

ALBAR HOSSAIN RAFI

Cybersecurity Engineer



albarhossain@gmail.com | +880 1971561819 | linkedin

PROFESSIONAL SUMMARY

Cybersecurity Engineer & Open-Source Security Advocate with hands-on experience in security operations, network detection and response. As a passionate open-source security advocate, I specialize in leveraging community-driven tools like Wazuh, ClamAV, Suricata, and Zeek to build transparent and resilient SIEM/XDR architectures, while effectively managing enterprise-grade solutions including Splunk, VirusTotal, Maltiverse, and Shuffle. Proficient in Python, C++, and Java, I bridge the gap between software engineering and security to develop smart, automated applications that mitigate SQLi, DDoS, and advanced malware threats.

WORK EXPERIENCE

Trainee Cybersecurity Engineer

Oct 2025 – Present

M/s. Tech4TIME

- Deployed Wazuh SIEM across critical server infrastructure, reducing mean time to detect (MTTD) by centralizing log collection and automating file integrity monitoring.
- Engineered robust monitoring solutions using Suricata and Zeek to analyze traffic patterns and detect anomalies.
- Configured OPNsense firewalls to implement network segmentation, isolating critical assets and reducing the attack surface by 20%.
- Hardened Linux web servers (Apache/Nginx) by implementing ModSecurity v3 WAF with the OWASP Core Rule Set (CRS) to mitigate SQL injection, XSS, and other OWASP Top 10 vulnerabilities.
- Utilized YARA for custom signature matching and GRR (Google Rapid Response) for remote live forensics and incident triage across endpoints.
- Designed security orchestration workflows using Tracecat and Shuffle, automating 28% of routine incident response tasks and significantly reducing alert fatigue for the SOC team.

Network Support Engineer

Jul 2025 – Sep 2025

InfoLink Limited

- Troubleshoot network issues and resolved connectivity problems across the core network while maintaining 99% uptime.
- Provided frontline support to resolve network connectivity issues for clients.
- Guided non-technical users through troubleshooting steps, ensuring service continuity.
- Applied fundamentals of IP addressing, subnetting, VLANs, DNS and DHCP to everyday troubleshooting tasks.

Rates and Tariffs Analyst

Feb 2023 – Jan 2025

Vervantis Inc.

- Developed Python automation scripts using Pandas to streamline complex data processing reducing processing time by 18% and demonstrating strong capability in scripting and data sanitization.
- Managed large-scale datasets using SQL, ensuring data integrity and accuracy.
- Collaborated with a remote, multicultural team to deliver high-quality results within established timelines.
- Assisted in budget preparation, monthly reporting, and workflow documentation.

EDUCATION

BSc in Computer Science & Engineering – 2025

American International University-Bangladesh

- CGPA: 3.75

Higher Secondary Certificate – 2020

Willes Little Flower School And College

- GPA: 5.00

SKILLS

- Security Engineering
- SIEM & Security Operations
- NDR & Firewall
- Web & Application Security
- Threat Hunting & Forensics
- SOAR Automation & Scripting
- Virtualization

CERTIFICATIONS

- Google Cybersecurity
- Cisco Introduction to Cybersecurity
- NDG Linux Essentials

PUBLICATIONS

The X-SIEM Framework: Integrating Rule-Based, ML, and LLMs for Cyber Threat Intelligence

EXTRA CURRICULAR

IEEE AIUB Student Branch

Member

- Actively participated in technical seminars, workshops, regional flagship events and industrial tours.

REFERENCES

Dr. Nahar Sultana

Assistant Professor, Faculty

American International University-Bangladesh

Email: nahar@aiub.edu

H. M. Saifullahil Mazid

Chief Operations Officer

Tech4Time, Dhaka, Bangladesh

Email: saifullahil.mazid@tech4time.com.bd

Cell phone: +880 1881873463