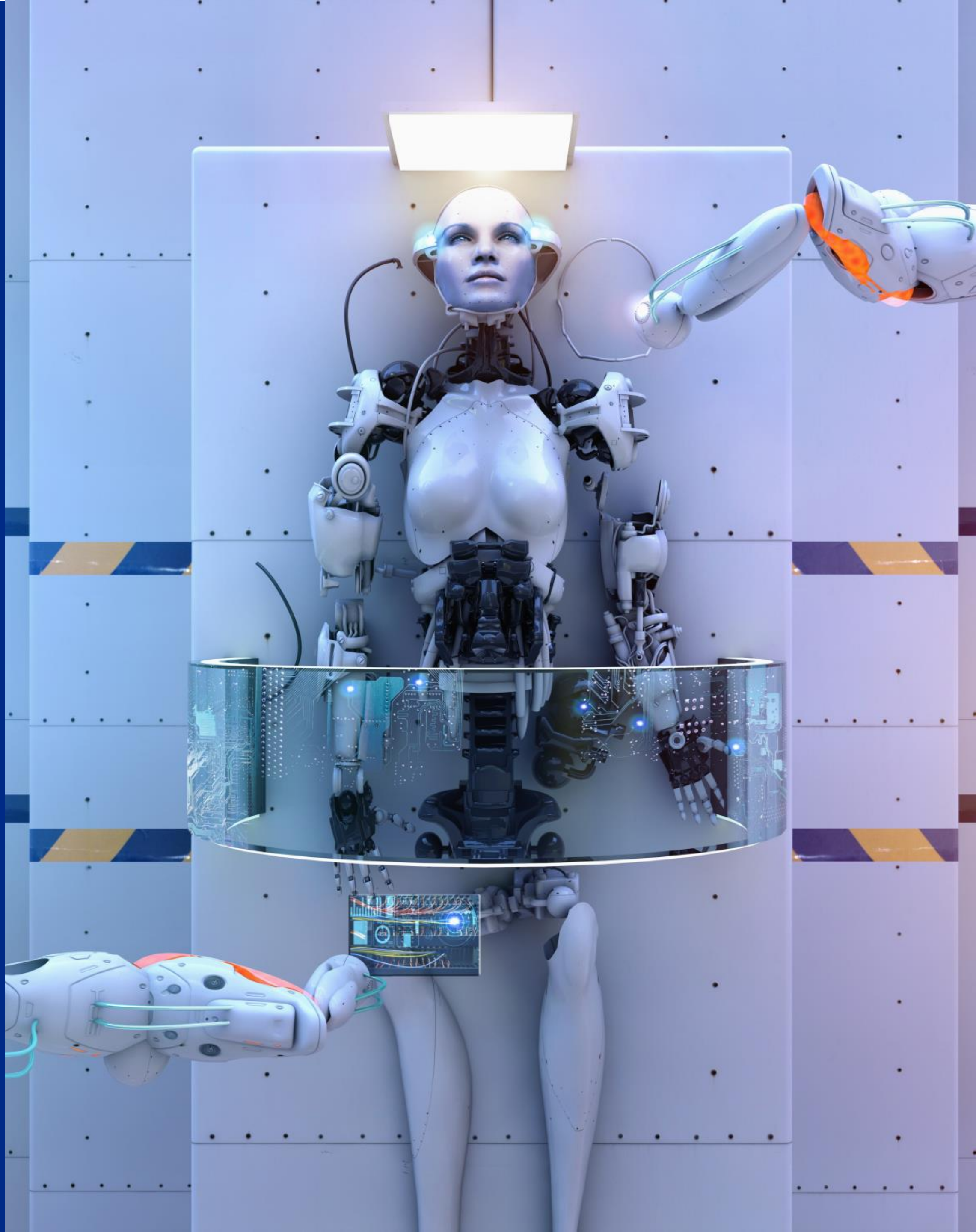
Summary for AI-BOM Workshop at RSAC 2024

Helen Oakley, CISSP, GPCS, GSTRT
Director of Secure Software Supply Chains & Secure Development, SAP
in /in/helen-oakley

May 20th, 2024

PUBLIC



Agenda

- About the AI-BOM workshop at RSA Conference 2024
- What is AI-BOM?
- What's Next?

