

SAMYUKTA KURIKALA

Boston, MA | samyuktakurikalawork@outlook.com | Available May 2026 | F-1 STEM OPT Eligible
[linkedin.com/in/samyukta-kurikala](https://www.linkedin.com/in/samyukta-kurikala) | github.com/Samyukta-14 | samyuktakurikala.netlify.app

EDUCATION

Northeastern University

M.S. in Cybersecurity | GPA: 3.72/4.0

Boston, MA

September 2024 – May 2026

SRM Institute of Science and Technology

B.Tech. in Computer Science and Engineering | GPA: 92.1%

Chennai, India

September 2020 – June 2024

TECHNICAL SKILLS

Security Tools: Splunk, Wazuh, Wireshark, Nmap, Volatility, Autopsy, Sysmon

Platforms & Languages: Windows, Linux (Ubuntu/Debian), Microsoft 365, AWS, Docker | Python, PowerShell, Bash, SQL

Core Skills: SIEM, EDR/XDR, IDS/IPS, Log Analysis, Alert Triage, Incident Response, Threat Hunting, Malware Analysis

Frameworks: MITRE ATT&CK, NIST CSF, NIST 800-53

Certifications: CySA+ (in progress), CompTIA Security+, ISC2 CC

PROFESSIONAL EXPERIENCE

Graduate Teaching Assistant – Cybersecurity Principles and Practices

Remote

Khoury College of Computer Sciences

January 2026 – May 2026

- Designing and developing hands-on labs covering risk management frameworks and core cybersecurity principles
- Evaluating student assignments on Linux security fundamentals, Python/Bash scripting, and risk analysis techniques
- Guiding 20+ graduate students during office hours on cybersecurity concepts, forensics, and compliance frameworks

Cybersecurity Project Intern

Remote

IRDE, Defence Research and Development Organisation (DRDO)

July 2023 – November 2023

- Conducted threat analysis to identify potential interception vulnerabilities and developed secure video transmission system using Raspberry Pi with AES-256 encryption and custom frame-shuffling algorithms
- Implemented password-authenticated access controls and built checksum-based integrity verification to detect tampering attempts during transmission
- Maintained detailed daily documentation and produced technical reports outlining security measures, testing results, and findings for project manager review

TECHNICAL PROJECTS

Enterprise SOC Home Lab | Wazuh, Docker, Sysmon, MITRE ATT&CK

- Deployed Wazuh SIEM/XDR with centralized log management from Windows workstation and hardened Linux bastion
- Developed 12 custom detection rules for threat hunting based on behavioral baselines; mapped IOCs to MITRE ATT&CK (T1110, T1078, T1059, T1136)
- Built dashboards for alert triage and security monitoring: source IP analysis, after-hours activity, login anomalies

Digital Forensics Investigations | Autopsy, FTK Imager, Volatility, Eric Zimmerman Tools

- Investigated 4 insider threat and data exfiltration cases; analyzed USB artifacts, registry hives, and shellbags to identify IOCs
- Performed malware analysis and identified anti-forensic activity through prefetch, jump list, and LNK file analysis
- Reconstructed user activity timelines to produce prosecution-ready reports with chain of custody documentation

Alert Triage & Incident Response | CyberDefenders, Wireshark, Volatility, VirusTotal

- Investigated 10+ simulated incidents covering malware, phishing, and intrusion scenarios; triaged alerts, extracted IOCs, and mapped findings to MITRE ATT&CK
- Created structured incident reports documenting investigation methodology, root cause analysis, and remediation actions

Secure Instant Messaging Application | Python, Cryptography, SRP, ECDH, AES-GCM

- Built encrypted peer-to-peer chat system with SRP authentication, ECDH key exchange for forward secrecy, and AES-256-GCM encryption
- Implemented session key derivation using HKDF, rate limiting to prevent abuse, and multi-user support

LEADERSHIP & RECOGNITION

WiCyS Scholarship Recipient – Competitively selected to attend 2026 Women in Cybersecurity Annual Conference

Top 50 Globally – WiCyS Target Cyber Defense Challenge | **6th Place** – SimSpace Cyber Range Challenge

Head of Finance – null NEU Chapter