MUTYALA SAI JASWANTH

📞 +91 8074447557 ✉ jaswanths.mutyala@gmail.com in jaswanth-mutyala ⚪ jaswanth-mutyala

EDUCATION

VIT-AP University   **Sep 2022 – May 2026**
B.Tech in Computer Science and Business Systems   *Amaravati, Andhra Pradesh*
CGPA: 8.69

TECHNICAL SKILLS

Languages: Python, SQL, Bash, C++, C.
Security & SIEM: Splunk (SPL), Wazuh, IBM QRadar, Wireshark, Nmap, Burp Suite, Sysmon, TCPDump.
Cloud & DevOps: AWS (GuardDuty, Lambda, EventBridge), Terraform (IaC), Docker, Git/GitHub, CI/CD.
Systems & Networking: Linux (Kali, Ubuntu, Parrot OS), Windows Internals, TCP/IP, DNS, VirtualBox/VMware.

RELEVANT COURSEWORK

- Computer Networks
- Operating System
- Cryptography
- Database Management
- Information Security
- Internet Of Things
- Data Structures
- Computer Architecture

PROJECTS

Automated Cloud Threat Remediation System | *AWS, Terraform, Python, DevSecOps*   **GitHub Link**
- Designed an event-driven security architecture on AWS using **GuardDuty** for threat detection and **EventBridge** for real-time alert routing.
- Engineered a serverless remediation function using **Python (Boto3)** and **AWS Lambda** that automatically isolates compromised EC2 instances, reducing incident response time (MTTR) from hours to <**60 seconds**.
- Implemented Infrastructure as Code (IaC) using **Terraform** to provision VPCs, Honeypots, and IAM roles, ensuring reproducible and version-controlled infrastructure.
- Integrated a DevSecOps pipeline using **GitHub Actions** and **Checkov** to automatically scan Terraform code for security misconfigurations before deployment.

APT Threat Hunting & Detection Lab | *Splunk, Sysmon, MITRE ATT&CK*   **GitHub Link**
- Engineered a SIEM environment using **Splunk Enterprise** on Ubuntu and **Sysmon** on Windows to ingest deep endpoint telemetry, simulating a corporate SOC architecture.
- Executed advanced attack simulations (Credential Dumping, Registry Persistence, C2) utilizing the **MITRE ATT&CK Framework** to generate realistic threat data.
- Developed custom **SPL (Search Processing Language)** detection rules to identify malicious PowerShell execution (T1059) and lateral movement, filtering false positives.
- Designed a "Threat Hunter" dashboard to visualize real-time alerts, correlating network traffic with process creation events for rapid incident analysis.

CERTIFICATIONS

ISO/IEC 27001:2022 Lead Auditor – *mastermind assurance, Issued July 2025*
- Developed expertise in evaluating an organization's information security posture against the ISO/IEC 27001 standard.

Google Cybersecurity Professional Certificate – *Coursera, Issued Mar 2025*
- Completed an 8-course program covering threat modeling, digital forensics, network security, and incident response.
- Analyzed data and security events using tools like Splunk, Chronicle SIEM, Linux CLI, and SQL.

LEADERSHIP / EXTRACURRICULAR

Mansi Art Club   **July 2024 – August 2025**
Vice President   *VIT-AP University*
- Co-founded the Mansi Art Club, building a 100+ member community and organizing 4+ major campus-wide creative events, including The Imagination Station (100+ participants) and Boho Workshop (80+ attendees).
- Managed a cross-functional team of 6 departments (Art, Design, Media, Outreach, Tech, Documentation), leading successful execution of initiatives with 95% team participation and tight deadline adherence.
- Directed event planning, logistics, and promotion strategies that boosted event engagement by 60% compared to initial projections.