Software supply chain

是什么？软件供应链，SBOM，SCA，……

为什么？用它来解决什么问题……

怎么做？哪些场景可以用……

软件供应链

主要关注三个事：

1、做为纯软件生产者，提高生产质量，保证生产流程安全可靠。DevSecOps

2、作为软件供应者，提供清晰可用、方便追溯的物料清单。SBOM

3、作为软件消费者（使用者），利用SBOM信息管理各层级安全漏洞。

SBOM

难点问题：

1、软件类别多、差异大，较难确定**元数据标准**。

2、SBOM**数据自身的安全**和有效性较难保障。

3、从哪些地方提取数据，并自动提取，也是难点。

4、依赖层级到多深是个头？完全的源头

自2018年以来，美国商务部的国家电信和信息管理局（NTIA）一直在协调行业努力，以提高软件采购过程的透明度，让组织了解他们构建、购买和使用的软件中的内容。拜登的行政命令要求产品提供软件材料账单（SBOM），这将帮助组织管理风险，让它们快速确定其产品中哪些脆弱的软件组件。

SCA Software Composition Analysis

https://bbs.huaweicloud.com/blogs/263415?utm_source=juejin&utm_medium=bbs-ex&utm_campaign=paas&utm_content=content

需要解决哪些问题？

只能想到一些好处：

1、类似CVE跟踪功能，对产品及时发布CVE有益

2、对外能提供SBOM，为产品使用者提供可见的组件供应链信息

3、打通产品生产、构建依赖链，便于分析供应风险

具体能解决目前什么痛点？

可能是上面的这些好处还没有急迫到让很多人疼痛的地步？^^

怎么做？

别人怎么做的之微软的SPDX，他们的元数据组织结构被认可度较高

https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/

讨论纪要：

1. 关注Sbom生成过程
2. SBOM动态过程中依赖，构建依赖：构建环境的依赖关系、构建本身的依赖（）
3. 包运行时依赖

4. Cve受影响包括包本身的依赖，构建工具的依赖，运行时的依赖
5. 审计链条，使用grafeas的审计逻辑
6. 操作系统发行版 SBOM的最佳实践（SBOM怎么来的，SBOM最后怎么用）
7. 构建期的SBOM和运行期的SBOM，两者的关系

8. 构建操作系统供应链的安全（SBOM + grafeas + 操作系统构建）

9. **操作系统构建供应链安全之SBOM全生命周期管理**