OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

软件供应链安全审计心得交流

演讲人：樊山

2024 OWASP中国安全技术论坛

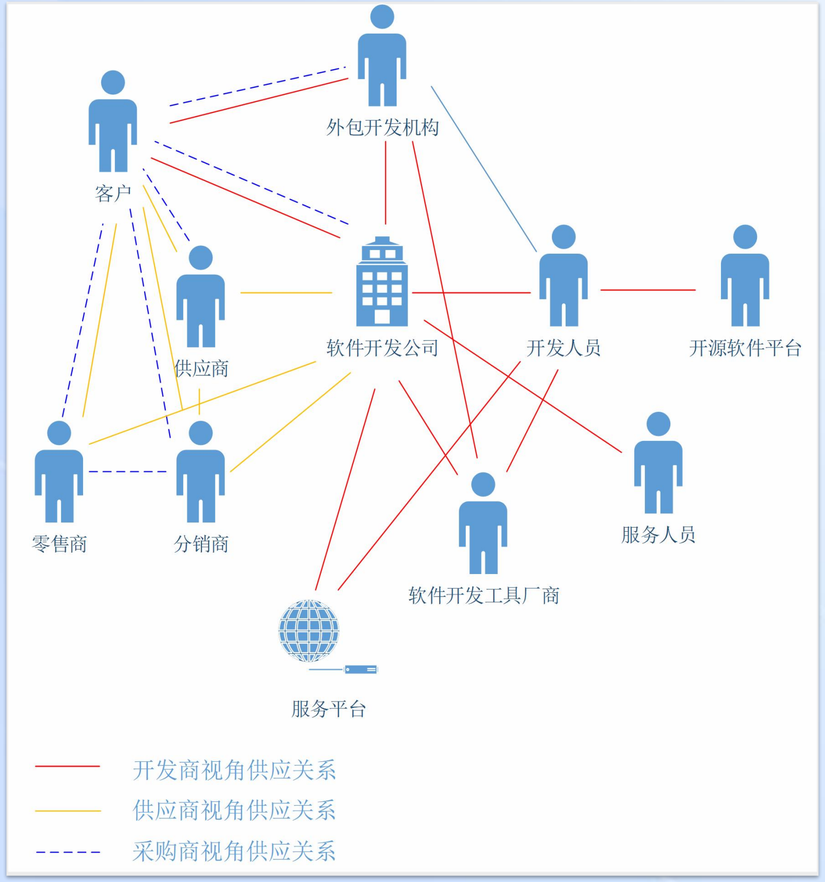
全球视野下的网络安全趋势

目录
CONTENTS

01

什么是软件供应链？

什么是软件供应链？



- 软件供应链是指软件产品的生产、销售和交付过程中涉及的所有环节和参与方。这些环节包括软件开发、测试、打包、部署、运维、销售、分销、客户支持等。软件供应链管理旨在优化整个流程，提高效率、降低成本、提高质量，并确保软件产品按时交付给客户。
- 软件供应链的参与方包括软件开发公司、供应商、分销商、零售商、客户和第三方服务提供商等。他们之间的合作和协调对于软件产品的成功交付至关重要。
- 软件供应链管理涉及到供应链规划、供应商管理、库存管理、订单管理、运输和物流管理等方面。通过有效的供应链管理，软件公司可以更好地应对市场需求变化，提高客户满意度，并实现持续的竞争优势。

02

软件供应链安全现状

软件供应链安全现状

- **第三方依赖：**许多软件开发团队依赖于第三方组件和库来加快开发速度和提高效率，但这也增加了软件供应链的复杂性和风险。第三方依赖的安全性和可信度可能存在问题，导致软件供应链受到威胁。
- **开源软件安全性：**开源软件在软件供应链中广泛使用，但开源社区的安全审查和漏洞修复可能不及时，这为黑客植入恶意代码提供了机会。
- **供应链合作伙伴安全：**软件供应链中的合作伙伴包括软件开发商、供应商、承包商等，他们的安全状况直接影响到整个软件供应链的安全性。如果合作伙伴的安全措施不够严密，就容易成为攻击的目标。
- **不完善的代码签名技术：**代码签名问题导致软件在更新过程中被恶意代码注入，更严重者构成APT攻击污染整个软件用户。
- **云服务安全：**许多组织将软件部署到云上，但云服务提供商的安全性也成为软件供应链安全的一个重要方面。云服务提供商的漏洞或被攻击，可能会波及到使用其服务的软件开发团队和最终用户。
- **物联网设备安全：**随着物联网设备的普及，物联网设备中的软件供应链也面临安全挑战。物联网设备的固件安全、远程管理安全等问题需要得到重视。

