MANIKANTA S

Contact Details

smanikanta2702@gmail.com

+91 7483405929

linkedin.com/in/Manikanta S

Bengaluru, India

Technical Skills

- SIEM (Splunk)
- Threat Intelligence
- MITRE ATT&CK
- Incident Detection & Response
- Log Analysis
- Security Alerts & Alarms

Tools & Platform

- Splunk
- MITRE ATT&CK
- Kali Linux
- Nmap
- OSINT

Expertise

- SOC Operations: Security event monitoring, SIEM (Splunk), alert and alarm handling, MITRE ATT&CK framework
- Incident Response: Log analysis, root cause analysis, case documentation, escalation, remediation support
- Network Security: Firewalls, IDS/IPS, VPN, SSL/TLS

Language

- English
- Hindi
- Kannada

Professional Summary

SOC-focused cybersecurity analyst with hands-on experience in SIEM monitoring using Splunk, threat detection, and incident response. Skilled in analyzing Windows event logs, identifying brute-force attacks, and mapping threats to MITRE ATT&CK techniques. Proficient in using Nmap and Kali Linux for vulnerability assessment. Seeking an entry-level SOC Analyst role to contribute to real-time security monitoring and threat mitigation.

Education

Bachelor of Engineering in Computer Science & Technology.
Dayananda *Sagar University, Bengaluru* **2021-2025**

Projects

Security Monitoring & Incident Detection using Splunk SIEM

- Monitored Windows event logs using Splunk to detect suspicious activities and potential threats.
- Identified brute-force attacks using EventCode 4625 and analyzed login failure patterns.
- Developed SPL queries to detect threats and automate alert generation.

Threat Detection & MITRE ATT&CK Mapping using Splunk & Kali Linux

- Simulated SSH brute-force attacks using Kali Linux to test detection capabilities.
- Configured Splunk Universal Forwarder to collect and transmit logs for centralized monitoring
- Mapped detected attacks to MITRE ATT&CK technique T1110 for structured threat analysis.

Experience

Cybersapiens United LLP **Sept 2025-Feb 2026**
Cybersecurity Intern – SOC

- Monitored and analyzed security events using Splunk SIEM to identify anomalies and potential threats.
- Detected and investigated brute-force attacks using Windows Event ID 4625, improving threat detection accuracy.
- Conducted vulnerability assessments using Nmap and Kali Linux to identify open ports and system weaknesses.
- Mapped detected threats to MITRE ATT&CK techniques to improve incident classification and response.
- Documented security incidents and prepared detailed reports with findings and remediation steps.

Certifications & Training

Cyber Security & Threat Hunting (SOC Specialization) – Cybersapiens

Certified Ethical Hacker (CEH) – Cybersapiens