Joshua Lerin Zacharia

Flagstaff, AZ | +1 (857) 207 6071 | joshzac@gmail.com | LinkedIn

SKILLS

Skills: CYBERSECURITY SKILLS

- ***Network Security:*** Wireshark, Nmap, TCP/IP analysis, packet inspection
- ***Detection & Monitoring:*** SIEM, Windows Event Logs, Threat Detection, Incident Response
- ***Offensive Security:*** Vulnerability Assessment, Penetration Testing, Enumeration
- ***Endpoint Security:*** Windows internals, registry, services, privilege management
- ***Cloud Security:*** AWS IAM, VPC, GuardDuty, CloudTrail, KMS

PROGRAMMING

• Python (primary), Bash, PowerShell, C/C++

AI FOR SECURITY

• Scikit-learn, XGBoost, SHAP, anomaly detection, behavioral modeling

EDUCATION

Northern Arizona University — **Flagstaff, AZ**
Masters in Information Technology — *Graduation Date: May 2026*

S.K. Somaiya College of Arts, Commerce and Science — **Mumbai, Maharashtra**
Bachelors in Science: Computer Science — *Graduation Date: Dec 2020*

PROJECT EXPERIENCE

Capstone Project

Continuous Behavioral Authentication System — *Jan 2026 - Present*

- Engineered a real-time continuous authentication system that verifies user identity during active sessions using behavioral biometrics (keystroke and mouse dynamics).
- Designed a data acquisition application collecting multi-session behavioral interaction data from 15+ participants.
- Built a 29-feature behavioral signature pipeline extracting typing cadence metrics and mouse kinematic features including velocity, acceleration, and curvature.
- Trained and evaluated Random Forest and SVM authentication models using cross-validation and biometric evaluation metrics (ROC, FAR, FRR, EER).
- Implemented multimodal fusion of keystroke and mouse dynamics to improve authentication robustness and reduce impersonation risk.
- Developed a sliding-window continuous authentication engine performing behavioral verification every 30 seconds.
- Packaged the system into a standalone Windows security application using PyInstaller, enabling offline deployment without cloud infrastructure.
- Designed the platform to detect session hijacking and insider misuse after login, addressing a critical limitation of traditional authentication systems

Personal Project

Autonomous Windows Security Configuration Manageme — *Jan 2026 - Present*

- Designed and implemented a multi-agent security monitoring system for Windows endpoints that continuously audits firewall rules, user privileges, registry policies, antivirus status, services, and OS patch levels using native Windows APIs (pywin32, WMI, winreg).
- Built a real-time security auditing engine that performs automated configuration scans every 5 minutes and monitors Windows Event Logs to detect unsafe system states and policy violations.
- Developed an AI-assisted remediation system using a local LLM (Llama via Ollama) with Retrieval-Augmented Generation (RAG) to generate actionable security guidance based on CIS, NIST, and Microsoft security baselines.
- Implemented a fully offline security assistant that provides natural-language explanations and PowerShell remediation steps for misconfigurations without requiring internet access or external APIs.

- Engineered a Windows service with desktop monitoring dashboard and real-time notifications, enabling security officers to review vulnerabilities and approve remediation actions interactively.
- Built a local knowledge retrieval pipeline using ChromaDB and SentenceTransformers to provide context-aware security recommendations from industry standards and vulnerability databases.
- Designed the system for continuous endpoint security monitoring, automated risk detection, and explainable remediation guidance, reducing manual configuration auditing workload for security teams.

Personal Project

Machine Learning–Driven Intrusion Detection *Nov 2025 - Present*

- Developed a machine learning–based Intrusion Detection System (IDS) to identify malicious network traffic using CIC-IDS2017 and UNSW-NB15 datasets.
- Engineered a full detection pipeline including feature extraction, imbalance handling, and attack classification across multiple threat categories.
- Applied SHAP-based explainability to identify critical network features driving attack detection, improving interpretability for security analysts.
- Compared supervised and anomaly-based detection methods to evaluate tradeoffs in real-world intrusion detection scenarios.

