KHALIQ UR REHMAN

Cyber Security Engineer | Cloud/DevOps Engineer

03045576706 y2khaliq@gmail.com www.linkedin.com/in/khaliqr/ Islamabad, Pakistan

SUMMARY

Dynamic Cybersecurity Engineer with over 3 years of experience in IT,Cloud Architecture, Information Security, and Cybersecurity. Proven expertise in developing and implementing security strategies to mitigate risks and ensured the confidentiality, integrity, and availability of critical data. Adept at vulnerability assessments, incident management, and maintaining compliance across AWS, Azure, and other platforms. Skilled in leading cross-functional teams to deliver secure, scalable solutions while bridging the gap between theory and practice through training programs. Dedicated to empowering teams and driving innovation in cybersecurity and cloud management.

SKILLS

Penetration Testing **Kali Linux** **Burp Suite** **Nmap** **Wireshark** **Hydra** **Elasticsearch (SIEM)**

Zabbix (Monitoring) **Suricata** **Snort** **FTK Imager** **MISP** **HashiCorp Vault** **Nginx** **pfSense**

OpenVPN **Nessus** **Nikto** **OpenVAS** **CIS Benchmarks** **OWASP ZAP** **MITRE ATT&CK Framework**

ELK Stack **Ethical Hacking** **GPO** **IDA Pro** **Ansible** **VMWare Cloud Director** **VMware ESXi**

Docker **Kubernetes** **Git** **Bitbucket** **CI/CD** **Jenkins** **Sonarqube** **Maven** **AWS** **Azure**

RHEL **Ubuntu** **CSI Linux** **Windows Server** **Active Directory** **Bash** **CCNA** **Cluster Configuration**

DHCP **Disaster Recovery** **DLP** **DNS** **Atlassian Data Center** **Jira Software** **Confluence** **Crowd**

Jira Service Management **Tabealu**

EXPERIENCE

CyberSecurity Engineer

ABACUS Consulting

08/2023 - Present Islamabad

ABACUS Consulting specializes in IT-Cloud Architecture and Information Security.

- Responsible for IT-Cloud Architecture, Information Security, Datacenter and Networks. Analysis, SRS, Audit, ISMS, Compliance and Governess.
- Responsible of leading IT-Cloud and Information Security Team for multiple projects.
- Develop, implement and monitor a strategic, comprehensive enterprise information security and IT risk management program to ensure CIA.
- Secure IT- Cloud architecture, Secure Application design, Application Security, Cyber Security tools implementations, SecOps and GRC.
- Preparation of SRS for Enterprise Software concerning Infrastructure / architecture and Information Security.
- Atlassian Project Management, SecOps, Azure, AWS, Huawei Cloud Administration.
- Manage security incidents and events to protect corporate IT assets, including intellectual property, regulated data and the company's reputation. Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action.
- Managing / supervision of day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans and communicate information about residual risk. Ensuring audit trails, system logs and other monitoring data sources are reviewed periodically and comply with policies and audit requirements.
- The **technology stack** includes but not limited to Enterprise Endpoint Protection Manager, ELK Stack Cluster - SIEM, EDR, DLP Solution, Secure designing of Datacenter, Enterprise Firewalls, WAF, Load Balancer, Docker/micro services, Penetration testing/ Vulnerability Assessment, Windows Active Directory, Ubuntu, RHEL, GPO, Cryptography, Digital Certificates, Secure VPN, ISMS, ISO 27001, 27005, NIST CSF, Cyber Kill Chain, MITRE, GDPR, SANS, GRC, CICD, JIRA Scrum, Disaster Recovery and Business Continuity

EXPERIENCE

Application Security Engineer

e-Medicare Solutions

09/2021 - 04/2022 Rawalpindi

e-Medicare Solutions focuses on software solutions for healthcare management.