美国NIST标准下的供应链安全管理（SP 800-161 r1）

风险管理活动	识别（I）	预防（P）	检测（D）	响应（R）	恢复（R）
					CSF框架
分类	NIST 网络安全框架 (CSF) 1.1 版：	FIPS 199，联邦信息和信息系统安全分类标准：	NIST SP 800-30，修订版 1，进行风险评估的指南：	NIST SP 800-37，修订版 2，信息系统和组织的风险管理框架：安全和隐私的系统生命周期方法：	
选择	NIST SP 800-39，管理信息安全风险：组织、任务和信息系统视图：		NIST SP 800-53 修订版 5，信息系统和组织的安全和隐私控制：	NIST SP 800-53B 修订版 5，信息系统和组织的控制基线：	
实施	NIST SP 800-160 卷 1，系统安全工程：		NIST SP 800-160 卷 2，开发网络弹性系统：系统安全工程方法：	NIST SP 800-181 修订版 1，国家网络安全教育倡议 (NICE) 网络安全劳动力框架：	
评估	NISTIR 7622，联邦信息系统的定义供应链风险管理实践：		NISTIR 8179，关键性分析过程模型：优先考虑系统和组件：	NISTIR 8286，识别和估计企业风险管理 (ERM) 的网络安全风险：	
授权	NISTIR 8286A，识别和评估企业风险管理的网络安全风险：	新增	NISTIR 8276，网络供应链风险管理的关键实践：来自行业的观察：	NIST.CSWP.02042020-1网络供应链风险管理案例研究	NIST.CSWP.02042020-2匿名消费电子公司
监视	NISTIR 8286B，优先考虑企业风险管理的网络安全风险：				NIST.CSWP.02042020-3 匿名消费品公司

恢复（R）
NIST.CSWP.02042020-4匿名可再生能源公司
NIST.CSWP.02042020-5梅奥诊所
NIST.CSWP.02042020-6 Palo Alto网络公司
NIST.CSWP.02042020-7希捷技术

美国NIST标准下的供应链安全管理（SP 800-161 r1）

访问控制	意识和培训	审计和问责	评估、授权和监督	配置管理	应急计划	识别和认证	事件响应	维护	介质保护
政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序
账户管理	扫盲培训和意识	事件记录	控制评估	基线配置	事件响应培训	识别和验证(组织用户)	事件响应培训	受控维护	介质存储
访问实施	基于角色的培训	审计记录和内容	信息交换	配置变更控制	事件响应测试	设备识别和认证	事件响应测试	维护工具	介质传输
信息流实施	培训记录	审计审查、分析和报告	行动计划和里程碑	影响分析	事件处理	标识符管理	事件处理	非本地维护	介质消毒
职责分离		不可否认	授权	变更访问限制	事件监控	识别和验证(非组织用户)	事件监控	维护人员	
远程访问		审计记录生成	持续监测	配置设置	事件报告	服务识别和认知	事件报告	及时维护	
无线接入		信息披露监控		最小功能	事件响应援助		事件响应援助	现场维护	
移动设备访问控制		会话审计		系统组件清单	事件响应计划		事件响应计划	维护监控和信息共享	
使用外部系统		跨组织审计记录		配置管理计划	信息泄露响应		信息泄露响应		
信息共享				软件使用限制					
可公开访问的内容				用户安装软件					
数据挖掘保护				信息位置					
访问控制决定				数据活动映射					
				签名组件					

