STRENGTHS

Risk communication
Turned complex threat findings into clear decisions, helping business and engineering leaders align priorities during architecture reviews.

AI security
Worked through prompt injection, RAG, and MCP concerns in real initiatives, becoming a practical resource for delivery teams.

Architecture reviews
Reviewed cloud and on premises designs with care. Teams gained clearer controls, diagrams, and next steps for implementation.

Control engineering
Connected firewalls, encryption, access controls, SIEM, and DLP with delivery needs, making security guidance easier to apply.

Cross team leadership
Coordinated business, engineering, operations, and client stakeholders. That steady collaboration kept difficult security work moving.

SKILLS

AI Security | Cloud Security | GCP | AWS | Azure | Vertex AI | Containers | genAI/ML | Prompt Injection | RAG Security | MCP Authentication | NIST | ISO/IEC 27001 | IDS/IPS | SIEM

LANGUAGES

English — Native

Spanish — Proficient

Odin Rangel

Lead Security Engineer, Security Architecture

(303) 555-6721 odin.rangel@example.com
linkedin.com/example/odinrangel Denver, CO 80206

SUMMARY

Lead security engineer with 9 years of **hands on technology experience** across AI security, **cloud security**, application architecture, and enterprise controls. Designs secure reference architectures for cloud and on premises platforms, conducts **full stack architecture reviews**, and translates threat analysis into practical safeguards. Applies GCP, containerization, network security, cryptography, secure software development, NIST, ISO/IEC 27001, and OWASP guidance across complex environments. Recent work includes genAI and ML security, prompt injection defenses, RAG authorization, MCP authentication patterns, and **local coding agent risk** mitigation. Communicates risk clearly, aligns priorities with business and engineering stakeholders, and provides implementation guidance that supports reliable delivery. Brings a collaborative approach to information protection and cloud security work, with focus on helping enterprise teams reduce exposure while moving important platforms forward.

EXPERIENCE

Lead Security Architect, AI and Cloud Security

Aster Ridge Cloud Security March 2024 - Present Denver, Colorado

Leads AI security, GCP architecture, RAG protection, MCP authentication, and enterprise control design across cloud and on premises platforms. Advises engineering, operations, business, and client stakeholders through architecture reviews, threat analysis, risk decisions, and implementation planning.

- Defined **AI security** requirements for RAG services, reducing ambiguity during architecture approval reviews.
- Mapped **MCP authentication** patterns and **dynamic client registration** risks into practical control guidance.
- Reviewed GCP and on premises designs, documenting threats, gaps, **mitigations**, and implementation decisions.
- Created **reference architectures**, **security models**, diagrams, and guides for cross functional delivery teams.
- Coordinated testing and corrective actions for complex security issues, supporting reliable production outcomes.
- Translated risk findings for business and engineering leaders, helping teams align priorities and delivery plans.

Senior Cloud Security Engineer, GCP Controls

Summit Arc Technologies January 2022 - February 2024 Boulder, Colorado

Led cloud security engineering for GCP environments and containerized platforms, with ownership across SIEM, DLP, IDS and IPS, access controls, and operational documentation. Connected security requirements with platform delivery through structured reviews, testing, and stakeholder coordination.

- Implemented **GCP** security controls for **containerized workloads**, improving consistency across shared platform deployments.
- Connected **SIEM** and **DLP** findings with response workflows, giving operations clearer paths for issue resolution.
- Reviewed IDS and IPS coverage, documenting control gaps and corrective actions for technical stakeholders.
- Produced operational guides that improved repeatability across **cloud security** reviews and deployment activities.
- Analyzed cloud risks with engineering and business teams, supporting practical prioritization of remediation work.
- Tested security changes before release, helping teams resolve defects before production deployment.

