SREESHNAV K

6363690473 Bangalore www.linkedin.com/in/sreeshnav-k-7794a0325 sreeshnav.k.kurup@gmail.com

ABOUT ME

Final-year B.Tech student specializing in Cybersecurity at Dayananda Sagar University. Possesses practical experience from internships at Cothon Solutions and Shamgar Solutions, focusing on threat analysis, system security implementation, and data operations. Skilled in vulnerability assessment, network security, and incident response. Eager to leverage academic knowledge and hands-on skills to secure a challenging role in an organization dedicated to mitigating evolving cyber risks.

EDUCATION

DAYANAND SAGAR UNIVERSITY, BENGALURU, INDIA | 2026 - PRESENT
B.Tech, Computer Science & Engineering (Cybersecurity)

KENDRIYA VIDYALAYA MEG AND CENTRE, BENGALURU, INDIA | 2022
Higher Secondary Education (CBSE)

SKILL

- Cybersecurity
- Large Language Models
- HTML
- Linux
- C++
- Threat Analysis
- SQL
- Networks and Network Security
- Digital Forensics
- Data Science
- Ethical Hacking

INTERNSHIP

Cothon Solutions | Bengaluru, India
Cybersecurity Intern | 01/2025 - 02/2025

- Developed and automated security scans by contributing to a Web Vulnerability Scanner using Python and OWASP ZAP, improving the efficiency of vulnerability reporting.
- Conducted threat analysis and vulnerability assessments on real-time systems to identify and document potential security weaknesses and misconfigurations.
- Analyzed network traffic and contributed to the development of a Machine Learning-based Intrusion Detection System (IDS) to detect and flag suspicious network behavior.

Shamgar Software Solutions | Bengaluru, India
Data Science Intern | 02/2025 – 05/2025

- Managed and processed large-scale structured datasets using Python (Pandas, NumPy) and SQL, ensuring data accuracy and integrity for operational reporting.
- Performed data cleaning, validation, and transformation on confidential records, enhancing the reliability of datasets used for analysis across internal platforms.
- Collaborated with the data science team to generate regular reports and visualizations, ensuring strict adherence to project deadlines and data quality standards.

CERTIFICATIONS

- Innovation Driven Entrepreneurship | SWAYAM (NPTEL)
  - Issued May 2025
- Digital Forensics | SWAYAM (NPTEL)
  - Issued Jan 2025
- Foundations of Cybersecurity | Google (Coursera)
  - Issued Dec 2024
- Connect and Protect: Networks and Network Security | Google (Coursera)
  - Issued Dec 2024
- AWS Workshop | NIT Calicut
  - Issued Oct 2024
- Nasscom AI Confluence | Nasscom AI
  - Issued Jul 2024
- Large Language Models (LLMs) | NIT Calicut
  - Issued Mar 2024
- Advanced Python | Udemy
  - Issued Mar 2024
- Certified Ethical Hacker (CEH) | YHills
  - Issued Dec 2022
- Cyber Security | E-Cell, IIT Hyderabad
  - Issued Dec 2022

PROJECTS

Web Vulnerability Scanner

- Technologies Used: Python, Flask, OWASP ZAP, ReportLab, Task Scheduler
- Engineered an automated scanning system to perform scheduled security assessments of web applications.
- Developed a Flask-based backend and dashboard interface to monitor vulnerabilities and generate downloadable PDF security reports.
- Integrated the system with Task Scheduler to ensure reliable, periodic execution of security scans and reporting.

Anomaly Detection System for Network Security

- Technologies Used: Python, Machine Learning (Scikit-learn, TensorFlow), Pandas
- Developed a machine learning model to detect and classify network anomalies in real-time, including DDoS attacks, intrusions, and potential data breaches.
- Implemented feature extraction and classification algorithms to achieve high accuracy in threat identification.
- Designed the system to provide immediate alerts for suspicious activities, enhancing network security posture.

Network Traffic Analysis & Intrusion Detection System (IDS)

- Technologies Used: Machine Learning, Python, Wireshark, Scikit-learn
- Built an IDS to analyze and classify network traffic (protocol type, packet size, source IP) as normal or suspicious.
- Trained and deployed machine learning models to effectively identify a range of threats, including malware, DDoS patterns, and unauthorized access attempts.

Phishing Simulation & Awareness Tool

- Technologies Used: Python, SMTP, HTML/CSS
- Created an educational platform to conduct controlled phishing simulations by dispatching realistic, simulated phishing emails to users.
- Developed a monitoring component to track recipient interactions (e.g., link clicks, data entry) to gauge security awareness.
- Designed the tool to provide actionable insights for organizations to strengthen their security training programs.