美国NIST标准下的供应链安全管理（SP 800-161 r1）

物理和环境保护	计划	程序管理	人员安全	个人可识别信息处理和透明度	风险评估	系统和服务采购	系统和通信保护	系统和信息完整性	供应链风险管理
政策和程序	政策和程序	信息安全计划的领导角色	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序	政策和程序
物理访问授权	系统安全和隐私计划	信息安全和隐私资源	人员筛选		安全分类分级	资源分配	共享资源中的信息	缺陷修复	供应链风险管理计划
监控物理访问	行为准则	行动计划和里程碑过程	访问协议		风险评估	系统开发生命周期	拒绝服务保护	恶意代码保护	供应链控制和流程
交付和移除	操作概念	系统清单	外部人员安全		漏洞监控和扫描	获取过程	边界保护	系统监控	来源
备用场地	安全和隐私架构	性能指标			风险响应	系统文档	传输机密性和完整性	安全警报、建议和指令	采购策略、工具和方法
系统组件的位置	中央管理	企业架构			临界分析	安全和隐私工程原则	手机密码	软件、固件和信息完整性	供应商评估和审查
资产监控和跟踪	基线选择	关键基础设施计划			威胁追踪		独立于平台的应用程序	信息管理和保留	供应链运营安全
设施位置		风险管理策略					保护静态信息	污染	通知协议
		授权流程					异构		防篡改和检测
		使命和业务流程定义					隐蔽和误导		系统或组件检查
		内部威胁计划	隐私计划	用于测试、培训和研究的个人身份信息的最小化	供应链风险管理策略		分布式处理和存储		组件真实性
		安全和隐私工作人员	隐私计划的领导角色		持续监控策略				
		测试、培训和监控	隐私计划信息的传播		用途		带外信息		
		安全和隐私团体和协会	披露的稽核处理	投诉管理			操作安全		
		威胁意识计划	个人身份信息质量管理	隐私报告			备用通信路径		
		保护有关外部系统的受控非机密信息	数据治理机构	风险框架					
				风险管理计划领导角色					

03

软件供应链安全审计依据

软件供应链安全审计依据

立法依据	《中华人民共和国网络安全法》第二十二、二十三条、三十三条 《关键信息基础设施保护条例》第二十条、二十一条
组织规范	各行业发布本行业有关软件供应链安全的文件，如：中国人民银行发布了《支付机构软件供应链管理规范》、工业和信息化部发布了《软件供应链安全管理指南》、中国证监会发布了《证券期货行业信息系统软件供应链安全管理指引》
可遵循的标准	目前我国尚无有关软件供应链安全管理标准，常见的国际标准以SP 800-161第1版《系统和组织的网络安全供应链风险管理实践》为主的相关标准和准则，如：SSDF、行政命令（EO）14028第4e节下的软件供应链安全指南、ESF 确保软件供应链安全（客户/软件开发商/集成商）推荐做法指南
审计发起方其他要求	ISO/IEC 27001：2022 信息安全、网络安全和隐私保护信息安全管理体系-要求、网络安全和基础设施局 (CISA)，供应商供应链风险管理 (SCRM) 模板

SSDF控制项

组织准备

- 定义软件开发的安全要求
- 实施角色和职责
- 实施支持工具链
- 定义和使用软件安全检查标准
- 实施和维护安全的软件开发环境

保护软件

- 保护所有形式的代码免遭未经授权的访问和篡改
- 提供验证软件版本完整性的机制
- 存档和保护每个软件版本

生产安全可靠的软件

- 设计软件以满足安全要求并降低安全风险
- 审查软件设计以验证是否符合安全要求和风险信息
- 验证第三方软件符合安全要求
- 在可行时重用现有的、安全可靠的软件，而不是复制功能
- 通过遵守安全编码实践创建源代码
- 配置集成开发环境、编译、解释器和构建流程以提高可执行安全性
- 审查和/或分析人员可读代码以识别漏洞并验证是否符合安全要求
- 测试可执行代码以识别漏洞并验证是否符合安全要求
- 将软件配置为具有默认安全设置

应对漏洞

- 持续识别和确认漏洞
- 评估、确定优先级和修复漏洞
- 分析漏洞以确定其根本原因

审计的三个视角

第一方审计

由组织内部或直接委托给第三方进行的审计活动。这种审计通常由组织内部的内部审计部门或者专门的合规团队执行，旨在评估组织自身的合规性、风险管理和内部控制制度。第一方审计通常涉及对组织的财务报告、运营流程、合规性和风险管理等方面的审计活动。

在软件供应链安全领域，第一方审计可能涉及对组织内部的软件开发流程、安全控制措施、供应商管理和风险评估等方面的审计活动。这有助于组织了解自身在软件供应链安全方面的现状，识别潜在的风险和问题，并采取相应的措施加强安全管理和保护。

第二方审计

第二方审计通常指的是由外部实体或组织内部其他部门进行的审计活动。在软件供应链安全领域，第二方审计可能涉及组织内部不同部门之间的相互审计，或者由组织委托给其他组织或实体进行的审计活动。

