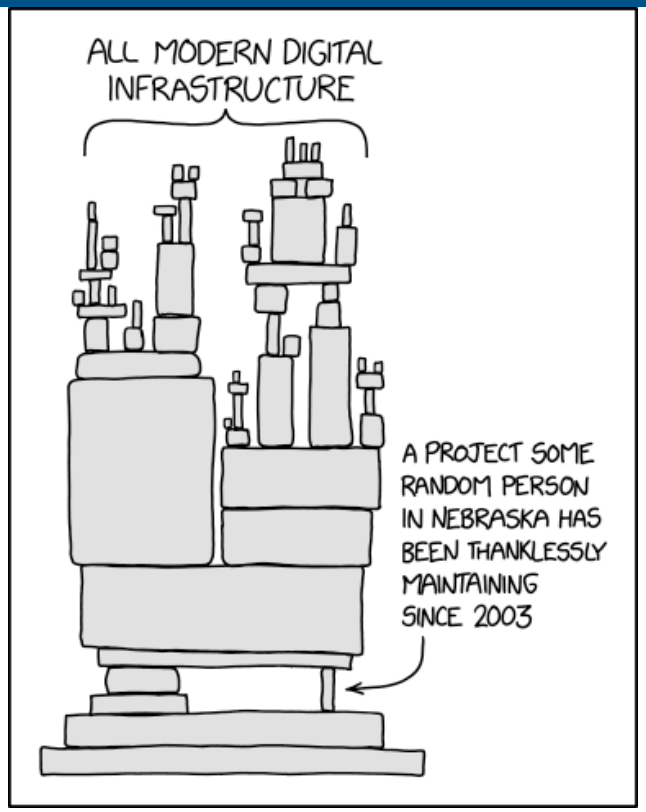
La nomenclature logicielle
Une introduction et une mise à jour intersectorielle

Allan Friedman, Ph. D.
CISA, Conseiller principal et stratège

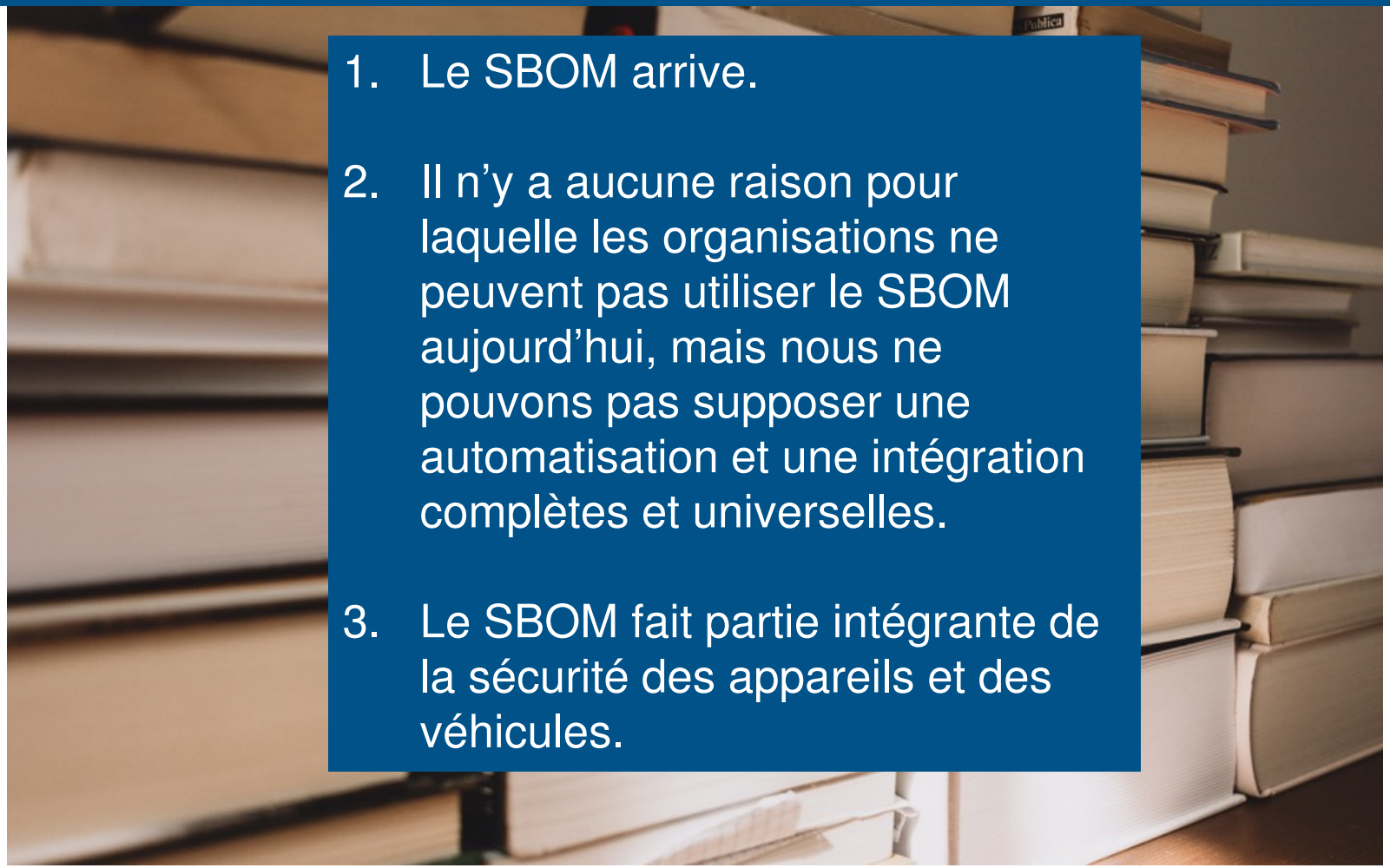
Cela vaudra-t-il la peine que je m'y attarde?

