

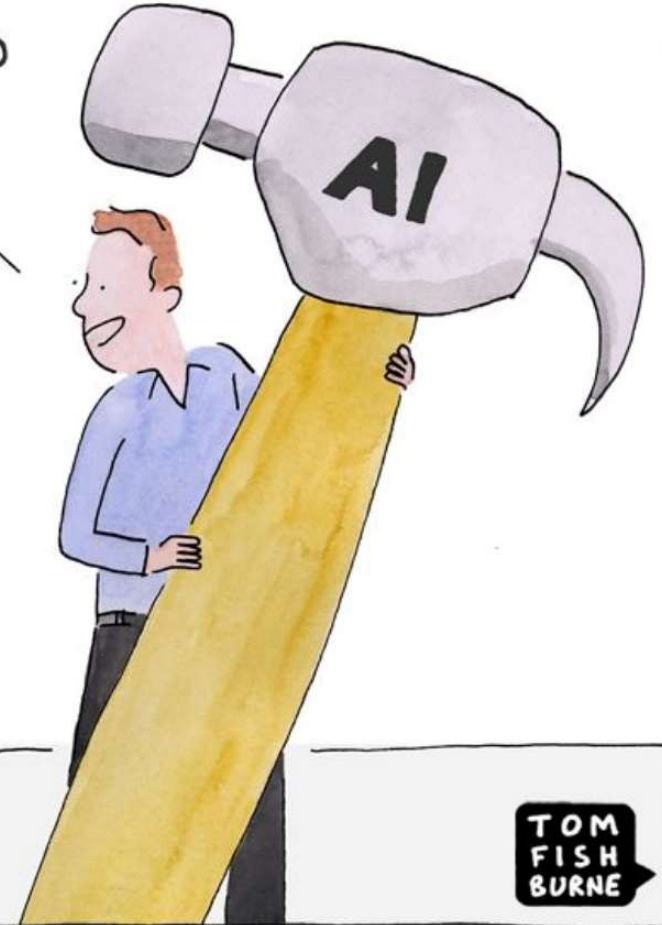
# Securing AI Ecosystems: The Critical Role of AIBOM in Mitigating Software Supply Chain Risks

---

by Helen Oakley, SAP

[in](#) /in/helen-oakley

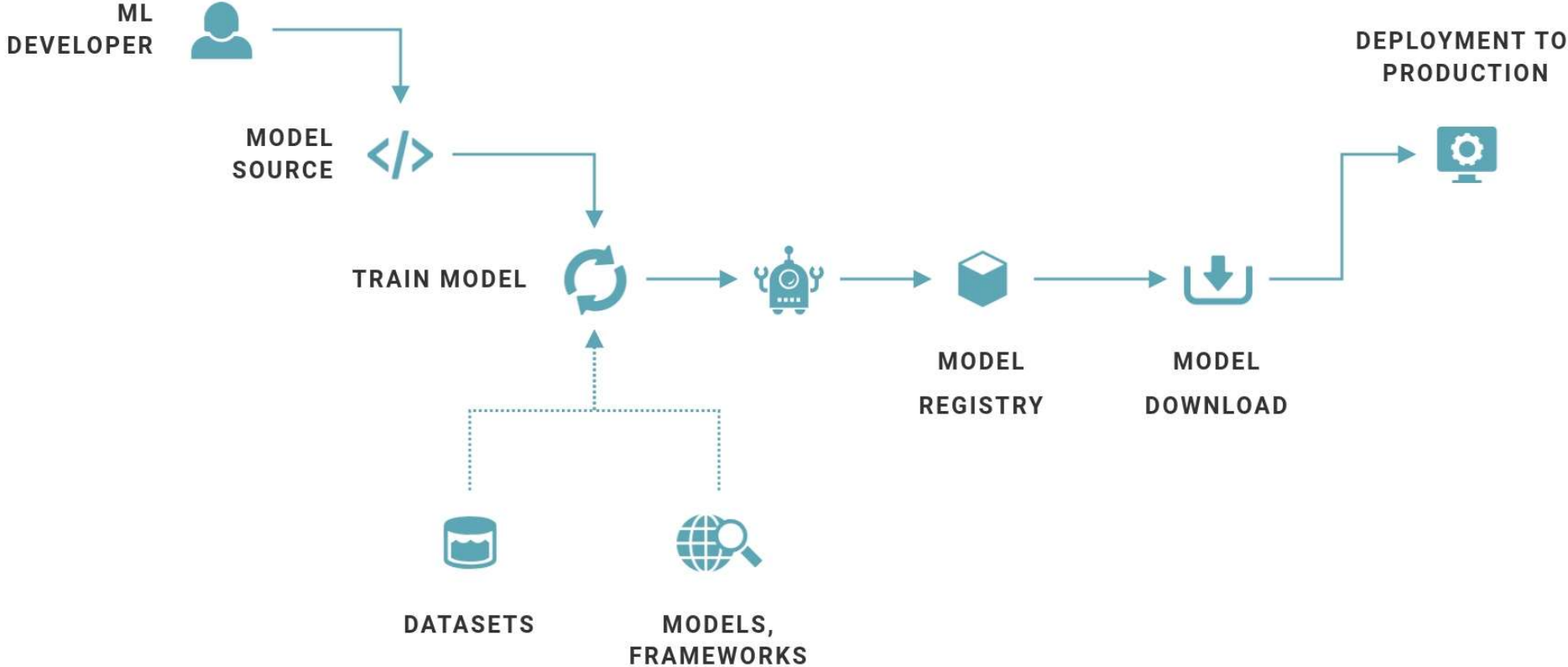
I think we may have a solution to all our problems.



