Recruiter & Hiring Manager FAQ (Evidence■Only, Public■Safe)
Dr. Stephen Dietrich■Kolokouris, PhD

This document provides direct, technically grounded answers to common recruiter, CISO, and government■contracting interview questions. All answers are framed for public■safe disclosure and align with evidence contained in the associated research and technical corpus.

What ML technologies have you used?

I have worked with applied machine learning primarily in decision■support and anomaly■detection contexts. This includes embedding models for semantic retrieval, entropy■based anomaly detection, simulation■driven risk modeling, and rule■augmented AI systems where deterministic logic constrains probabilistic outputs. My focus is not generic model training, but operationalizing ML within security, infrastructure, and strategic analysis workflows.

What is your RAG stack?

My Retrieval■Augmented Generation stack uses document loaders for controlled corpora, recursive text splitting for dense technical material, vector embeddings for semantic indexing, FAISS for similarity search, and a constrained LLM interface for synthesis. The system is intentionally designed for evidence traceability, auditability, and public■safe outputs.

How do you validate AI outputs?

Validation is handled through multiple layers: deterministic pre■scoring where applicable, retrieval■only grounding to prevent hallucination, citation enforcement at the document level, and post■generation checks that block unsupported claims. If evidence is not present in the corpus, the system explicitly states that limitation.

How do you handle restricted or classified environments?

I design systems with strict separation between public■safe knowledge and restricted operations. In controlled environments, I follow need■to■know principles, air■gapped workflows, policy■driven access controls, and documentation discipline. Public artifacts describe architecture and methodology without disclosing sensitive details.

What is your typical 30/60/90 plan—when asked?

When requested, I frame 30/60/90 plans as optional operational tools rather than defaults. They are tailored to context: first understanding constraints and evidence, then stabilizing systems and controls, and finally scaling or hardening. I avoid generic timelines unless the role explicitly requires them.

Additional Common Scenarios & Answers

How do you explain complex systems to non■technical stakeholders?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you balance speed vs. security?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you ensure auditability in AI systems?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you work with cross■functional teams?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you approach vendor and supply■chain risk?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you design tools for regulated environments?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you prevent AI hallucination in production systems?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you measure impact in security and data projects?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you document complex systems?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.

How do you justify architectural decisions to leadership?

I address this through structured analysis, clear documentation, evidence■based decision■making, and alignment with operational constraints. My approach emphasizes traceability, risk reduction, and long■term maintainability rather than short■term optimization.