# 供应链安全

## ****内容介绍****

本篇是系列文章的第九篇，分享一下自己对供应链安全的理解。

## 供应链安全是什么

信息安全里面的供应链安全，是狭义范围的供应链安全，其最终安全问题是体现在应用系统上的问题。

应用系统的供应链安全，实际上是由三个部分组成的。

分别是应用安全里面软件开发中的依赖包（log4j），基础安全里面的应用运行组件（phpstudy），办公安全里的开发IDE（xcodeghost）。

## 安全需求来源与演变

供应链安全中，表现最明显的安全问题是软件依赖包的安全问题。

这是因为随着开发的敏捷性需求越来越重要，越来越多的开发都选择使用依赖组件的方式来完成开发。

而这种依赖组件，可能是公司开发的，个人开发的，甚至可能是恶意开发的。

组件一般是开源的，所以任何人都可能从源码中发现其本身存在的漏洞。这也是依赖包安全问题频发的一个原因。

而不管是应用组件如phpstudy，还是开发IDE如xcodeghost，发现或是在其中植入恶意代码，在实践中都是比较困难的。

基于以上信息，供应链安全最后的落脚大多都在应用安全范畴内。

## 安全理念演变

软件供应链安全方面，国内外各有相关的模型及白皮书提出。谷歌提出了 SLSA框架，微软提出了 SCITT框架，CNCF 提出了 in-toto框架。绿盟以及悬镜都开放了各自的白皮书。

理念中，不只是自己要对企业的软件供应链进行管控，也要按标准，将自己打造成安全的供应链。

其体系化的理念都跟应用安全有相当部分的重合，具体白皮书内容在此不再赘述。

## 供应链安全的建设落地

步骤：

状态调研及评估：调研安全建设状态，评估建设完成度。

决策工作内容：结合应用调研结果，结合公司整体的建设方案，来决定工作内容，内容顺序，落地方案。

供应链安全建设中，优先级最高的是依赖包供应链的安全建设，其次是基础IT组件，其次是办公终端IDE安全。

依赖包的管控，成体系的方案，有从准入到最后的废弃管理等。

但实际落地，还是要根据公司情况进行。

一般公司的安全部门都可以完成的，也就是在应用安全里的代码审计部分，实现自动化的统计依赖包，建立清单，跟随代码审计更新。

然后在获知漏洞情报时，及时检查本身的依赖，并安排处理措施。

至于依赖包准入，依赖包研究，统一性要求，自身SBOM生成等内容，其都涉及到整体开发流程管控，落地需要匹配的实际条件。

## QA

VX：qinbingjie1101