AI SECURITY ENGINEERING FIELD GUIDE · 2026

Chapter 06 · Model Supply Chain Security

Standalone learning module for LMS delivery and required reading.

FORMAT	USE	SCOPE	AUDIENCE
Standalone PDF	LMS reading module	Single chapter	Learners

CHAPTER 06

Model Supply Chain Security

INSPECT

Model source, license, hash, loader, dependency, dataset, registry, and promotion path.

PRODUCE

AI bill of materials, provenance record, license review, and registry control notes.

> Models are artifacts. Treat them like code with provenance, integrity, and deployment risk.
>
> FIELD GUIDE

> **FIELD GUIDE: ARTIFACT REVIEW**
>
> Inspect the origin, license, format, dependencies, registry controls, fine-tuning data, and promotion path for every model artifact.

This domain covers model artifacts, open-source models, hosted models, adapters, fine-tunes, datasets, eval sets, loaders, dependencies, registries, signatures, licenses, and artifact promotion. It matters when teams download, fine-tune, convert, host, or deploy models outside a fully managed provider boundary.

Supply-chain review should follow the artifact from source to serving. The model file, loader, container, dataset, adapter, and registry record all matter because compromise or confusion at any step can change production behavior.

> **FIELD USE**
>
> Ask for the model's bill of materials before reviewing performance. If the team cannot name source, license, format, hash, loader, datasets, registry owner, and promotion path, the artifact is not review-ready.

