VCRI
THE VALUE CHAIN RISK INSTITUTE

VCRI LEARN · AI SUPPLY CHAIN

# What is an AIBOM?

An AI bill of materials: the ingredient list for an AI system, from the model to the tools it can call.

Joshua Marpet and Cairn Viktor

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY YOU CARE

# An AI agent can change without a code release

An agent is AI software that plans and takes actions with tools, not just answers questions.

### The model

Swap in a new model version, or let a hosted provider update a snapshot, and behavior changes.

### The prompt

Edit one line of the system prompt, the standing instructions, and behavior changes.

### The tools

Connect one more tool server, and the agent can now reach new data and take new actions.

**If nobody wrote down what it was made of, nobody can tell you what changed.**



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

FROM SBOM TO AIBOM

# Same idea, new ingredients

| INGREDIENT | WHY IT BELONGS ON THE LIST |
|---|---|
| **Model** | The trained weights doing the reasoning: which one, which version, from whom |
| **Datasets** | What the model was trained or tuned on, and what it retrieves from |
| **Prompts** | Standing instructions that steer every answer |
| **Tools and MCP servers** | What the agent can reach and do: files, tickets, email, code |
| **Harness and memory** | The framework that runs the loop, and what it remembers between sessions |

MCP: Model Context Protocol, an open-source standard for connecting AI applications to external systems (modelcontextprotocol.io)


valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE STANDARD

# CycloneDX already speaks AI

CycloneDX is the bill of materials standard developed under the OWASP Foundation. Same file format as an SBOM, more component types.

### June 2023

CycloneDX 1.5 added machine learning transparency, which it calls ML-BOM.

### April 2024

CycloneDX 1.6 extended it, including its support for AI and ML model cards.

### In the 1.6 schema

Component types include `machine-learning-model` and `data`, and a component can carry a `modelCard`.

Sources: cyclonedx.org v1.5 and v1.6 release announcements; CycloneDX 1.6 JSON schema



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

A COMMON MIX-UP

# Why a model card is not enough

A model card is a datasheet for the engine. An AIBOM is the parts list for the whole car.

### What a model card is

A short document that comes with a trained model: evaluation results, intended use, and other details.

Proposed by Mitchell and colleagues in 2019.

### What it misses

It describes one ingredient, the model.

Your deployed system also has your prompts, your tools, your memory and your data. None of those are on the model card.

Source: Mitchell et al., Model Cards for Model Reporting, 2019 (arxiv.org/abs/1810.03993)



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

A FREE TOOL

# VCRI's AIBOM Constellation Inventory

- Lists everything an AI agent depends on (model, harness, MCP servers, plugins, tools, prompts, memory, datasets, runtime, credential references) with versions and content hashes.
- Writes the list as a CycloneDX 1.6 AIBOM.
- One Python file, standard library only. No network access, runs no other programs.
- Never writes secret values. Credentials are recorded as a name and a scope.
- Inventory only: it does not score or rate anything. Open source under Apache-2.0.

Source: github.com/value-chain-risk-institute/constellation-inventory (README, constellation.py), v0.1.1, October 2026



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

LOOK AT ONE

# Real output, one hosted model and one prompt

```
{
  "type": "machine-learning-model",
  "name": "hosted-model",
  "version": "2026-09 snapshot",
  "supplier": { "name": "model vendor" },
  "properties": [
    { "name": "vcri:role", "value": "model" },
    { "name": "vcri:evidence", "value": "stated" } ]
},
{
  "type": "data",
  "name": "system prompt",
  "hashes": [{ "alg": "SHA-256", "content": "e032d86c..." }],
  "properties": [
    { "name": "vcri:role", "value": "prompt" },
    { "name": "vcri:evidence", "value": "observed" } ]
}
```

**observed**

The tool hashed the bytes on disk, like this prompt file.

**stated**

Someone typed it in and nothing was checked. A hosted model is always stated: its weights are not on your disk.

**Why it matters**

You can see which entries are evidence and which are claims.



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

HOW YOU USE IT

# Four commands

Run `diff` on a schedule and you have a drift alarm for your agent.

**init**
Write a starter manifest. Edit it to list your agent's parts.

→

**build**
Turn the manifest into a CycloneDX AIBOM. Add `--discover` to read known MCP client config files.

→

**check**
List gaps: missing versions, suppliers or hashes.

→

**diff**
Compare against the last approved AIBOM. Exits with code 1 if anything was added, removed, re-versioned or re-hashed.

Source: Constellation Inventory README



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT TO DO MONDAY

# Write down one agent

- Pick one AI assistant or agent your team runs. Name the person accountable for it.
- List its parts: model and version, prompts, tools and MCP servers, memory, data sources.
- Run `python3 constellation.py init`, fill it in, then `build` and `check`.
- Ask your AI vendors: which model and version does your product use, and will you tell us when it changes?
- Save the AIBOM. Next month, run `diff` and see what moved.

Tool: github.com/value-chain-risk-institute/constellation-inventory (free, Apache-2.0)



valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

# Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn



valuechainrisk.org/learn · CC BY 4.0