MD TAREK

Cybersecurity Analyst | SOC & Threat Intelligence | Vulnerability Assessment & Security Automation

Barguna District, Barisal, Bangladesh | 01903878932 | mdtarekcom376@gmail.com | linkedin.com/in/mdtarek404 | tareksec.dev

PROFESSIONAL SUMMARY

IT professional with 3+ years of experience transitioning into cybersecurity, including 10 months of dedicated, hands-on SOC analyst skill-building alongside a background in SEO and technical web analysis. Directed AI-assisted development of two security automation tools — a phishing/URL triage system (deployed live) and a SIEM-integrated alert triage workflow — both mapping threats to MITRE ATT&CK. Hands-on experience with vulnerability scanning (Acunetix, WordPress/Wordfence), network traffic analysis (mitmproxy, Scapy), and Microsoft Sentinel/Defender (KQL, incident investigation, threat hunting); currently preparing for the Microsoft SC-200 certification. Seeking an entry-level SOC Analyst or Cybersecurity Intern role to apply and grow these skills under experienced analysts.

TOP SKILLS

- **SOC & Threat Analysis:** Alert Triage · Incident Investigation · Threat Hunting · Cyber Threat Intelligence (CTI)
- **Frameworks:** MITRE ATT&CK · Cyber Kill Chain · Email Security (SPF / DKIM / DMARC)
- **Tools & Platforms:** Wazuh SIEM · Microsoft Sentinel / Defender · KQL · VirusTotal
- **Vulnerability Assessment:** Acunetix · Web App Vulnerability Scanning · WordPress Hardening (Wordfence)
- **Network Security:** MITM / Traffic Analysis (mitmproxy, Scapy) · Network Reconnaissance
- **AI-Assisted Development:** Directed AI coding tools to build, deploy & maintain web platforms (Node.js, SQL, Supabase) — e.g., okkhorpathagar.com

PROJECTS

Phishing Triage & Kill Chain Analyzer (Live: email.techvrs.com)

- Directed AI-assisted development of an automated tool that analyzes suspicious emails and URLs using VirusTotal and urlscan.io APIs.
- Independently deployed, configured, and maintain the tool live in production; maps identified threats to Cyber Kill Chain stages and MITRE ATT&CK techniques.

AI-Powered Alert Triage System (GitHub)

- Directed AI-assisted development of a local SOC lab tool that integrates with Wazuh SIEM to auto-tag alerts with MITRE ATT&CK techniques.
- Tested in a personal lab environment to explore automated alert classification and triage workflows.

Local Network Traffic Analysis & MITM Lab (GitHub)

- Built a hands-on lab using mitmproxy and Scapy to intercept and analyze traffic on an authorized local network, covering reconnaissance, interception, and custom traffic analysis scripting.
- Documented defense and mitigation strategies against MITM-style attacks, including certificate pinning and VPN usage.

Web Vulnerability Scanning & WordPress Security Hardening

- Used Acunetix and related web vulnerability scanners to identify security flaws across WordPress sites and web applications.
- Diagnosed and remediated vulnerabilities using Wordfence, reducing attack surface and improving overall site security posture.

LLM Fine-Tuning on Azure VM

- Trained and fine-tuned a large language model on custom datasets using Azure virtual machine infrastructure, gaining hands-on experience with cloud-based ML workflows.

EXPERIENCE

Independent Security Researcher Oct 2025 - Present (10 months)

Self-Employed

- Directed AI-assisted development of a SOC alert triage system and a phishing/URL triage tool, mapping detected threats to MITRE ATT&CK techniques.
- Built security automation workflows for alert investigation, threat classification, and SOC analyst assistance.
- Applied SIEM alert triage, threat intelligence, and incident analysis concepts through hands-on personal SOC lab projects.
- Practiced Microsoft SC-200-aligned concepts including incident response, KQL-based investigation, and security operations workflows.

Founder Ongoing

ArtX Studio (techvrs.com) — Web Design, Development & Security

- Run an independent web design, development, and SEO studio; partner with techvrs.com to offer web security audits and hardening for client sites.

SEO Specialist (Part-time, Remote) Oct 2025 - Feb 2026 (5 months)
BayShore Communication - Dhaka, Bangladesh

- Worked part-time and remotely alongside independent cybersecurity study, analyzing website performance and preparing data-driven reports.
- Identified technical issues affecting website performance and user experience using analytics tools.
- Managed remote tasks, client communication, and on-time project delivery.

SEO Specialist - Link Building Nov 2024 - Sep 2025 (11 months)
Freelance

- Developed and executed off-page SEO strategies focused on backlink research and outreach.
- Conducted outreach campaigns and maintained organized tracking reports to monitor SEO progress and results.

CERTIFICATIONS

- Google Cybersecurity Professional Certificate (v.2)
- Cisco Certified Ethical Hacker - Cisco Networking Academy (2026)
- EC-Council NDE-112-51: Network Defense Essentials (NDE)
- AWS: Foundations of Prompt Engineering
- Pursuing: Microsoft SC-200 (Security Operations Analyst)

EDUCATION

Higher Secondary Certificate (HSC), Science
Barguna Govt. College | Expected February 2027