Aditi Indre

aditi.indre@slu.edu +1(314)319-1424 linkedin.com/in/aditi-indre github.com/Aditiicodes

EDUCATION

Saint Louis University, *St. Louis, MO*
Master of Science in Cybersecurity (*GPA: 4.0*) *Jun. 2024 – May. 2026*
1+1 joint degree with Mumbai University, Mumbai, India (2024–2025)
Relevant coursework: Digital Forensics, Incident Response, Network Security, Cryptography

University of Mumbai, *Mumbai, India*
Bachelor of Science in Computer Science (*CGPA: 3.39/4.0*) *Jun. 2021 – May. 2024*
Relevant coursework: Computer Networks, Operating Systems, Database Management Systems

WORK EXPERIENCE

CyberFrat, *Mumbai, India*
Cybersecurity Operations Intern *Apr. 2025 – Aug. 2025*
- Monitored and triaged security alerts using Splunk and Wireshark, performing log analysis and network traffic inspection across enterprise environments, reducing average alert resolution time by 20%.
- Conducted vulnerability assessments with Nmap and Metasploit to uncover exploitable weaknesses, and partnered with technical teams on security audits, access management reviews, and cybersecurity best-practice remediation.

Excelerate, *Remote*
Project Manager Intern, Digital Strategy *Jun. 2025 – Jul. 2025*
- Directed cross-functional teams through an Agile digital transformation initiative, owning timelines, stakeholder communication, and deliverables, while tracking project metrics and reporting progress to management for on-time delivery.

YHills, *Mumbai, India*
Data Science Intern *Jun. 2023 – Aug. 2023*
- Built predictive machine learning models in Python and SQL, executing data pre-processing, feature engineering, and Tableau visualization to surface patterns and trends that improved model performance and data-driven decisions.

PROJECTS

Financial Market Monitoring & Suspicious Activity Detection Platform
Independent Project [*Source Code*] *Aug 2026*
- Flagged anomalous trading across 12 NASDAQ-100 equities by engineering a Python Z-score detection engine scoring four fraud typologies against 90-day baselines, with risk tiering and control mapping to the NIST CSF 2.0 framework.

ProxLink (Home Lab Server)
Group Project [*Source Code*] *Apr 2026*
- Hosted Linux and Windows VMs on Proxmox, configured Opnsense Firewall with Snort for intrusion prevention(IPS) to block unauthorized access, and enabled remote access to VMs using Netbird VPN tunnel, strengthening cloud security.

CloudPot (AWS Honeypot)
Cloud Security Research [*Source Code*] *Apr 2026*
- Captured 10K+ unauthorized SSH logins in 30 days via a Cowrie honeypot on AWS EC2 in an isolated VPC subnet, streaming telemetry to CloudWatch and S3 for Athena analysis, producing IOCs and attacker TTP profiles.

OWASP Juice Shop Penetration Testing
Independent Project [*Source Code*] *Mar 2026*
- Uncovered 10+ critical web application vulnerabilities by executing full-stack penetration testing against OWASP Juice Shop with Burp Suite, OWASP ZAP, and manual exploitation, documenting remediation mapped to the OWASP Top 10.

SKILLS

Languages: Python, Bash, SQL, PowerShell, JavaScript, C, C++, Java, HTML, PHP
Tools & Platforms: Splunk, Wireshark, Nmap, Burp Suite, Metasploit, Nessus, CrowdStrike Falcon, Semgrep, SonarQube, Ghidra, Autopsy, AWS, Microsoft Azure, GCP, Terraform, Docker, Kubernetes, GitHub, Linux (Kali, Ubuntu), Active Directory
Technical Skills: Network Traffic Analysis, Log Analysis, Incident Detection & Response, Vulnerability Assessment, Digital Forensics, Threat Detection Engineering, MITRE ATT&CK, OSINT, Cryptography, Firewalls, IDS/IPS, VPNs
Project & Analysis: Agile Methodologies, SDLC, Requirements Gathering, Risk Assessment, Risk Tracking, Stakeholder Communication, Status Reporting, Data Analysis, Data Visualization, Research & Report Writing
Certifications: CompTIA Security+, ISC2 Certified in Cybersecurity (CC)

ACHIEVEMENTS

- Awarded competitive Black Hat USA and DEF CON 34 scholarships (2026)
- Published first-author research on deepfake threats to digital media authenticity, *IJRASET*, Mar 2025. [DOI]
- Presented research poster on the WannaCry ransomware attack and EternalBlue SMB vulnerability at CCSC Central Plains 2026.