TOM  
FISH  
BURNE

# The ML Software Supply Chain

ML Pipeline



# Malicious Models

Code Execution on Load



PICKLE



DILL



JOBLIB



TORCHSCRIPT



NUMPY



KERAS H5



SAVEDMODEL

<https://jfrog.com/blog/data-scientists-targeted-by-malicious-hugging-face-ml-models-with-silent-backdoor/>



## ● **NASCENT MLOPS**

Comparing CVEs in the past two years:

- MLflow: 15 critical, 23 high
- Jenkins: 2 critical, 9 high

## ● **MALICIOUS MODELS**

RCE as a feature

## ● **MALICIOUS DATASETS**

May contain RCE feature

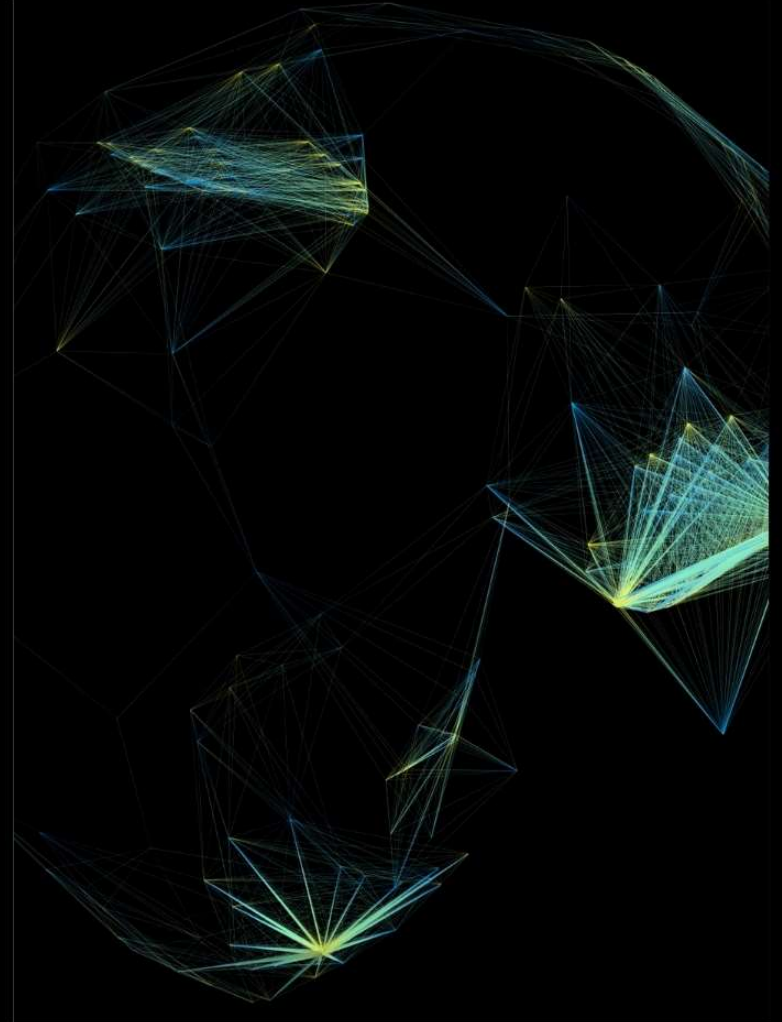
Poisoned datasets

# AIBOM

Artificial Intelligence Bill of Materials

## An Enabler for AI Software Transparency and Security

- ENHANCING AI SOFTWARE TRANSPARENCY
- IMPROVING SECURITY
- FOSTERING TRUST
- FACILITATING INNOVATION





[CISA.gov/SBOM](https://www.cisa.gov/sbom)

# AIBOM Tiger Team

[GitHub.com/aibom-squad/AIBOM-Tiger-Team](https://github.com/aibom-squad/AIBOM-Tiger-Team)

# AIBOM Tiger Team Working Group

## Scope and Objectives

- **Foster Industry-Wide Collaboration and Standards Alignment**

Engage with industry experts to gather insights, foster collaboration, align with frameworks like NIST AI RMF, and drive consensus on AIBOM best practices.

- **Align with Technical Standards (SPDX, CDX)**

Collaborate with CPDX and CycloneDX to communicate AIBOM requirements and ensure the inclusion of relevant fields to support AI-specific scenarios.

- **Define Core Use Cases for AIBOM Interoperability**

Identify and document essential use cases to establish clear requirements and priorities for AIBOM standardization, with a focus on supporting interoperability across different systems.