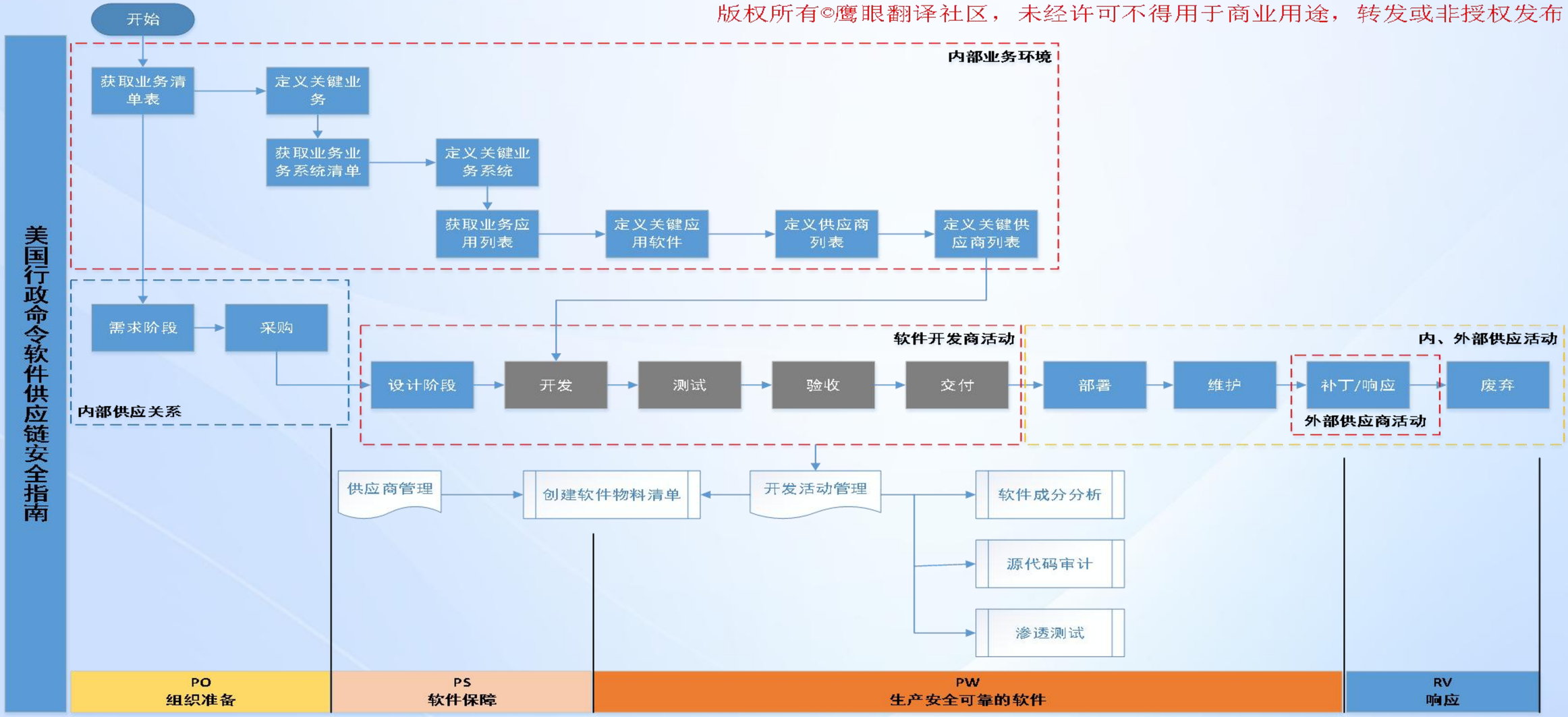
第三方审计

第三方审计是由独立于被审计组织和审计机构之外的独立实体进行的审计活动。在软件供应链安全领域，第三方审计通常由专业的安全审计公司、认证机构或独立的审计团队执行。这种审计活动旨在对软件供应链的安全性、合规性和风险管理进行独立的评估和验证。

04

软件供应链安全审计思路

软件供应链安全审计思路



SSDF框架

版权所有©鹰眼翻译社区，未经许可不得用于商业用途，转发或非授权发布

定义组织关键业务

商业组织	国家关键信息基础设施
财务损失（包含直接损失和间接损失） 社会影响 法律责任（含合同、个人隐私） 企业形象	国家安全　法律责任 社会稳定　人身安全 经济影响　公众利益 国计民生　个人损害

