Amazon Inspector SBOM Export ではじめるソフトウェアサプライチェーンセキュリティ

2023/09/06

Kenta Goto

Amazon Web Services Japan G.K.
Solutions Architect

自己紹介

- 名前
  - 後藤 健汰（ Kenta Goto ）
- 所属
  - ISV/SaaS Solutions Architect
- 好きな AWS サービス
  - Amazon EKS
- 趣味
  - サウナ

@kennygt51

Agenda

- ソフトウェアサプライチェーンと SBOM
- Amazon Inspector SBOM Export ご紹介
- デモ
- まとめ

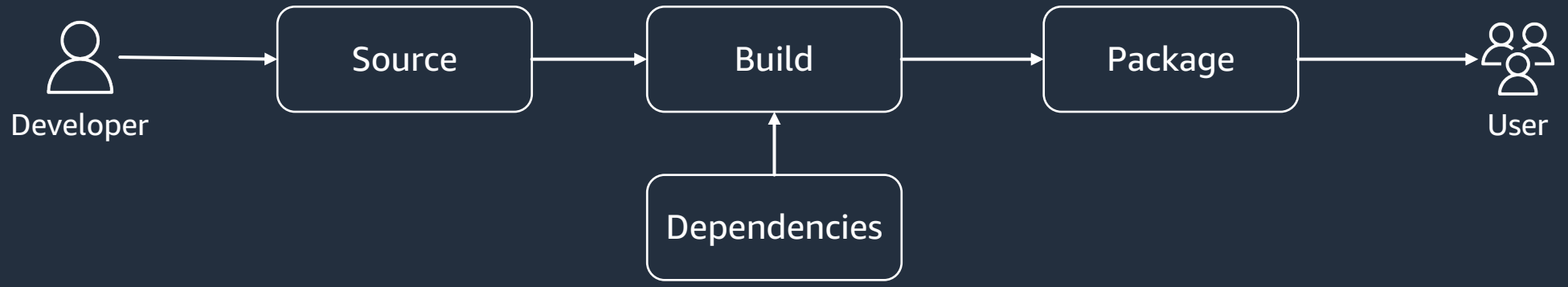
Agenda

- ソフトウェアサプライチェーンと SBOM
- Amazon Inspector SBOM Export ご紹介
- デモ
- まとめ

ソフトウェアサプライチェーン

ソフトウェアサプライチェーンとは

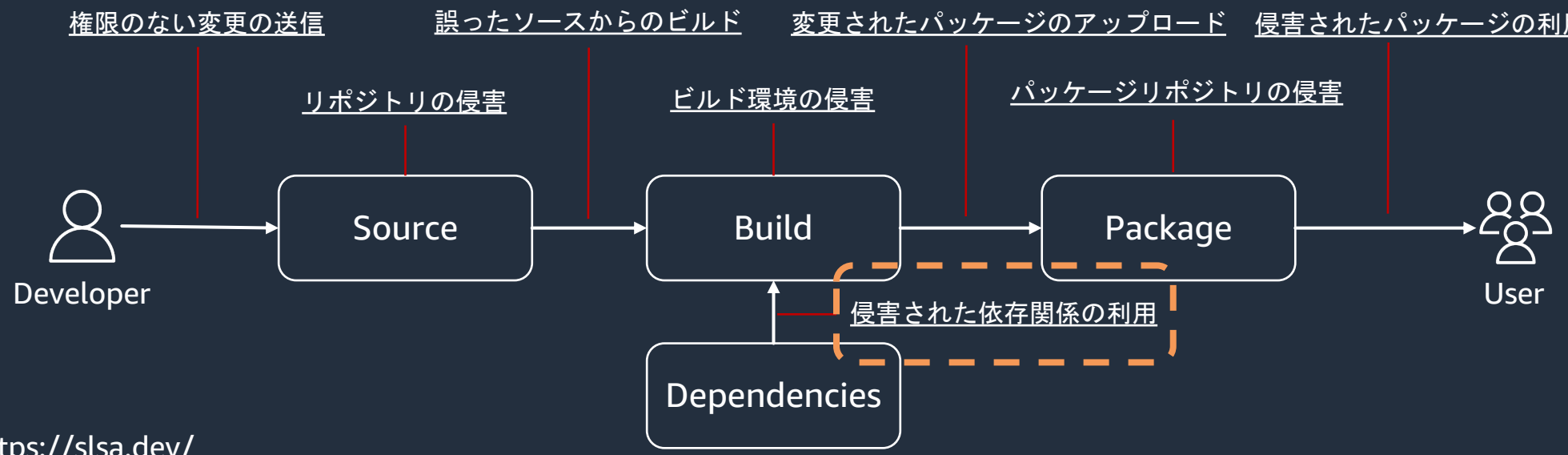
- ソフトウェアが本番環境にデプロイされるまでの一連のプロセス
- ソフトウェア開発ライフサイクルに関わる要素（コード、設定ファイル、ライブラリなど）と、その依存関係が組み合わさって構成される
- OSS を含む依存ライブラリの利用やソフトウェア・組織の拡大にともない、複雑化する