FreshStory Foods and Beverages Pvt Ltd.

Secure AWS Cloud Infrastructure with DevOps *May 2025 - Jul 2025*

- Engineered a fully automated CI/CD pipeline using AWS CodeCommit, CodePipeline, CodeBuild, and CodeDeploy with ALB health checks and CloudWatch monitoring, enabling zero-downtime releases, automated rollbacks, versioned artifacts in S3, and cutting deployment time from ~3 hours to under 15 minutes.
- Implemented a hardened AWS security posture using IAM least-privilege policies, KMS encryption, VPC subnet isolation, GuardDuty, Inspector, and CloudTrail logging, resulting in quarterly VAPT compliance and remediation of all identified vulnerabilities.

PUBLICATIONS

Zacharia, J. L., & Akinola, A. T.

Stability and Load Balancing in Software-Defined Networks: Challenges, Measurement, and Security Implications. ***Submitted for review***, 2025.

- Analyzed the interconnected triad of SDN dependability, demonstrating how instability and load imbalance amplify security vulnerabilities (e.g., delayed rule enforcement, DoS attacks), and surveyed mitigation frameworks such as FortNOX , FRESCO , and AVANT-GUARD
- Investigated and synthesized adaptive strategies for improving SDN stability and scalability, including elastic control frameworks (ElastiCon), hierarchical arc

WORK EXPERIENCE

Northern Arizona University **Flagstaff, AZ**

Teaching Assistant *Aug 2025 - Jan 2026*

- Assisted the course instructor with daily instructional tasks, including lesson support, classroom facilitation, and organizing course materials.
- Evaluated and graded assignments, quizzes, and exams with accuracy and fairness, ensuring alignment with established rubrics and academic standards.
- Supported classroom discussions by answering questions, guiding problem solving, and encouraging student participation.

FreshStory Foods and Beverages Pvt Ltd. **Bangalore, Karnataka**

System Analyst and CyberSecurity Officer *Dec 2022 - Dec 2024*

- Analyzed and optimized enterprise information systems to improve performance, security, and operational efficiency.
- Implemented and managed security controls, firewalls, access management policies, and IDS/IPS to strengthen the organization’s cybersecurity posture.

- Monitored and secured network infrastructure, ensuring compliance with industry security standards and internal policies.
- Oversaw secure system integrations, major system upgrades, and new technology deployments across on-prem and cloud environments.

CONFERENCES

Game Developers Conference **San Francisco, CA**

Attendee *Mar 2026 - Mar 2026*

- Attended Game Developers Conference 2026, focusing on AI-driven systems and security challenges in large-scale distributed platforms, including anti-cheat systems, abuse detection, and secure cloud infrastructure.
- Attended Game Developers Conference 2026, engaging with major tech players including NVIDIA, Google Cloud, Microsoft Xbox, and Tencent to study AI-driven game infrastructure and large-scale system design
- Analyzed industry shift toward generative AI in gaming, including tools for NPC behavior, content generation, and real-time adaptation, with strong presence from companies like NVIDIA and Google leading AI integration efforts
- Evaluated emerging intersection of AI + cybersecurity, including adversarial risks (model abuse, cheating, automation exploits) and opportunities for AI-based detection systems, informed by interactions with AI-focused startups and tooling vendors across the expo floor.

Game Developers Conference **San Francisco, CA**

Attendee *Mar 2025 - Mar 2025*

- Gained exposure to anti-tamper and game protection technologies, including insights from Denuvo’s security-focused sessions, deepening understanding of DRM, cheat prevention, and large-scale game integrity strategies.
- Engaged with developers, publishers, and engineering teams to explore advancements in real-time rendering, AI-assisted game workflows, cloud gaming pipelines, and DevOps practices within the interactive entertainment industry.
- Participated in technical sessions, hands-on workshops, and networking with industry professionals across game development, security, and cloud technologies.

CERTIFICATIONS

GOOGLE: Google Cybersecurity Professional Certificate

UDEMY: Machine Learning A-Z: AI, Python & R Certificate