- Les arguments en faveur de la transparence
- Qu'est-ce qu'un SBOM?
- Pourquoi ne le faisons-nous pas aujourd'hui?
- Ce que nous avons fait jusqu'à présent
- Lacunes : ce sur quoi nous travaillons encore
- Statut du SBOM aujourd'hui



https://xkcd.com/2347/

TL;DR (Trop long, je n’ai pas lu)

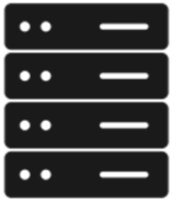


1. Le SBOM arrive.
2. Il n’y a aucune raison pour laquelle les organisations ne peuvent pas utiliser le SBOM aujourd’hui, mais nous ne pouvons pas supposer une automatisation et une intégration complètes et universelles.
3. Le SBOM fait partie intégrante de la sécurité des appareils et des véhicules.

La transparence peut aider les marchés à prospérer

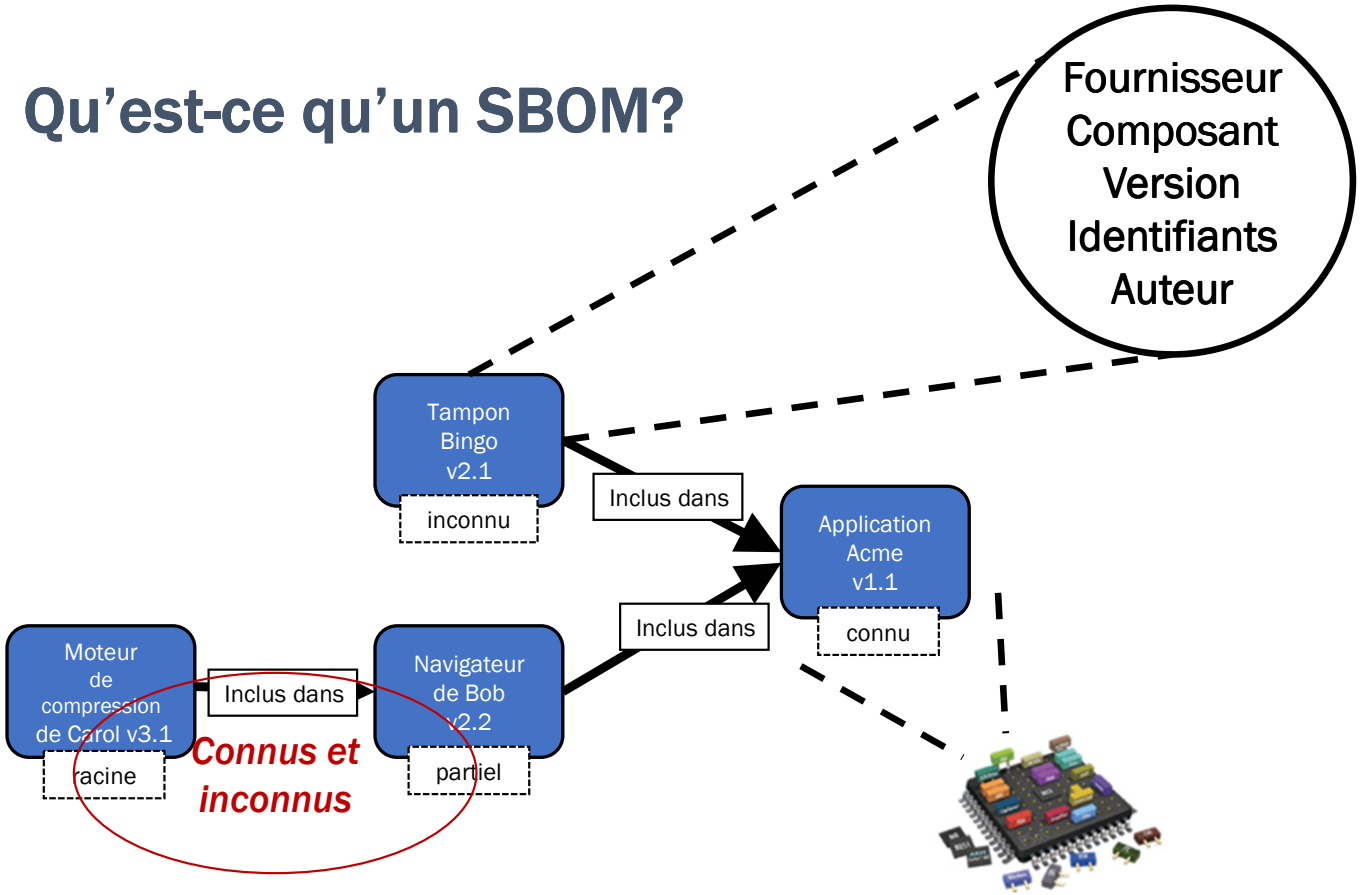
- Ingrédients alimentaires et étiquettes alimentaires
- Les fiches de données de sécurité dans l'industrie chimique
- Nomenclature matérielle dans l'industrie
- La dénomination et le suivi des composants peuvent favoriser l'innovation (p. ex., EVC)

« Sachez ce que vous avez »



LOG4J

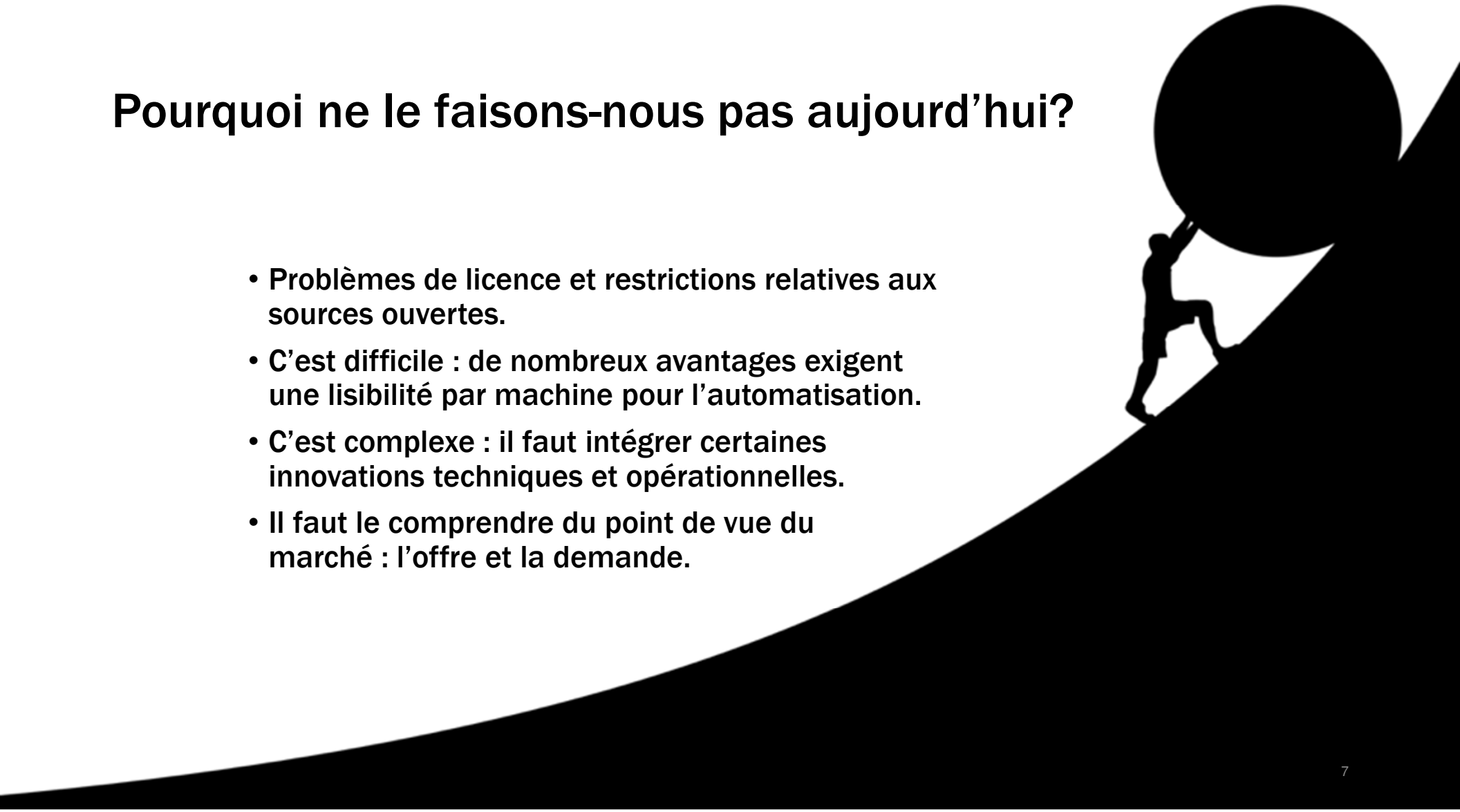
Qu'est-ce qu'un SBOM?