- **Publish Best Practices**

Establish foundational best practices for creating, managing, and utilizing AIBOM.

# AIBOM Use Cases (Work in Progress)

## 1 | Compliance

Ensure AI models meet regulatory requirements, adhere to internal policies, and address customer compliance needs.

## 2 | Vulnerabilities & Incident Response

Use AIBOM to quickly identify and mitigate risks in response to AI incidents or vulnerabilities.

## 3 | Assessing Risk in Open Source Models & Datasets

Evaluate the reputation, license risks, and maintenance status of open-source models and datasets before use.

## 4 | Third-party AI/ML Risk Management

Manage risks associated with third-party AI interactions and data use, incl. purchasing decisions and continuous monitoring.

## 5 | Secure-by-Design

Incorporating AIBOM into the software development lifecycle to ensure secure and transparent AI/ML systems.

## 6 | Intellectual Property & Fair Usage

Ensure models comply with IP rights and usage restrictions by scanning licenses and assessing dataset relevance.

## 7 | Model Change Management & Lifecycle

Use AIBOM for model traceability, lifecycle management, and efficient rollback or retraining processes.

## 8 | Model Experiment Tracking

Track experimental data and outcomes to inform future AI model development and deployment decisions.

## 9 | Glossary & Terms

1 | **MODEL SOURCE**

e.g. LLM - Rakuten7B-instruct

2 | **MODEL VERSION**

3 | **MODEL PERFORMANCE METRICS**

Used for benchmarking model performance, incorporating metadata like recall, precision, error index, confidence index

