AKSHAY R

SOC enthusiast passionate about detecting, analyzing, and defending against cyber threats. Building hands-on experience through SOC monitoring, SIEM analysis with Splunk and Wazuh, and practical labs on TryHackMe.

akshay.ramesha.vr@gmail.com | +91 6362724403 | Kerala, India | akshay-r-82253a244 | akshay-portfolio

WORK EXPERIENCE

CyberSapiens

SOC Analyst intern — Oct 2025 - Present

- Monitored and analyzed security alerts in a SOC environment, identifying anomalies and escalating potential incidents.
- Supported incident response through log analysis, root-cause investigation, and threat validation.
- Performed vulnerability assessments and web application testing using Burp Suite, Nmap, Wireshark, Postman, and Kali Linux.
- Applied MITRE ATT&CK framework to track adversary techniques and strengthen monitoring and detection.
- Documented incident and vulnerability reports with remediation recommendations and supported compliance audits (ISO 27001, SOC 2, GDPR).

PROJECTS

Detecting nmap scans using Wazuh and Suricata — Oct 2025 - Oct 2025

- Built an Nmap scan detection lab using Wazuh and Suricata.
- Successfully detected scans using Suricata's threat rules and visualized results on the Wazuh dashboard, gaining hands-on experience in threat detection.

Splunk SSH Log Visualizer — Oct 2025 - Oct 2025

- Designed a Splunk dashboard to visualize SSH authentication activity, including successful and failed logins.
- Detected potential brute-force patterns and mapped attacker origins using geolocation visualization.
- Enhanced incident investigation by correlating login events with IP reputation data.

Detecting successful ssh bruteforce with Wazuh — Oct 2025 - Oct 2025

- Simulated SSH bruteforce attack using Hydra and detected it with Wazuh, identifying multiple authentication failures followed by a successful login.
- Demonstrated Wazuh's threat detection capabilities and highlighted the importance of early detection.

Suricata + Splunk Integration Lab — Nov 2025 - Nov 2025

- Built a lab to detect network scans and suspicious traffic using Suricata IDS and Splunk.
- Correlated Suricata alerts with UFW firewall logs for deeper detection visibility.
- Demonstrated how IDS + firewall + SIEM analysis strengthens detection engineering skills.

ImageCrypt — Oct 2025 - Oct 2025

- A simple Python tool to encrypt and decrypt files, embedding metadata (original filename and extension) directly in the payload.
- It also allows secure key generation with automatic clipboard copy for convenience.

For more hands-on projects, visit my GitHub

EDUCATION

Yenepoya institute Mangalore

Computer Science - 79.8 — Oct 2022 - Aug 2025

• Served as class leader, coordinating sessions and supporting peers with technical issues.
• Took initiative to connect with cybersecurity professionals during sessions, building valuable learning relationships.
• Led and participated in group projects, organizing presentations and task assignments based on teammates' strengths.

SKILLS

- Blue team (Primary): SOC Monitoring, SIEM (Wazuh, Splunk), IDS (Suricata), Firewall (ufw), Threat Intelligence, Incident Detection & Response, Log Analysis, MITRE ATT&CK, Security Alerts & Alarms, WireShark
- Red team (Secondary): BurpSuite, Nmap, Metasploit, Kali Linux, Hydra
- Programming languages: Python scripting, Bash scripting
- Soft skills: Teamwork, Logical thinking, Communication

CERTIFICATE

ETHICAL HACKER

Cyber Security Advanced Certificate by IBM

- Participated in IBM-tied specialisation program during my degree, attending weekly sessions and completing 2 projects.
- Gained hands-on experience and industry insights through this collaborative learning initiative.

Foundation of Cybersecurity by Google

- Completed Google's 'Foundations of Cybersecurity' course on Coursera, gaining foundational knowledge of cybersecurity principles, threat detection, risk management, and security best practices.

Networking Security by ISC2

Completed a comprehensive Ethical Hacking certification covering core offensive security concepts, penetration testing methodologies, and cyber threat analysis. Assessed and certified by CyberSapiens United LLP (UAF Accredited, ISO 27001).