

RAZA AZEEM

Al Wakrah Qatar | +92-335-7735900, +974-71723675

raza_azeem@outlook.com, razaazem@gmail.com

Websites, Portfolios, Profiles

- www.linkedin.com/in/razaazeem
- <https://razaazem.github.io/Portfolio/>








Professional Summary:

Experienced Cybersecurity Analyst with a strong foundation in securing Operational Technology (OT) and Industrial Control Systems (ICS) environments. Proven track record in SOC operations, threat detection, and incident response across IT and OT networks. Seeking a role as a SOC Analyst or SOC Engineer to apply my skills in monitoring SCADA/ICS systems, conducting vulnerability assessments, and implementing robust security frameworks. Dedicated to enhancing cyber resilience through proactive threat hunting, compliance with industry standards, and continuous improvement of security postures in dynamic, mission-critical environments.

Educations:

| Bahria University | (2023) | Abbottabad University (AUST) | (2019) |
|---|--------|---|--------|
| MS Information Security | | BS Computer Science | |
| Relevant Courses: Information Security Management, Digital Forensics, Cyber Security, Penetration testing, Cloud computing security. | | Relevant Course: Database Management System, Compiler Construction, Computer and Network Communication, Management Information System. | |

Skills & Tools:

-  Perimeter & Network Security: Darktrace, Nozomi Networks, SolarWinds SEM, Nmap, Wireshark.
-  Endpoint Protection & Access Control: CrowdStrike Falcon, CyberArk, Trellix EPO.
-  Security Monitoring & SIEM: Splunk, Wazuh, Microsoft Azure Sentinel, Teramind.
-  Vulnerability & Penetration Testing: Nessus Professional, Nikto, Acunetix, Burp Suite, Metasploit, MobSF.
-  Security Awareness: KnowBe4.
-  Backup & Recovery: Veritas, Acronis.
-  Infrastructure & Virtualization: VMware ESXi, VMWare Workstation.

Professional Experiences:

Qatar Chemical Industry (QCS)

ICS Cybersecurity Technician

(2025 -- Present)

Key Responsibilities:

- Monitored SCADA/ICS environments using Nozomi Networks and Darktrace for real-time anomaly detection and threat hunting.
- Integrated Trellix ePO for end-to-end security visibility.
- Implemented Trellix DLP to enhance data protection across systems.
- Managed Hirschmann switches for secure network segmentation.
- Applied regular Microsoft patches and updated antivirus signatures on Windows systems, enhancing system security across all platforms.
- Conducted thorough security assessments on servers and workstations, ensuring compliance with industry standards.
- Managed server backups stored on NAS, ensuring data integrity and availability.
- Performed preventive and corrective maintenance, including system hardening, to improve operational efficiency.
- Collaborated with different project teams for maintenance and troubleshooting, supporting ICS operations during critical incidents.

CareCloud, Islamabad, Pakistan

SOC Analyst

(2024 -- 2025)

Key Responsibilities:

- Monitored and triaged security alerts using CrowdStrike Falcon EDR and SolarWinds SEM, identifying and investigating suspicious activity across endpoints and network infrastructure.
- Conducted deep-dive investigations with CrowdStrike Falcon, leveraging its threat graph and behavioral analytics to trace malicious activity and support rapid containment.
- Collaborated with Incident Response and IT teams to remediate threats, escalate critical findings, and implement preventive controls.
- Used screen monitoring tools such as Teramind to track user behavior and detect policy violations or insider threats.
- Created threat intelligence briefs to support blue-team operations and improve detection capabilities.
- Led KnowBe4 security awareness training campaigns, reducing phishing susceptibility and promoting a culture of cyber hygiene across the organization.

Pakistan Tobacco Company / HRSPL
IT MWP Engineer

(2022 -- 2024)

Key Responsibilities:

- Conquer diverse IT challenges: Provide expert technical support for all users, tackling issues related to security, hardware, software, network connectivity, and OT/ICS.
- Master incident resolution: Resolve incidents logged on ServiceNow, adhering to established procedures and SLAs. Utilize CyberArk for secure remote support and manage privileged account access controls.
- Safeguard OT/ICS systems: Proactively monitor performance and security, identifying and addressing potential issues.
- Collaborate with OT/ICS personnel to optimize functionality.
- Conduct thorough yearly and quarterly audits to ensure compliance.
- Team up with SIEM Security: Investigate compromised systems in collaboration with SIEM security, contributing to a robust security posture.

Emigrates

Help Desk Engineer

(2019 -- 2020)

Key Responsibilities:

- Managed and maintained system infrastructure, including servers, storage, and networking devices.
- Installed and configured software and hardware, including operating systems, security software, and applications.
- Troubleshooted and resolved system problems, such as performance issues, network outages, and hardware failures.
- Performed system backups and restores to ensure data protection.
- Monitored system performance and made necessary adjustments to maintain optimal performance.
- Provided technical support to users on system issues, such as account access issues and software problems.