Sudarshan Rangappa

sudarshan_rangappa@proton.me +91 8302720020 Portfolio Linkedin

Profile

Motivated and technically skilled cybersecurity enthusiast with hands-on experience in building and managing a virtual cyber defense lab. Proficient in security information and event management (SIEM), endpoint monitoring, network detection, and incident response. Seeking an entry-level cybersecurity analyst role to apply practical knowledge of threat detection, log analysis, and automation using modern tools like Wazuh, Splunk, Suricata, and Shuffle SOAR.

Education

National Forensic Sciences University [NFSU] 08/2023 – 07/2025
Master of science Cyber Security [Msc Cyber Security] Gandhinagar, India

Presidency college 06/2020 – 07/2023
Bachelor of computer applications [BCA] Bengaluru, India

Projects

Integrated Cyber Defence Environment
Designed and deployed a comprehensive cybersecurity operations lab integrating industry tools:

- Configured Wazuh (SIEM/HIDS), Splunk (log analysis), Suricata (NIDS), OpenVAS (vulnerability scanning), Cowrie (honeypot), and Shuffle (SOAR)
- Centralized log collection from Windows Server (Active Directory), Windows 11, and Linux endpoints
- Built automated incident response workflows and tested detection using simulated attacks.

Location-Based IoT Security Key
Developed a location-aware authentication system using ESP8266 (NodeMCU) and GPS module:

- Implemented geofencing to enforce access control based on physical location
- Demonstrated secure IoT communication, hardware-level access restriction, and real-time alerting logic

Tools & Skills

SIEM Administration (Wazuh/Splunk) · SOAR Implementation (Shuffle) · NIDS Configuration (Suricata) · Vulnerability Scanning (OpenVAS/Nessus) · Log Correlation · Incident Handling Procedures · Endpoint Security (Wazuh Agent) · Network Traffic Analysis (Wireshark) · Digital Forensics (Autopsy/FTK Imager) · Honeypot Management (Cowrie) · Active Directory Basics · TCP/IP Networking · Linux System Administration (Debian/Ubuntu) · Windows Server Administration · Virtualization (VMware/VirtualBox) · Python Scripting · Bash Scripting · PowerShell (Basic) · Penetration Testing Tools (Metasploit/Nmap) · Cloud Security Concepts (AWS/Azure/GCP Basics) · Firewall Concepts · OS Hardening · Docker Basics

Certificates

Certified Ethical Hacker [CEHv11] **JAN 2023**
(ECC6238917054)