# YASH NAGARE

Brooklyn, NY 11220 | (347) 203-4550 | yash.nagare@nyu.edu | linkedin.com/in/nagareyash | github.com/nagareyash | nagareyash.com

## EDUCATION

**New York University,** New York, NY (*M.S. Cybersecurity*) GPA: 4.0/4.0 May 2027

- *Relevant Coursework*: Application Security, Offensive Security, Introduction to Operating Systems, Network Security, Applied Cryptography, Information Security and Privacy

**Mumbai University,** Mumbai, India **(***B. Tech. Cybersecurity, Minor in Data Science*) CGPA: 8.61/10 Jun 2025

- *Relevant Coursework*: Data Structures & Algorithms, Operating Systems, OOPS, Computer Architecture, Cryptography, Database Management & Security, Web Application Security, Network Security, Virtualization & Cloud Computing, VAPT, Ethical Hacking

## SKILLS & CERTIFICATIONS

- **Cybersecurity:** Penetration Testing, ICS/OT Security, Binary Exploitation, Reverse Engineering, Malware Analysis, Vulnerability Assessment, Application Security, SCADA, Cyber-Physical Systems, Cyber Threat Intelligence, APT Analysis, Network Traffic & Log Analysis, Network Design, Honeypot, Cloud Security, SOC Analysis, Incident Response, Machine Learning, Threat Modeling
- **Languages & Tools:** Python, Java, C, C++, PowerShell, BASH, Git, VMware ESXi, Windows AD, Docker, Azure, STIX 2.0, AWS, MySQL, FastAPI, Elasticsearch, Wazuh, ELK Stack, Splunk, Volatility, Metasploit, Tenable, Wireshark, Nmap, Burpsuite, MITRE Caldera, Claroty, Ghidra, Binary Ninja, Pwntools, IDA, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Tableau, PowerBI
- **Certifications & Frameworks:** CEH, Google Cybersecurity Professional, Cisco Cybersecurity Essentials, CISA 210W-03, CISA 210W-04, ISO/IEC 27001, HIPAA, PCI DSS, GDPR

## EXPERIENCE

*Embedded Systems Developer*, **Meshnet Electronics LLP,** Mumbai, India Jan 2025 – Jun 2025

- Created IIOT gateway modules in Embedded C on FreeRTOS platform with VPN, store & forward, and file compression
- Implemented security for HTTP and WEBUI functionalities, and upgraded the Arduino's JSON library to enhance system resilience
- Reviewed and implemented secure coding practices using Snyk & Cppcheck across software components to proactively resolve bugs
- Hosted the VPN server on AWS, configuring NGINX with TLS/SSL encryption to enhance accessibility & gateway reliability

*Cybersecurity Researcher,* **Veermata Jijabai Technological Institute (VJTI) COE CNDS,** Mumbai, India Jan 2024 – Jun 2025

- Configured OT and IT systems in a research environment using VMware ESXi for cybersecurity testing and deployment
- Deployed SIEM-capable security operations (SOC) using ELK and IDS tools (Snort, Suricata, Wazuh, & Zeek) for ICS
- Engineered an end-to-end attack chain model from IT to OT using the MITRE ATT&CK framework for threat modeling
- Installed a Kiwi syslog server pipelining with ELK for centralized dashboarding and real-time log analysis across network assets

*Cybersecurity Researcher,* **CyberPeace,** Mumbai, India Aug 2022 – July 2024

- Led research initiatives by identifying critical security gaps, devising innovative cybersecurity strategies, and presenting findings
- Deployed a Threat Intelligence Platform using open-source honeypot technologies (Snare, Tanner, Dionaea) capturing 500+ sessions
- Simulated real-world vulnerabilities, monitored attacker behaviors, & gathered actionable threat intelligence using ELK Stack
- Developed a capture the flag & bug bounty (HackTheWay) platform to enhance cybersecurity skills among practitioners

## PROJECTS

**UniSOC: An Asset Management Platform for ICS Environment with SIEM & SOAR – VJTI** 2024-2025

- Engineered UniSOC as a comprehensive asset management solution for Industrial Control System environments using Python
- Processed PCAP files with Scapy for real-time ICS asset identification, classification, and monitoring following IEC 61850 standards
- Designed a scalable agent-based architecture with vulnerability scanning, endpoint monitoring & threat detection capabilities
- Presented UniSOC to leading industry firms, including Siemens, Schneider, Delhi Metro, Thermax, Tata Power, and Adani

**Threat Intelligence Extraction Framework (TIEF) – VJTI** 2024-2025

- Led development of TIEF, a framework automating the extraction of cyber threat intelligence using BERT-based architecture
- Converted unstructured data into STIX 2.0 objects from diverse sources such as Advanced Persistent Threat (APT) reports and blogs
- Linked extracted intelligence with the MITRE ATT&CK framework to enable integration into SIEM for improved threat hunting
- Published TIEF framework in the Q1 Journal of Cybersecurity & Privacy by MDPI, advancing cyber threat intelligence research

**TrustTrace – A Multimedia Deepfake Detection Tool (**trusttrace.net.in**) – CyberPeace** 2023-2024

- Led development of multimedia deepfake detection platform identifying manipulated media with high accuracy using ML models
- Integrated multi-modal detection with CNN/RNN, real-time verification and end-to-end encryption for secure data processing
- Implemented anonymized content processing with OpenCV and automated reporting for transparent and evidence-backed insights
- Achieved 93% detection accuracy across image, video, and audio deepfakes with real-time processing

## ACHIEVEMENTS & LEADERSHIP

- Published 12 papers in **Scopus-indexed & Q1 journals**, also securing a patent in 2024
- Received a **research grant** worth $17,000 from Cyberpeace to develop and deploy the project TrustTrace
- Achieved 2nd place ranking in **CSAW Operational Technology Security** Challenge Competition 2025 in US/Canada Region