NAVINJITH K

EC-Council Certified SOC Analyst (CSA) | Cybersecurity

Kozhikode, Kerala, India • Email: navinjith5@gmail.com • Phone: +91 8289975405 • LinkedIn: linkedin.com/in/navinjith-k-871107254 • GitHub: github.com/navinjith5-oss

PROFESSIONAL SUMMARY

EC-Council Certified SOC Analyst (CSA) and Cyber Forensics graduate currently pursuing Master of Computer Applications (MCA). Demonstrated internship experience supporting real-time Security Operations Center (SOC) threat monitoring, SIEM log analysis, vulnerability assessments, and Tier 1 incident triage. Creator of SecureLoop AI, an open-source security assessment prototype integrating Nuclei scanning and JSONL normalization. Strong foundation in digital forensics, MITRE ATT&CK; framework mapping, and defensive security workflows.

CERTIFICATIONS & CREDENTIALS

- **EC-Council Certified SOC Analyst (CSA)** – EC-Council
- **Certified IT Infrastructure and Cyber SOC Analyst (CICSA)** – RedTeam Hacker Academy
- **IBM Advanced Cybersecurity Certificate** – IBM
- **The Joy of Computing Using Python (Elite + Silver, 75%)** – NPTEL (IIT Ropar)

TECHNICAL SKILLS

Security Operations: SOC Monitoring (Tier 1), Threat Detection & Triage, SIEM Log Analysis, Network Security Monitoring, Incident Response Support, Threat Intelligence, Vulnerability Assessment & Management, Security Reporting.

SIEM & Security Tools: Splunk, IBM QRadar, Microsoft Sentinel, Wireshark, Nessus, Kali Linux, Maltego, SpiderFoot, Basic Burp Suite knowledge, Nuclei.

Frameworks & Fundamentals: MITRE ATT&CK; (Familiarity), Malware Analysis Fundamentals, Firewall & IDS/IPS Management Fundamentals, Risk Assessment & Mitigation Fundamentals, Disaster Recovery Planning Fundamentals.

Development & Systems: Python (FastAPI), React, JavaScript, Vite, Docker (Lab/Container Management), JSON/JSONL, HTTPX, Git.

CYBERSECURITY EXPERIENCE

Cybersecurity Intern – RedTeam Hacker Academy | Kerala, India

August 2024 – March 2025

- Assisted with real-time threat monitoring and Tier 1 incident response procedures within training and simulated SOC environments.
- Analyzed authentication logs, network event streams, and endpoint telemetry to assist in identifying anomalies and triaging security events.
- Conducted vulnerability assessments using industry scanners and drafted structured security assessment and incident reports.
- Gained operational hands-on exposure to SIEM tools (Splunk, IBM QRadar, Microsoft Sentinel) and standard SOC triage workflows.

FEATURED CYBERSECURITY PROJECT

SecureLoop AI | Web Security Assessment Prototype – Open Source

Public Code Repository: https://github.com/navinjith5-oss/secureloop-ai1

- Built a Python/FastAPI prototype integrating Nuclei scanning, JSONL finding normalization, and a React results interface.
- Implemented scan authorization confirmation, background execution, status tracking, severity filtering, and Docker lab management.
- Prototyped rule-based CWE attack-chain mapping and Groq-generated explanations and remediation suggestions in a separate workflow with PostgreSQL storage.

EDUCATION

Master of Computer Applications (MCA) – Adi Shankara Institute of Engineering and Technology (In Progress)

Bachelor of Computer Applications (BCA) in Cyber Forensics – Yenepoya University (2021 – 2024)

LANGUAGES

English, Malayalam, Hindi