Serin Tony

Boston, MA | +1(857) 397-5349 | **tony.s@northeastern.edu** | Portfolio | Linkedin | GitHub

Education

Northeastern University, Boston, MA *Sep 2025 - Present*

Master of Science in Cybersecurity (GPA 3.83)

Coursework: Critical Infrastructure Protection (risk management, compliance documentation, third-party risk assessment, NIST CSF 2.0, security policies, crisis decision-making), Network Security (firewalls, VPNs, wireless security, threat detection), Security Fundamentals & Compliance (CIA triad, GDPR, security governance), Cybersecurity Technologies (Linux administration, scripting, cloud security)

Mar Athanasius College of Engineering, Kerala, India *Jun 2018 - Aug 2022*

Bachelor of Technology in Computer Science and Engineering (GPA 8.12)

Professional Experience

Systems Engineer, Tata Consultancy Services, India *Aug 2022 - Aug 2025*

- Developed and secured Life & Health reinsurance application for a global leader, ensuring compliance with financial services security standards.
- Identified and mitigated XSS, IDOR, and CSRF vulnerabilities during security assessments and audits of legacy GWT to Angular migration by collaborating with cross-functional teams on improving security posture and performance by 40%.
- Integrated REST and GraphQL APIs with strict access-control validation and input sanitization.
- Supported Agile/DevSecOps workflows with continuous patching, linting, and dependency-scanning best practices.

Python Developer, Tata Consultancy Services, Remote (Internship) *Mar 2022 - Jun 2022*

- Automated secure web data extraction with Python, reducing manual effort by 80%.
- Implemented validation, error-handling, and sanitization to prevent injection and insecure deserialization issues.
- Enhanced data accuracy and reliability for production use

Projects

Critical Infrastructure Security Analysis - WMATA Metrorail Network *Sep 2025 -Dec 2025*

- Modeled Washington Metro as a cyber-physical network to assess vulnerability to cascading failures and targeted attacks.
- Calculated spectral radius, betweenness centrality, and node robustness using Python to identify high-risk chokepoints.
- Analyzed attack scenarios on federal transit hubs and evaluated resilience under random vs. intentional disruptions.
- Applied DHS critical infrastructure frameworks to recommend security controls and redundancy improvements.
- Analyzed threat-countermeasure tradeoffs using DHS/CISA protection frameworks.

Intrusion Detection System Using Hybrid Deep Learning *Jun 2021 - Jun 2022*

- Designed and trained an intrusion detection system to identify DDoS, port scanning, and botnet activity.
- Analyzed network traffic and reduced false positives through feature engineering.
- Mapped detection logic to common attack patterns aligned with MITRE ATT&CK (foundational).
- Automated data preprocessing and model evaluation using Python.

Technical Skills

Offensive Security & Penetration Testing: Web Application Security (SQLi, XSS, CSRF, IDOR), API Security Testing, Vulnerability Assessment, Security Monitoring, Exploit Development, Threat Modeling (STRIDE), OWASP Top 10, MITRE ATT&CK

Security Tools: Burp Suite, OWASP ZAP, Nmap, Wireshark, Kali, Metasploit, Nessus, OpenSSL, Splunk (SIEM), Snort (IDS), Elastic

Programming & Scripting: Python, Bash, JavaScript, PowerShell, Java, C/C++, TypeScript, Shell Scripting

Cloud & DevSecOps: AWS (IAM, S3, CloudTrail), Docker, CI/CD Security, Dependency Scanning, GCP

Platforms & Collaboration: Windows, Linux, Git, GitHub, Jira, Confluence, CI/CD workflows, VS Code, IntelliJ

Labs & CTF Experience: TryHackMe (Top 6%), HackTheBox, BugCrowd, VulnHub

Certifications

- Google Associate Cloud Engineer
- Microsoft GitHub Copilot Certification
- IBM Specialization in IT Fundamentals for Cybersecurity
- "Usable Security" – University of Maryland