Vemula Sai Kumar

(551) 235-2122 | LinkedIn | saikumarvemula.us@gmail.com

https://svemula17.github.io/

Profile Summary

Cybersecurity graduate student with hands-on experience in SIEM monitoring, log analysis, and network traffic investigation using Splunk and Wireshark. Skilled in identifying security misconfigurations, analyzing alerts, and understanding attacker behavior in cloud and networked environments.

Education

Yeshiva University, Katz School of Science and Health — New York, NY
Master of Science in Cybersecurity — May 2026
Overall GPA: 3.9

CMR College of Engineering and Technology — Hyderabad, India
Bachelor of Technology. — Sep 2021
Overall GPA: 3.9

Skills

- **Security Operations & Monitoring:** SIEM Fundamentals (Splunk), Security Monitoring, Log Analysis, Alert Investigation, Event Correlation, Incident Detection, Basic Threat Hunting
- **Network Security & Analysis:** Wireshark, Packet Analysis, TCP/IP, DNS, VPNs, Firewalls, Network Traffic Inspection, IDS/IPS Concepts
- **Vulnerability & Risk Awareness:** Vulnerability Assessment, Security Misconfigurations, Risk Analysis, Security Controls (Foundational), Incident Awareness
- **Automation & Scripting:** Python (basic automation), Bash, GitHub (fundamentals), DVWA
- **Tools & Documentation:** Microsoft Excel, Word, PowerPoint, SharePoint, Office 365, Adobe Acrobat
- **Soft Skills:** Project Management, Critical Thinking, Analytical Skills, Communication, Attention to Detail, Initiative-Driven, Curiosity, Resilience

Certifications

- **CompTIA Security +**
- **Google Cybersecurity Professional Certificate (Coursera):** Foundations of Cybersecurity, Play It Safe: Manage Security Risks, Connect and Protect: Networks and Network Security, Tools of the Trade: Linux and SQL, Assets, Threats, and Vulnerabilities and Sound the Alarm: Detection and Response, Automate Cybersecurity Tasks with Python, Put It to Work: Prepare for Cybersecurity Jobs
- Certified in Cybersecurity Specialization — $(ISC)^2$ / Coursera
- Java Programming, HTML and CSS, Object-Oriented Programming (OOP) And SQL

Work Experience

Phoenix Business Consulting pvt ltd — Hyderabad, India
SAP ABAP Consultant — Aug 2022 – Sep 2024

- Designed and maintained **relational database objects** (Tables, Views, Search Helps), ensuring efficient data retrieval, integrity, and structured data management.
- Developed **Classical, Interactive, and ALV reports**, enabling accurate data analysis, operational visibility, and informed decision-making.
- Implemented SAP reporting logic with focus on **data accuracy, validation, and performance optimization**, reducing processing inefficiencies.
- Created and customized **SAP Scripts and Smart Forms** to automate generation of business-critical documents while preserving data consistency.
- Collaborated with functional teams to translate business requirements into **secure and reliable ABAP solutions**.
- Improved system usability and performance through **structured program design and debugging**, minimizing runtime issues.
- Worked extensively with **enterprise ERP data models**, strengthening understanding of business processes and data flows.

Projects

AI-Powered Cloud Security Posture & Deception Platform Aug 25-Dec 25

Tools & Technologies: **Python, AWS (Boto3), Azure SDK, GCP SDK, Flask, React, TensorFlow, Scikit-learn, Slack API, Terraform**

- Designed and contributed to an AI-powered cloud security platform to detect misconfigurations, assess risks, and improve cloud security posture.
- Performed cloud risk assessment and threat modeling for AWS services including IAM, S3, EC2, Security Groups, Lambda, and RDS.
- Developed risk matrices and threat scenarios identifying critical issues such as excessive IAM permissions, public S3 buckets, and open security groups.
- Mapped cloud threats to MITRE ATT&CK techniques and CIS Benchmarks to support security analysis and compliance readiness.
- Collaborated with a cross-functional team to integrate honeypots for capturing attacker behavior and detecting lateral movement.
- Supported real-time alerting and remediation workflows, reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Ensured alignment with **HIPAA, PCI DSS, SOC 2, ISO 27001, and GDPR** compliance requirements.

AWS Image Upload & AI Tagging System(Cloud *Security / Serverless Architecture Project*)

Tools & Technologies: AWS S3, Lambda, API Gateway, DynamoDB, Rekognition

- Designed and contributed to an AI-powered cloud security platform to Architected a **secure serverless application** using AWS S3, Lambda, API Gateway, DynamoDB, and Rekognition following **least-privilege and defense-in-depth principles**.
- Implemented **secure direct-to-S3 upload mechanism** with **presigned URLs**, minimizing attack surface and preventing unnecessary compute exposure.
- Designed and enforced **fine-grained IAM policies and role separation** to control access between services and prevent privilege misuse.
- Integrated **AWS Rekognition** for automated content analysis while ensuring **secure handling of user-generated data**.
- Built **event-driven processing pipeline** with S3 triggers and Lambda, reducing persistent infrastructure risks.
- Addressed **CORS and API security configurations** to prevent cross-origin vulnerabilities and unauthorized requests.
- Improved operational security through **CloudWatch logging and monitoring**, enabling visibility into system events and anomalies.
- Optimized DynamoDB data access patterns to reduce inefficient scans and mitigate potential performance-related security risks.
- Migrated from AWS SDK v2 to **modular SDK v3**, reducing dependency footprint and lowering potential vulnerability exposure.
- Applied **cost-efficient and resilient cloud security design**, leveraging managed services to reduce patching and maintenance risks.

Security Operations Home Lab

Tools & Technologies: Kali Linux, Ubuntu, Splunk, Wireshark, Nmap

- Designed and maintained a personal SOC-focused home lab to simulate real-world security monitoring and investigation scenarios.
- Configured Splunk to ingest and analyze system and security logs for detecting suspicious activity.
- Simulated attack techniques including brute force attempts and network port scanning using Kali Linux.
- Performed log analysis and event investigation to identify anomalies and potential indicators of compromise.
- Captured and examined network traffic using Wireshark to study protocol behavior and suspicious patterns.
- Practiced incident analysis workflows, strengthening detection, investigation, and troubleshooting skills.