Loksharan Saravanan

Jersey City, NJ | (551) 359-1885 | loksharan.soc@gmail.com | linkedin.com/in/loksharan | github.com/loksharan-soc

EDUCATION

The City College of New York, City University of New York, The Grove School of Engineering
Master of Science in Cybersecurity *Expected May 2026*
Relevant Coursework: Secure Systems Engineering, Secure Operating System, Adversarial AI and Network Security

Rajalakshmi Engineering College, Chennai, India
Bachelor of Engineer in Computer Science and Engineering *May 2021*
Relative Coursework: Computer Networks, Data Structures and Algorithms, Cryptography and Network Security

TECHNICAL SKILLS

Languages: C, C++, Python, SQL
Tools: Wazuh(SIEM), Velociraptor(EDR), Snort(IDS), Wireshark
Operating Systems & Virtualization: Windows, Ubuntu, Kali Linux, pfSense, VirtualBox
Cybersecurity: Threat Hunting, Log Analysis, Endpoint Detection & Response, Incident Response, Malware Artifact Analysis
Frameworks & Web: Flask
Certifications: CompTIA Security+ (in progress)

PROFESSIONAL EXPERIENCE

Infosys Limited, Power Programmer | Chennai, India *Aug 2021 – Aug 2022*
- Developed and maintained backend systems using Python and SQL, improving data handling and workflow automation.
- Collaborated in cross-functional group projects to deliver full-stack solutions within Agile development cycles.
- Wrote and optimized SQL queries for data extraction, transformation, and analysis in enterprise applications.
- Participated in code reviews, debugging, and testing activities to ensure robust and maintainable code.

PROJECTS

Wazuh Detection Lab
- Built a virtual Security Operations Center (SOC) using Ubuntu server and Windows agent.
- Simulated brute-force and PowerShell attacks; analyzed alerts on the Wazuh dashboard.
- GitHub: Github.com/Loksharan-soc/wazuh-detection-lab

Velociraptor Threat Hunt
- Used Velociraptor EDR to detect suspicious file drops and privilege escalation in a Windows VM.
- Analyzed malware artifacts to identify potential threats.
- GitHub: Github.com/Loksharan-soc/velociraptor-edr-lab

Login Honeypot (Flask App)
- Developed a fake login portal to capture attacker credentials and IP addresses.
- Mapped attacker activity to MITRE ATT&CK technique T1110 (Brute Force).
- GitHub: Github.com/Loksharan-soc/login-honeypot

Virtual Cybersecurity Career Challenge (2025)
- Engaged in a comprehensive, hands-on cybersecurity competition simulating real-world threat scenarios.
- Applied skills in threat detection, incident response, and vulnerability analysis to solve challenges.
- Collaborated with peers to develop strategic defense tactics against cyber attacks.
- Currently awaiting official certification of participation.

PUBLICATIONS

- Gnanavel, S., Sreekrishna, M., DuraiMurugan, N., Jaeyalakshmi, M., & **Loksharan, S.** (2022). **The Smart IoT-Based Automated Irrigation System Using Arduino Uno and Soil Moisture Sensor**. In 2022 **4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 188–191). IEEE.** https://doi.org/10.1109/ICSSIT53264.2022.9716368.
- Co-authored a research paper on IoT-enabled automated irrigation systems, focusing on integrating Arduino sensors for efficient soil moisture management.