

Quazi Ahmed

(708)-253-3525 • dev.quazi@gmail.com

Fully Work Authorized • No Visa Sponsorship Required

PROFESSIONAL SUMMARY

Passionate Cybersecurity Analyst with a strong foundation and proficiency in cybersecurity, specializing in vulnerability assessment and incident response. Actively pursuing opportunities to enhance cybersecurity expertise and stay updated with the latest trends and advancements through diverse courses, certifications, and personal projects.

PROFESSIONAL EXPERIENCE

Junior Software Developer

11/2022 - 06/2023

CloudCity Partners, New York, NY (Remote)

- Developed user interface for mobile app for media company using Bootstrap and CSS in collaboration with three junior developers, resulting in simple and intuitive interface.
- Assisted software engineers with design implementation.
- Designed websites and arranged website hosting on AWS using S3 storage and RDS database.

Project Research Associate (Information Security)

01/2018 - 01/2022

Birla Institute of Technology Mesra, Ranchi, India

- Led all technical and research aspects of project, researched technical requirements, and determined what tools would be used.
- Developed enhanced algorithm for data security and encryption and increased BIT level to 512.
- Conducted research and developed algorithms for data optimization.
- Collaborated with team of 5-7 technical employees.

Assistant Professor (CS & IT)

06/2015 - 08/2017

Syed Hashim College of Science & Technology, Hyderabad, India

- Taught 60 students per semester on material including programming with C, operating systems, and databases including MySQL, Oracle Database.
- Guided 5 students per semester in producing independent coding projects using C.
- Developed teaching materials for new course focused on algorithms, data structures, etc.

System Administrator

08/2013 - 12/2014

Syed Hashim College of Science & Technology, Hyderabad, India

- Implement and enforce robust security protocols to safeguard the 60 lab systems and their data, including user access controls and continuous system monitoring.
- Regularly updated and maintained the Windows operating systems and software on all 60 lab systems to ensure security and optimal performance.
- Provide technical assistance and support to lab users across the 60 systems, addressing login issues, assisting with software installations, and troubleshooting problems.

CORE COMPETENCIES

- Vulnerability
- Assessment and Remediation
- Effective Communication
- Incident Handling
- Creative Problem Solving
- Threat Assessment Attention to Detail

PROJECTS

Vulnerability Assessment Lab

08/2023 -09/2023

- Set up and configured Windows virtual machine (VM) on VirtualBox
- Installed and configured Nessus vulnerability scanner on the Windows VM.
- Conducted comprehensive vulnerability scans using Nessus, including credential scans.

- Identified and analyzed vulnerabilities in the system and installed vulnerable software for testing purposes.
- Developed and implemented effective remediation strategies to address identified vulnerabilities.

Password Management System in AWS

010/2023 - 11/2023

- Created Passbolt, a self-hosted password manager, to securely store and manage complex passwords.
- Utilized AWS cloud services to host Passbolt, ensuring scalability, availability, and reliability.
- Implemented HTTPS encryption to safeguard sensitive data transmitted to and from the password manager.
- Configured and maintained the domain hosting for the password manager, ensuring accessibility and security.
- Provided functionality within Passbolt for secure storage of complex passwords, enhancing data protection and user convenience.

Multi Honeypot Platform

12/2023 - 01/2024

- Deployed T-Pot on Azure Cloud to enhance security measures.
- Configured virtual machine and network to support the installation and operation of T-Pot.
- Monitored and analyzed honeypot data to detect and respond to potential cyber threats.
- SIEM Implementation in Azure Cloud
- Successfully deployed Microsoft Sentinel a SIEM solution in Azure Cloud.
- Implemented advanced techniques and configurations to enhance the SIEM solution's threat detection capabilities
- Created custom analytics rules using KQL to enable the detection of specific security events and patterns.
- Conducted incident investigations using SIEM tools and techniques to analyze cybersecurity incidents.
- Implemented remediation actions to mitigate and resolve identified cybersecurity incidents.

AI Enabled Incident Response Automation

02/2023 - Present

- Developed a ChatGPT solution on the Azure Cloud platform designed to enhance cybersecurity incident management.
- Implemented strict access controls and permissions ensuring a secure environment for handling sensitive incident data and response actions.
- Conducted necessary fine-tuning and optimizations to maximize AI performance, ensuring its ability to deliver valuable insights and recommendations.
- Created an automation within the SIEM system to seamlessly integrate AI and streamline overall cybersecurity operations.

EDUCATION

Master of Technology (M.Tech), Information Security

Birla Institute of Technology Mesra, Ranchi, India

CERTIFICATES

- CompTIA Security+
- AWS Cloud Practitioner