MANIFEST

MAY 2025

Generating and Scanning AI SBOMs

The Problem

There is a lot of information on the internet about open weight models and public datasets, but the data is unstructured, inconsistent, and distributed across many different locations. This means security, compliance, or AI governance teams must perform tedious, manual workflows to analyze, scan, inventory, approve, and continuously monitor this AI infrastructure.

> There are no comprehensive AI SBOM generators on the market today that capture robust data on AI infrastructure that enterprise teams can use for compliance and security workflows.

How Manifest Generates AI SBOMs

Open models & datasets

Manifest's AI SBOM generator generates valid SBOMs, consistent with NTIA minimum elements, for open weight models and open source datasets.

1. **Extract basic model information**

   Manifest uses a combination of API queries and advanced extraction methods to gather and structure basic information about a model, including:

   a. **Model metadata*:*** name, version, supplier, license, and more.
   b. **Model architecture**: including architecture, model family, model type.
   c. **Additional data**: model task, tags, Arxiv papers, and more.

2. **Fill in missing data**

   Important data on Hugging Face can be missing or in unexpected locations, which Manifest's AI SBOM generator can still extract. For example, license data may appear in the README file in unstructured text, which means it wouldn't appear in API queries.

3 Extract dataset information

The generator structures information about standalone datasets or those associated with a model, including name, version, author, number of rows, size, data types, columns, and more.

4 Discover deeper risk data

Missing Datasets
Identify training, evaluation, and benchmarking datasets even if not listed on Hugging Face.

Model Committers
Identify users who have contributed to a model or dataset, including their affiliations and social media handles

Supplier Information
Enrich information about the supplier, including their country of operation, to assess risk and facilitate AI restriction policies.

Internally customized models

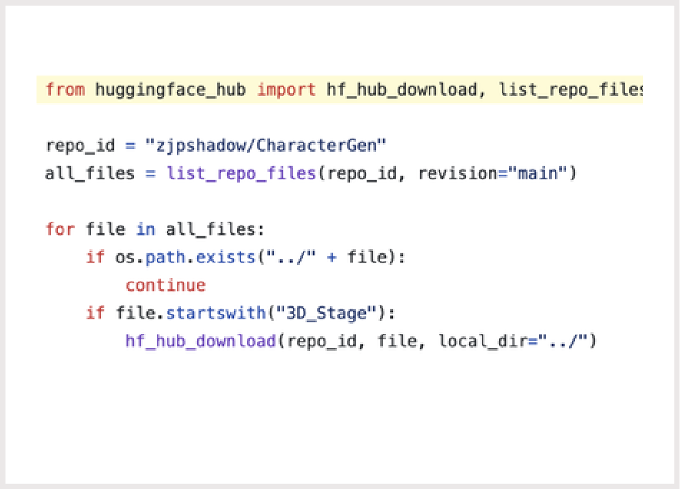
Manifest can also create AI SBOMs for models that your organization develops internally, such as by fine-tuning or training base models.

Manifest provides a lightweight python library that can integrate into any Python notebook, such as Databricks, Jupyter notebooks, Azure AI Studio, MLFlow, and more. The library generates structured AI SBOMs that contain data such as the base model, training datasets, other parameters, and new model metadata.

Detecting models in source code

Manifest's cli tool can detect model usage in source code, and incorporate those models into the SBOM generated for that code. This is critical for

1. **Preventing Shadow AI:** if developers integrate AI infrastructure that's not approved or tracked by security and compliance teams
2. **Associated models with software:** all models must be deployed into software for actual usage, and knowing which models (and their versions) are deployed into what containers or repositories, and then into which end-products is critical.



```python
from huggingface_hub import hf_hub_download, list_repo_files

repo_id = "zjpshadow/CharacterGen"
all_files = list_repo_files(repo_id, revision="main")

for file in all_files:
    if os.path.exists("../" + file):
        continue
    if file.startswith("3D_Stage"):
        hf_hub_download(repo_id, file, local_dir="../")
```

Risk Scanning in AI SBOMs

Manifest's AI platform can scan for multiple types of risks in models and datasets, including:

Known vulnerabilities or security risks

Identify known vulnerabilities in models, such as pickle deserialization vulnerabilities, suspicious files in datasets, or known incidents about a model or data.

Lack of transparency

Flagging open models or datasets with limited information about how they were trained or developed, how to use them, restrictions, or other instructions.

Dataset risk

Security or legal risks in the underlying datasets used to train models can impact the legality and business risk of using the model.

Problematic (AI) licenses

Scan both models and datasets for traditional software licenses, as well as Responsible AI licenses (RAILs) that inform whether a model can be used depending on the use case.

Supplier Risk

Identify whether the supplier of a model is an organization or an individual, where that entity is based, and whether they are a trusted entity.

Model Lineage and Provenance

Understand the lineage of a model, including its parent or base model, to identify the model's provenance.

Other AI SBOM Capabilities

Merge with other SBOMs

If a model is deployed into software, such as a container or a source code repository, Manifest can merge the model's associated AI SBOMs with the SBOM of the target software artifact to create a comprehensive BOM.

Create and maintain an AI Inventory

With Manifest, users can store AI SBOMs to create and maintain a comprehensive inventory of models, datasets, and other AI infrastructure across the enterprise.

Get Ahead on AI Security

Want to shape the of future of AI security? Manifest offers free design partnerships to companies who want to take part in building the next AI SBOM solution.

Email us at aibom@manifestcyber.com