards.
- Deployed new solutions, including QRadar SIEM, Sophos EDR, F5 and Firemon, at multiple DCs to better help monitor the activity within the organization and their continuous improvement.
- Prepared SOPs to help reduce the analysis and review time in day-to-day BAUs (business as usual tasks)
- Automate regular and tedious tasks with Python, Bash and Powershell scripts
- Help team with client queries and requirements located in different parts of the world including US, UK, AUS, EU and other regions.
- An active participant in knowledge transfer to junior members of team, and guide them in their day to day tasks.
- Managing several InfoSec related projects across the company and ensure their timely completion also ensuring smooth communication among several teams in an international and remote environment.

### Assitant Manager - Information Security

**Feb 2019 – Jan 2021 | NayaPay Pvt. Ltd - Karachi, PK**

- Prepared organization to achieve ISO27001 and PCI-DSS compliance
- Performed the regular Internal Security Audits, identify control gaps for remediation and recommend appropriate mitigation
- Performed Vulnerability Assessments and Penetration Testing including network, systems and applications. Provided support with remediation and implementation of security controls to mitigate risks.
- Developed the information security processes and procedures as applicable to informational assets, networks, and equipment and helped maintain the compliance.
- Saved organization operation cost by implementing open-source SIEM OSSIM with OSSEC
- Lead the Utimaco Atalla AT1000 HSM implementation project and successfully deployed it within timeline
- Implemented secrets and keys management through HashiVault
- Refined and improved the Software Delivery Life Cycle (SDLC) with added documentation, OWSAP guidelines and Jenkins
- Made several training videos related to security awareness, new and emerging threats, company policy and procedure for new and existing employees.
- Negotiated with vendors, improved upon the original offering and saved the company additional costs in procuring HSM and firewall devices.

#### **Principal Consultant**

**Nov 2016 – Jan 2019 | SPaWn Corporation - Karachi, PK**

- Started a partnership-based Information Security consulting firm, where I not only provided the consulting services but also did business development, sales, marketing and contract negotiations.
- Prepared an organization for PA-DSS compliance certification
- Prepared an organization for PCI-DSS compliance certification
- Policy and Procedure documentation covering full PCI-DSS and ISO27001 compliance requirements
- Android application assessment with manual static code review

#### **Consultant**

**Jun 2014 – Oct 2016 | Risk Associates Pvt. Ltd - Karachi, PK**

- Worked on diverse projects for our clients related to, PCI-DSS and PA-DSS audits and gap mitigation consulting, Penetration Testing and Vulnerability assessments, Secure code reviews and Pre-sale consulting of security products (SIEM, Oracle Security and TrendMicro)
- Lead the Blackbox and Grey Box penetration testing projects of national and international clients including, banks, gaming and software companies
- PCI-DSS compliance audits of Banks and Payment Service Providers and Operators
- Lead PA-DSS project of a payment switch vendor (first PA-DSS 3.0 project of company)
- Lead the software security code review project (first project in company history)
- Information Security policies and procedure development of a major Pakistani Bank.
- Proof of concept demos of NNT SIEM, TrendMicro suite and Oracle TDE, DB Vault and AVDF

### **Freelancing (June 2010 - May 2014)**

Started my own computer repair workshop did freelancing and enrolled in a Master's program. The work I did during freelancing include: vulnerability scans and pen-testing, cloud and VPS setup, Site migration, data backups, troubleshooting, website development for local businesses and System administration (Redhat, Windows Server and Active Directory)

### **Content Expert**

#### **Nov 2008 – Apr 2010 | GFK Utilize Pvt. Ltd, Karachi - PK**

Here I picked up advanced search engine skills as I searched and developed content for various IT and consumer electronic products, which included market research and maintaining the quality of the content and as per customer requirement. I trained new team members on content creation as well as market research. Assisted team lead in developing and maintaining department objects.

---

## **Education**

### **M.S Telecom & Networking (2012 - 2014)**

Bahria University, Karachi

### **B.E Electronics (2004 – 2007)**

Mehran University of Engineering and Technology, Jamshoro

---

## **Certifications**

- Offensive Security Certified Professional – OSCP
- Sophos EDR Certified Admin
- Oracle Database 11g Security Implementations Specialist - (1Z0-528)
- Juniper Network Certified Internet Associate-Enterprise Routing (JNCIA-ER)
- Juniper Network Certified Internet Associate-Enterprise Switching (JNCIA-EX)
- Juniper Network Certified Internet Associate-JUNOS (JNCIA-JUNOS)

---

## **Additional Relevant Courses**

- Certified Information Systems Security Professional – CISSP (on-going)
- CompTIA Security+ (SY0-601) Exam Prep via LinkedIn Learning
- Python for Offensive PenTest via Udemy
- Computer Science and Programming (from MIT) via EDX
- Computer Networks (from University of Washington) via Coursera

---

## **Skills**

- Knowledgeable and Hands-on experience with most aspects of CyberSecurity: Penetration Testing, Vulnerability Assessment, Digital Forensics, Threat Analysis, Risk Assessment, Firewalls/UTMs, IDS/IPS, SIEM, SOAR, Attack Vectors and Defense Strategies.
- Strong understanding and experience with ISO 27001, PCI-DSS and PA-DSS frameworks with internal and external audits.

- Experience with incident response, memory forensics, TTPs, IOCs and ATT&CK Framework
- Experience of working with a range of CyberSecurity tools: AT1000 HSM, QRadar and OSSIM SIEM, Sophos EDR, Firemon, HashiVault, and TrendMicro Products, Firewalls, Vulnerability Scanners (Nessus, Nexpose, OpenVAS, Acunetix, MobSF) and others.
- Familiarity with basic reverse engineering principles and reversing compiled code using OllyDbg, WinDBG and Ghidra.
- Experienced with drafting information Security policy and procedure of an organization.
- Dexterity with System Administration (Linux and Windows) and DevOps core concepts (Git, Jenkins, Kubernetes, and Ansible)
- Very good understanding of networking fundamentals, such as TCP/IP, Switching and Routing protocols
- Automate regular tasks in Python, Bash, Powershell and Javascript, and understanding C/C++.
- Proven management skills to manage multiple projects, priorities and deadlines in a fast-paced working environment
- Solid written communication skills and experience drafting reports and use cases
- Possession of very good quality oral and written skills in communicating the issues to higher management in clear and concise manner.
- A quick learner and out of the box thinker with superb problem-solving skills
- Work efficiently with little to no supervision.