

報道関係者各位

サイバーセキュリティクラウド、脆弱性管理ツール『SIDfm VM』に「SBOM 管理機能」を新たに追加

グローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）が脆弱性管理ツール『SIDfm VM（エスアイディーエフエム ヴイエム）』に新機能として「SBOM 管理機能」を追加したことをお知らせします。



■ 開発背景

サプライチェーンの弱点を悪用したサイバー攻撃による被害が増加している背景を受け、世界および国内で様々な取り組みが進められています。米国では 2021 年 5 月にサイバーセキュリティ強化のための大統領令が発令され、SBOM（Software Bill of Materials）作成の指示が出

されました。日本では経済産業省が 2023 年 7 月に「ソフトウェア管理に向けた SBOM の導入に関する手引」を公開しました。これらの取り組みにより、SBOM の導入サポートや生成ツールが多く登場し、SBOM を導入する企業が徐々に増加しています。

SBOM はサプライチェーンの透明性を高めるために活用され、特に脆弱性管理の分野での利用が期待されています。ソフトウェア提供者および利用者は、自社が提供または利用しているソフトウェアを構成する OSS（オープンソースソフトウェア）などの要素を含めた SBOM を活用し、効果的な脆弱性管理を実現したいというニーズが高まっています。

SBOM の導入サポートや作成ツールは多く存在し、ソフトウェア提供者が利用者に対して SBOM を納品することは比較的容易になってきています。しかしその一方で、効果的な脆弱性管理を実施するためには、SBOM に記述されている OSS などに新たな脆弱性が報告された場合に迅速に気づき、適切に対処する必要があります。SBOM 導入前と比べて管理対象のソフトウェアが増えることから、脆弱性情報の収集と対処判断の効率化がより一層求められます。

さらに、対処プロセスも複雑化しています。SBOM が納品された製品ごと（場合によってはバージョンごと）に、サプライチェーンに対するコミュニケーションや対処状況の管理、製品のアップデートまでの暫定対処などが必要となり、組織的な取り組みが求められます。

■新機能「SBOM 管理機能」とは

脆弱性管理を一元化できる「SIDfm VM」に、SBOM のファイルをインポートできる機能を追加しました。これにより、ホストの構成情報と紐づけることで管理対象ホスト単位で SBOM をインポートしているかどうかが一目で確認できます。また、インポートされた SBOM を、自動で脆弱性データベースとの照合用データに変換し、脆弱性を早期に検出することが可能になりました。

さらに、ホストの構成情報として紐づけることで、「SIDfm VM」のカスタムカテゴリやルール設定機能を用いて、必要な担当者に必要な情報のみを自動で連携することも可能となりました。

これにより、セキュリティ管理者は各担当者やサプライチェーンの対処状況を、SBOM 以外でも管理しているホストの脆弱性と合わせて一元的に把握することができます。

登録ホスト一覧画面
データ取込 ログアウト マスタ情報 ホストの新規登録

色	ホスト名	OS	Agent 取得 プロダクト名	手動登録 プロダクト名	CPE 数	基礎日	メモ	操作
●	sbomtest	Ubuntu 22.04 LTS	パッケージ登録	登録プロダクト変更	0	2011/07/18		SBOM情報 ホストの削除

合計 1 件

アクションボタン
カテゴリ一括更新
プロダクト一括更新
基礎日一括更新
メモ一括更新
インポート
エクスポート

SBOM管理画面
 SBOM取込み後のイメージ

ホスト名: sbom-test SBOM追加情報登録

色	ファイル名	SBOMから取得したOS情報	最終取込日時	照合データ	操作
□	ubuntu_22_trivy_cyclonedx.json	ubuntu-22.04	2024/07/18 19:10:41	照合データ	SBOM更新 削除

新規追加
履歴削除

SBOM照合情報

※パッケージ照合が○のものにはパッケージで脆弱性照合を行い、CPEは利用しません。

SBOMファイル内文字列	CPE	パッケージ照合
pkg.deb/ubuntu/apr@2.4.12?arch=arm64&distro=ubuntu-22.04	cpe:2.3:a:debian:advanced_package_tool:2.4.12?arch=arm64&distro=ubuntu-22.04	○
pkg.deb/ubuntu/bash@5.1-6ubuntu1.1?arch=arm64&distro=ubuntu-22.04	cpe:2.3:a:gnu:bash:5.1:alpha:***** cpe:2.3:a:gnu:bash:5.1:beta:***** cpe:2.3:a:gnu:bash:5.1:rc1:***** cpe:2.3:a:gnu:bash:5.1:rc2:***** cpe:2.3:a:gnu:bash:5.1:rc3:*****	○
pkg.deb/ubuntu/coreutils@8.32-4.1ubuntu1.2?arch=arm64&distro=ubuntu-22.04	cpe:2.3:a:gnu:coreutils:8.32:***** cpe:2.3:a:gnu:coreutils:8.32:*****:x64*	○
pkg.deb/ubuntu/openssl@3.0.2-0ubuntu1.15?arch=arm64&distro=ubuntu-22.04	cpe:2.3:a:openssl:openssl:3.0.2:*****	○
pkg.gem/i18n@0.6.9	cpe:2.3:a:ruby:i18n:0.6.9:*:*:*:*:*:ruby	
pkg.gem/json@1.8.1	cpe:2.3:a:rubygems:json:1.8.1:*****	
pkg.gem/jquery-rails@3.1.0	cpe:2.3:a:rubyonrails:jquery-rails:3.1.0:*****	
pkg.gem/rack@1.5.2	cpe:2.3:a:rack:projectrack:1.5.2:***** cpe:2.3:a:rack:projectrack:1.5.2:*****:ruby**	
pkg.gem/rails@4.1.1	cpe:2.3:a:rubyonrails:rails:4.1.1:***** cpe:2.3:a:rubyonrails:ruby_on_rails:4.1.1:*****	

- SIDfmVM サービスサイト : <https://sid-fm.com/vm/>

※現時点で対応しているフォーマットは以下です。(形式は json と xml の 2 種類)

- SPDX: 2.2, 2.2.1, 2.2.2, 2.3, 2.3.1
- CycloneDX: 1.1, 1.2, 1.3, 1.4

■ 「SBOM 管理機能」の活用イメージ

活用例として、医療業界における医療機器メーカー (MDM) と医療機関 (HCP) のそれぞれの立場で、「SBOM 管理機能」を用いて実現できることをご紹介します。

1：医療機器メーカー（MDM）の場合：薬機法の基本要件基準への対応

- ・納品機器バージョン毎の SBOM 管理（リポジトリ管理）
- ・リポジトリ毎の脆弱性の検出・通知（自動）
- ・検出した脆弱性の影響を素早く日本語や数値で理解（納品先の医療機関やサプライチェーンとのコミュニケーションの効率化、脱属人化）

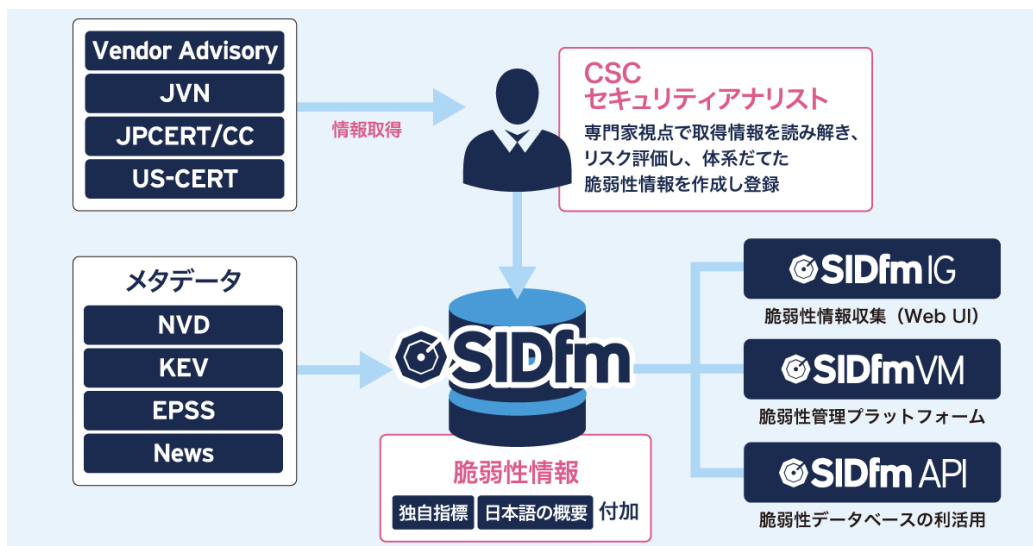
2：医療機関（HCP）の場合

- ・提供される SBOM に対する脆弱性の有無を確認
- ・検出された脆弱性について影響度合いを日本語や数値で理解
- ・脆弱性を含む対象機器を特定

■脆弱性情報収集・管理ツール『SIDfm』について

脆弱性情報収集・管理ツール『SIDfm』は、脆弱性対応の運用を効率化するツールです。OS・アプリケーション・ネットワーク製品の脆弱性情報を世界中から自動で収集・蓄積します。自社に必要な情報だけをすぐに特定できる機能により対策すべき脆弱性とその対策内容が一目でわかります。さらに、脆弱性の対処進捗の記録・管理まで行うことができます。

『SIDfm』の最大の特徴はコンテンツの質です。NVD、KEV などのメタデータとベンダーのアドバイザリー情報、JVN などの情報をセキュリティアナリストが専門家視点で読み解きリスク評価し「独自指標」「日本語の解説」を付加した脆弱性情報を提供しています。『SIDfm』の情報だけで、概要から影響を受けるバージョンや対処方法などが日本語ですぐに理解・把握できるため、優先すべき脆弱性の対処にリソースを集中させることができます。



■ 株式会社サイバーセキュリティクラウドについて

住所：東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階

代表者：代表取締役社長 兼 CEO 小池敏弘

設立：2010 年 8 月

URL：<https://www.cscloud.co.jp/>

「世界中の人々が安心安全に使えるサイバー空間を創造する」を企業理念に掲げ、世界有数のサイバー脅威インテリジェンスを駆使した Web アプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの 1 つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。



【本件に関するお問い合わせ】

株式会社サイバーセキュリティクラウド マーケティング部 担当：井田

TEL : 03-6416-1579 FAX : 03-6416-9997 E-Mail : mkt@cscloud.co.jp