业务名称	业务简介	功能列表	业务部门	开发商	开发时间	等保级别	RTO	RPO

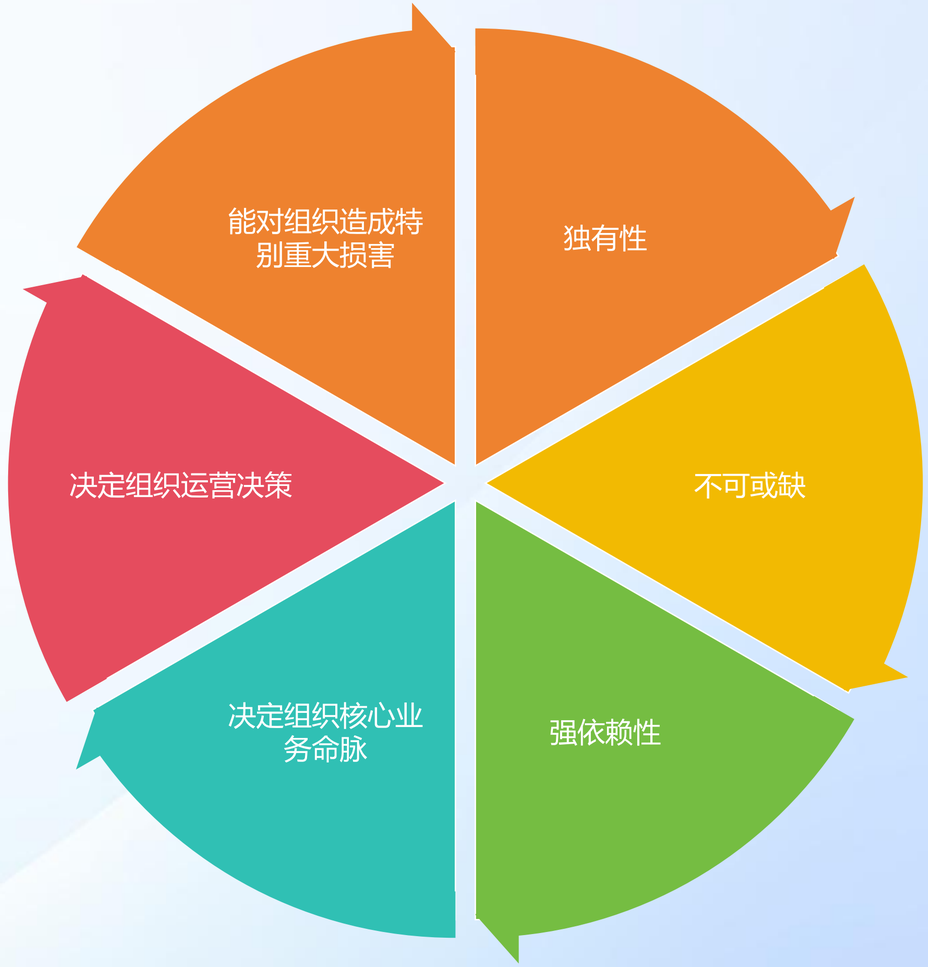
- 关键业务是指组织或企业的主要经营活动，这些活动对于实现企业使命和目标至关重要。关键业务通常包括产品或服务的开发、生产、销售、营销、客户服务等方面。企业需要将资源和精力集中在关键业务上，以确保业务的持续发展和成功。
- 评价关键业务的指标可以从两个层面讨论；

定义组织关键功能/组件

- 业务不是单一的，业务平台化后，业务功能比系统化，也就意味着，一个业务系统可能会有多个独立的业务子系统构成；

定义组织关键供应商

- 关键供应商是指在供应链中起着重要作用，对企业业务和生产具有重要影响的供应商。这些供应商通常提供关键零部件、原材料或服务，对企业的生产和运营具有重要影响。
- 关键供应商的选择和管理对企业的稳定运营和业务发展至关重要。企业需要对关键供应商进行风险评估和供应链管理，确保其稳定供应和质量可控。同时，建立良好的合作关系和供应商管理体系，能够有效降低供应链风险，保障企业的生产和运营。



定义审计深度与广度


N级供应关系管理
二级供应关系管理
一级供应关系管理
深度
需求
采购
设计
编码
测试
验收
交付
部署
维护
补丁/响应
废弃
采购商视角
（第一方视角）
软件开发商审计
（第二方视角）
采购商视角
（第一方视角）
软件开发商审计
（第二方视角）
采购商视角
（第一方视角）
综合审计
广度

软件供应链审计的两个平面

供应关系

- 采购商
- 开发商
- 供应商

生命周期

- 需求
- 采购
- 设计
- 编码
- 测试
- 验收
- 交付
- 部署
- 运行
- 补丁/响应
- 废弃

软件供应链安全审计活动-采购商平面1

采购商平面1

审计类型：第一方审计
生命周期：需求、采购、验收、部署、废弃
涉及部门：需求部门、采购部门、ICT部门、网安部门
审计手段：文件审核、访谈
审计依据：《中华人民共和国网络安全法》《关键信息基础设施保护条例》《网络安全审查办法》、网络安全等级保护相关标准
审计要点：
需求部门-需求文件（是否包含安全需求）
采购部门-采购活动管理、采购组织、采购流程、供应商背景调查及审核、服务人员审核、采购合同审核（重点有关软件代码归属权，开发模式及补丁/应急响应条款）