ソフトウェアサプライチェーンに潜む脅威

- ソフトウェア開発ライフサイクルのどこかで侵害が成功すると、サービスを利用するユーザーも影響を受ける
- 各工程において、様々な脅威が発生する

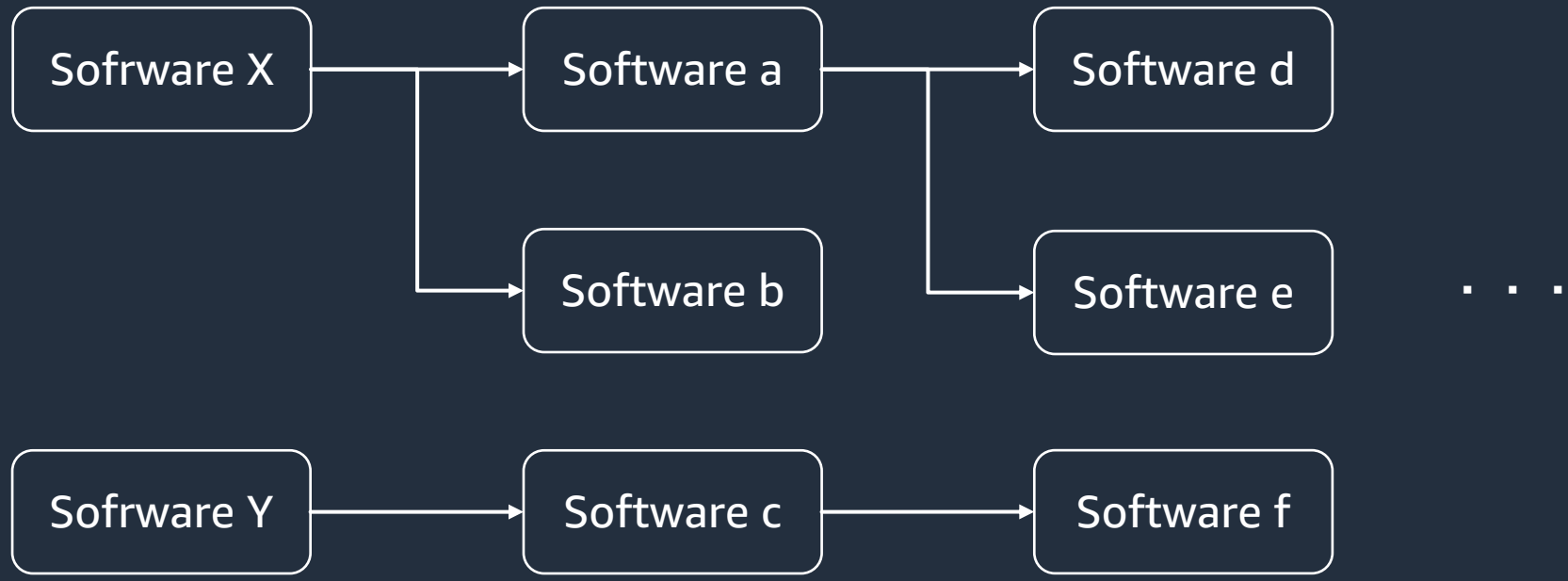
SLSA framework（※1）