- Conducted **Static Application Security Testing (SAST)** and **Dynamic Application Security Testing (DAST)** to identify and mitigate vulnerabilities in software applications, ensuring secure and high-quality product delivery.
- Performed comprehensive **Vulnerability Assessments and Penetration Testing (VAPT)** to proactively address potential security risks and enhance product resilience.
- Played a key role in improving the security and quality of the company's flagship software product, successfully implemented across **45+ hospitals**, significantly increasing its value and reliability.
- Discovered and documented bugs and vulnerabilities in the software through detailed **manual testing**, and collaborated closely with development teams to ensure timely resolution.
- Created comprehensive defect reports and tracked them throughout the development lifecycle, ensuring all issues were resolved effectively and aligned with quality standards.
- Delivered software installation services and conducted client training sessions to ensure proper software usage, while addressing client-specific requirements.
- Contributed to the development and enforcement of security best practices and quality standards, directly enhancing the product's security posture and overall quality.
- By blending my expertise in **application security**, **software quality assurance**, and **client collaboration**, I successfully enhanced the security and functionality of the company’s product, ensuring it met the highest industry standards.

TRAINER EXPERIENCE

Cybersecurity Instructor

PNY Trainings

11/2023 Rawalpindi, Pakistan

PNY Trainings provides professional training in various IT domains.

- Delivering **comprehensive training sessions** on **Advanced Cybersecurity Concepts**, including **Ethical Hacking (CEH), Penetration Testing, Network Security (CCNA), and System Security (MCSA, RHCSA)** to university students and industry professionals.
- Conducting **hands-on labs** for **penetration testing, vulnerability assessment, bug bounty programs, Bash scripting, Python for hacking, and cryptography**, ensuring practical skill development.
- Training students on **network security fundamentals**, covering **Cisco and network hardening techniques**.
- Educating participants on **secure software development principles**, including **Web Application Security, SQL Injection, and OWASP Top 10 vulnerabilities**.
- Teaching **Windows Server Administration (MCSA)**, focusing on **Active Directory, Group Policy Management, Hyper-V, DHCP, DNS, and VPN setup**.
- Setting up and managing **hacking labs** with **Kali Linux and other cybersecurity tools** for real-world penetration testing exercises.
- Providing knowledge on **security frameworks and compliance standards**, including **ISO 27001, NIST CSF, GDPR, and Cybersecurity Incident Management**.
- Coaching students on **Information Security Risk Management, Cyber Incident Response, and Business Continuity Planning**.
- Preparing students for **certifications such as CEH, RHCSA, CCNA, and MCSA**, bridging the gap between academic learning and professional careers.
- Mentoring and guiding professionals in **career development, cybersecurity roles, and industry best practices**, helping them transition into security-focused job roles.
- This role enables me to **empower students and professionals with industry-relevant cybersecurity skills**, helping them build **secure, scalable IT solutions** in alignment with global standards.

Cybersecurity Trainer

Logitrain Training

04/2022 Australia

Logitrain Training conduct trainings for IT jobs

- **Delivered Comprehensive Cybersecurity Training**: Conducted online training sessions on **ethical hacking, penetration testing, network security, and cloud security** for professionals and students.
- **Hands-On Labs & Practical Exercises**: Designed and facilitated hands-on labs using tools like **Kali Linux, Burp Suite, and Wireshark** to teach real-world cybersecurity skills.
- **Curriculum Development**: Developed training materials and modules aligned with industry standards, including **OWASP Top 10, MITRE ATT&CK, and NIST CSF**.
- **Mentored Students**: Provided one-on-one guidance to help participants prepare for certifications like **CEH, CompTIA Security+, and CISSP**.
- **Stayed Updated with Industry Trends**: Incorporated the latest cybersecurity threats, tools, and techniques into training programs to keep content relevant and up-to-date.

TRAINER EXPERIENCE

Cybersecurity Trainer

OMNI Academy

Islamabad

OMNI Academy provides professional training in various IT domains.

- **Delivered Foundational & Intermediate Cybersecurity Training**: Conducted classroom-based training sessions on **ethical hacking (CEH), computer forensics (CHFI), network security, and penetration testing** for students and professionals.
- **Hands-On Labs & Practical Exercises**: Designed and facilitated interactive labs using tools like **Kali Linux, Metasploit, Nmap, and Autopsy, FTK Imager** to teach real-world cybersecurity skills.
- **Curriculum Development**: Created and updated training materials focused on **ethical hacking techniques, digital forensics, OWASP Top 10 vulnerabilities, and MITRE ATT&CK framework**.
- **Prepared Students for Certifications**: Guided participants in preparing for **CEH (Certified Ethical Hacker)** and **CHFI (Computer Hacking Forensic Investigator)** certifications, ensuring a strong understanding of exam objectives.
- **Improved Engagement & Learning Outcomes**: Used interactive teaching methods, including live demonstrations, Q&A sessions, and practical exercises, to enhance student understanding and retention.
- **Stayed Updated with Emerging Threats**: Integrated the latest cybersecurity trends, attack techniques, and defense strategies into training programs to ensure relevance.