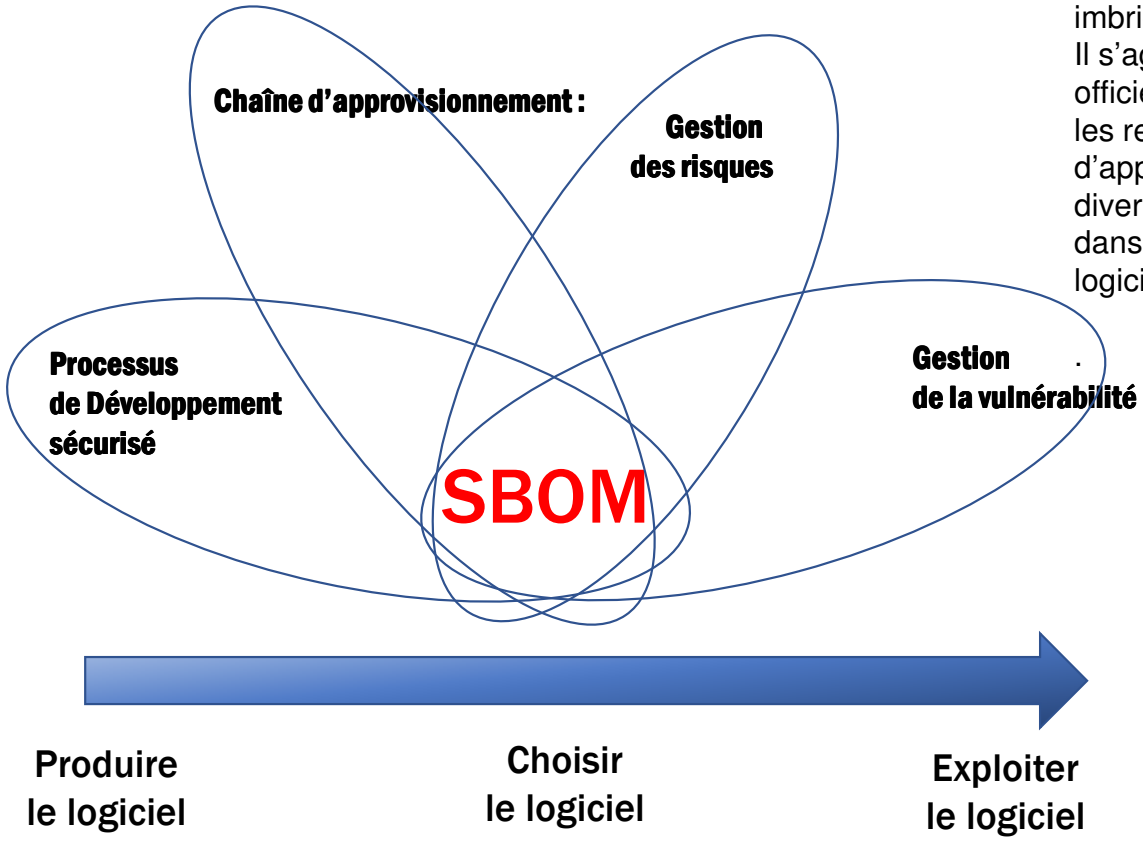
6

Pourquoi ne le faisons-nous pas aujourd'hui?

