QUASHAYA J. GOREE

AI SECURITY PRACTITIONER | AI ENGINEER ASSOCIATE

213-973-8457
qjgoree@gmail.com
Bakersfield, CA, USA
LinkedIn.com/in/quashayajgoree
github.com/Jusharra

PROFESSIONAL OVERVIEW

AI Security Practitioner specializing in secure RAG pipelines, MCP architecture, agentic AI systems, and multi-agent automation across cloud and no-code platforms. Experienced building identity-aware AI workflows, AI DLP gateways, classification-as-code, and defensive guardrails for model access, retrieval, and data movement. I am skilled in Microsoft AI Foundry, Azure AI Search, OpenAI, Pinecone, Supabase, Terraform IaC, and CI/CD for AI deployment. Delivered secure voice AI and workflow automation using VAPI, Make.com, Twilio, and multi-agent orchestration while aligning AI systems to NIST AI RMF, ISO 42001, and OWASP AI Security guidance.

CORE COMPETENCIES

AI Engineering & Automation
Retrieval Augmented Generation (RAG) Architecture • Model Context Protocol (MCP) Architecture • Agentic AI Systems • Multi-Agent Orchestration • Voice AI Automation • No-Code AI Tools • Content Safety • Knowledge Base Development • Vector Retrieval (pgVector) • Generative AI • Content Security • Text Embeddings • LLM Model Training • Human In the Loop • AI Workflows • Language Services • Document Intelligence • Secure Model Hosting • Agent Tuning • PowerShell • Bash • Secure API Integrations • Webhook Automation • Supabase Backends (RLS/JWT) • pgVector Pipelines • Data Sanitization & Transformation Logic • PyTorch • SDLC • AI Lifecycle • AI/ML Bill of Materials

AI Security & LLM Defense
Identity & Privilege Abuse • Prompt Injection Defense • Guardrails • AI Security Architecture • Bias mitigation • Response Filtering • Isolation Boundaries • Secure Embedding Pipelines • Secure Retrieval • Agentic SOC Automation • Secure RAG Pipeline Hardening • AI Risk Taxonomies • Access Control and Authentication Planning • Secure vector database • Secure Data Pipeline

AI Governance & Regulatory Alignment
ISO/IEC 42001 • ISO/IEC 27001 • ISO/IEC 27701 • AI Risk Management • NIST AI RMF • SOC 2 • HIPAA • Data Residency Controls • Data Classification • Evidence Automation • Ethical & Responsible AI • AI Risk Assessments • AI Impact Assessments •AI Threat Modeling • Policy-as-Code (PaC) • Data Loss Prevention (DLP) • Data Labeling • AI Data Engineering • TPRM • Classification-as-Code (CaC) • Continuous Compliance • Control Automation • Risk Register Automation • STRIDE • EU AI Act 2024/1689 • OWASP LLM

Cybersecurity & Cloud Security
Identity Access Management (IAM) • Role-Based Access Control (RBAC) •Attribute-Based-Access-Control (ABAC) • Privilege Access Management (PAM) • Multi-Factor Authentication (MFA) • Single Sign-On (SSO) • Web Proxy • Email Security • SIEM/XDR • Threat Detection • Cloud Security Architecture • Incident Response • Zero Trust • Conditional Access Policies • Security Alert Configuration • Security Group Management • • SQL Server Database • Logging & Monitoring • Azure Policies • Security Control Policies • SAML • OIDC • Infrastructure-as-Code (IaC) • CI/CD Pipelines • Analytical Data Storage and Processing • Data Modeling and Visualization •SAST • DAST • Azure Functions • • CloudFormation • App Registration • Enterprise Application Management • VPC • VPNet • Operational Data • Data Ingestion

EDUCATION

College Coursework
Wilberforce University
Civil Engineering
2004 - 2006

College Coursework
Savannah State University
Mass Communications
2006 - 2007

CERTIFICATIONS

CompTIA
A+, Network +, Security +, CySA+

Microsoft
AZ-500: Azure Security Engineer

AKYLADE
A/AISF AI Security Foundation
A/AISP AI Security Practitioner

ISC2
CISSP – (In Progress – Target Q1 2026)

Mastermind
ISO/IEC 27001:2022 Lead Auditor
ISO/IEC 42001:2023 Lead Auditor

PROFESSIONAL EXPERIENCE

Sr. Cybersecurity Analyst — Liberty Dental Plan of CA| Nov 2022 – Apr 2024 | Long Beach, CA (Remote)

- Led enterprise IAM operations for 1,500+ users across Entra ID, BeyondTrust PAM, Zscaler, Proofpoint, and 60+ SaaS platforms—standardizing identity controls and reducing access-related audit findings to zero.
- Engineered Conditional Access, RBAC models, device trust policies, and BYOD security architecture via Intune + Entra ID, reducing unmanaged-device risk by 60%.
- Built automated access review workflows using Microsoft Identity Governance, cutting quarterly certification time by 85% and ensuring least-privilege accuracy across departments.
- Deployed Microsoft Purview DLP and AIP sensitivity labels enterprise-wide, reducing sensitive-data leakage and lowering DLP incident volume by 33%.
- Authored end-to-end identity SOPs and standardized access workflows, improving onboarding speed by 50% and cutting identity-related support escalations.

Cybersecurity Analyst II — City of Hope | Mar 2020 – Nov 2022 | Irwindale, CA (Remote)

- Managed daily IAM lifecycle for 16,000+ users in a hybrid Azure AD + on-prem AD environment, including MFA, SSO, provisioning, access approvals, and identity troubleshooting.
- Supported large-scale SSO deployments (SAML/OIDC) by managing certificates, entitlement mapping, and troubleshooting, reducing identity escalations by 40%.
- Collaborated with SailPoint IdentityIQ teams to validate automated provisioning rules, ensuring accurate RBAC enforcement and reducing manual access correction.
- Responded to identity and access incidents using Cortex XSOAR/XDR, reducing repeat violations and strengthening incident triage processes.
- Remediated AD–Azure sync issues and attribute conflicts to maintain a clean hybrid identity environment and ensure reliable cloud authentication.

Service Desk Engineer II — OpenX | Jul 2018 – Mar 2020 | Pasadena, CA (Global Remote)

- Served as global IAM lead for Azure AD + GCP, managing provisioning, onboarding/offboarding, RBAC assignments, and entitlement governance for worldwide teams.
- Designed, implemented, and administered Ping Identity SSO for 30+ applications, reducing authentication friction and lowering identity-related tickets by 55%.
- Led cloud identity migration from GCP/on-prem AD to Azure AD, improving sync reliability, identity consistency, and reducing account provisioning time.
- Managed Jamf-based Mac identity provisioning, ensuring role-based deployment of applications and credentials for distributed global teams.
- Automated onboarding, cleanup, and provisioning tasks using PowerShell, reducing manual IAM workload during staffing reductions.
- Contributed to the implementation of a new self-service access platform by defining entitlements, access workflows, and identity governance rules to streamline approvals.

AI Security Engineer | Independent Consultant | Apr 2024 – Present

- Designed and secured **AI-driven applications and agentic workflows** across healthcare and service-based use cases, embedding security controls into **AI pipelines, data flows, and voice AI systems** from design through deployment.
- Built and enforced **AI security guardrails** for generative and agentic AI systems, including **prompt filtering, role-based access controls (RBAC), data minimization, audit logging, and human-in-the-loop safeguards**.

PROFESSIONAL DEVELOPMENT

Per Scholas:
Computer Technician Training
Completed 2016

SANS:
SEC510
Public Cloud Security (AWS, GCP, Azure)
Completed 2020
Continuous Monitoring and Security Operations
Completed 2021

LinkedIn Learning Courses:
-SOC 2 Compliance Essentials Training.
-Advanced SOC 2 Auditing: Proven Strategies for Auditing the Security, Availability and Confidentiality TSCs.
-Leveraging AI for Governance, Risk, and Compliance.
-Understanding and Implementing the NIST AI Risk Management Framework (RMF).
-Governance, Risk, and Compliance (GRC) for the Cloud-Native Revolution.
-Cybersecurity Foundations, Governance, Risk, and Compliance (GRC).
-Cloud Security for DevSecOps Engineers: From Security Models to API Protection.
-Threat Modeling for AI/ML Systems
-Advanced AI Governance: Operationalizing AI Controls and Continuous Monitoring.
-ISO/IEC 42001:2023: Understanding and Implementing the Artificial Intelligence Management System (AIMS) Standard
-Responsible AI on AWS: Bedrock Guardrails, Amazon Q Security, and SageMaker Clarify.
-Introduction to MLSecOps
-Advanced Threat Modeling and Risk Assessment in DevSecOps