Cloud Solution Architect & Instructor

Hazza Institute of Technology

06/2024 Gilgit, Pakistan

Hazza Institute of Technology provides professional trainings in various IT domains and engineering

- Delivering **comprehensive training programs** on **Cloud Computing and Cloud Native Technologies** to university graduates and industry professionals, ensuring both foundational and advanced knowledge transfer.
- Designing and conducting hands-on labs covering **Linux Administration (RHCSA), Docker, Docker Compose, Docker Hub, Jenkins, SonarQube, Maven, Git, GitHub, and cloud platforms like Azure and AWS**.
- Educating participants on **CI/CD pipelines** and **DevOps best practices**, enabling them to implement automation and streamline software development workflows.
- Guiding students through **containerization and orchestration** concepts, ensuring practical exposure to modern cloud environments.
- Providing real-world industry insights into **cloud security, infrastructure as code (IaC), and scalable architecture design** for cloud-based applications.
- Training professionals on **version control (Git/GitHub)**, **code quality assessment (SonarQube)**, and **automation tools (Jenkins, Maven)** to enhance development efficiency.
- Mentoring and preparing participants for cloud certifications and industry roles, bridging the gap between academia and enterprise cloud adoption.
- By combining **practical hands-on training** with **industry-relevant tools and methodologies**, I empower learners with the skills required to **design, deploy, and manage scalable cloud-native solutions** in today's evolving IT landscape.

EDUCATION

MS Cybersecurity

SZABIST Islamabad

09/2021 - 07/2023 Islamabad

BS Software Engineering

COMSATS University Islamabad

09/2016 - 09/2020 Islamabad

PROJECTS

EPADS (e Pak Acquisition and Disposal System)

01/2023 - 02/2023 Pakistan

As part of the EPADS project, I deployed and implemented a suite of technologies to enhance operational efficiency, security, and reliability:

- **Zabbix**: Configured for comprehensive monitoring of resources and network infrastructure, enabling real-time insights, proactive issue detection, and system optimization.
- **HashiCorp Vault**: Integrated for secure key storage and centralized management of sensitive credentials, including IDs and passwords, ensuring robust encryption and access control.
- **Elasticsearch**: Deployed and configured for advanced threat detection and real-time log analysis from compromised endpoints with varying timestamps. I also conducted a DOS attack on a Windows endpoint using Kali Linux to test threat detection and incident response and created custom rules for triggers and alerts.
- These implementations significantly improved the system's security, monitoring capabilities, and incident management processes, supporting the efficient acquisition and disposal of e-pack resources while enhancing my expertise in cybersecurity and system administration.

LICENSES & CERTIFICATIONS

Microsoft Certified: Azure Administrator Associate
Microsoft Certified: Azure Administrator Associate

TRAINING / COURSES

- **CEH |Certified Ethical Hacker (Corvit Trainings)**
- **Cloud Native Computing Boot Camp (MOIT&T)**
- **RedHat Certified System Administrator (MRGT Trainings)**
- **RHCSA |RedHat Certified System Administrator (Corvit Trainings)**
- **Microsoft Certified: Azure Administrator Associate (MRGT)**
- **Certified Cloud Security Engineer (CCSE) (MRGT Trainings)**
- **Digital Forensics for Pen Testers- Hands-on Learning (Udemy)**
- **AWS Certified Cloud Practitioner (MRGT Trainings)**
- **Windows Forensics with Belkasoft (Balkasoft)**

KEY ACHIEVEMENTS

Application Security Enhancement
Successfully improved the security and quality of the application used in 45+ hospitals, greatly increasing its value and reliability.

Certificate of Excellence Instructor
Awarded for outstanding contributions as an **instructor**, demonstrating expertise in **Cybersecurity** while effectively imparting knowledge to students throughout the year.

RESEARCH INTEREST

- **Cloud Environment Security**
- **Malware Analysis**
- **Dark web forensics**
- **Machine Learning techniques in Cyber Security and Digital Forensics**
- **Vulnerability Exploitation and Defense**