采购商平面2

ICT部门-运维管理、第三方账号管理、第三方访问控制管理、远程连接管理、补丁管理、变更管理、事件管理、问题管理、应急响应管理
网安部门-三同步（同步规划-需求文件、设计文件；同步建设-开发手册；同步使用-运维管理）、软件安全性测试、软件安全性验收、应急响应管理、威胁情报共享

采购商（客户）最佳实践

#SSDF	开发商	供应商	采购者
PO.1	2.2.3安全开发实践	2.1.1定义软件安全检查的标准	
PS.1	2.2.1.1源代码管理检查过程 2.2.1.4代码评审 2.2.6外部开发扩展 2.3.2选择与整合 2.4.1构建链利用 2.5.3分布式系统的安全	2.2.1保护所有形式的代码免受未经授权的访问 2.2.2提供验证软件发布完整性的机制（PS.1，PW.9）	
PS.3	2.2.1.1源代码管理检查过程 2.2.1.2自动和手动动态和静态安全漏洞扫描 2.3.2选择与整合 2.3.3从已知且值得信赖的供应商处获得组件 2.4.1构建链利用	2.2.3归档并保护每个软件版本	
PW.1	2.3.2选择与整合	2.3.1设计软件以满足安全要求	
PW.3	2.2.3安全开发实践 2.3.2选择与整合 2.3.3从已知且值得信赖的供应商处获得组件 2.3.4组件维护 2.3.5软件材料清单（SBOM）	2.3.2验证第三方软件是否符合安全要求	2.1采购/购买（1）需求定义建议控制（viii）（viii） 2.2部署（6）（2）测试-功能（c）建议控制（ii）验证SBOM中的内容 2.2部署（6）部署（3）承包/建议控制（v）（viii）（ix）（x）

采购商（客户）最佳实践

#SSDF	开发商	供应商	采购者
PW.6	2.2.3.2使用不安全的开发构建配置 2.4.1构建链利用	2.3.3配置编译和构建过程	
PW.7	2.2.1.4代码评审 2.2开源管理实践 2.2.6外部开发扩展 2.3.2选择与整合 2.3.3从已知且值得信赖的供应商处获得组件	2.3.4评审和/或分析人类可读代码	
PW.8	2.2.1.3回归测试自动化的夜间构建 2.3.2选择与整合 2.4.1构建链利用	2.3.5测试可执行代码	
PW.9	2.2.3.2使用不安全的开发构建配置 2.4.1构建链利用	2.2.2提供验证软件发布完整性的机制（PS.1，PW.9） 2.3.6默认情况下，将软件配置为具有安全设置	
RV.1	2.3.4组件维护 2.4.1构建链利用	2.4.1持续识别、分析和补救漏洞	

客户组织相关性

#	依赖项
1	产品的SBOM（或类似的软件物料清单工件）
2	用于产品更新的SBOM（或类似的软件物料清单工件）
3	用于产品升级的SBOM（或类似的软件物料清单工件）
4	产品分发包的可验证完整性（例如散列/签名）
5	产品更新的可验证完整性（例如散列/签名）
6	产品升级的可验证完整性（例如散列/签名）
7	供应商产品分销系统/方法基础设施的可验证完整性（如散列/签名）
8	分发包中产品组件的可验证完整性（例如散列/签名）
9	网络安全的自我认证工件——其开发过程和支持其产品开发的基础设施的卫生（见工件附录）自我认证由负责官员或高管签署
10	供应商关于从评估到交付产品期间对功能、漏洞和支持的所有更新和修改的通知
11	供应商提供的记录地理位置、供应商所有权/控制权、DUNS（如适用）、过去业绩等属性的工件
12	供应商提供的记录属性的工件，如可用地理位置、供应商所有权/控制权、DUNS、SBOM中确定的第三方供应商的过去业绩
13	供应商发送的工件将采用标准格式（例如SBOM）
14	供应商关于供应商所有权、地理位置和供应商、供应商和第三方控制权变更的通知
15	供应商关于网络事件、调查和缓解措施以及交付时对产品或产品开发环境的任何影响的通知
16	供应商关于网络事件、调查和缓解措施以及采购后对产品或产品开发环境的任何影响的通知（支持和维护期间）