In a Nutshell

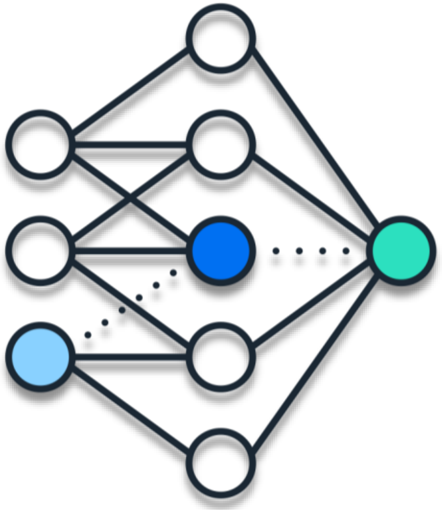
https://github.com/aibom-workshop/rsa-2024

- WHY?
  - To discuss common challenges and opportunities for AI-BOM in supporting AI software transparency and supply chain security, align on direction and next steps
- Gathered experts in AI and cybersecurity across the industry
- Curated lightning talks on on-going efforts for AI-BOM in the community
  - Overview from CycloneDX & SPDX
  - What is an AI-BOM, use cases, AI policy, managing AI vulnerabilities, regulations, and more
- Groups breakouts to discuss list of challenges
- Defined next steps: CISA.gov tiger team registration for AI-BOM

AI Software transparency

MLSECOPS

- DATA OPS
- MODEL OPS
- DEV OPS



AI/ML Bill of Materials

- AI-BOMs: describes the purpose
- AI-BOMs are part of SBOMs

AI Risk Assessment

- AI-BOMs lifecycle & management
- AI-BOMs for Threat Modeling

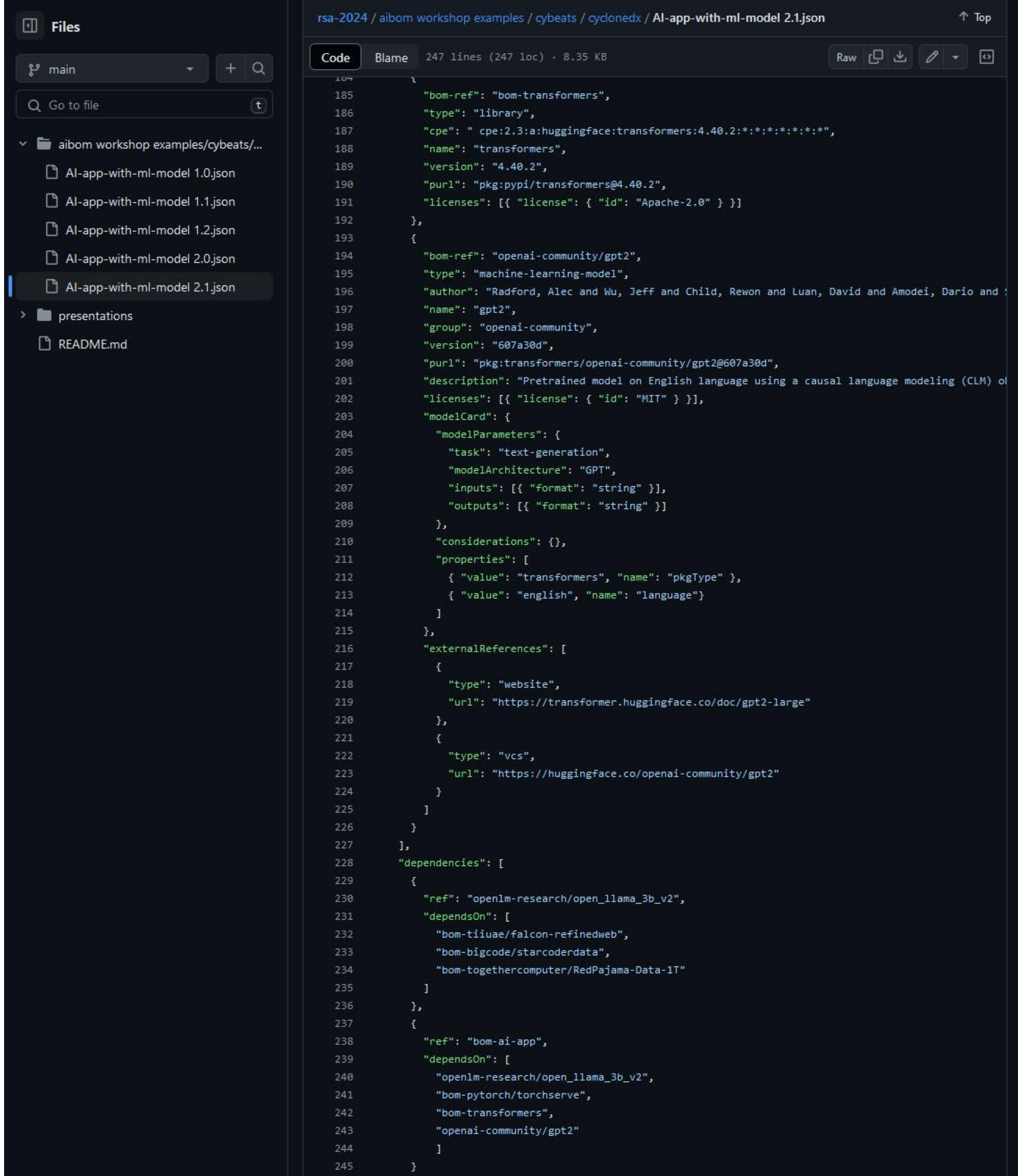
What’s an AI-BOM exactly?