※1 https://slsa.dev/

ソフトウェアの脆弱性管理の複雑化

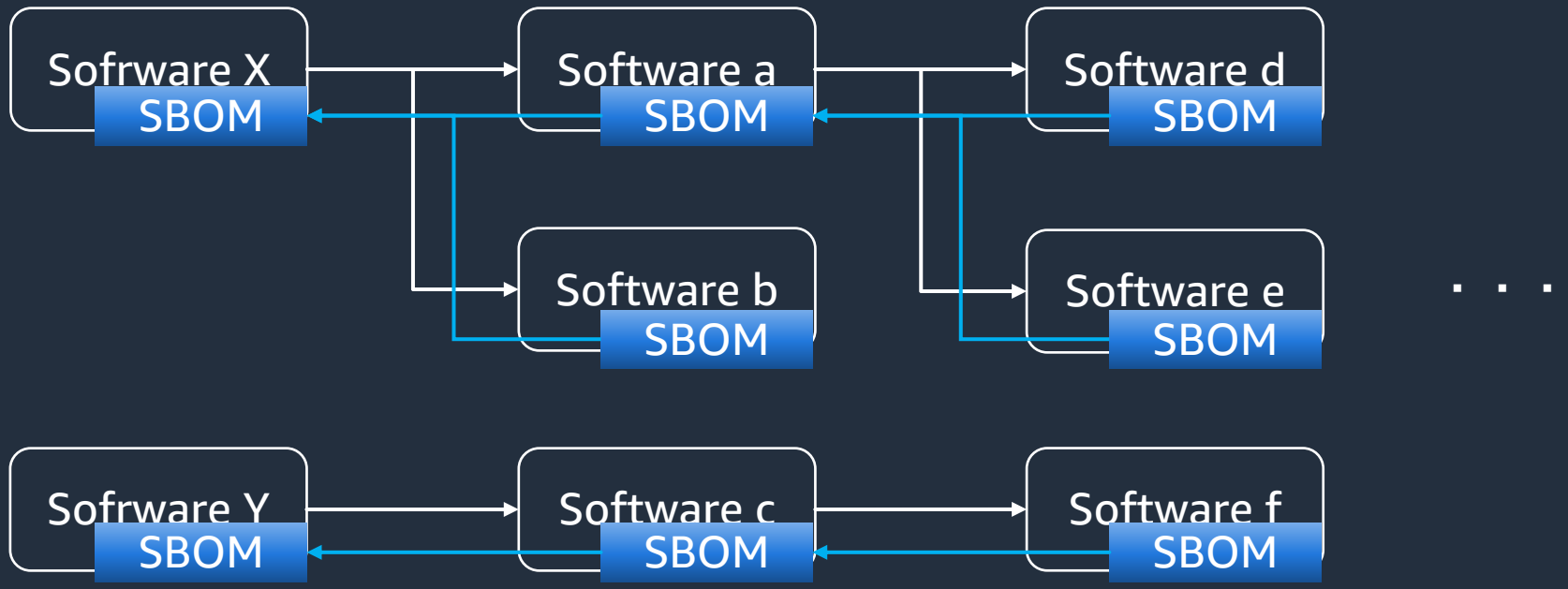
- OSS の利用が一般化する中で、推移的な依存関係が生まれるため、コンポーネントとしてどのようなソフトウェア・ライブラリが含まれているかを把握するのは難しい



