MD SUJON MIA

IT & SECURITY OPERATIONS PROFESSIONAL

Dhaka, Bangladesh · +880 1677 473791 · sujonmia.0612@gmail.com

linkedin.com/in/md-sujon-mia · tryhackme.com/p/agentTequila · github.com/agentTequila

450+	100+	9 years	1,200+	3
STAFF SUPPORTED	ENDPOINTS MONITORED	LEADING TEAMS	PEOPLE TRAINED	LIVE INCIDENTS HANDLED

PROFILE

I do IT and security operations at a 24/7 national news channel. Thirteen years in business operations, nine of them in a leadership role, before this. Three outlets opened, 1,200+ people trained in skill development, customer service and leadership. Now the job is keeping transmission up: newsroom, production and broadcast-control faults, identity and access for 450+ staff, 30 CCTV cameras and 7 access-control systems, and support for reporters in all 64 districts. I set up Wazuh to monitor 100+ Windows and macOS endpoints, built dashboards, and worked through patching for vulnerable software and packages. Three incidents have gone the full distance: NLBrute and HitlerBrute, the RDP brute-force toolkits running on a production server under a built-in account nobody was using, and Neshta.A spreading through removable media and network shares. What I want next is SOC, security analyst and IT security lead/operations roles, remote or in Dhaka.

CORE COMPETENCIES

SECURITY OPERATIONS	IT OPERATIONS & INFRASTRUCTURE	LEADERSHIP & GOVERNANCE
Wazuh SIEM monitoring and log triage	Windows Server / 10 / 11, macOS, Linux CLI	Team leadership and training
Incident response, full lifecycle	Active Directory, Group Policy and access control	SOP, runbook and knowledge-base authoring
RDP and credential-attack detection	Endpoint and patch management	Audit, risk and compliance documentation
Malware triage, IOC handling and eradication	TCP/IP, DNS, DHCP, subnetting	Training design and delivery (1,200+ trained)
Network forensics (Wireshark, TCPDump, Nmap)	Service desk and asset management	C-suite, vendor and cross-team reporting
Python automation, AI-assisted build and OSINT	CCTV and access-control systems	Process improvement and vendor negotiation

PROFESSIONAL EXPERIENCE

Channel One, 24/7 News Television · Dhaka

December 2025 – Present

Executive IT (IT & Security Operations)

- IT and security operations for a channel that never goes off air. Keep newsroom, production and broadcast-control faults moving against deadlines.
- Identity and access for 450+ staff: accounts, MFA, permissions, with least privilege applied to the network and to the doors. 30 CCTV cameras and 7 access-control systems sit in the same job.
- Support reporters in all 64 districts, plus technical and non-technical staff, through user guides, SOPs and escalation paths written for whichever audience they are.
- Learned broadcast from scratch, signal path through playout to the control room, because you cannot judge which security changes are safe until you know what must not stop.
- Set up Wazuh to monitor 100+ Windows and macOS endpoints, built dashboards, and worked through patching for vulnerable software and packages.
- Wrote windows-power-tool (see Projects) after the same admin jobs kept coming back by hand.

SELECTED INCIDENT RESPONSE WORK

NLBrute & HitlerBrute: RDP brute-force toolkits, production Windows Server

Both are credential-attack utilities that guess Remote Desktop logons, which is why no antivirus signature catches them. I found them by triaging endpoint alerts. The binaries sat on the desktop of WDAGUtilityAccount, a built-in Defender Application Guard account with no reason to exist on that server, and the processes were still running in Task Manager. I contained the host, killed the processes, removed the tooling, closed the account path, then hardened RDP exposure.

Neshta.A: file infector

Neshta.A infects executables, persists through the registry and spreads on removable media and network shares. I isolated the host, cleaned it, checked it was clean, then tightened the endpoint controls so it didn't come back.

Independent Professional Development (Security Transition) · Dhaka

June 2025 – December 2025

- Six months between roles spent on security: Blue Team Junior Analyst (Security Blue Team), Practical Security Fundamentals & Help Desk (TCM Security), and the Google Cybersecurity Professional Certificate, six of its seven courses done.
- Built the home lab the rest of this CV leans on. Active Directory attack and defence, Wazuh, malware analysis, and CTF practice.

Awake Coffee Roasters, Specialty Coffee · Dhaka

July 2024 – June 2025

Head of Coffee Excellence (Operations Manager)

- Ran the business end to end. Wrote the SOPs, moved stations until the workflow stopped snagging, ran monthly performance reviews, and set the menu from sales data instead of taste.
- Trained 300+ people (curriculum, delivery, assessment), most of them students or first-time café owners, and fronted the brand in B2B negotiations.

