POOJA KIRAN

Security Engineering Leadership | Product Security | AI & Agent Security

Tempe, AZ | +1 480-776-7745 | poojakiranbhardwaj@gmail.com | LinkedIn | GitHub | Portfolio

Professional Summary

Security engineer with an M.S. in Information Technology and experience in **team coordination, technical review, security engineering, and business planning**. As **Business & Compliance Lead** in a Honeywell Aerospace × ASU externship, assigned responsibilities to **three remote peer leads**, reviewed team deliverables, coordinated stakeholder research, and presented cybersecurity and budget proposals to industry evaluators. Also built an **MCP Agent Security Gateway** validated by **782 passing tests** and collaborated with a security startup founder on identity telemetry integration.

Leadership & Security Engineering Experience

Business & Compliance Lead Aug 2025 – Dec 2025

Honeywell Aerospace × Arizona State University | Technology Innovation Lab Externship | Tempe, AZ

- Assigned responsibilities to **three remote peer project leads** during designated AEROSEC lab phases; reviewed technical, customer-research, and prototype work, tracked deliverables, and reported to mentors to keep the **four-member team** aligned on project decisions.
- Interviewed **4 of 12 industry participants** and coordinated findings with research and technical teammates; translated aviation security risks into proposed requirements for **API authorization**, **encryption**, **audit logging**, and **vendor-risk management**.
- Led business and financial planning, **compared 4 commercial security solutions**, and developed a **proposed $120,000 first-year budget** with a **12-month operating plan**; presented market, security-risk, and financial assumptions across **3 pitches to Honeywell evaluators** to support feasibility decisions.

Independent AI Security Researcher & Engineer Aug 2024 – Present

Self-Directed Research | Tempe, AZ

- Built the **MCP Agent Security Gateway** with **Python, FastAPI, and MCP/JSON-RPC** to guard against unauthorized AI-agent actions, prompt injection, and sensitive-data exposure; implemented **69 detection signatures**, **default-deny authorization**, and **9 Elastic Security rules**, supported by **782 passing tests** and **81.93% statement coverage** in a documented CI run.
- Worked directly with an **early-stage security startup founder** to integrate **privacy-preserving identity telemetry** into the MCP gateway; delivered authenticated client paths for **3 identities** and secured **independent verification of event attribution**, helping clarify **customer-onboarding requirements and deployment limitations**.
- Developed **open-source security tools** to identify excessive **AWS IAM permissions**, assess **AI model supply-chain risks**, and investigate security events; implemented **25 IAM analysis rules** and validated **244 identity-security tests** and **296 attack-detection tests**, delivering reproducible findings and documented controls for developers and security teams.

Graduate Teaching Assistant | IT Grader Jan 2025 – Oct 2025

Arizona State University | Ira A. Fulton Schools of Engineering | Tempe, AZ

- Reviewed code, milestones, and final projects for approximately **85 undergraduate students per semester**; provided **rubric-based technical feedback** to help students correct web application defects and meet project requirements.
- Evaluated **52 graduate cybersecurity assignments** covering **risk assessment**, **security compliance**, **infrastructure security**, and **configuration management**; identified gaps in technical reasoning and explained corrections against course criteria.
- Coordinated **grading and student communication** with instructors, addressed technical questions and grading disputes, and escalated exceptions to maintain **consistent assessment and timely feedback** across courses.

Selected Security Engineering Results

MCP Agent Security Gateway | Python, FastAPI, MCP/JSON-RPC, Elastic SIEM Oct 2025 – Oct 2026

- **Built** a default-deny **MCP/JSON-RPC** gateway with capability checks, **anti-SSRF** rules, 69 named prompt-injection signatures, hash-chained audit records, and nine **Elastic Security** detection rules.
- **Verified** agent-to-tool enforcement and failure paths using **Python 3.12 CI**; recorded **782 passing tests** and **81.93% statement coverage** in the cited run.

AWS Agent Identity Guard | Python, AWS IAM, SARIF 2.1.0 Apr 2025 – Oct 2026

- **Developed** 25 **AWS IAM** static-analysis rules for broad grants, **iam:PassRole**, **sts:AssumeRole**, and trust-policy risks; exported findings in **SARIF 2.1.0** for CI review.
- **Validated** the rule suite in cited CI: **244 tests passed** and three credential-dependent tests were skipped; did not claim live AWS effective-permission results.

HF Model Provenance Scanner | Python, SafeTensors, GGUF, ONNX, Keras Nov 2024 – Oct 2026

- **Built** non-executing checks for unsafe serialization, embedded code, **model provenance**, and dependencies across **SafeTensors**, **GGUF**, **ONNX**, and **Keras** inputs.
- **Detected** suspicious content in **33/33 curated adversarial fixtures**; confirmed **260 passing CI tests** and **75.67% statement coverage** without describing fixtures as real-world detection rates.

Attack Detection Engine / Aegis HealthSec | Python, FastAPI, PostgreSQL, ARM/CAN Aug – Oct 2026

- **Extended MITRE ATT&CK v19** detection with offline **CAN**, **C/C++ firmware**, and **ARM ELF32** analysis using synthetic lab inputs and reproducible tests.
- **Integrated** clinical-access detection and a **FHIR R4 AuditEvent** parser with event normalization, deterministic correlation, and **PostgreSQL** incident persistence on unmerged development branches.
- **Tested** an authenticated **FastAPI** investigation workflow with analyst actions and audit history; Milestone E reported **296 local tests passing** with real PostgreSQL, while hosted CI remained blocked.

Technical Skills

Security reviews and risk: Security design review, **threat modeling**, risk analysis, risk assessment, **API authorization**, web-services security, software testing, CI security checks

Cloud, network, operating systems: AWS IAM, DNS, HTTP, TLS, Zeek/Suricata-style telemetry, Linux /proc TCP, **HMAC-SHA256**, **Ed25519**

Delivery and leadership: Python, **C++**, **FastAPI**, **Docker**, **pytest**, **GitHub Actions**, **CodeQL**, SARIF, **Elastic SIEM**, remote peer task assignment, deliverable reviews, stakeholder presentations, compliance research, budgeting

Video content protection (concepts): DRM license flows, encrypted HLS/DASH, CloudFront signed URLs, AWS MediaPackage/SPEKE

Education

Arizona State University May 2026
M.S., Information Technology (Security) | GPA: **3.87/4.00**

M. S. Ramaiah University of Applied Sciences Aug 2023
B.Tech., Computer Science & Engineering

Certifications & Training

AWS Academy Graduate - Cloud Architecting Apr 2025

AWS Academy Graduate - Cloud Security Foundations Nov 2025