CycloneDX

- AI/ML use case (as of v1.6)
- Model parameters, quantitative analysis, other considerations

SPDX

- AI Profile + Data Profile (as of v3.0)
- Characteristics (type of model, autonomy type, etc.), transparency (info about training, data processing, etc.)


Files
main
Go to file
t
aibom workshop examples/cybeats/...
AI-app-with-ml-model 1.0.json
AI-app-with-ml-model 1.1.json
AI-app-with-ml-model 1.2.json
AI-app-with-ml-model 2.0.json
AI-app-with-ml-model 2.1.json
presentations
README.md
rsa-2024 / aibom workshop examples / cybeats / cyclonedx / AI-app-with-ml-model 2.1.json
Top
Code
Blame
247 lines (247 loc) · 8.35 KB
Raw

```
      {
        "bom-ref": "bom-transformers",
        "type": "library",
        "cpe": " cpe:2.3:a:huggingface:transformers:4.40.2:*:*:*:*:*:*:*",
        "name": "transformers",
        "version": "4.40.2",
        "purl": "pkg:pypi/transformers@4.40.2",
        "licenses": [{ "license": { "id": "Apache-2.0" } }]
      },
      {
        "bom-ref": "openai-community/gpt2",
        "type": "machine-learning-model",
        "author": "Radford, Alec and Wu, Jeff and Child, Rewon and Luan, David and Amodei, Dario and
        "name": "gpt2",
        "group": "openai-community",
        "version": "607a30d",
        "purl": "pkg:transformers/openai-community/gpt2@607a30d",
        "description": "Pretrained model on English language using a causal language modeling (CLM) o
        "licenses": [{ "license": { "id": "MIT" } }],
        "modelCard": {
          "modelParameters": {
            "task": "text-generation",
            "modelArchitecture": "GPT",
            "inputs": [{ "format": "string" }],
            "outputs": [{ "format": "string" }]
          },
          "considerations": {},
          "properties": [
            { "value": "transformers", "name": "pkgType" },
            { "value": "english", "name": "language"}
          ]
        },
        "externalReferences": [
          {
            "type": "website",
            "url": "https://transformer.huggingface.co/doc/gpt2-large"
          },
          {
            "type": "vcs",
            "url": "https://huggingface.co/openai-community/gpt2"
          }
        ]
      }
    ],
    "dependencies": [
      {
        "ref": "openlm-research/open_llama_3b_v2",
        "dependsOn": [
          "bom-tiiuae/falcon-refinedweb",
          "bom-bigcode/starcoderdata",
          "bom-togethercomputer/RedPajama-Data-1T"
        ]
      },
      {
        "ref": "bom-ai-app",
        "dependsOn": [
          "openlm-research/open_llama_3b_v2",
          "bom-pytorch/torchserve",
          "bom-transformers",
          "openai-community/gpt2"
        ]
      }
```

https://github.com/aibom-workshop/rsa-2024/blob/main/aibom%20workshop%20examples/cybeats/cyclonedx/AI-app-with-ml-model%202.1.json