AKYLADE:
A/AISF Foundation Course
A/AISP Practitioner Course

- Conducted **AI system security reviews** covering data ingestion, inference paths, storage, and model interaction surfaces, identifying risks such as **prompt injection, data leakage, model misuse, and unauthorized access**.
- Collaborated with product stakeholders and partners to define **secure AI architectures**, ensuring AI-enabled workflows met **enterprise security, privacy, and governance expectations**.
- Implemented **AI observability and traceability controls**, including structured logging, request/response tracking, and secure data handling to support auditability and incident investigation.
- Supported **AI governance and risk management** initiatives by mapping technical controls to **NIST AI RMF, ISO 27001, ISO 42001**, and emerging AI regulatory requirements.
- Developed security automation using **Python, cloud-native services, and CI/CD pipelines**, enabling repeatable deployment of AI security controls across environments.
- Created documentation and guidance for **secure AI development practices**, helping non-security stakeholders understand guardrails, risks, and compliance expectations.

Vitalé Health Concierge (Client Platform)

- Built a secure AI-powered voice intake system using voice AI (VAPI), Supabase, and cloud APIs, enabling patients and caregivers to interact with AI agents while enforcing authentication, role-based access, and data protection controls.
- Implemented AI guardrails to restrict data collection, control conversation scope, and prevent unauthorized disclosure of sensitive information during voice interactions.
- Designed backend data architecture in Supabase with row-level security (RLS) and audit logging to ensure each partner organization operated within isolated, compliant data boundaries.
- Integrated secure routing and escalation logic to transfer calls or data to approved partners, supporting traceability, accountability, and safe handoff to human operators.

Intriage Flow (AI Patient Intake & Triage Platform)

- Engineered a secure AI-driven intake and triage workflow leveraging LLMs, Supabase, and automation tools, embedding security controls into data ingestion, processing, and storage.
- Applied RBAC, JWT-based authentication, and audit logging to protect sensitive intake data and ensure only authorized roles could access or act on AI-generated outputs.
- Aligned platform design with HIPAA-informed security principles, emphasizing data minimization, access control, and traceable decision-making.
- Implemented AI guardrails to restrict data collection, control conversation scope, and prevent unauthorized disclosure of sensitive information during voice interactions.
- Designed backend data architecture in Supabase with row-level security (RLS) and audit logging to ensure each partner organization operated within isolated, compliant data boundaries.

ComplyGuardian — AI-Driven GRC-as-a-Service Platform

- Designed and built a **multi-agent GRC automation platform** using **Azure AI Foundry, Azure OpenAI, MCP (Model Context Protocol), and Pinecone**, enabling automated risk evaluation, evidence collection, policy generation, vendor review support, and incident advisory workflows.
- Implemented **agent-level Zero Trust controls** using **Azure Managed Identities, Supabase RLS/JWT, and MCP permission boundaries**, ensuring strict data isolation, least-privilege tool execution, and secure agent-to-agent communication.
- Integrated **Microsoft AI Content Safety** to enforce guardrails around policy generation, risk summaries, and governance outputs, reducing the risk of hallucinations, unsafe content, or non-compliant recommendations.
- Built **secure frontend governance dashboards** using **Lovable**, backed by **Supabase** for structured evidence storage, audit logging, and role-based access across GRC stakeholders.
- Automated control mapping and governance workflows aligned with **SOC 2, ISO 27001, ISO 42001, NIST AI RMF**, reducing manual governance and reporting effort by **~85%** in simulated enterprise environments.
- Architected the platform to support **third-party software review workflows**, enabling technical security signal aggregation, evidence traceability, and governance decision support prior to production approval.

