# KANAN SHAH

(916)886-9829 | kananshah4040@gmail.com | linkedin | GitHub

## SUMMARY

Software Engineer specializing in **Python, Java, and machine learning-based detections** for secure, cloud-native environments. Experienced in **data analytics, monitoring systems, and compliance automation** using Azure and DevOps practices. Passionate about building scalable detection solutions that enhance visibility and ensure operational security at enterprise scale.

## EDUCATION

**California State University, Sacramento** **Jan 2021 - May 2025**

*Bachelor of Science, Computer Science*

- **Coursework:** Database Management Systems, Data Structures and Algorithms, Artificial Intelligence, Data Analytics and Mining, Operating Systems, Machine Learning, Software Engineering, Object Oriented Programming

## TECHNICAL SKILLS

- **Programming Languages:** Java, Python, JavaScript, SQL, Bash
- **Data & ML:** Pandas, NumPy, Scikit-learn, PySpark (familiar), OpenCV
- **Cloud & DevOps:** Azure, Docker, Kubernetes, Git, Maven
- **Frameworks:** Spring Boot, React.js, Next.js, Flask
- **Security & Monitoring:** OAuth2, Secure API Design, Data Privacy Compliance, Log Analysis
- **Practices:** Integration Testing, API Development, Root Cause Analysis, Quantitative Data Evaluation, Agile/Scrum

## EXPERIENCE

**Secure AIs** **Aug 2025 - Present**

*AI Engineer* *Sacramento*

- Designed and deployed **machine learning-based detection pipelines** that identified anomalies in enterprise systems and automated incident triage, increasing detection accuracy and reducing investigation time by **30%**.
- Conducted **data quality assessments and feature engineering** across large-scale network logs, integrating compliance validation and continuous monitoring into an **Azure-based detection infrastructure** supporting production-grade scalability.
- Partnered with software, hardware, and security teams to ensure traceability and compliance with internal validation protocols.

**California Department Of Public Health** **Feb 2024 - Dec 2024**

*Software Engineering Intern* *Sacramento*

- Designed and maintained **backend Flask APIs** and database layers to support dynamic mobile application features. This implementation enhanced system reliability and ensured seamless data flow between the app's frontend and backend components.
- Developed **business logic modules** to translate complex requirements into efficient, reusable backend services. These modules improved overall system performance and reduced code redundancy across the project.
- Conducted **post-release retrospectives** to refine testing processes and improve delivery efficiency. The insights gathered were used to optimize workflow management and strengthen continuous integration practices within the team.

**HeadStarter AI** **Jul 2024 - Sep 2024**

*Software Engineer Fellow* *San Francisco*

- Built **full-stack data analytics applications** using React and Flask that visualized and synchronized enterprise log streams, enhancing observability and accelerating data-driven troubleshooting across multiple projects.
- Designed **automated monitoring tools** and event-driven pipelines that tracked API health, latency, and error rates, improving visibility and debugging efficiency within a continuous deployment environment.

## PROJECTS

**Cloud-Based Anomaly Detection Pipeline**

- Developed an **end-to-end detection framework** using Python, Scikit-learn, and PySpark to analyze network and application logs for security anomalies, integrating statistical models and ML-based classifiers with Azure Event Hub for real-time alerting.
- Implemented data ingestion, transformation, and validation modules that maintained consistent data quality and achieved **92% detection precision** on benchmarked datasets through iterative tuning and evaluation.

**Network Monitoring & Compliance Dashboard**

- Designed and implemented a **centralized log monitoring and compliance visualization dashboard** using Flask, React.js, and PostgreSQL, providing live traffic insights and security policy enforcement metrics.
- Containerized microservices with **Docker** and secured access using **OAuth2 authentication**, ensuring scalable deployment and adherence to enterprise-grade data privacy and access control standards.