BENYAMIN TAFRESHIAN

bentsec@proton.me | (617) 356-2487 | Boston, MA | linkedin.com/in/benyamint/ | github.com/btafreshian

PROFESSIONAL EXPERIENCE

Boston University | Boston, MA **February 2024 - Present**

Research Assistant | February 2024 - Present

- Improved adversarial resilience of machine learning–based intrusion detection models by 30%, strengthening network defenses against AI-driven threats
- Investigated vulnerabilities in ML algorithms to identify exploitable weaknesses and designed countermeasures that increased threat detection reliability by 15%
- Delivered 50+ research briefings translating technical findings into actionable recommendations for security teams as part of detection and mitigation strategy

Teaching Assistant (Network Security) | January 2025 - May 2025

- Led hands-on SOC simulation labs using Splunk, pfSense, and Wireshark, training 15+ graduate students on log analysis and incident response techniques
- Guided students through configuration of firewalls and IDS tools, reinforcing understanding of network defense fundamentals and reducing detection time by 60%
- Created standardized lab documentation and exercises mapping attacks to MITRE ATT&CK techniques to enhance applied learning consistency
- Provided real-time coaching on correlating network telemetry with indicators of compromise (IOCs) to strengthen students' analytical precision

Poyan Sannat Farnad | Tabriz, Iran **May 2019 - September 2023**

Cybersecurity Analyst | November 2020 - September 2023

- Reduced cyber risk 25% by implementing enterprise-wide IT security policies and enforcing continuous compliance reviews
- Lowered recurring IT incidents 15% commercially minded by conducting vulnerability assessments and coordinating remediation with cross-functional teams

Cybersecurity Intern | May 2019 - September 2019

- Improved network uptime 20% by supporting configuration and maintenance of routers, switches, and firewalls
- Reduced incident resolution time by 4 hours by diagnosing and troubleshooting connectivity issues across multi-site systems

PROJECTS

96-Bit Block Cipher

- Increased cipher diffusion and key strength by designing a 96-bit encryption algorithm using Rijndael S-boxes and Rubik's Cube-inspired P-boxes
- Improved resistance to linear and differential attacks through formal cryptanalysis and statistical testing

Fraud Detection in Big Data using Apache Ignite

- Processed 10,000+ transactions/sec in real time integrating Kafka, Ignite, and scikit-Learn models via PyIgnite for fraud detection
- Achieved 95% accuracy with inference latency under 100 ms, supporting distributed SQL queries and Spark fallback pipelines

RedditEngage: ML-Based Comment Score Predictor

- Processed 37M+ Reddit comments on a 4-node Spark cluster, engineering 19 behavioral and linguistic features for modeling
- Achieved AUC 0.706 using a custom SGD classifier with SHAP-based interpretability to improve transparency and accuracy

EDUCATION

Master of Science in Computer Science (MS) (Concentration: Security) | Boston University, Boston, MA | **May 2025**
Bachelor of Science in Computer Engineering (BS) | University of Tabriz, Tabriz, Iran | **September 2020**
CERTIFICATIONS: ISC2 Certified in CyberSecurity (CC) (January 2025)

SKILLS

Python | C | C++ | Bash | PowerShell | Splunk | MITRE ATT&CK Navigator | OWASP ZAP | Burp Suite | Qualys | Maltego | Wireshark | tcpdump | Snort | pfSense | Autopsy | FTK Imager | Sleuth Kit | AWS | Google Cloud (IAM, Monitoring, Logging) | Docker | Git | JIRA | PostgreSQL | MongoDB | Network Security | Threat Intelligence | Threat Hunting | Incident Response | Vulnerability Management | Compliance Auditing | Risk Assessment | Security Frameworks (NIST, ISO 27001) | OSINT Collection | SIEM Analysis | SOC Operations | Firewall Configuration | Endpoint Security | Cloud Security | Data Correlation | Log Analysis | Communication | Team Collaboration | Problem Solving | Adaptability