MD Zahedul Islam

CONTACT INFORMATION

Email: zahed.arman44@gmail.com

Work Phone: +1(929)6082288

Google Scholar: https://scholar.google.com/citations?hl=en&user=a09FPo0AAAAJ

Address: Queens, NY

EDUCATION

M.Sc in Cybersecurity, Mercy University, Dobbs Ferry, NY — Fall 2024

CGPA : 3.93 out of 4.00 (Graduated with Distinction)

B.Sc in Electrical & Electronics Engineering

American International University Bangladesh (AIUB), Dhaka, Bangladesh. — Fall 2013

SELECTED PUBLICATIONS

Islam, M.Z., Siam, M. A., Ahmed, I., Khan, M. A. U. H., Islam, M. A., & Milon, M. H. (2025). *Fortifying Healthcare and Essential Infrastructure with AI-Driven Cybersecurity Technologies. 2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC), IEEE.*

https://doi.org/10.1109/ICMCTC62214.2025.11196395

Islam, M.Z., Ahmed, I., Parveen, R., Rimon, S. M. T. H., & Janjua, J. I. (2025). *Revolutionizing Healthcare for Critical Diseases with AI and Enhancing Security via Low-Latency Edge Intelligence. 2025 International Conference on AI-Driven STEM Education and Learning Techniques (AISTEMEDU), IEEE.*

https://doi.org/10.1109/AISTEMEDU67077.2025.11403932

RESEARCH EXPERIENCE & PROJECTS

Graduate Researcher — January 2024 - May 2024

CAE INSuRE+E Program

- Investigated invariant behaviors in malicious activities using industry-standard tools.
- Developed threat detection analytics using the MITRE ATT&CK framework.
- Simulated adversary techniques using CreateProcessWithTokenW for access token manipulation.
- Configured and deployed Splunk, Splunk Forwarder, and Splunk Add-on for Microsoft for security monitoring.
- Conducted malware analysis to identify patterns and improve detection capabilities

Intrusion Detection System with Snort

- Installed and configured Snort IDS to monitor network traffic and detect security threats.
- Developed and tested custom Snort rules to detect DDoS, MITM, and brute-force attacks.
- Integrated Snort with firewall systems to enhance network security defenses.
- Documented security incident responses and optimized detection techniques.

PROFESSIONAL EXPERIENCE

Upskil Consultancy INC, Jackson Heights, NY- Remote — May 12, 2026- Present

Cybersecurity Analyst

- Monitor enterprise network and security infrastructure to identify, analyze, and respond to cybersecurity threats.
- Perform vulnerability assessments, security risk analysis, and remediation activities to strengthen organizational security posture.
- Investigate security incidents through log analysis, alert correlation, and identification of indicators of compromise (IOCs).
- Configure and maintain firewalls, intrusion detection systems, endpoint security solutions, and identity-based access controls.

Upskill Consultancy INC, Jackson Heights, NY- Remote Jan 12, 2026 - May 11, 2026

Network Engineer

- Monitored and supported enterprise network infrastructure, including routers, switches, firewalls, and cloud-based network components
- Performed network troubleshooting, incident resolution, firewall-rule reviews, access-control enforcement, and vulnerability mitigation.
- Maintained network configurations and documentation while supporting network monitoring and security operations.

Arnex Solutions LLC, Princeton, NJ-Remote April 11, 2025 - Jan 10, 2026

Network Engineer

- Implemented and maintained network security controls, including firewall policies, ACLs, VPNs, and secure network segmentation.
- Monitored network traffic and security alerts to identify suspicious activity and potential security incidents.
- Supported incident response through log analysis, IOC identification, vulnerability assessment, and remediation.
- Reviewed network configurations and implemented logging and monitoring improvements to reduce attack surface and strengthen security visibility.

Nokia, Dhaka, Bangladesh January, 2018 - November, 2022

Technical Engineer

- Configured and supported enterprise network security infrastructure using Juniper SRX and Palo Alto firewalls, including IPSec VPNs, NAT, security zones, and firewall policies.
- Designed and implemented 802.1X wired and wireless authentication using Cisco ISE for corporate and BYOD environments.
- Integrated Cisco ISE with Active Directory and configured authentication and authorization policies for identity-based network access control.
- Monitored network security alerts, performed incident analysis, and conducted firmware and patch management to mitigate vulnerabilities.
- Supported secure infrastructure and cloud migrations, including movement of virtual machines and applications from on-premises environments to AWS.

ZTE Corporation, Dhaka, Bangladesh August, 2015 - December, 2017

Technical Support Engineer

- Installed, configured, and maintained **Red Hat Enterprise Linux (RHEL) systems** across development,staging,and production environments.
- Integrated routers, switches, and firewalls into enterprise environments and implemented network segmentation and role-based access controls.
- Integrated Cisco ISE with switches, wireless controllers, and firewalls using dynamic VLAN assignment and downloadable ACLs.
- Configured and supported secure wireless access using 802.1X, EAP/PEAP, certificate-based authentication, Aruba ClearPass, and Cisco ISE.
- Performed network monitoring and log analysis using SNMP, syslog, SD-WAN dashboards, and Splunk.

CERTIFICATIONS

Red Hat Certified System Administrator (RHCSA)

Red Hat Certified Engineer (RHCE)

Cisco Certified Network Associate (CCNA)

TECHNICAL SKILLS

Security: Snort IDS, Splunk, Wireshark, Nmap, Metasploit, Nessus, SIEM, Firewall Configuration
Networking: TCP/IP, DNS, DHCP, VLAN, VPN, 802.1X, Cisco ISE, Network Segmentation, IPTables
Systems: Linux (RHEL, Ubuntu, Kali), Windows, Windows Server, Active Directory
Cloud & Virtualization: AWS Security, VMware, VirtualBox Programming & Data: Python, SQL
Security Operations: Incident Response, Threat Hunting, Log Analysis, Vulnerability Assessment, Security Hardening.
Documentation : LaTeX