PARTHICK M S
Email: parthick123@gmail.com LinkedIn: https://linkedin.com/in/parthick-ms
Phone: +91 7306115839 | Portfolio: https://parthick.online | Kerala, India

CAREER OBJECTIVES

Entry-level SOC Analyst with hands-on experience in security monitoring, threat detection, Vulnerability assessment, and incident response. Skilled in SIEM tools, endpoint security and penetration testing fundamentals, seeking a SOC role where I can actively monitor threats, document incidents, and learn from senior security analyst in a real-time security operations environment.

EDUCATION

B.Tech in Computer Science Engineering

Mangalam College of Engineering, APJ Abdul Kalam Technological University

2021 – 2025

TECHNICAL SKILLS

SOC Operations	Security Monitoring, Threat Detection, Threat Hunting, Incident Response, Alert Triage, Incident Documentation
SIEM & Log Analysis	Splunk, Wazuh, Log Correlation, Event Analysis
Security & Pentesting tools	Kali Linux, Nmap, Burp Suite, Metasploit, Wireshark, Nessus, VirusTotal
Vulnerability Management	Vulnerability Assessments, OWASP Top 10
Endpoint & Identity Security	Microsoft Defender
Network Security	IDS/IPS, Packet Analysis, Firewall
Operating Systems	Windows, Kali Linux
Programming & Scripting	Python
GRC & Compliance	ISO 27001 Basic, Risk Assessments

PROJECTS

SSH Brute-Force Detection using Splunk (Hands-on Lab)

- Simulated real-world SSH brute-force attacks using Kali Linux Hydra to generate authentication attack telemetry.
- Configured Splunk SIEM to ingest and monitor Linux authentication logs (/var/log/auth.log) for security event analysis.
- Developed custom SPL detection logic using regex (rex) with time-based aggregation (5-minute window) and threshold rules to identify repeated failed login attempts.
- Created and validated a scheduled high-severity alert to detect and notify brute-force activity in a SOC-style monitoring environment.

Snort Integration with SIEM (Hands-on Lab)

- Built a Wazuh SIEM lab integrated with Splunk and Snort IDS to monitor Windows and Linux endpoints; analysed security alerts using the MITRE ATT&CK framework.
- Detected phishing attempts using email header analysis and VirusTotal lookups.
- Investigated brute-force attempts in Windows event logs using Splunk queries.
- Created incident reports following the NIST Incident Response framework.

Firewall Configuration and Traffic Monitoring (Hands-on Lab)

- Configured a pfSense firewall including interfaces, NAT rules, and 5+ custom firewall policies.
- Monitored live network traffic to analyze allowed and blocked connections.
- Optimized access control rules to improve network security posture.
- Reduced unnecessary network traffic by approximately 20% through rule tuning.
- Detected brute-force attack patterns and blocked malicious source IPs using pfSense firewall rules.

CERTIFICATIONS

- Certified SOC Analyst (CSA) - EC-Council (MAY-NOV 2025)
- Certified IT Infrastructure and Cyber SOC – Red Team Hacker Academy (MAY-NOV 2025)