SEAL
SECURITY ALERTING

APLIKACE SEAL – MODUL SBOM

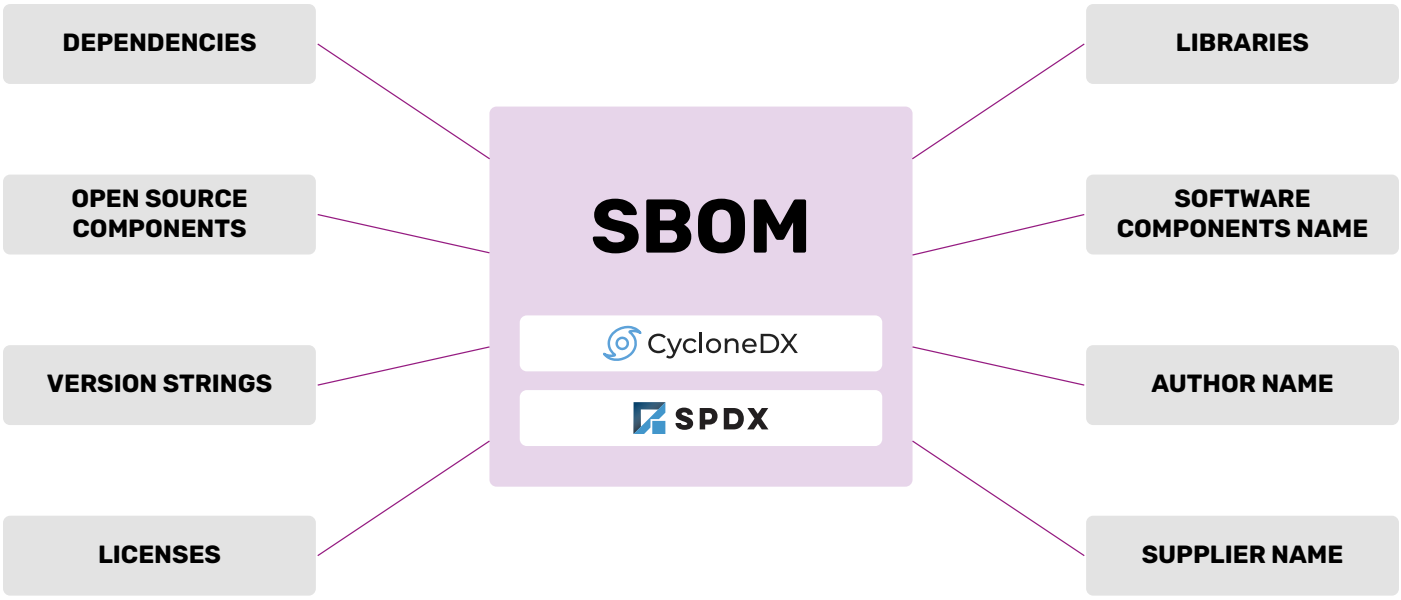
„Vyvíjejte a používejte bezpečný software bez zranitelností.“

Modul **SBOM (Software Bill of Materials)** aplikace SEAL přináší moderní přístup ke správě softwarového inventáře. **Tento modul umožňuje dodavatelům a uživatelům aplikací hlubší porozumění a kontrolu nad používanými softwarovými komponentami.** Díky tomu lze efektivně spravovat bezpečnostní rizika a zvýšit transparentnost celého softwarového řetězce.

Dnešní software typicky využívá stovky knihoven třetích stran, ve kterých jsou průběžně objevovány problémy a zranitelnosti a vydávány nové verze. Toto hlídat ručně bez využití pomocných nástrojů je téměř nemožné. Známý příklad je knihovna Log4j a její zranitelnost Log4Shell. SBOM modul v aplikaci SEAL umožňuje **snadno, automaticky a pravidelně kontrolovat, zda některá z použitých knihoven v aplikaci neobsahuje zranitelnost**. Pokud je zranitelnost objevena, je možné odeslat e-mail s notifikací. V aplikaci lze zjistit podrobnosti, zda existují nové opravené verze, je možné se ke zranitelnosti vyjádřit, atd.

Hlavní výhody a funkce modulu SBOM zahrnují:

- **Automatizovaný import SBOM dokumentů:** Umožňuje snadný import SBOM dokumentů prostřednictvím webového rozhraní nebo HTTP API.
- **Vyhodnocení zranitelností:** Pravidelné automatické vyhodnocení zranitelností komponent z veřejně dostupných zdrojů a možnost ruční analýzy dopadů zranitelností vývojovými týmy.
- **Nastavitelná e-mailová hlášení:** Informuje uživatele nebo vývojové týmy o nových zranitelnostech, což umožňuje rychlou reakci a řešení problémů.
- **Zvýšení transparentnosti a důvěryhodnosti:** Možnost sdílení SBOM dokumentů a analýz dopadů zranitelností s koncovými uživateli. Lze zveřejnit vybrané verze projektu pomocí unikátního odkazu, včetně informací o komponentách, zranitelnostech a vyhodnocení jejich dopadu.
- **Integrace s řešením CI/CD:** Podpora pro integraci s existujícími Continous Integration a Continous Delivery procesy, což umožňuje automatizaci a snížení zátěže na vývojové týmy.
- **Správa více aplikací a projektů:** Možnost spravovat různé projekty, jejich verze a nastavit potřebná přístupová oprávnění jednotlivým členům týmu.
- **Flexibilní systém rolí a oprávnění:** Lze nastavit vlastní role s různou úrovní oprávnění a ty dále přidělit uživatelům. SBOM modul tak může sloužit i větším vývojovým týmům, kde různé skupiny pracují na různých projektech a neměli by všichni vidět vše.



Modul poskytuje nejen přehled o použitých komponentách a jejich bezpečnostním stavu, ale také nástroje pro jejich efektivní správu a mitigaci potenciálních rizik, čímž zvyšuje celkovou bezpečnost a spolehlivost dodávaných aplikací.

VYUŽITÍ MODULU SBOM

PRO DODAVATELE APLIKACÍ (VÝVOJÁŘSKÉ SPOLEČNOSTI)

Průměrný počet komponent současných aplikací je v řádu stovek. Takto vysoký počet je způsoben rekurzivními závislostmi použitých komponent (jedná se o tzv. nepřímé závislosti). Při tomto množství je nemožné sledovat bezpečnost komponent bez specializovaného SCA (*Software Component Analysis*) řešení jako je modul SBOM aplikace SEAL.

Modul SBOM umožňuje **importovat existující SBOM dokumenty a sledovat zranitelnosti komponent u všech aplikací organizace**. Aplikace v pravidelných intervalech vyhodnocuje zranitelnosti komponent z veřejně dostupných dat a umožňuje následnou ruční analýzu dopadů zranitelností vývojovým týmem aplikace.

S pomocí **HTTP API je možné integrovat existující Continous Integration (CI) / Continous Delivery (CD) řešení** a automaticky tak nahrávat aktuální verze SBOM dokumentů ihned po sestavení. Aplikace pracuje jen s SBOM dokumentem a **nepotřebuje proto přístup ke zdrojovému kódu aplikace.**

Na jednom místě je možné získat přehled o stavu všech komponent napříč aplikacemi a pomoci tak vývojovým týmům s udržením aktuálního a bezpečného stavu aplikací.

Upozornění vývojového týmu na nové zranitelnosti probíhá automaticky pomocí nastavitelných e-mailových hlášení a není tak nutné pravidelně ručně kontrolovat stav komponent v aplikaci nebo sledovat stránky, repositáře a diskuzní fóra použitých komponent.

S využitím licenčních politik je možné zachytit komponentu s nevhodnou softwarovou licencí (např. copyleft jako je GPL).

SBOM dokument je možné zveřejnit nebo sdílet se zákazníkem včetně vypracované analýzy dopadů a zvýšit tak transparentnost a důvěryhodnost dodávané aplikace.

PRO UŽIVATELE APLIKACÍ (KONCOVÉ ZÁKAZNÍKY)

Importem SBOM dokumentů používaných aplikací je možné **získat přehled o použitých softwarových komponentách** napříč organizací a **zjistit** tak **včas přítomnost zranitelných komponent** v infrastruktuře organizace. To obrací tradiční závislost spotřebitele na dodavateli – uživatel aplikace se může v tomto případě dozvědět o zranitelnostech dříve než dodavatel a dotčené aplikace může odstavit nebo k nim zpřísnit přístup pomocí firewallu.

Pomocí nastavitelných e-mailových hlášení se IT správci dozví automaticky o nových zranitelnostech, aniž by museli pravidelně kontrolovat stav komponent v modulu SBOM.

VÝVOJ APLIKACÍ A SOUVISLOST S SBOM A VEX

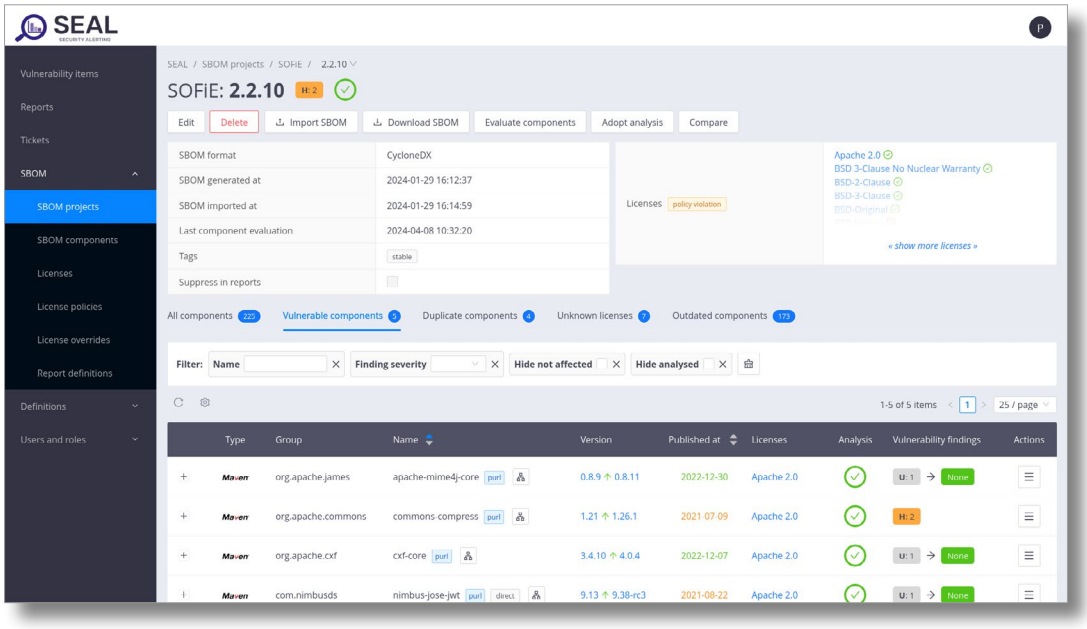
VYUŽITÍ OPEN-SOURCE KNIHOVEN V APLIKACÍCH

Podle studie společnosti *Synopsis* obsahují prakticky všechny současné aplikace volně dostupné open-source komponenty ve formě balíčků či knihoven. Většina obsahuje alespoň jednu zranitelnou komponentu a téměř polovina alespoň jednu komponentu s vysokým bezpečnostním rizikem.

Aplikace jsou spotřebitelům dodávány jako uzavřená ucelená řešení a uživatel tak nemá povědomí o obsažených komponentách a jejich bezpečnostních rizicích. V případě mediálně známých zranitelností (např. Log4Shell) jsou pak dodavatelé aplikací zahlceni žádostmi o vyjádření, zda právě jejich software obsahuje konkrétní zranitelnou komponentu – a to i v případech, kdy aplikace běží na zcela jiné technologické platformě.

SBOM A VEX

Doba mezi objevením a zneužitím zranitelností se v posledních letech znatelně snižuje a je proto nutné více než dříve sledovat v reálném čase zranitelnost použitých komponent. Tento proces nesmí být omezen pouze na dodavatele aplikací, ale musí být možný i pro jejich uživatele. K tomu pomáhá tzv. SBOM dokument (*Software Bill Of Materials*), strojově zpracovatelný soupis všech použitých komponent v aplikaci.



Práci na koncepci SBOM dokumentu zahájila v roce 2018 americká federální agentura NTIA, poté dohled převzala americká federální agentura pro kybernetickou bezpečnost CISA. V rámci CISA vznikla navíc koncepce tzv. VEX dokumentu (*Vulnerability Exploitability eXchange*), strojově zpracovatelného dokumentu obsahující vyjádření dodavatele aplikace ke zranitelnosti komponent. **V roce 2021 pak americká federální vláda vydala nařízení *Improving the Nation's Cybersecurity (14028)* jehož součástí je doporučení dodávat SBOM dokumenty k veškerému softwaru.**

V současné době jsou nejpoužívanějšími implementacemi SBOM dokumentu CycloneDX a SPDX. Pro VEX dokumenty pak CycloneDX a OpenVEX. Pro obě implementace existují komerční i volně šiřitelné nástroje pro vytváření SBOM dokumentů ze zdrojových kódů aplikací.

VEX dokumenty jsou výsledkem analýzy zranitelnosti komponent a vytvářejí je SCA nástroje (*Software Component Analysis*) jako je aplikace SEAL a modul SBOM. Analýzu je nutné provádět lidskou silou a pečlivě přitom zvažovat všechny možné souvislosti.

SBOM A POŽADAVKY REGULÁTORŮ

NIS2 SMĚRNICE EU

NÚKIB

According to Article 21 (Cybersecurity risk-management measures), essential and important entities must take appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of networks and information systems.

The measures shall be based on an "all-hazards approach" that aims to protect network and information systems and the physical environment of those systems from incidents and shall include "at least" the following:

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

VLÁDA USA – PROSTŘEDNICTVÍM CISA

Výkonný příkaz o zlepšení kybernetické bezpečnosti byl vydán vládou USA v květnu 2021 a zdůrazňuje význam SBOM při zvyšování bezpečnosti dodavatelského řetězce softwaru.

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

https://www.cisa.gov/sbom

Více informací: **www.sonpo.cz**

Aplikace SEAL je vlastněna společností:
SONPO, a.s. | Klapkova 546, 182 00, Praha 8
www.sonpo.eu | sales@sonpo.eu

Sonpo