MY CAREER

- Lead Security Architect, AI and Cloud Security at Aster Ridge Cloud Security (2.5 Years)
- Senior Cloud Security Engineer, GCP Controls at Summit Arc Technologies (2.1 Years)
- Security Engineer, Application and Network Security at Canyon Forge Software (2.5 Years)
- Software Security Engineer, Secure Development at Frontier Logic Systems (1.7 Years)

Security Engineer, Application and Network Security

Canyon Forge Software June 2019 - December 2021 Fort Collins, Colorado

Delivered application security, cryptography, **network security**, and **secure deployment** initiatives for software platforms. Partnered with developers and operations teams on threat analysis, control design, testing, documentation, and production readiness.

- Applied cryptographic **controls** to application designs, improving protection for sensitive data in transit and storage.
- Performed threat modeling for software releases, turning findings into prioritized engineering actions.
- Reviewed firewall and network security designs, clarifying exposure and control requirements for delivery teams.
- Integrated **secure coding** checks into deployment workflows, strengthening release readiness across application teams.
- Investigated security defects through structured testing, documenting corrective actions for engineering and operations.
- Created implementation guidance that helped developers apply security controls consistently across product releases.

Software Security Engineer, Secure Development

Frontier Logic Systems September 2017 - May 2019 Colorado Springs, Colorado

Supported **secure software development**, threat modeling, and security automation across application engineering teams. Built practical security guidance, participated in architecture discussions, and helped teams address **vulnerabilities** through repeatable review and testing practices.

- Developed threat models for application features, giving engineering teams clearer security decisions during planning.
- Automated recurring security checks, improving review repeatability across software development workflows.
- Applied OWASP guidance during code reviews, helping teams address common application security weaknesses earlier.
- Documented **secure deployment** practices that improved handoffs between development and operations teams.
- Tested remediation changes against identified risks, supporting stronger release confidence and issue closure.
- Explained security findings to developers, turning technical concerns into actionable implementation steps.

PROJECTS

Enterprise GenAI Security Architecture 2025

Created a practical security architecture for genAI services, covering prompt injection, RAG poisoning, RAG authorization, MCP authentication, and local coding agent risk. Documented threat models, control decisions, and implementation guidance for enterprise adoption.

GCP Information Protection Blueprint 2024

Developed a cloud security blueprint connecting GCP architecture, containerized workloads, access control, encryption, network security, SIEM, and DLP. Produced reference diagrams and review guidance for consistent platform decisions.

LEADERSHIP & AWARDS

- Recognized by architecture stakeholders for clear risk communication and practical security guidance across complex platform reviews.
- Commended by delivery teams for resolving difficult security issues through structured analysis, testing, and documented corrective actions.
- Selected for leadership on AI security, RAG protection, and MCP authentication initiatives spanning multiple technical domains.

EDUCATION

Bachelor's Degree in Computer Science

University of Colorado Denver GPA: 4.0 2017 Denver, Colorado

Coursework: *Computer networks, information security, software engineering, operating systems*

CERTIFICATIONS

- Google Professional Cloud Security Engineer 2025
- Certified Information Systems Security Professional 2023

TECHNICAL SKILLS

- **Cloud Security Platforms:** GCP, AWS, Azure
- **GCP Security Controls:** VPC Service Controls, Organization constraints, Cloud Armor
- **AI Security:** genAI, ML security, Vertex AI
- **RAG Security:** RAG authorization, RAG poisoning, retrieval security
- **MCP Security:** MCP authentication, dynamic client registration, client trust
- **Network Security:** firewalls, IDS/IPS, network segmentation
- **Information Protection:** DLP, encryption, access control
- **Security Operations:** SIEM, security monitoring, incident analysis
- **Secure Development:** secure coding, secure deployment, threat modeling
- **Security Standards:** NIST, ISO/IEC 27001, OWASP Top 10 for LLMs
- **Container Security:** containers, containerized workloads, image security
- **Programming:** polyglot programming, application architecture, security automation

PROFESSIONAL AFFILIATIONS

- Information security architecture communities, focused on practical cloud, AI, and enterprise control design.
- Cloud security engineering peer network, sharing implementation guidance across GCP, containers, SIEM, and DLP.

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST