JIBIN JOSE

SOC ANALYST

Kollam, Kerala 691501 | +91 7025940667 | jibinjosebiju@gmail.com | lLinkedIn | GitHub

Entry-level SOC Level 1 Analyst with hands-on experience in SIEM monitoring, alert triage, log analysis, vulnerability assessment, and incident detection gained through cybersecurity internships. Proficient in Splunk SIEM, Burp Suite, and OpenVAS, with a strong foundation in TCP/IP networking, OWASP Top 10, and Windows/Linux security. CompTIA Security+ and EC-Council Certified SOC Analyst (CSA) certified, seeking SOC Analyst or Blue Team roles.

EDUCATION

Bachelor of Technology in Computer Science and Engineering **Nov 2021 - May 2025**

TKM institute of technology Kollam APJ Abdul Kalam Technological University

- 6.77.
- Relevant Coursework: Cybersecurity, Cloud Computing, Database Management, Artificial Intelligence, Data Structures

Higher Secondary (Computer Science)CBSE **June 2019 - March 2021**

- Percentage: 79%

PROJECTS

SOC Analyst Home Lab – SIEM Monitoring & Incident Response

- Built a SOC Level 1 home lab to simulate real-world security monitoring and incident response
- Configured Splunk SIEM to ingest and analyze Windows and Linux logs
- Created custom alerts and dashboards to detect failed logins, brute-force attempts, and suspicious activity
- Performed alert triage, log correlation, and initial incident analysis
- Mapped detected threats to the MITRE ATT&CK framework
- Documented incidents with impact analysis and remediation recommendations

Web Application Vulnerability Assessment (OWASP Top 10)

- Conducted manual and automated vulnerability assessments on a vulnerable web application
- Identified OWASP Top 10 vulnerabilities including SQL Injection, XSS, and Security Misconfigurations
- Used Burp Suite for interception and exploitation testing and OpenVAS for automated scanning
- Validated findings, assessed risk severity, and recommended mitigation strategies
- Created professional vulnerability assessment reports aligned with security best practices

Phishing Detection & Email Security Analysis

- Analyzed phishing email samples to identify malicious indicators and social engineering techniques
- Performed email header analysis to trace sender IPs, mail servers, and spoofed domains
- Investigated malicious URLs and attachments using threat intelligence tools
- Classified phishing attempts and documented findings in a SOC-style incident report
- Recommended email security controls and user awareness measures

CERTIFICATIONS

- **CompTIA Security+** — **Jan 2026**
- **EC-Council Certified SOC Analyst (CSA)** — **Jan 2026**
- **REDTEAM Internship: Cybersecurity (Vulnerability Testing and Penetration Testing)** — **March 2025**

EXPERIENCE

Cybersecurity Analyst Internship

REDTEAM Hacker Acadamy Pvt Ltd, Trivandrum

- Conducted vulnerability assessments and penetration testing on web applications using BurpSuite and OpenVAS, identifying security risks and recommending mitigation strategies.
- Utilized Splunk for log analysis, assisting in SIEM monitoring and incident detection.
- Collaborated with teams to document findings in line with security best practices.

TECHNICAL SKILLS

- SOC Operations: SOC L1 Monitoring, Alert Triage, Incident Detection & Response, Threat Analysis, MITRE ATT&CK
- SIEM & Logs: Splunk SIEM, Windows & Linux Log Analysis, Security Alerts & Use Cases
- Security Fundamentals: Vulnerability Assessment, OWASP Top 10, Malware Basics, Phishing Analysis, Risk Mitigation
- Tools & Tech: Splunk, Wazuh, Burp Suite, OpenVAS, AWS Cloud Security Fundamentals
- Networking & Systems: TCP/IP, HTTP/HTTPS, DNS, SSL/TLS, Windows & Linux
- Programming: Python Basics, SQL, HTML, CSS, JavaScript, MySQL
- Professional Skills: Incident Reporting, Analytical Thinking, Team Collaboration

ACCOMPLISHMENTS

- Internship at REDTEAM (Cybersecurity Analyst)
- Internship at Corizo (Cybersecurity) & (Cloud Computing)
- Internship Training in Python
- Cyber Security Conference at REDTEAM Security Summit 2023
- Organized a Workshop on Ethical Hacking at TKMIT as Part of CSI

ADDITIONAL INFORMATION

- Languages: English (Fluent), Hindi, Malayalam (Native)
- Interests: Security Operations & Monitoring, Incident Response, Threat Analysis, Open-Source Contributions, Purple Team Collaboration, Continuous Security Improvement
- Available for relocation and flexible work arrangements