RAHUL K

SOC Analyst

Emerging SOC Analyst with strong foundational skills in threat detection, incident response, and network security. Trained in industry-standard tools like Splunk, Wazuh, and EDR platforms through real-world simulations and internships. Demonstrated ability to analyze security events, identify threats, and apply mitigation strategies in fast-paced environments. Eager to contribute to an organization's cybersecurity posture with a proactive and detail-oriented approach.

- rahulkeezhath@gmail.com
- +916282314460
- Malappuram, Kerala , India.
- https://cybersecurity-portifolio.netlify.app/
- https://www.linkedin.com/in/rahulkeezhath
- https://github.com/rahulkeezhath

PROJECTS

Security Monitoring with Splunk

Utilized the Splunk platform to collect, analyze, and visualize security logs for threat detection and incident response. Created dashboards, set up alerts, and developed queries to monitor and investigate suspicious activities in real time..

Threat Detection and Compliance Management using Wazuh

Leveraged the Wazuh platform to collect, analyze, and visualize security logs for threat detection and incident response. Developed custom rules and dashboards to monitor system integrity, detect vulnerabilities, and ensure compliance with security standards.

Real Time Dashboard with Zeek and Threat Analysis

Deployed Zeek to monitor and analyze network traffic for security threats. Forwarded Zeek logs to Splunk using Splunk Forwarder for centralized log analysis, threat detection, and real-time alerting through custom dashboards and queries.

Intrusion Detection System Deployment using Snort

Installed and configured Snort for network threat detection, developed custom rules, set up logging and alerts, and optimized detection to reduce false positives.

Log Management and Visualization with ELK Stack

Deployed and configured the ELK Stack to collect, parse, and visualize security logs, enabling real-time monitoring, threat detection, and analysis through custom dashboards.

TECHNICAL LABS

Live SOC Monitoring on LetsDefend

Gained hands-on experience inlive SOC operations by detecting, analyzing, and responding to real-world security incidents using SIEM tools and case management on the LetsDefend platform.

TryHackMe - SOC Analyst Simulation

Investigated real-worldsecurityincidentsin a simulated SOC environment, analysing logs, detecting threats, and responding to cyber-attacks using SIEM and EDR tools.

CyberDefenders Blue Team Labs Participation

Engagedin realistic, browser-based labs simulatingreal-world cybersecurity scenarios, enhancing skills in threat detection, incident response, digital forensics, and malware analysis

EXPERIENCE

CyberSecurityIntern | RedTeam Hacker Academy

Perinthalmanna,Kerala | 2025 - Present

- Assisted in monitoring, analyzing,andresponding to security events and incidents in a SOC environment.
- Practiced ethical hacking methodologies using industry tools such as Burp Suite, Nmap, Wireshark, and Metasploit.
- Strengthened knowledge of cybersecurity frameworks, incident response processes, and risk management strategies.

Accounting and Operations | Modern Construction

Malappuram,Kerala | 2023 - 2025

- Managed daily accounting tasks including invoicing, billing, and bookkeeping using [e.g., Tally, Excel]..
- Collaborated with senior management to streamline workflow and improve operational efficiency.

Full Stack Developer Intern | Brototype

Calicut,Kerala | 2022-2023

- Developedandmaintainedweb applications using technologies like HTML, CSS, JavaScript, React.js, Node.js, and MongoDB.
- Participated in code reviews, debugging, and deployment of applications on cloud platforms (e.g., Render, Netlify).

TECHNICAL SKILLS

- ✓ Security Information and Event Management (SIEM) -
- ✓ Splunk, Wazuh
- ✓ Threat Intelligence & Incident Response
- ✓ Log Analysis
- ✓ Vulnerability Assessment & Risk Mitigation
- ✓ Operating Systems: Windows, Linux

Networking & Security Tools: Wireshark, Nmap

EDUCATION

STJOSEPHSCOLLEGE,DEVAGIRI | Calicut, Kerala

Bachelor of Computer Science

2019 – 2022

CERTIFICATIONS

- **Certified IT Infrastructure and Cyber SOC Analyst (CICSA) – Red Team Hacker Academy**
- **Certified SOC Analyst (CSA) – EC-Council**
- **Cybersecurity Analyst Job Simulation - Tata Group**
- **Bug Bounty Hunting - Red Team Hacker Academy**