Indulge F&B Ltd (United Group) · Dhaka

September 2022 – June 2024

Shift Manager

- Opened three sites: Satarkul and Gulshan-1 from a bare shell, then the Gulshan-2 central branch. Hiring, training and process each time, and the first launch's numbers earned me the second.
- Ran multi-outlet operations: staffing, performance reviews, stock planning, order flow, and the monthly sales decks I presented to the CEO and General Manager.

Career Break (Skill Development) · Dhaka

June 2021 – August 2022

- TryHackMe Junior Penetration Tester path (8 modules, 39 labs) and Cisco Networking Academy, alongside the first version of the home lab.

North End Coffee Roasters, Specialty Coffee · Dhaka

February 2012 – May 2021

- Promoted four times in nine years, café assistant to Assistant Manager, Training & Development. Leading teams from 2015, and the last four years carried alongside a full-time degree.
- Assistant Manager, Training & Development (2019–2021): built the curriculum from nothing and kept rewriting it. Trained 150+ staff and 1,200+ external people in skill development, customer service and leadership, audited branches on quality, service and leadership, then aimed the training at whatever the audits turned up.
- Assistant Manager (2018–2019): first manager on a brand-new branch. Scheduling, stock, cash, daily reporting to the GM, and a local presence built from zero, Google Maps listing included, which lifted sales in the area.

SELECTED PROJECTS

Three Python tools. I design and test them and AI writes a good share of the code, since my Python is basic and the tools still needed to exist.

windows-power-tool

PYTHON · TKINTER · AUG 2026 – PRESENT

A portable Windows admin toolbox: one self-elevating EXE, twelve tools, nothing to install. USB storage control, event-log collection to TXT/CSV/native EVTX, system profiling, installed-app inventory, user and group management, live process and service control. Built on the job at Channel One because the same manual tasks kept recurring. Destructive actions confirm first and locked files are never force-deleted. github.com/agentTequila/windows-power-tool

security-monitor

PYTHON · WINDOWS REGISTRY · SEP 2025

Blacklist-based software monitoring for Windows and Linux. Reads installed software from the registry uninstall keys and from dpkg/rpm, matches it against a configurable blacklist, grades findings HIGH/MEDIUM/LOW and emails a report on a schedule. Report-only by default, and enforcement is strictly opt-in. Ships as a portable EXE that installs itself as a SYSTEM scheduled task. github.com/agentTequila/security-monitor

ReconForge

PYTHON · SHODAN · VIRUSTOTAL · OCT 2025

A cross-platform OSINT toolkit: 44 modules across 64+ platforms and six target types, with a CLI and a GUI that share one scan engine. Passive by default; active modules need an explicit flag and a confirmation. API keys are optional, and the AI insights can run fully local through Ollama so scan data never leaves the machine. github.com/agentTequila/ReconForge

EDUCATION

Bachelor of Business Administration, Major in Accounting

2017 – 2021

Dhaka International University · Dhaka

- CGPA 3.46 / 4.00, 126 credits. 100% merit tuition waiver on admission-test performance. Taught entirely in English, and I worked full-time the whole way through.

CERTIFICATIONS & TRAINING

CERTIFICATION	ISSUER	YEAR
Google Cybersecurity Professional Certificate (6 of 7)	Google (Coursera)	2025 – 2026
Certified Ransomware Protection Officer	International Cyber Threat Task Force	2025 – 2026
Blue Team Junior Analyst	Security Blue Team	2025
Practical Security Fundamentals / Practical Help Desk	TCM Security Academy	2025
Junior Penetration Tester Path, 8 modules, 39 labs	TryHackMe	2022
Cybersecurity, Networking, IT & OSINT Foundations	Cisco Networking Academy / WithYouWithMe	2022 – 2023

HANDS-ON PRACTICE

- 107 TryHackMe rooms done, including SOC Level 1 and Junior Penetration Tester: log analysis, alert triage, detection, containment, remediation. CTF practice and some web-application testing alongside, all public on the profile.
- Home lab on VirtualBox. Active Directory attack and defence with BloodHound, Kerberoasting and Golden/Silver Ticket, Wazuh for centralised logging, malware analysis, Wireshark and TCPDump captures, and vulnerability work with Nmap and Metasploit.

LEADERSHIP, SERVICE & LANGUAGES

- Bangladesh National Cadet Corps (Air Force), 2011 – 2013. Corporal in year one, Cadet Sergeant by the last, which meant leading people who were the same age as me.
- Bangladesh Scouts, 2008 – 2010. Community service and teamwork.
- Bangla native · English full professional proficiency, the language I studied my degree in and work in daily.

Available with 30 days' notice · open to remote, hybrid and relocation