Groups Breakouts – Topic Discussion for AI-BOM

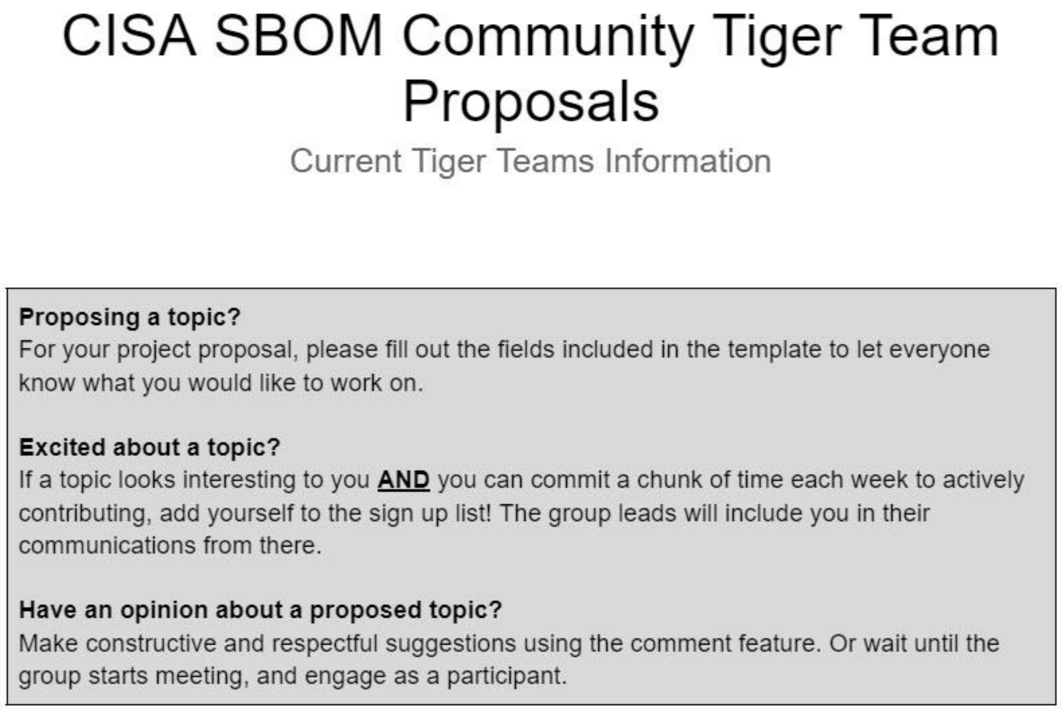
#	Topic	Description	Notes
1	What fields should (and should not be) in an AIBOM?	This topic explores the essential and non-essential components to include in an AIBOM, such as model weights and visualizations of model performance. (Examples: model weights, visualizations of model performance)	Discussed essential components such as model name, version, framework, training datasets, etc. Considered whether model weights should be included due to size. Also discussed model metrics and hashes.
2	Minimum elements of AIBOM	Discusses the minimum set of elements required in an AIBOM to ensure comprehensive coverage and functionality.	
3	Collection of data for AIBOM properties	Examines the process of collecting and managing data for AIBOM properties. (Example: data about training)	Challenges in collecting data for AIBOM properties were discussed, including author credibility, data provenance, and validation. Emphasized the need for standardized methods of data collection.
4	Standardized framework for AI dev & DevOps (MLOps)	Explores the development and DevOps practices necessary to establish a standardized framework for AI. (Example: model versioning)	
5	AI “Risks” and “Vulnerabilities” (as it pertains to fields in the AIBOM)	Analyzes the risks and vulnerabilities associated with AI systems, specifically in relation to the AIBOM fields.	Discussed the differentiation between AI vulnerabilities (MLVs) and traditional CVEs. Explored the challenges of identifying AI-related risks. Highlighted the importance of signing mechanisms for data provenance.
6	Creating or identifying infrastructure for AI risks	Discusses the establishment or identification of infrastructure similar to NVD, CVE, CVSS, EPSS, and KEV for managing AI-related risks.	Emphasized the extension of the existing CVE-based system to include ML vulnerabilities. Proposed creating standardized scoring systems and establishing CNAs for ML risks.
7	AIBOM use cases (including biz operations & risk management)	Explores various use cases of AIBOM in business operations and risk management to demonstrate its practical applications.	Identified use cases including medical devices, malware detection, vulnerability management, and transparency. Highlighted compliance needs around bias, fairness, and accountability.

What’s Next?

- Visit GitHub from the workshop to learn more
  - Topics
  - Presentations
  - Recordings
  - Examples

https://github.com/aibom-workshop/rsa-2024

- Register for CISA SBOM Community Tiger Team group for AI-BOM →



CISA SBOM Community Tiger Team Proposals

Current Tiger Teams Information

Proposing a topic?
For your project proposal, please fill out the fields included in the template to let everyone know what you would like to work on.

Excited about a topic?
If a topic looks interesting to you **AND** you can commit a chunk of time each week to actively contributing, add yourself to the sign up list! The group leads will include you in their communications from there.

Have an opinion about a proposed topic?
Make constructive and respectful suggestions using the comment feature. Or wait until the group starts meeting, and engage as a participant.

https://docs.google.com/document/d/11UU_Wiaemi7zBs3sE-MgovieyPx1XJEOaju2EM5btts/edit?usp=sharing

Thank you!

Helen Oakley, CISSP, GPCS, GSTRT
Director of Secure Software Supply Chains & Secure Development, SAP
in /in/helen-oakley