TOOLS & TECHNOLOGIES

OPENAI CHATGPT
ANTHROPIC CLAUDE
PERPLEXITY
AWS BEDROCK
PINECONE
LYZR
CREWAI
VAPI
BOLT.NEW
LOVABLE
SUPABASE
SQL SERVER
MICROSOFT AI FOUNDRY
AZURE AI STUDIO
AZURE COPILOT
TERRAFORM
AZURE DEVOPS
GITHUB ACTIONS
GITLAB
AZURE ENTRA ID
AWS SECURITY HUB
AWS CONFIG
OPA/REGO
CHECKOV
AWS LAMBDA
AZURE PYTHON SDK
MICROSOFT DLP
MICROSOFT AIP
AWS AUDIT MANAGER
MAKE.COM
WINDSURF
AZURE OPENAI
AZURE AI SEARCH
OCTAVE
FAIR
NMAP
VAPI/Twilio
Azure Databricks
Azure Stream Analytics
Azure Data Factory
Azure Synapse Analytics
Azure Data Lake storage
Streamlit
Microsoft Office 365

Client AI voice systems (Healthcare • Customer Service • Logistics • Order Intake)

- Built a secure AI-powered voice intake system using voice AI (VAPI), Supabase, and cloud APIs, enabling patients and caregivers to interact with AI agents while enforcing authentication, role-based access, and data protection controls.
- Engineered multi-industry voice AI platforms for healthcare, customer service, order intake, and concierge automation using VAPI, Twilio, Make.com, OpenAI, and Supabase backends.
- Implemented identity verification, secure intake workflows, role-based routing, and PHI-safe data handling, reducing human processing time by 70–85% in workflow simulations.
- Integrated multi-agent orchestration, vector-augmented responses, and real-time event automation to deliver scalable, production-grade AI voice systems.

SOC 2 Evidence Collection AI Agent - AWS, Terraform, Lambda, GitHub Actions, Policy-as-Code)

- Built an autonomous evidence collection engine using AWS Security Hub, Audit Manager, Lambda, Terraform, and CI/CD, reducing manual audit prep by 90%.
- Implemented policy-as-code + compliance-as-code pipelines to continuously validate SOC 2 controls and flag drift in real time.
- Eliminated repeat audit failures by generating automated, audit-ready reports and continuous control monitoring.

Compliance-as-Code Terraform Guardrails — AWS Config, OPA/Rego, Checkov, CloudTrail, EventBridge

- Engineered a guardrails engine enforcing NIST 800-53, SOC 2, ISO 27001, and ISO 42001 using Terraform, AWS Config, OPA, and Checkov.
- Deployed automated remediation workflows via Lambda + EventBridge, S3, reducing misconfiguration exposure by 80%+.
- Integrated Claude for LLM-assisted control reasoning, SES notifications, and real-time compliance alerts.

AI Governance Knowledge Base — Pinecone RAG, MCP, S3, AWS Audit Manager + Security Hub

- Built a secure RAG-powered governance hub with Pinecone vector search, MCP-secured tool access, and identity-aware document retrieval.
- Automated governance workflows (policy drafting, control mapping, dataset documentation) with SES + AI-assisted validation.
- Reduced governance cycle times by 70% while aligning architecture to NIST AI RMF and ISO 42001 guidance.

AI Prompt & Response DLP Gateway — Classification-as-Code, OPA/Rego, S3, AI DLP, Data Movement-as-Code

- Designed a Zero-Trust LLM gateway enforcing prompt/response sanitization, PII/PHI detection, and policy-as-code before data reached vector stores.
- Implemented OPA guardrails, data movement rules, and classification-as-code pipelines to prevent sensitive data leakage.
- Achieved >90% reduction in LLM data exposure in simulated enterprise DLP evaluations.

Identity-Aware Healthcare RAG + MCP Identity Governance Control Plane

- Built an identity-aware AI security control plane using Azure Entra ID, Azure OpenAI, Pinecone RAG, and MCP, enforcing RBAC/ABAC across AI retrieval and IAM actions to prevent unauthorized data access in a healthcare context.
- Implemented MCP-based IAM automation to perform MFA, Conditional Access, role validation, user lifecycle actions, and privileged access checks, with all actions logged to Azure Log Analytics and Blob Storage for auditability.
- Applied governance-as-code and CI/CD security gates using Terraform, OPA/Rego, and Azure DevOps, generating automated HIPAA- and ISO-aligned evidence and reducing manual identity and compliance review effort by 70%+.