

# AYKHAN PASHAYEV

+1 (857) 867-0482 | aykhan.pashayev001@gmail.com | LinkedIn | GitHub | Portfolio

## TECHNICAL SKILLS

---

**Cloud & Security Engineering:** AWS (CloudTrail, CloudWatch, IAM, GuardDuty, S3, EC2, VPC, Config, KMS, WAF, Security Hub, Secrets Manager, EventBridge, SNS, Lambda, DynamoDB), IAM Hardening & Least Privilege, Threat Detection & Incident Response, Vulnerability Assessment, Penetration Testing, Encryption & Key Management

**Automation & Infrastructure:** Python, Bash, Terraform, CloudFormation, GitHub Actions, Docker, Kubernetes, CodePipeline, Postman, Git, Linux (Kali, Ubuntu), Wireshark

**Frameworks & Compliance:** MITRE ATT&CK, NIST 800-53, ISO/IEC 27001, SOC 2

**Certifications:** CompTIA Security+ (2024), AWS Certified Solutions Architect – Associate (2025)

## PROJECTS

---

### Radius — Cloud Identity Threat Detection System

Mar 2026 — Apr 2026

- Architected an event-driven IAM threat detection platform ingesting org-wide CloudTrail events across 8 Lambda functions — implementing 7 detection rules covering privilege escalation, root activity, and API bursts — and computing per-identity Blast Radius Scores (0–100) to quantify compromise impact; validated with 192-test suite at 89% coverage deploying property-based testing
- Constructed automated incident response pipeline spanning detection, SNS alerting, and identity enforcement — auto-disabling compromised IAM principals and revoking active sessions within seconds; audit trail persisted to KMS-encrypted DynamoDB across 7 tables

### AnomAI — AWS IAM Anomaly Detection Platform

Jan 2026 — Apr 2026

- Led 5-person team to architect and deploy an event-driven IAM anomaly detection pipeline — S3-triggered Lambda ingesting CloudTrail logs in real time, running 6 self-calibrating anomaly detectors operating adaptive statistical baselines to detect abnormal IAM behavior; surfaced 16 IAM incidents across a 120-day dataset with zero manual threshold tuning
- Provisioned full infrastructure-as-code leveraging Terraform across CloudTrail, S3, DynamoDB, Lambda, and EventBridge; exposed findings via Flask REST API and analyst dashboard — enabling security teams to query IAM incidents and triage anomalies without direct AWS Console access

### Incident Response Auto Remediation with AWS Config and Lambda

Jul 2025

- Established self-healing security pipeline using AWS Config rules and Lambda to detect and auto-remediate unauthorized security group changes in real time — enforcing least-privilege port policy (80/443 only) with MTTD under 1 second and MTTR of ~4 seconds; generated CloudWatch forensic audit trails for post-incident review

## EXPERIENCE

---

### Tutor & Research Assistant | Florida International University | FIU STARS | Miami, Florida

Sep 2025 — Apr 2026

- Submitted first-authored research paper accepted to Cyber Recon 2026 — achieved 83.3% expert agreement across 4+ domain reviewers with zero high-risk false positives; trained a rule-constrained Gemini-based AI pipeline to evaluate security requirement completeness against ISO/IEC 15408, mentored by U.S. Air Force Intelligence Squadron Captain
- Provided weekly tutoring to 20 students per week across Python, C, Java, Operating Systems, and Networking — debugging student code hands-on and breaking down complex OS and networking concepts through diagram; consistently retained students semester-long based on repeat attendance and positive grade outcomes

### Hardware Lab Assistant | Florida International University | KFCIS | Miami, Florida

Sep 2024 — Apr 2025

- Maintained high-availability lab infrastructure (Kali Linux, Windows, local servers) supporting 150+ students per semester — owning configuration, updates, and incident troubleshooting end-to-end
- Designed a progressive CTF environment from scratch with three escalating difficulty tiers spanning Linux fundamentals, encryption, and network forensics — running weekly sessions for 4–5 participants in offensive and defensive security techniques

## EDUCATION

---

### B.S. Computer & Information Systems Security | Florida International University | Miami, FL

May 2026

- GPA: 3.82/4.0 | Undergraduate Certificate in Cybersecurity Intelligence & Information Policy

## LEADERSHIP & ACTIVITIES

---

### CCDC Regional Qualifier

Feb 2026

- Led 5-person team to 16th place out of 49 teams — prepared and executed full defensive security strategy in under one week against teams of 8–12 with year-long preparation cycles