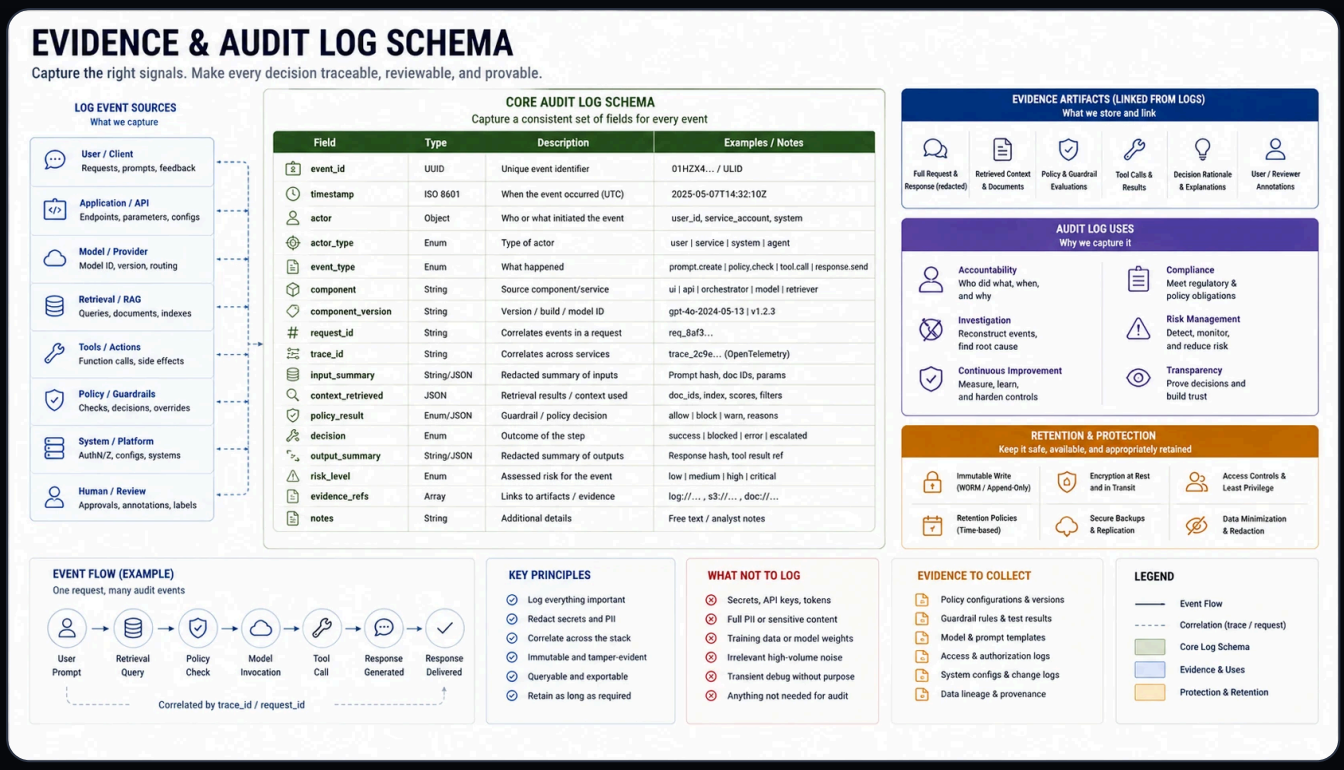

FIGURE 1: FIGURE 7: MODEL SUPPLY-CHAIN BILL OF MATERIALS TRACING ARTIFACT ORIGIN, FORMAT, LOADER, REGISTRY CONTROLS, FINE-TUNING DATA, AND PROMOTION PATH

WHAT BREAKS HERE?

- Unknown model provenance enters production.
- Unsafe serialization formats execute code during load.
- Licenses or use restrictions conflict with product use.
- Fine-tuning data or eval data leaks sensitive content.
- Registry controls allow unreviewed model promotion.
- Adapters, quantized variants, or converted formats lose the review trail.

WHAT TO INSPECT

- Model sources, download paths, hashes, signatures, cards, licenses, and release notes.
- File formats, loaders, conversion tools, dependencies, and container images.
- Dataset sources, fine-tuning records, eval sets, and synthetic data generation.
- Registry permissions, promotion gates, rollback paths, and deployment records.
- Vulnerability monitoring for model-serving dependencies and model packages.
- Adapter, LoRA, quantization, conversion, and merge records.

WHAT TO ASK

- Where did the model come from, and who approved it?
- Can the team prove the artifact has not changed since review?
- What code runs when the model loads?
- What data was used to fine-tune or evaluate the model?
- Which license terms, export limits, or use restrictions apply?
- Who can promote, replace, or roll back a model?
- Which derivative artifacts inherit the original review, and which need new review?

WHAT TO TEST

- Hash and signature verification.
- Unsafe format loading and dependency behavior.
- Registry permission abuse and unapproved promotion.
- Fine-tune data exposure and eval-set contamination.
- Rollback from a bad model version.
- Reproducibility of model lineage records.
- Replacement of a reviewed model with an unreviewed adapter, container, or converted artifact.

CONTROLS AND GUARDRAILS

- Approved-source policy for models, adapters, datasets, and loaders.
- Artifact integrity checks with hashes, signatures, and immutable registry records.
- Safe loading formats and restricted deserialization.
- Model intake review for license, provenance, data, intended use, and known risks.
- Registry RBAC, promotion gates, rollback procedures, and monitoring.
- AI bill of materials for models, prompts, data, evals, tools, and generated-code assets.
- Review triggers for derivative model artifacts and serving-container changes.

EVIDENCE TO COLLECT

- Model bill of materials.
- Provenance and integrity records.
- License review notes.
- Registry access logs.
- Fine-tuning data review.
- Vulnerability and dependency scan results.
- Promotion and rollback evidence.
- Derivative artifact lineage records.

OUTPUT ARTIFACTS

- Model supply-chain review.
- AI bill of materials.
- Model intake checklist.
- Registry control assessment.
- Remediation backlog.

RELATED SERVICES AND WORKBENCH TOOLS

TYPE	RELATED PATHS
Workbench	Artifact Analyzer, Surface Scanner, AI Control Crosswalk
Services	AI Product Security Assessment, Product Security Baseline, Enterprise AI Security Readiness
Handbook	AI Supply Chain, Model and Provider Risk, Evaluation and Regression Testing

ARTIFACT: MODEL SUPPLY-CHAIN EVIDENCE

Produce an AI bill of materials, provenance record, license review, registry access evidence, and promotion-control notes.

Model Supply Chain Security AISECURITY.LLC