- Problèmes de licence et restrictions relatives aux sources ouvertes.
- C'est difficile : de nombreux avantages exigent une lisibilité par machine pour l'automatisation.
- C'est complexe : il faut intégrer certaines innovations techniques et opérationnelles.
- Il faut le comprendre du point de vue du marché : l'offre et la demande.



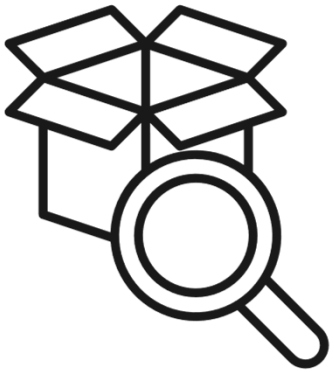
Une nomenclature logicielle (SBOM) est en fait une liste d'ingrédients ou un inventaire imbriqué.
Il s'agit d'un « enregistrement officiel contenant les détails et les relations de la chaîne d'approvisionnement des divers composants utilisés dans la construction d'un logiciel ».



La transparence dans le cycle de vie

source

construction



analyse binaire

Mise en œuvre d'un SBOM favorable à l'automatisation

La CISA travaille activement à l'harmonisation de ces communautés

Solution : « Vulnerability Exploitability eXchange » (VEX) mise en œuvre dans le FASC de OASIS


« Nous aimons cette idée…
On le fera quand on nous y obligera. »

Décret exécutif 14028 (12 mai 2021)
« Améliorer la cybersécurité de la nation »

- « La confiance que nous accordons à notre infrastructure numérique doit être proportionnelle au degré de fiabilité et de transparence de cette infrastructure... »
- Le DE définit le SBOM et détermine la proposition de valeur dans la section 10(j)
- Section 4 : amélioration de la sécurité de la chaîne d'approvisionnement des logiciels.
  - 4(f) — définir les « éléments minimums » du SBOM.
  - 4(e)(vii) — directives définies sur « la fourniture à un acheteur d'une nomenclature logicielle (SBOM) pour chaque produit ».
  - 4(k) et 4(n) — transposer les directives en règles.

Éléments minimaux du SBOM

Champ de données	Documenter les informations de base sur chaque composant qui doit faire l'objet d'un suivi : fournisseur, nom du composant, version du composant, autres identifiants uniques, relation de dépendance, auteur des données du SBOM et horodatage.
Soutien à l'automatisation	Soutenir l'automatisation, notamment par la génération automatique et la lisibilité par machine, afin de permettre une mise à l'échelle dans l'écosystème logiciel. Les formats de données utilisés pour générer et consommer les SBOM comprennent les balises SPDX, CycloneDX et SWID.
Pratiques et processus	Définir les opérations de demande, de génération et d'utilisation du SBOM, y compris : la fréquence, la profondeur, les connus et inconnus, la distribution et la livraison, le contrôle d'accès et la prise en compte des erreurs.

Mises en œuvre propres au secteur

- Soins de santé
- Technologie infonuagique
- Finances
- Énergie
- Automobile

L’état du SBOM en 2022

- L’outillage est encore émergent, notamment pour la consommation.
- Pas de plateformes éprouvées et évolutives pour le partage et l’échange de données du SBOM.
- Les hypothèses concernant l’interopérabilité sans faille n’ont pas été testées.
- Les vulnérabilités ne mettent pas toutes les organisations en danger.

Il n’y a aucune raison pour laquelle les organisations ne peuvent pas utiliser le SBOM aujourd’hui, mais nous ne pouvons pas supposer une automatisation et une intégration complètes et universelles.

SBOM : Partie d’un déjeuner complet

Pour plus de renseignements :
www.cisa.gov/SBOM

Des questions?
SBOM@cisa.dhs.gov
allan.friedman@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA