June 17, 2021
Masato Terada
IT Security Center
Information-technology Promotion Agency, Japan

Request For Comments
Collaboration possibilities between VDB and SBOM

My comment is “SWID Naming Specification for collaboration between VDB and SBOM”.
CVE has CNA. CVE Numbering Authorities (CNAs) are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

SWID Naming Specification is to apply a framework like CNA to SWID for collaboration between VDB and SBOM.
The characteristic of SWID Naming Specification is the following (Figure 1, Figure 2).

- SWID assigned framework for VDB
- Apply structured identifier compatible with CPE as the SWID
- Distributed management for VDB of Structured identifier of SWID

Example
{"swid": "nvdpid:1.0:sample.gov:secinfodbx:3.2"}
{"swid": "jvnpid:1.0:sample.or.jp:dbx:2.4"}

wfn:[
authority="nvdpid",
specification version="1.0",
vendor="sample.gov",
product="secinfodbx",
version="3.2"]

Figure 1: Structured identifier compatible with CPE

:

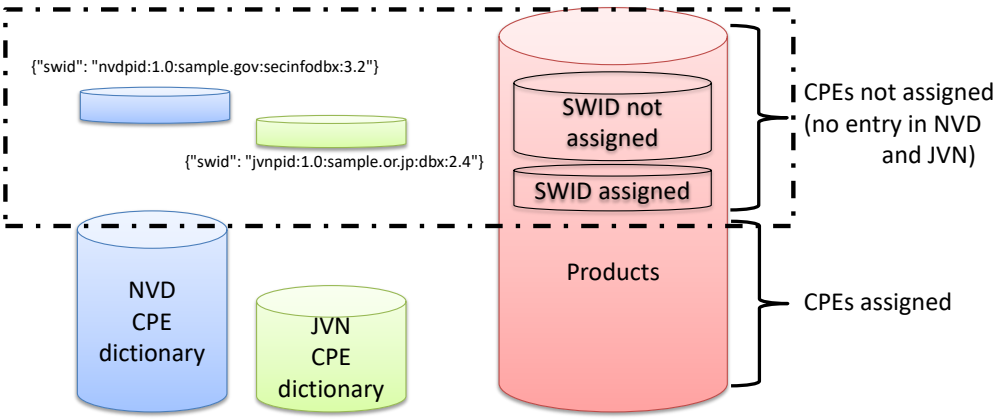

Figure 2: Distributed management of Structured identifier by VDB

Appendix: Overview of concept “Collaboration possibilities between VDB and SBOM”

- Integration of information sharing data using STIX/TAXII

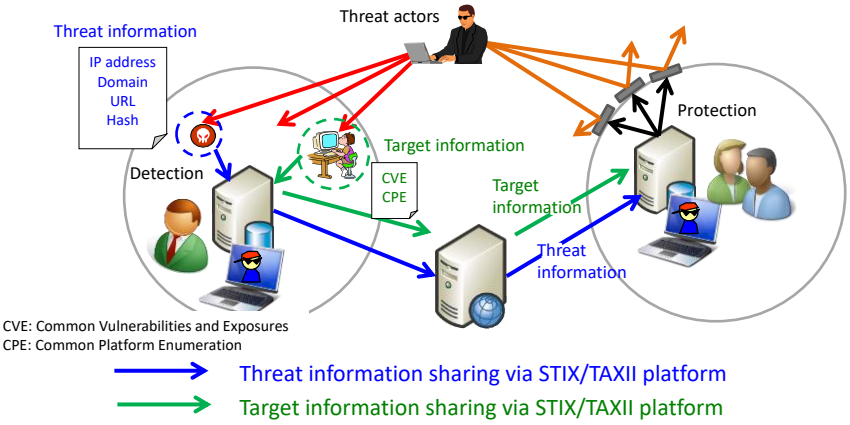

Figure 3: Integration of information sharing data flow

- Collaboration possibilities between VDB and SBOM

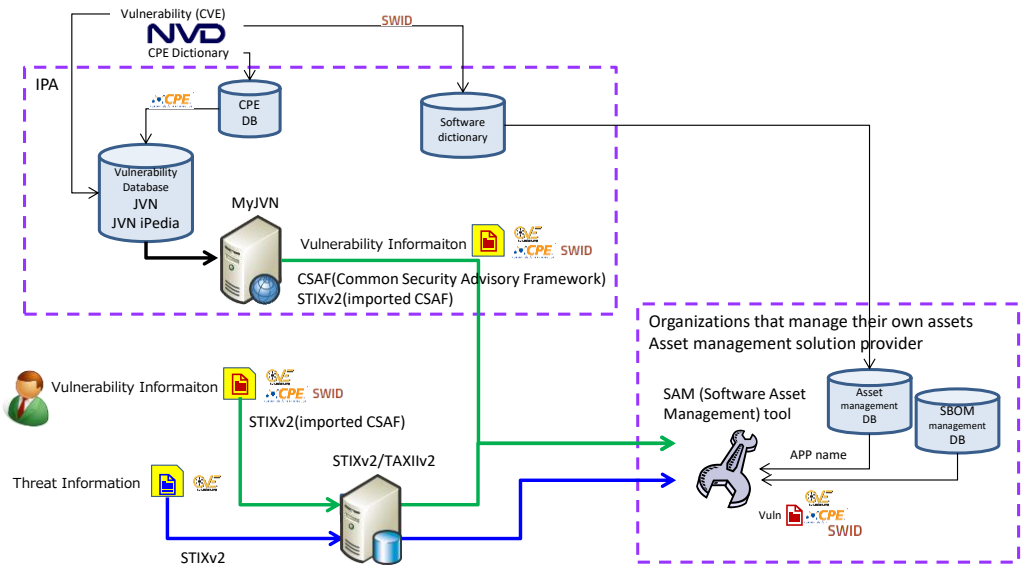

Figure 4: VDB, SBOM and STIX collaboration data flow

- <tech challenge> embedded CSAF in STIX </tech challenge>

  Vulnerability information Distributed using the STIX 2.x Extension

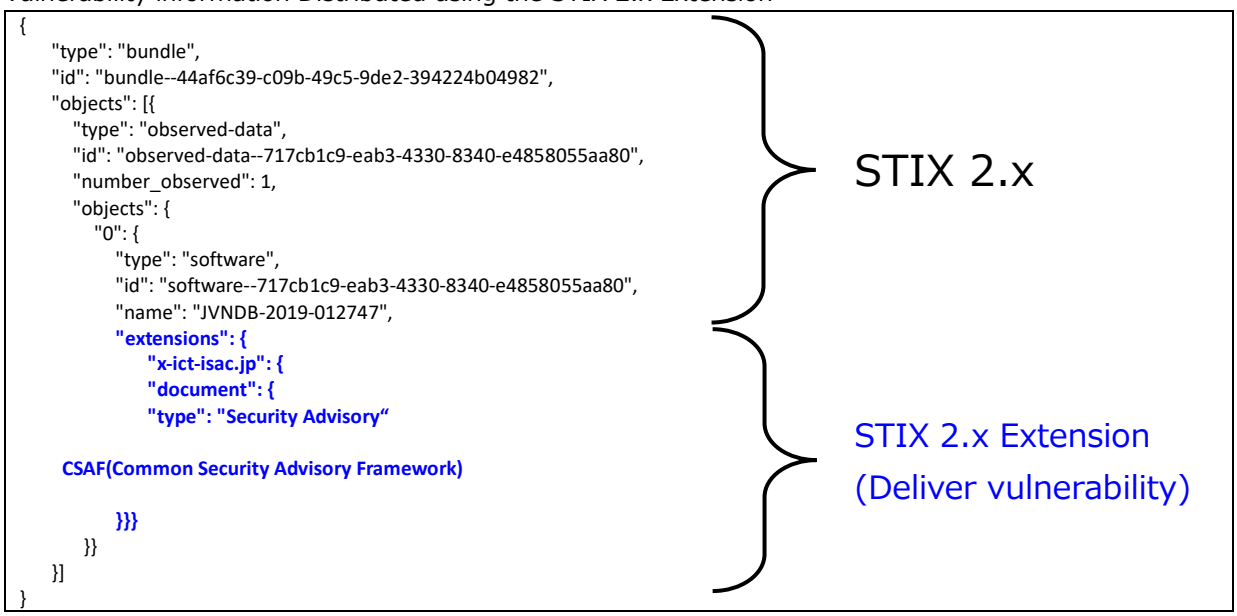

Figure 5: embedded CSAF in STIX

- <tech challenge> SWID naming specification </tech challenge>

  SWID Naming Specification in Software dictionary

  - Based on CPE
  - Application to SBOM in process model

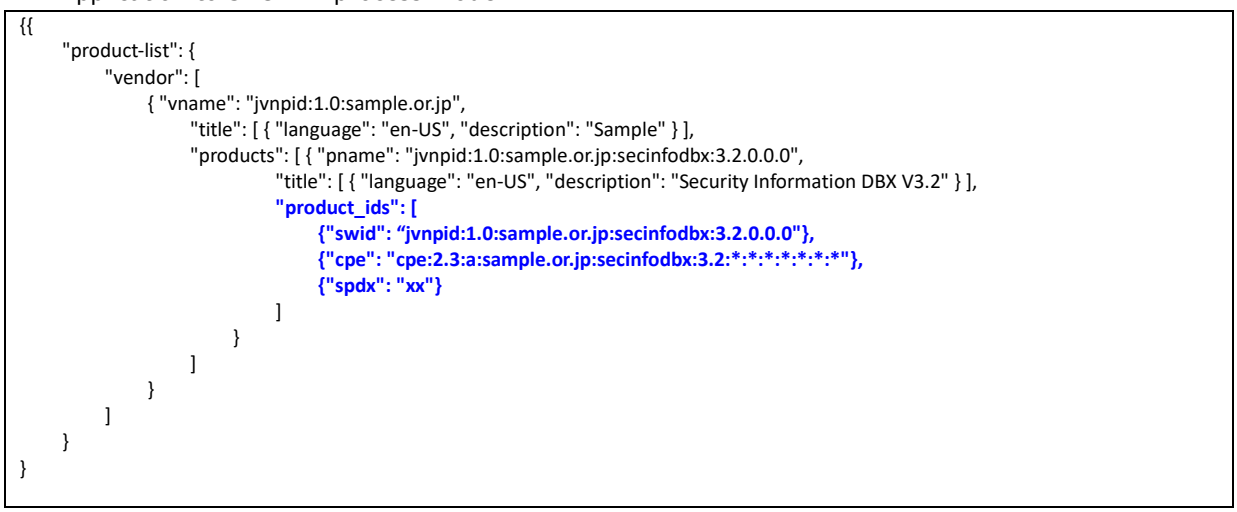

Figure 6: Software dictionary