JEET VIJAYWARGI

+1 617-952-3393 | jeetsatishv@gmail.com | https://linkedin.com/in/jeetvijaywargi | https://github.com/jeetsatishv

EDUCATION

Carnegie Mellon University **Aug 2024 - Dec 2025**
Masters of Science, Artificial Intelligence Engineering - Information Security *Pittsburgh, PA*
- **GPA:** 3.9/4.0
- **Coursework:** ML with Adversaries, Applied Information Assurance, Security in Networked Systems, AI Applications in Info Sec, Hacking & Offensive Security, Network Forensics, Telecommunication Networks

Boston University **Aug 2020 - May 2024**
Bachelors of Art in Computer Science, Minor in Business Administration & Management *Boston, MA*
- **GPA:** 3.7/4.0
- **Achievements:** Dean's List: 7 out of 8 Semesters
- **Coursework:** Software Engineering, AI, Data Science Tools, Cybersecurity, Entrepreneurship

EXPERIENCE

FalconEye Cybersecurity
SOC Analyst **Jun 2025 - Dec 2025**
- Executed ransomware recovery protocols across 200 OT/factory endpoints, assisting the incident response team to achieve a 3-hour RTO and rapidly restore critical production lines
- Centralized endpoint telemetry in Cortex XDR and authored Palo Alto firewall policies (inbound, outbound, NAT), improving network visibility and reducing incident response latency
- Drafted incident response runbooks mapped to MITRE ATT&CK TTPs, and validated resilient 3-2-1 backup architectures via rigorous recovery drills

Serene Pharma
Security Engineering **Jun 2024 - Aug 2024**
- Designed the network topology for a multi-site Palo Alto firewall deployment, establishing a unified security baseline across facilities
- Modernized enterprise backbone to 1/10/40Gb with redundant aggregation switches, eliminating single points of failure
- Conducted a targeted risk assessment of enterprise backup practices, proposing a resilient offline storage model and periodic restore testing to mitigate ransomware threats

Cybersecurity & Infrastructure Engineering **Jun 2023 - Aug 2023**
- Replaced unmanaged legacy switches with centrally managed networking equipment in critical areas, improving visibility, troubleshooting, and uptime
- Automated provisioning using DUCKY scripts, cutting setup time ~80% and ensuring endpoint consistency
- Engineered LangChain-powered Telegram bot ecosystem to modernize internal workflows: developed a semantic search assistant for medical reps and a real-time factory status dashboard for executives, significantly reducing manual reporting overhead

PROJECTS

Passkey Misbinding Authentication Vulnerability Research **Dec 2025**
- Demonstrated critical WebAuthn logic flaw: manipulating client-side identity data during registration allows account takeover
- Built full exploit pipeline using Flask, Docker, and Python to automate IDOR attacks against the passkey registration API

Adversary Emulation & Incident Reconstruction **Nov 2025**
- Executed a controlled end-to-end insider threat simulation using Metasploit/Meterpreter to establish a reverse shell and a SOCKS + proxychains pivot through a compromised Windows host to access internal services behind pfSense segmentation.
- Exploited SQL injection in an internal Python app against MySQL, confirming data exposure and DoS risks via database logs
- Performed Network Traffic Analysis and deep log analysis using SecurityOnion (PCAP/Zeek) to reconstruct attack timelines, applying DFIR methodology to propose code-level mitigations

Network Security Projects **May 2025**
- Programmed in C using raw sockets to craft custom packets (ICMP/TCP SYN floods), built a network sniffer, and validated DDoS mitigation strategies (SYN cookies) against IP spoofing attacks
- Provisioned a PKI in OpenSSL; deployed routed OpenVPN (tun) with OpenSSH bastion, subnet routing, and CRLs
- Programmed Open vSwitch with a Ryu controller: enforced OpenFlow port-restricted firewall, added switch-stats-driven flood detection and rate limiting, and hardened controller links with insider-access controls, border filtering, structured alerts/logs

Edge-Detect IDS for Raspberry Pi **May 2025**
- Built a lightweight Intrusion Detection System on Raspberry Pi using PyTorch, applying principles of Network Security Monitoring (NSM) to detect malicious behavior
- Engineered a real-time pre-processing pipeline that aggregates raw PCAP data into 25 normalized flow features (e.g., TCP flags, packet size statistics) for immediate inference
- Achieved 91.9% accuracy (1.2MB model), delivering alert digests, reproducible training scripts, and LIME-based interpretability

SKILLS

- **Programming Languages & Systems**: Python, Java, C, Linux/Unix, Bash Scripting, Docker
- **Cloud Technologies & DevOps**: Amazon Web Services, Google Cloud Compute, Automation
- **Database Technologies**: PostgreSQL, Neo4j, Firebase, SQL
- **Data & AI Skills**: Machine Learning, Deep Learning, Natural Language Processing, Data Analytics
- **Security**: Splunk, Cortex XDR, Metasploit, Wireshark, Burp Suite, SecurityOnion, Palo Alto Firewall, EDR/XDR
- **Concepts**: Incident Response & Forensics, Network Security Monitoring (NSM), Zero Trust, Threat Modeling, Vulnerability Assessment, Intrusion Detection, Network Traffic Analysis, Frameworks (MITRE ATT&CK, NIST, OWASP Top 10), Log Analysis, Rule & Signature Development

ACHIEVEMENTS

- **TEDx Speaker:**Selected from 50+ applicants to deliver a talk on mathematical concepts. (Viewed 1.5k+ times on TEDx YouTube)