4 | **MODEL DEPENDENCIES**

5 | **MODEL LICENSING INFO**

6 | **DATA SOURCE**

e.g. synthetic data, customer data, open-source data

7 | **DATA TYPES / CLASSIFICATION**

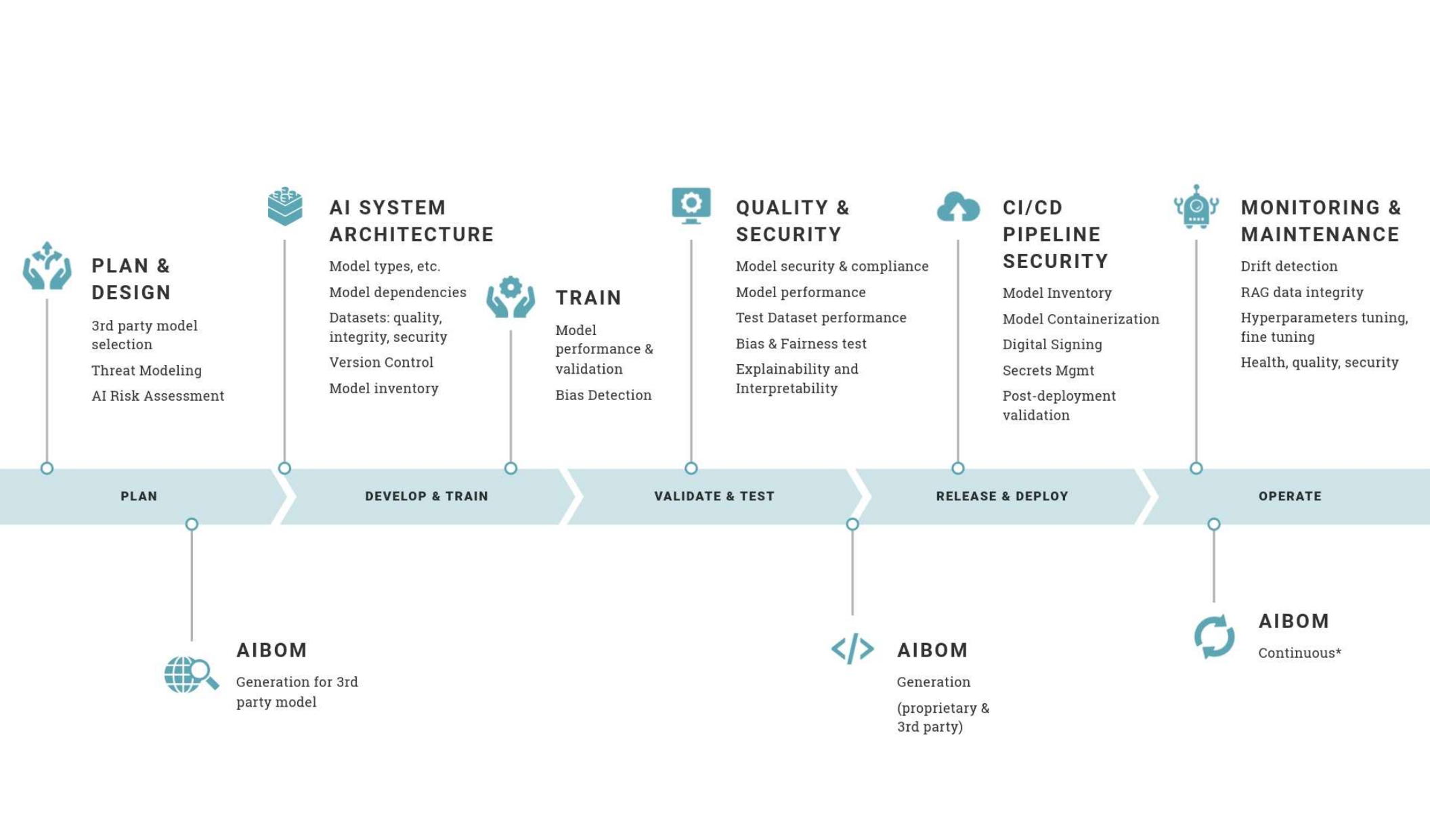
e.g. personal, sensitive



# AIBOM Fields

The Minimum Set

aka AIBOM MVP



# AIBOM INTEGRATION INTO MLSECOPS

THE ENABLER FOR AI SOFTWARE  
TRANSPARENCY AND SECURITY

# AIBOM

ARTIFICIAL INTELLIGENCE BILL OF  
MATERIALS





# Join AIBOM Tiger Team

Bi-weekly on Mondays at 2pm ET

[GitHub.com/aibom-squad/AIBOM-Tiger-Team](https://github.com/aibom-squad/AIBOM-Tiger-Team)