ATHARVA AUTI

Los Angeles, CA 90007 | (323) 212-7455 | auti@usc.edu | linkedin.com/in/auti | github.com/aatharvauti | auti.dev

EDUCATION

University of Southern California (M.S. in Cybersecurity Engineering) Grade A, 4.0/4.0 *Aug 2024 – Aug 2026*

- **Relevant Coursework:** INF **519** Foundations & Policy for Information Security, CSCI **530** Security Systems, INF **523** Computer Systems Assurance, ITP **475** Advanced Digital Forensics, INF **529** Security and Privacy in Informatics

Mumbai University (Bachelor of Engineering in Cybersecurity, Minors – AI ML) Grade A, 9.51/10 *Aug 2020 - Jun 2024*

- **Relevant Coursework:** Data Structures & Algorithms, Operating Systems, OOP Systems, Computer Architecture, Cryptography, Database Management & Security, Web Application Security, Network Security, Virtualization & Cloud Computing, Cyber Laws

EXPERIENCE

Veermata Jijabai Technological Institute (VJTI) COE CNDS *(Cybersecurity Researcher)*, India *Jun 2023 – Jul 2024*

- Configured **OT & IT systems** from scratch in a research environment using **ESXi** to deploy **SIEM**-capable Security Operations by setting up **ELK** with **IDS – Snort, Suricata, Wazuh,** & **Zee**k for comparative analysis. Implemented security controls on **Cisco L3 switches**, **Fortigate** & **Sophos** firewalls to conduct red-teaming exercises using **MITRE ICS,** working on **Threat Modeling** & **CTI**
- Led Android application security research for **reverse engineering**, utilizing **Binary Ninja, GDB, IDA Pro, and Ghidra** to analyze APK files and **ARM assembly code**, identifying vulnerabilities through **decompiled code & runtime analysis** to secure applications

Cyberpeace Foundation, SAKEC (*Cybersecurity Researcher*), India *Oct 2022 – May 2023*

- Led research initiatives by identifying gaps, devising advanced cybersecurity **strategies**, and presenting **findings** to support the NGO's mission of enhancing **cybersecurity awareness and education** across vulnerable sectors such as **healthcare** & **finance**
- Developed & deployed a **Threat Intelligence Platform** using **open-source** honeypot technologies (Snare, Tanner, Dionaea) to simulate **vulnerabilities**, monitor attacker **behaviors**, & gather actionable **threat data** using security controls in the **educational** sector

National Threat Intelligence Response Team (*Cybersecurity Research Intern*), India *Sep 2021 – Feb 2022*

- Conducted research on **digital forensics incident response**, focusing on the **preservation, recovery,** & **analysis** of digital evidence while **ensuring compliance** with chain of custody requirements in courts for cases, including **cyber fraud, scams,** & **hacking**
- Demonstrated a comprehensive report on digital **evidence collection methodologies, handling,** & **maintenance of records.**

PROJECTS

HoneyTrack – Lead for Engineering Project (auti.dev/honeytrack) – Mumbai University, *2021-2024*

- Devised a Honeypot cum **SIEM** tool operating **Python & BASH** scripts combined using **Docker** to automate deployment. Configured **ELK** for log visualization, handling over **20 million logs** from 60 days of **cloud attack** monitoring & improving analysis capabilities
- **Copyrighted** (2022) & published at **IEEE** SCEECS 2023 & Scopus **Journal** of Emerging Technologies & Innovative Research 2023

MobSecOps – An Android Security Framework (auti.dev/mobsecops)– IIT Delhi, *2024*

- Enhanced the Mobile Security Framework (MobSF) by integrating updated modules for static analysis aligned with **OWASP Mobile Top 10 (2023)** vulnerabilities, ensuring comprehensive assessments of **app components, permissions,** and **native libraries**
- Developed advanced **dynamic** analysis features, incorporating **FRIDA scripts** for runtime monitoring, **SSL Certificate Pinning** detection, **root/jailbreak** detection, and **code tampering analysis** to evaluate Android application behavior in real-time
- Integrated **Llama 3 generative AI** model using **HuggingFace,** getting insights by analyzing APK files dynamically, proactively generating patterns, and adapting to evolving attack vectors for enhanced defense against emerging mobile threats

Asset Management for Operational Technology with SIEM & SOAR (auti.dev/elastic) – VJTI, *2023-2024*

- Designed and developed an asset management tool for **Industrial Control System** environments, enabling identification, classification, and real-time monitoring of critical assets while adhering to **IEC 61850 standard**s for **MMS** & **GOOSE** protocols
- Integrated advanced features and functionalities such as **CVSS**-based vulnerability lookup, **endpoint** service identification, device **health** & **threat** monitoring, and **live & PCAP**-based analysis to improve **SOC capabilities** and decision-making
- Enhanced data processing efficiency and **scalability** by implementing **chunking** and **threading** techniques, ensuring quick handling and analysis of capture files over 100 GB in complex industrial applications with an IT data center environment

SKILLS & CERTIFICATIONS

- **Skills:** Penetration Testing, SCADA & Cyber-Physical (Industrial Control) Systems, Cyber Threat Intelligence, Analytics, Risk & Compliance, Information Assurance, Network Traffic & Log Analysis, Network Design, Cloud Security, SOC Analysis, Consulting
- **Languages & Tools:** Python, Java, C, C++, PowerShell, BASH, Git, VMware ESXi, Proxmox, Windows AD, Terraform, Docker, Kubernetes, Azure, GCP, AWS, MySQL, PostgreSQL, React, NodeJS, ExpressJS, Flask, FastAPI, Elasticsearch, Splunk, EZTools, EnCase, KAPE, Autopsy, Volatility, Metasploit, Nessus, Tanium, SandboxAQ, HashiCorp, Microsoft Word, Excel, PowerPoint
- **Frameworks:** ISO/IEC 27001, SOC 2, HIPAA, PCI DSS, CCPA, GDPR, MITRE, Lockheed Martin CKC, CTF (CIA), CIS, CSA, CCM
- **Certifications:** ISC2 CC, Cisco – Networking Essentials, Cloud Security Alliance, Zscaler Workshops, Palo Alto – Cloud, Network Security, & SOC, IBM Cybersecurity & Blockchain, Basel OSINT, Credits for Cryptography & CISSP by Charles Sturt University

ACHIEVEMENTS & LEADERSHIP

- Secured **17th** (4800+ teams) with the USC CTF Team & **123rd** (8000+ individuals) in **National Cyber League** *Fall 2024* across the U.S.
- **1st position** at IIT Delhi's Cybersecurity Hackathon *2024* (Cython) against 500+ teams – **Android Security Framework with GenAI**
- **Runner-up** at AI LA Cerebral Beach Hackathon *2024* Cybersecurity – **Blockchain Smart Contract Auditing using Multiagent AI**
- Presented a **talk** at the **Elasticsearch Community Event** on **Leveraging Cybersecurity using ELK & developing a SIEM tool**