开发人员组织相关性

#	依赖项
1	提供客户的问题
2	根据需要提供给定的哈希
3	SDLC政策和程序
4	安全架构，高级设计
5	经过代码/安全培训的有资格的团队组成
6	独立QA个人/团队
7	独立安全审计个人/团队
8	带存储库的开源评审委员会（OSRB）
9	产品发布管理/资源
10	SBOM

#	依赖项
11	开发位置和信息
12	第三方SBOM
13	第三方许可
14	发布说明（详细说明已修复的漏洞）
15	漏洞通知
16	向客户发布更新和修补程序，以解决产品中发现的新漏洞或弱点
17	成功的要求和标准
18	隐含的行业安全要求
19	提供操作环境中的问题，获取更新和修补程序
20	用户的漏洞通知和报告

软件供应链安全审计活动-开发商平面

- **审计类型：**第二方审计
- **生命周期：**设计、编码、测试、编译、验收、部署、补丁/响应
- **涉及部门：**软件开发商
- **审计手段：**文件审核、访谈、技术验证、场地查验
- **审计依据：**《关键信息基础设施保护条例》；软件开发商已有的开发管理准则，如：CMMI、SDLC；行业最佳实践NIST SSDF

软件供应链安全审计活动-开发商平面-审计要点1

- **供应商管理要求**
  - 软件开发活动相关管理文件；
  - 软件开发项目相关过程文件，包括但不限于：A.可行性分析(研究)报告；B.　　软件(或项目)开发计划；C.软件需求规格说明；D.接口需求规格说明；E.系统/子系统设计(结构设计)说明；F.软件(结构)设计说明；G.接口设计说明；H.数据库(顶层)设计说明；I.(软件)用户手册；J.操作手册；K.测试计划；L.测试报告；M.软件配置管理计划；N.软件质量保证计划；O.开发进度月报；P.项目开发总结报告；Q.软件产品规格说明；R.软件版本说明等；依据：GB/T 8567-2006 计算机软件文档编制规范
  - 代码库管理：
    - 文审：代码库管理相关制度
    - 技术验证：代码库代码完整性检测、入库代码流程管理、抽查代码库代码

软件供应链安全审计活动-开发商平面-审计要点2

- **供应商管理要求**
  - 开发环境管理-现场查看
  - 开发工具管理，包括但不限于：开发终端、云终端、编码工具，测试工具，编译工具；-访谈、现场查看，技术验证
  - 保密协议
- **开发人员管理要求**
  - 开发人员列表
  - 开发人员能力证明
  - 开发人员安全意识教育-访谈、测试
  - 个人背景调查及保密协议

软件供应链安全审计活动-开发商平面-审计要点3

- **设计阶段-**
  - 设计文件与需求文件的覆盖率；-依据《网络安全法》三同步要求
  - 基于威胁建模的设计活动
  - 合规性安全功能设计
- **编码阶段**
  - 第三方代码和组件的引入管理
  - 软件安全编码手册和安全编码实践
  - 不良好的硬编码IP和令牌的行为
  - 维护钩子
  - 特权功能与特权账号
  - UML应与设计文件一致
  - 版本管理
  - 软件物料清单
    - 软件物料清单（SBOM）包含构建软件中使用的各种组件的详细信息和供应链关系的正式记录。软件开发人员和供应商通常通过组装现有的开源和商业软件组件来创建产品。SBOM 列举产品中的这些组件。

软件供应链安全审计活动-开发商平面-审计要点4

- 软件物料清单示例：

数据字段	描述
供应商名称	创建、定义和标识组件的实体的名称。
组件名称	指定给原始供应商定义的软件单元的名称。
组件的版本	供应商使用的标识符，用于指定先前确定版本的软件更改。
其他唯一标识符	用于标识组件或用作相关数据库的查找关键字的其他标识符。
依赖关系	描述上游组件X被包括在软件Y中的关系。
SBOM数据的作者	为该组件创建SBOM数据的实体的名称。
时间戳	SBOM数据汇编的日期和时间记录。

