Vatsal Sapovadiya

Rajkot, Gujarat
vatsalsapovadiya22@gmail.com — Linkedin — GitHub

Professional Summary

Cybersecurity fresher with strong hands-on exposure to SOC fundamentals, SIEM monitoring, and network traffic analysis through labs, projects, and internships. Experienced in analyzing logs, detecting brute-force activity, and understanding attacker behavior using Splunk, Wazuh, and Linux. Actively seeking an entry-level SOC Analyst or Cybersecurity Intern role.

Technical Skills

- **SIEM & SOC:** Splunk, Wazuh, Alert Triage, Log Correlation, Incident Analysis, MITRE ATT&CK
- **Network Security:** Wireshark, TCP/IP Analysis, Network Traffic Monitoring
- **Operating Systems:** Linux, Windows
- **Cybersecurity Domains:** SOC Operations, Defensive Security, Network Security
- **Programming & Automation:** Python, Django
- **Hands-on Platforms:** LetsDefend, Hack The Box, CyberDefenders, CTFs

Experience

Cybersecurity Intern — CodeAlpha May 2025 – Jun 2025

- Analyzed network traffic using Wireshark to identify suspicious patterns and protocol-level anomalies.
- Inspected packets and logs to detect potential brute-force attempts and abnormal connections.
- Documented findings and attack observations following SOC-style reporting practices.

Intern — CreArt Solutions Sep 2022 – Oct 2022

- Developed a Django-based web application using Python with secure authentication mechanisms.
- Implemented input validation and CSRF protection to reduce common web security risks.

Projects

Honeypot-Based Cyber Deception System

- Deployed a Cowrie SSH honeypot to capture real-world brute-force attacks and attacker command execution.
- Analyzed credential harvesting attempts, attack timelines, and adversary behavior in an isolated lab environment.
- Built a lightweight dashboard to visualize attacker activity and log-based insights.

SIEM Implementation using Wazuh

- Deployed and configured a Wazuh SIEM lab to detect brute-force attempts, malware activity, and file integrity changes.
- Performed alert triage and basic SOC-style investigations across Linux and Windows endpoints.

Synthetic Handwriting Security Analysis

- Built a GAN-based synthetic handwriting generator to explore document forgery risks.
- Assessed security implications including signature spoofing and misuse of biometric-like traits.

Education

Bachelor of Technology in Computer Science & Engineering 2024 – Present
Charotar University of Science and Technology (CHARUSAT)

Diploma in Information Technology 2021 – 2024
Government Polytechnic Rajkot
CGPA: 8.6

Certifications

- Palo Alto Networks Academy – Security Operations Fundamentals
- EC Council - Into the Trenches: Security Operations Center
- Google – Introduction to Cybersecurity
- Splunk – Introduction to SIEM
- Fundamentals of Red Hat Enterprise Linux 9
- CCNA (Pursuing)

Additional Information

Languages: English, Hindi, Gujarati