BASALINGAPPA DESAI

SOC ANALYST

CONTACT

+91 8867892066

teju124desai@gmail.com

Bengaluru,Karnataka

Linkedin

Cybersecurity Portfolio

SKILLS

- SIEM: Splunk, FortiSIEM
- SOAR: Cortex XSOAR
- Vulnerability Mgmt: Qualys, Nessus
- Threat Intel: Cisco Talos, VirusTotal, MX Toolbox, IBM X-Force
- IR & Analysis: Alert Triage, Log Analysis, Event Correlation, Phishing Analysis
- Ticketing: ServiceNow
- Dashboards: SPL Queries, Correlation Rules
- OS: Windows, Linux
- Scripting: Python
- Soft Skills: Problem Solving, Analytical Thinking

CERTIFICATION

- 🛡️ FortiSIEM 7.2 Analyst
- 🔐 Fortinet Certified Fundamentals in Cybersecurity
- 📊 SOC & SIEM (Splunk) for Beginners – 2025
- 🧪 Qualys Vulnerability Management
- 🎓 Junior Cybersecurity Analyst – Cisco
- ☁️ AWS Security Incident Response Overview
- 🌐 Introduction to the Threat Landscape 3.0
- 🧩 SOC Analyst Strong Foundation Course

EDUCATION

Bachelor of Engineering

BLDEA's Dr. P.G.Halakatti college of Engineering and Technology

Vijayapura

2021-2025

PROFESSIONAL SUMMARY

- Cybersecurity fresher with hands-on exposure to SIEM alert monitoring, event correlation, and basic incident investigation.
- Proficient in Splunk and Cortex XSOAR with practical experience in alert triage and enrichment.
- Skilled in vulnerability assessment using tools like Qualys, Nessus, Cisco Talos, and VirusTotal.
- Strong analytical thinking, problem-solving ability, and a proactive learning mindset.
- Eager to contribute to SOC operations and grow into a reliable SOC Analyst.

JOB RESPONSIBILITIES &EXPERIENCE

Intern - Worldsec Technologies, Bengaluru, India FEB 2025 – SEP 2025

SOC Analyst

- Monitored customer networks 24×7 using Splunk SIEM to detect and analyze security threats.
- Performed proactive monitoring, investigation, and mitigation of various security incidents.
- Analyzed alerts, distinguished true positives from false positives, and escalated incidents as per SLAs.
- Created, updated, and resolved tickets in ServiceNow with proper documentation.
- Investigated phishing emails, malicious domains, and suspicious IPs using threat-intel tools.
- Supported log onboarding from Windows, Linux, and other platforms ensuring accurate data ingestion.
- Installed and configured Splunk apps, add-ons, and Universal Forwarders for optimized log collection.
- Upgraded and troubleshot Splunk Forwarders to maintain continuous monitoring.
- Developed SPL-based dashboards, reports, and correlation searches to enhance threat visibility.
- Collaborated with cross-functional teams to improve SIEM data quality and operational workflows.
- Gained experience with Splunk architecture: Indexer, Search Head, Heavy Forwarder, Deployment Server.
- Provided real-time assistance during high-priority incidents to support incident response.
- Conducted routine checks and resolved minor issues to ensure security tools functioned without interruption.
- As a SOC Analyst fresher, I worked with Cortex XSOAR to review, monitor, and triage alerts as part of the incident response workflow.