软件供应链安全审计活动-开发商平面-审计要点5

- **软件成分分析**
  - 软件成分分析是指对软件的各个组成部分进行分析和研究，包括软件的代码、库文件、配置文件、文档等。通过软件成分分析，可以了解软件的结构和功能，发现潜在的问题和安全隐患，提高软件的质量和可靠性。
- **软件成分分析通常包括以下内容：**
  - 代码分析：对软件的源代码进行分析，包括代码的结构、逻辑、算法等方面，以及代码中可能存在的错误和漏洞。
  - 依赖分析：分析软件所依赖的外部库文件、组件和服务，以及它们之间的关系和影响。
  - 配置文件分析：分析软件的配置文件，包括配置参数、环境变量、权限设置等，以及它们对软件行为的影响。
  - 文档分析：分析软件的相关文档，包括用户手册、技术文档、设计文档等，以了解软件的功能和使用方法。
  - 软件成分分析可以帮助软件开发者和测试人员发现软件中的问题和潜在风险，及时进行修复和改进，提高软件的质量和可靠性。同时，也可以帮助用户了解软件的特性和使用方法，提高软件的易用性和用户满意度。

漏洞编号	漏洞简介	发布时间	风险等级	所属CWE	利用难度	漏洞分数	影响的组件信息						修复方案
							组件名称	版本	所属语言	作用域	依赖方式	代码位置	
SZ-2021-29933	暂无描述	2021-01-20	中危	CWE-Unknown	中	7.5	ejs	2.7.4	JavaScript	dev	间接依赖	chbn.20230619	方式1：【升级版本】pkg:npm/ejs 升级v3.1.7(包含)以上版本

软件物料清单Vs.软件成分分析

软件物料清单	软件成分分析
• 软件物料清单是对软件中使用的各种组件、库文件、第三方软件、开源软件等的清单列表。 • 它记录了软件中所有的组成部分，包括其版本、许可证信息、依赖关系等。 • 主要用于安全性和合规性管理，以追踪软件中使用的第三方组件和开源软件的版本、漏洞信息、许可证信息等。	• 软件成分分析是对软件内部结构、功能、依赖关系等进行分析的过程。 • 它包括对软件的源代码、依赖的库文件、配置文件、文档等进行分析，以了解软件的构成和行为。 • 主要用于发现软件中的问题和潜在风险，了解软件的特性和使用方法，提高软件的质量和可靠性。
• 关注于软件中使用的各种组件和相关信息的清单列表，以支持安全性、合规性和供应链管理	• 关注于对软件内部结构、功能和行为的分析，以支持软件质量管理和用户使用

软件供应链安全审计活动-开发商平面-审计要点6

测试阶段

- 测试报告或记录，包含单元测试、集成测试和验收测试
- 测试环境
- 测试人员
- 测试工具
- 测试用例
- 样本抽测

软件供应链安全审计活动-开发商平面-审计要点7

编译阶段

- 使用最新版本的编译器、解释器和构建工具。
- 在部署或更新编译器、解释器和构建工具时遵循变更管理流程，并审核工具的所有意外变更。
- 定期验证编译器、解释器和构建工具的真实性和完整性。

软件供应链安全审计活动-开发商平面-审计要点8

验收阶段

- 验收计划
- 验收报告
- 确证：需求-设计-功能实现一致

软件供应链安全审计活动-开发商平面-审计要点9

部署阶段

- 软件安全配置手册
- 基于云环境下的软件部署与配置管理
- 软件部署授权管理
- 与软件部署相关的配置管理、变更管理
- 部署后对测试页面，测试账号，特权账号等相关信息的删除和处理

补丁/响应

- 开发商管理补丁流程、版本号管理
- 开发商软件漏洞识别、分析、修复能力和补救计划

软件供应链安全审计活动-供应商平面

组织

- 定义软件安全检查标准

保护软件

- 保护所有形式的代码免受未经授权的访问
- 验证软件版本完整性的机制
- 归档和保护每个软件版本

生产安全可靠的软件

- 设计软件以满足安全要求
- 验证第三方供应商软件是否符合安全要求
- 配置编译和构建过程
- 审查和分析代码可读性
- 测试可执行代码
- 默认情况下，将软件配置为具有安全能力的设置

应对漏洞

- 持续识别、分析和补救漏洞

05

软件供应链安全审计的瓶颈

软件供应链安全审计的瓶颈

06

软件供应链安全治理思考

软件供应链安全治理思考

如何有效落实“同步规划、同步建设、同步使用”的立法原则

- 软件供应链管理组织如何建立，完善软件供应活动的相关制度流程
- 软件供应链相关标准和准则的制定
- 软件开发商如何规范开发行为、建立安全开发控制、提高开发人员的安全开发能力和水平
- 采购方如何识别和标准化开发活动的管理
- 采购方如何识别商业现货软件带来的风险
- 威胁情报共享机制必须建立和完善
- 第三方组件的使用将长期困扰软件供应链安全
- 源代码管理和非可视化供应关系将使软件供应链安全变得愈发复杂

OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

THANKS

感谢您的观看

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势