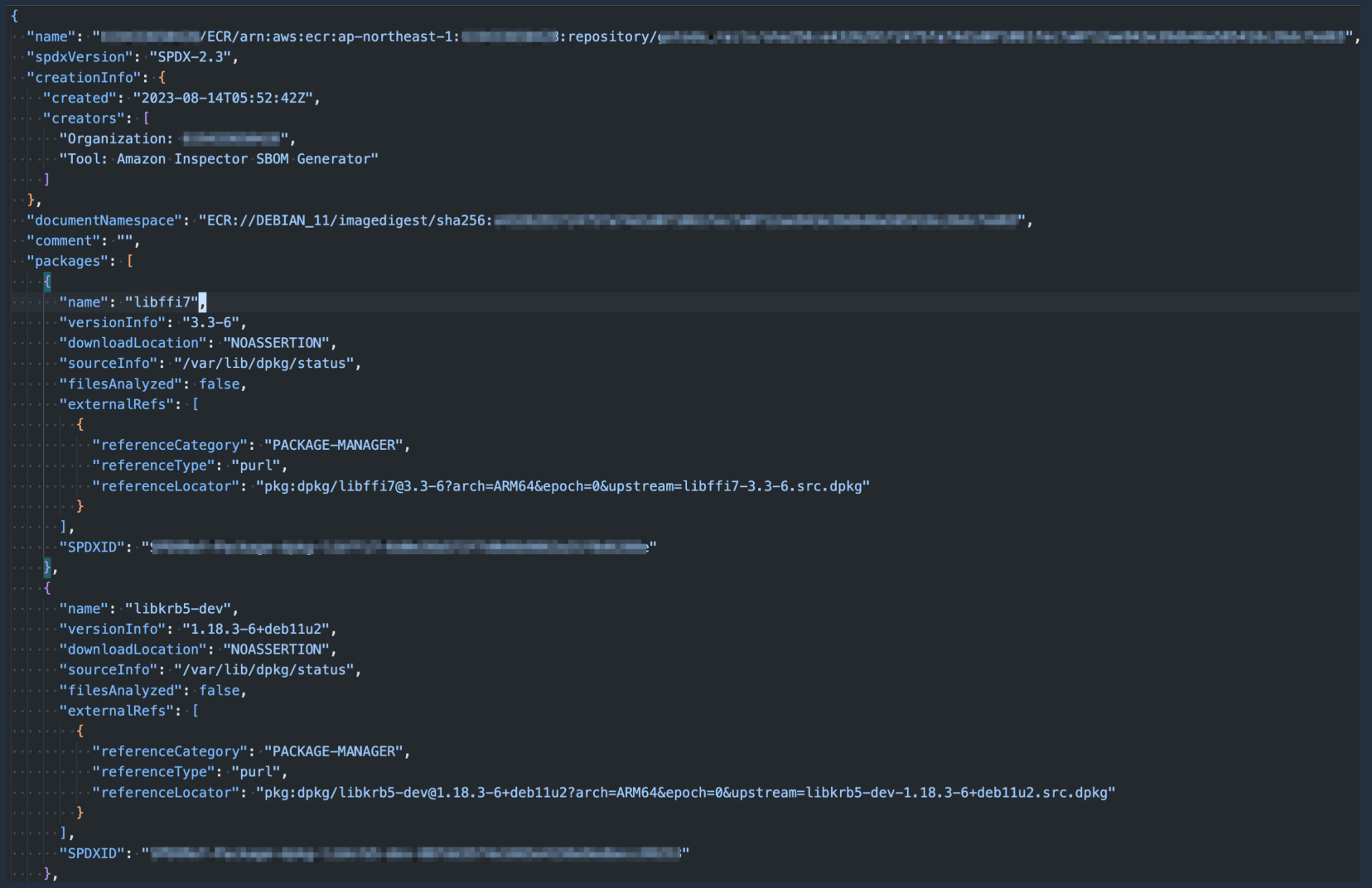
SBOM (Sofrware Bill of Materials)

SBOM (Sofrware Bill of Materials) とは

- ソフトウェアを構成するコンポーネントや依存関係を一覧化したリストのこと
- 標準化された仕様が複数存在する (特定の言語に依存しない)



SBOM (Sofrware Bill of Materials) とは



一般的な SBOM 標準フォーマット

- SPDX (Software Package Data Exchange)
  - Linux Foundation の SPDC Workgroup によって開発されている
  - 2021 年 9 月に ISO/IEC 5962:2021 (※1) として公開
  - オープンソースのライセンスコンプライアンスに関連する情報を扱うために開発が始まったもの
- CycloneDX
  - OWASP Foundation によって開発されている
  - セキュリティに特化した SBOM フォーマットを目標として開発が始まったもの

※1 https://www.iso.org/standard/81870.html

SBOM 導入によるメリット

- SBOM 導入が進むことで、以下のメリットが期待される

脆弱性管理

- 脆弱性残留のリスク
- 脆弱性対応機関の短縮
- 脆弱性管理にかかるコストの低減

ライセンス管理

- ライセンス違反リスクの低減
- ライセンス管理にかかるコストの低減

開発生産性向上

- 開発遅延の阻止
- 開発にかかるコストの低減
- 開発期間の短縮

『ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 Ver. 1.0』より (※1)

※1 https://www.meti.go.jp/press/2023/07/20230728004/20230728004-1-1.pdf

Agenda

- ソフトウェアサプライチェーンと SBOM
- Amazon Inspector SBOM Export ご紹介
- デモ
- まとめ

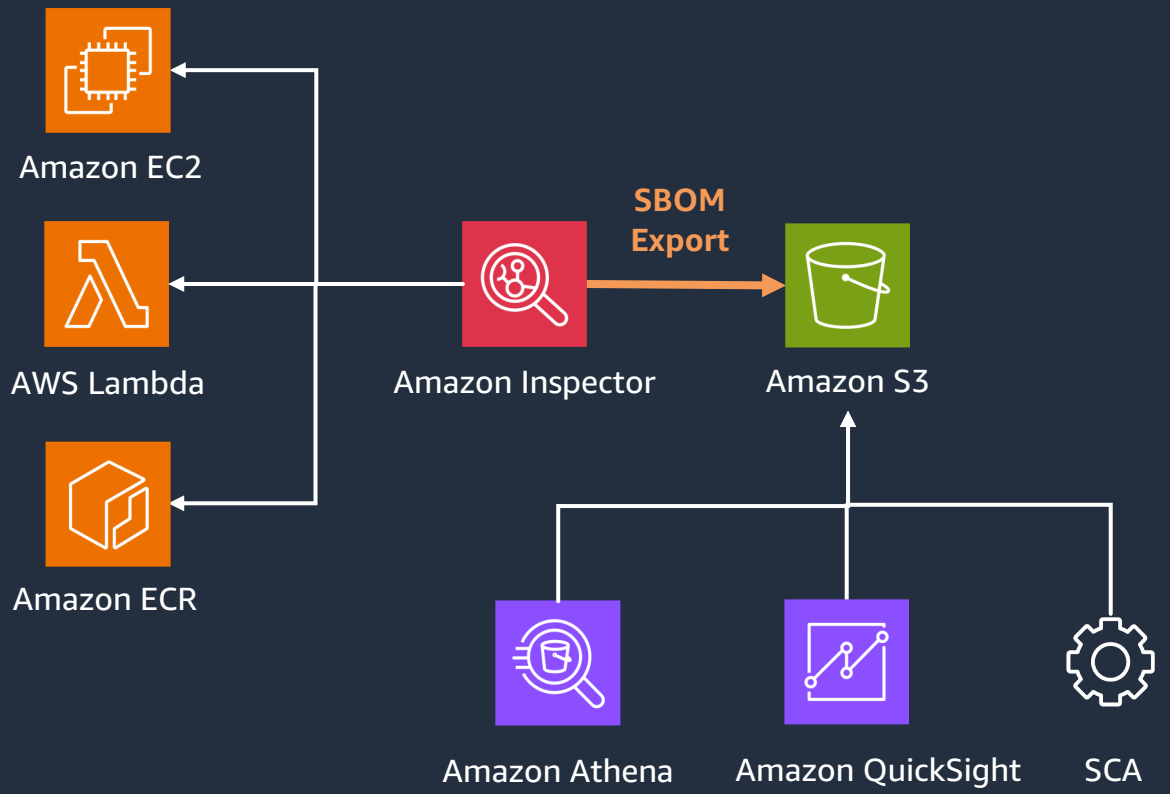
Amazon Inspector

ソフトウェアの脆弱性や意図しないネットワーク露出領域を継続的なスキャンで検知する脆弱性管理サービス

- ワンクリックで有効化
- リソースの自動検出と継続スキャン
- ダッシュボードによる容易な脆弱性管理
- 独自含むスコア算出による優先順位付け
- AWS Organizations との連携で大規模な管理
- AWS Security Hub、Amazon EventBridge との連携で検知から対応までをサポート
- Amazon EC2、Amazon ECR、AWS Lambda に対応

Amazon Inspector SBOM Export

Amazon Inspector で監視している全てのリソースについて、
Software Bill of Materials (SBOM) を、S3 バケットに業界標準形式でエクスポート



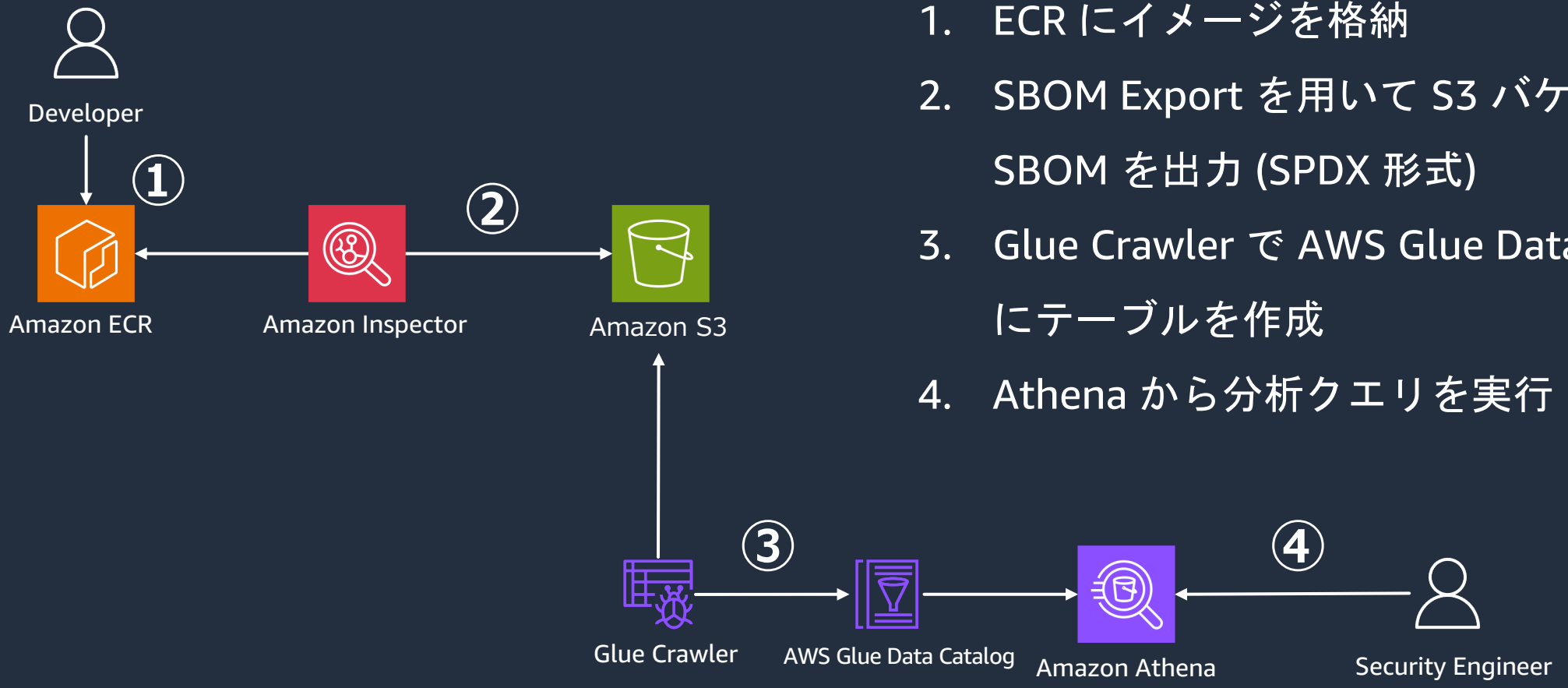
- サポート SBOM フォーマット：
  CycloneDX / SPDX
- AWS Organizations 単位、リソース単位でのエクスポートが可能
- Amazon Inspector でアクティブに監視されているすべてのリソースが対象（※）
- 無料
- Amazon Athena、Amazon QuickSight、SCA ツールでの分析

※ 2023/08 時点で Amazon EC2 Windows インスタンスは未サポート

Agenda

- ソフトウェアサプライチェーンと SBOM
- Amazon Inspector SBOM Export ご紹介
- デモ
- まとめ

デモ



1. ECR にイメージを格納
2. SBOM Export を用いて S3 バケットに SBOM を出力 (SPDX 形式)
3. Glue Crawler で AWS Glue Data Catalog にテーブルを作成
4. Athena から分析クエリを実行

Agenda

- ソフトウェアサプライチェーンと SBOM
- Amazon Inspector SBOM Export ご紹介
- デモ
- まとめ

本セッションのまとめ

- ソフトウェアサプライチェーンの複雑化に伴う脅威の増加

- SBOM の導入が進むことで、脆弱性管理・ライセンス管理・開発生産性向上といったメリットが期待される

- Amazon Inspector SBOM Export を利用することで、業界標準形式で SBOM エクスポートを実現

- Amazon Athena や Amazon QuickSight による分析が可能

Thank you!