CNIS
云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

2024 WEST LAKE DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会 12th

软件供应链安全提升企业核心竞争力

林明峰

安恒信息 副总裁

CNIS
云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

目 录
CONTENTS

CNIS
云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

01

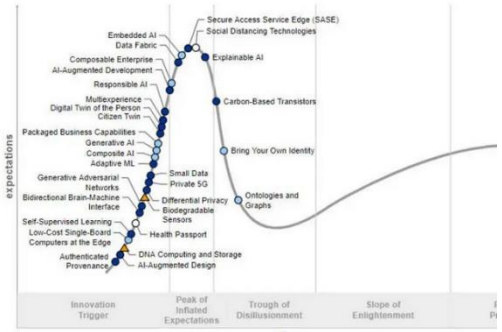
软件供应链安全四个趋势

软件供应链成为重要挑战

Gartner将软件供应链安全列为2023年的第二大威胁，并预测到2025年全球45%的组织将遭受一次或多次软件供应链攻击。

国际局势

全球局势不稳定性不确定性增加，加大的软件供应链安全风险。



技术趋势

数字化的发展和应用深入，会形成软件应用大爆发趋势。

国家战略

科技自立自强的战略迫切需要强健的软件供应链安全做保障。

开发模式

用开源组件构建应用的开发现状，会导致安全漏洞数量巨增。

软件供应链漏洞问题频发

- 伴随着上云大趋势，软件供应链的复杂度不断增加，软件供应链安全风险不断加剧，针对软件供应链薄弱环节的网络攻击随之增加，受地域政治等因素影响的断供案例频频发生，软件供应链成为影响软件安全的关键因素之一。

- 2015年，苹果公司的Xcode开发集成环境被植入恶意代码并在非官方渠道发布，事件影响用户数超过1亿。
- 2017年，勒索软件NotPetya利用供应链发起攻击，影响全球59个国家的政府、银行、机场等机构的系统。

- 2017年，黑客利用Equifax系统中未修复的漏洞发起攻击，导致了系统中大规模数据泄露。
- 2020年，SolaWinds遭到供应链攻击，包括美国关键基础设施、军队、政府等在内的超18000+客户受到影响。

Apache LOG4J™

- 2021年，Apache Log4j程序中发现了远程代码执行0Day漏洞，该漏洞号称“史诗级漏洞”，时至今日其影响力仍然巨大。

docker

- 2020年，云平台开源软件DockerEE和DockerHub受美国政策影响，禁止被列入实体清单的组织使用。
- 2022年，RedHat旗下的开源操作系统CentOS 8停止维护支持，CentOS 7也计划于2024年停止维护。

软件供应链安全的复杂性

引用信通院2023年软件供应链治理发布数据显示：

190

***平均每个项目引入组件数**

55

***平均每个项目缺陷组件数**

161

***平均每个项目存在漏洞数**

供应链系统容易受到来自外部和链条上各自实体内部不利因素的影响，就会客观地形成供应链风险

- 多环节协作
- 需求多样性
- 跨地域
- 环境复杂
- 多企业协作
- 安全能力发展不均
- 责任不清晰

各类因素交织，导致终端企业承受相关风险，但是却很难进行管理，也缺少相关理论和技术进行支持

软件供应链安全问题存在全生命周期

CNIS 云网基础设施安全国家工程研究中心 National Engineering Research Center of Cloud and Network Infrastructure Security

■ 运营商软件涉及的供应商、集成商等合作方众多，供应链复杂。供应链安全挑战集中在供应链安全风险评估定责、以及供应商管理、ICT资产管理、关键核心技术依赖等方面。

供应链安全风险评估及追溯定责

- 供应链复杂：运营商供应链涉及硬件、软件、集成、开发、交付、运维、服务等多种类产品供应链条，风险多样且难以甄别。
- 政策面支持：尚缺乏可直接参考的法律、法规及标准规范。

生产商/供应商/集成商

- ✓ 厂商产品、服务资质评估
- ✓ 厂商品牌、信誉可信度评估
- ✓ 供应商产品管理、人员管理
- ✓ 集成商人员管理、服务管理
- ✓ ……

BOM / SBOM 管理

- ✓ BOM物料台账管理
- ✓ SBOM物料台账管理
- ✓ 物料清单供应链风险识别与评估
- ✓ 供应链风险防护与处置
- ✓ 供应链安全应急响应
- ✓ ……

关键核心技术过程管理

- ✓ 软件代码规范性管理
- ✓ 软件开发过程规范管理
- ✓ 软件开发环境与工具
- ✓ 软件开源软件依赖
- ✓ 软件开发人员管理
- ✓ ……

02

软件供应链安全建设四个要点

软件供应链安全解决思路

CNIS 云网基础设施安全国家工程研究中心 National Engineering Research Center of Cloud and Network Infrastructure Security

软件供应链安全治理框架

合规要求：法律法规 | 国家标准 | 行业标准 | 防范应用漏洞 | 关注开源风险 | 反APT技术栈

安全管理：制度 | 流程 | 人员 | 培训

技术服务：威胁 | 代码 | 攻防 | 应急

1. 采购阶段

- **安全管理-供应商来源控制**
  1. 供应商资质审查与可信分级
  2. 供应商安全监督管理规范
  3. 供应商安全考核指标
  4. 供应流程风险分析
  5. 供应商服务与应急处置

2. 集成开发

- **安全管理-SDL**
  1.外包人员开发管理规范
  2.开发环境和工具安全管理规范
  3.安全开发管理体系
  4.安全开发流程建设
  5.安全开发知识体系建设
  6.安全开发训练体系建设
- **安全工具-DevSecOps**
  1. 安全开发一体化平台
  2. 软件成分分析工具SCA
  3. 静态安全审计工具SAST
  4. 应用交互式测试工具IAST
  5. 威胁建模分析工具
  6. 黑盒安全扫描工具DAST

3. 软件交付

- **安全管理-验收**
  1. 采购软件安全验收规范
  2. 软件安全部署规范
- **技术服务-检测**
  1. 系统上线前安全评估
- **安全工具-检测**
  1. 供应链安全管理
  2. 软件成分分析工具SCA
  3. 静态安全审计工具SAST
  4. 应用交互式测试工具IAST
  5. 黑盒安全扫描工具DAST
  6. 容器环境安全检测工具

4. 安全运营

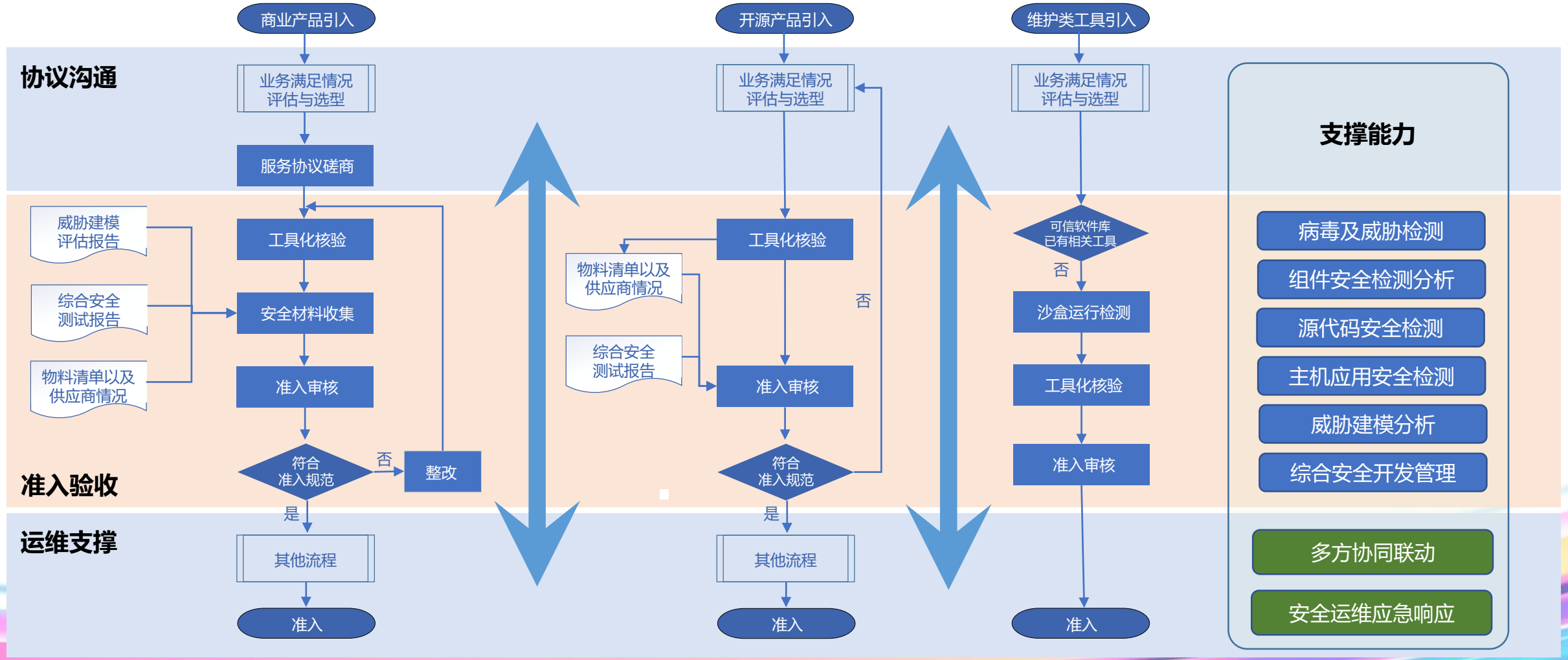
- **安全管理-运营**
  1. 安全运营体系建设
- **安全工具-监测**
  1. 软件成分分析工具SCA
  2. 应用安全防护系统RASP
  3. 安恒全链路安全运营工具套装
- **技术服务-运营**
  1. 安全运营服务
  2. 渗透测试服务
  3. 常态化红蓝对抗
  4. 应急响应服务
  5. 软件供应链安全防护有效性验证服务

安全工具：平台 | STAC | SAST | SCA | IAST | DAST | 监测工具

以合规为基础，以安全为追求·持续保障企业软件供应链安全

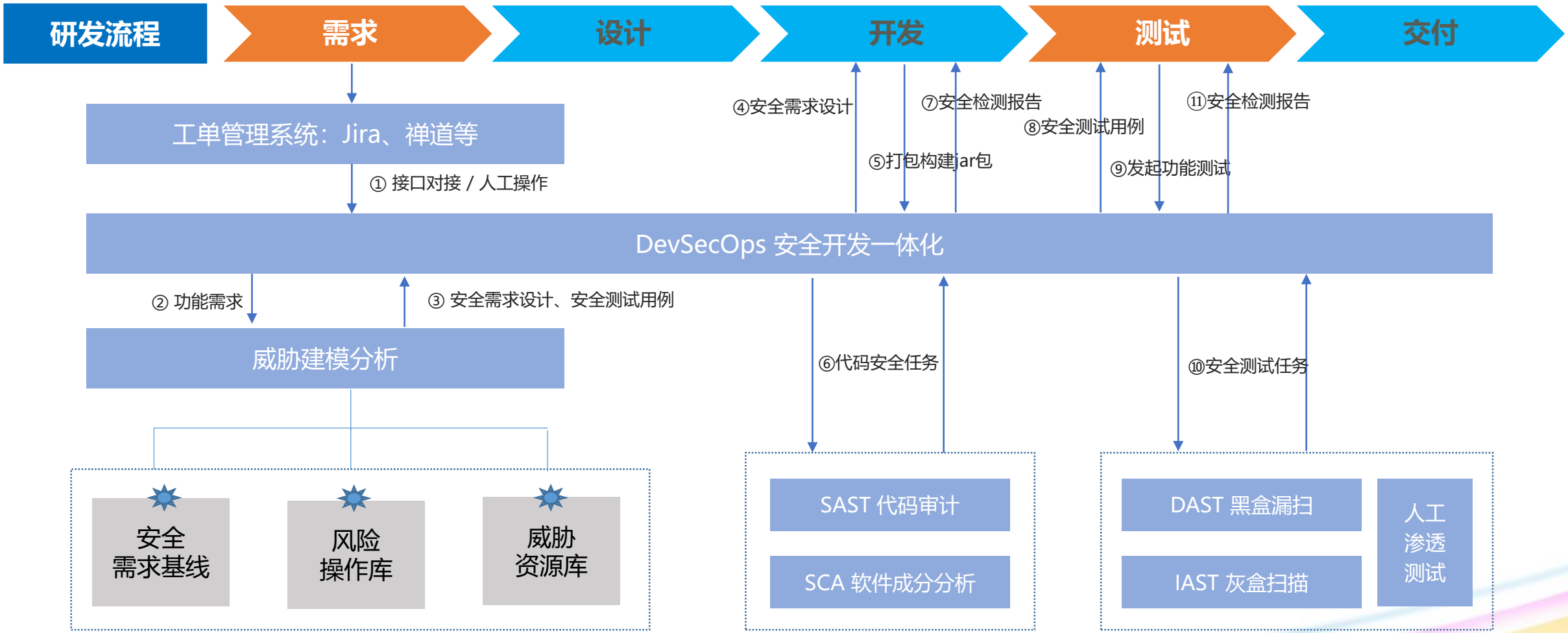
采购引入阶段

■软件产品采购引入时，需要根据管理现状框架，将企业策略、供应链安全控制要求与程序层的设计实现融入在整体安全管理体系中，流程上要求供应商出具产品安全测试报告，包括但不限于源代码检测报告、组件成分分析报告、漏扫报告等，根据产品重要程度通过工具进行安全抽检工作，保证产品安全可控性，做到风险来源控制。



集成开发阶段

■ 软件产品集成开发阶段，在研发流程的全过程中，可着重以需求和测试阶段作为两抓手主体切入，保障安全开发一体化推进。



➢ 行业安全需求标准基线

➢ 根据前期威胁建模提出的需求，将在研发与测试阶段通过SAST、SCA、IAST工具进行验证闭环。

应用交付阶段

■ 软件产品交付验收阶段，关键在于两大基线的建立：交付安全基线与验收安全基线。

应急响应与缓解预案

- 产品服务提供相关文档和工具处理相关的风险响应和缓解需要以及相关培训计划

漏洞和补丁管理机制

- 产品服务支持漏洞与补丁的修正与更新，并配备有相关的管理机制

变更和配置管理交付

- 归档产品/服务的配置管理文档，包括软件清单、配置清单、物料清单、相关安全报告、检测报告等

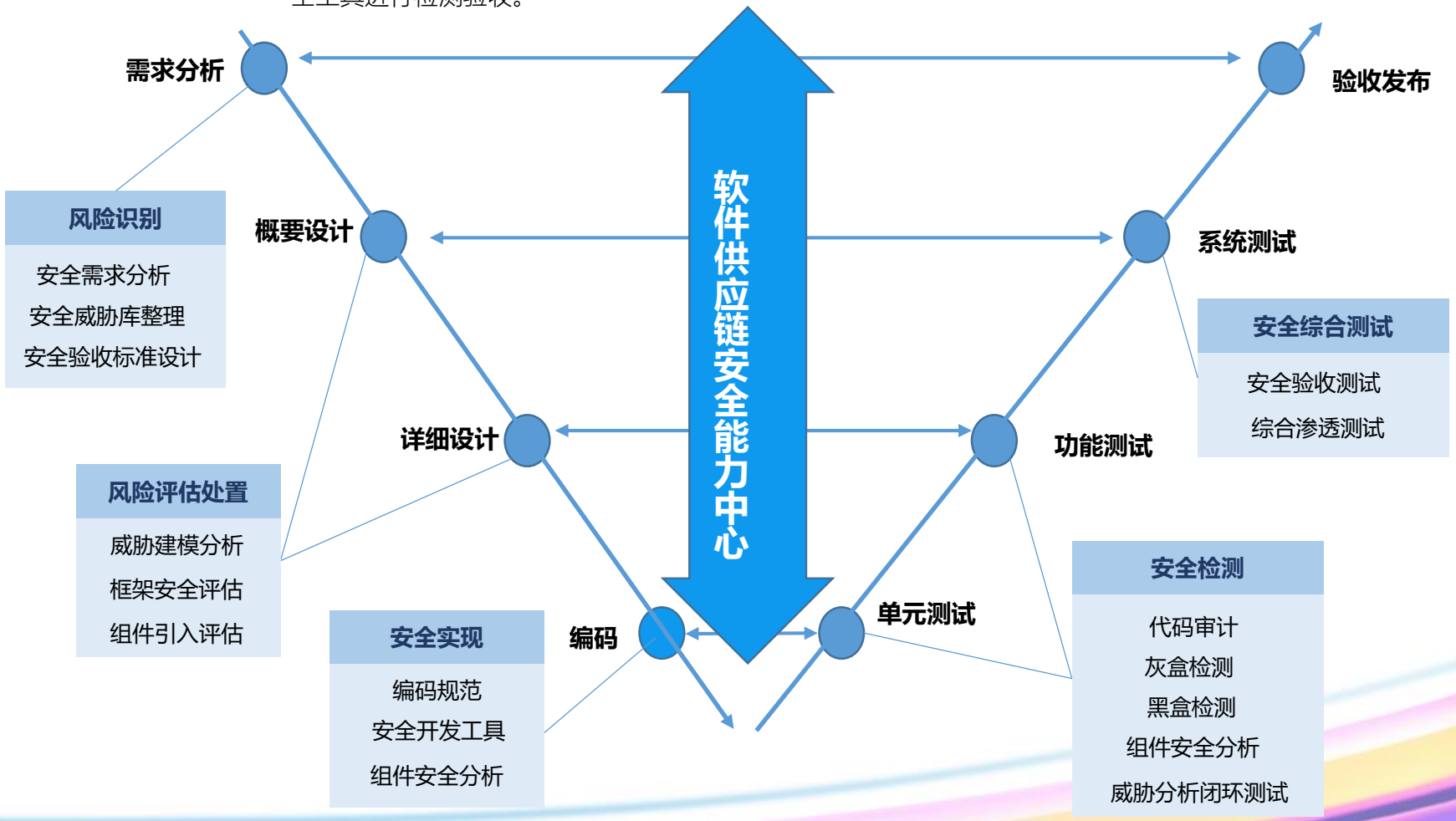
安全发布渠道和机制

- 产品服务通过可信渠道发布，包括专职人员以及可信第三方平台，提供自验证机制

安全交付基线

- 产品服务的交付符合相关的安全质量基准线，产品配置符合相关配置基线

- 以安全开发一体化为检测核心，建立产品研发全生命周期每个环节的**验收安全基线**，结合安全工具进行检测验收。



持续运维阶段

■软件产品持续运维阶段，**需要对发生在软件和软件补丁获取渠道的软件供应链安全事件、软件安全漏洞披露事件进行快速的安全响应**，控制和消除安全事件所带来的 安全威胁和不良影响，进而追溯和解决造成安全事件的根源所在。

软件供应链画像 + 纵深防御防线建设

威胁情报	事件响应	入侵追踪和取证	业务应急恢复
供应链安全事件 软件安全漏洞披露事件 开发工具污染 ……	风险临时响应措施构建 风险排查机制和能力 风险处置 ……	入侵追踪 犯罪取证 事后安全分析加固 ……	系统安全恢复 应用服务安全恢复 数据安全恢复 网络病毒灾难恢复 ……

安全运营平台能力、运营工具

人员、制度、体系

03 软件供应链安全核心能力

构建 1+N 的软件供应链服务安全体系

CNIS 云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

- ✓ 形成以**产品为核心，咨询服务、技术服务**为补充的软件供应链安全体系。
- ✓ 以**软件供应链安全平台**为核心
- ✓ 以**威胁建模平台、软件成分分析（SCA）、代码审计平台（SAST）、交互式安全检测（IAST）、明鉴安全扫描（DAST）**为检测工具链
- ✓ 以**应用运行时防护（RASP）**为核心防御手段
- ✓ 以统一防护策略贯穿整个流程

安全开发一体化平台

CNIS 云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

■ **安全开发一体化平台**，是基于Gartner提出的DevSecOps理念，将安全（Security）嵌入DevOps流程中，实现软件敏捷开发过程安全性能保障的功能性平台。其主要功能包括项目管理、资产及第三方组件管理、安全需求分析与设计平台、漏洞管理、集成工具以及知识库。

安恒安全开发一体化平台

安全设计/编码能力

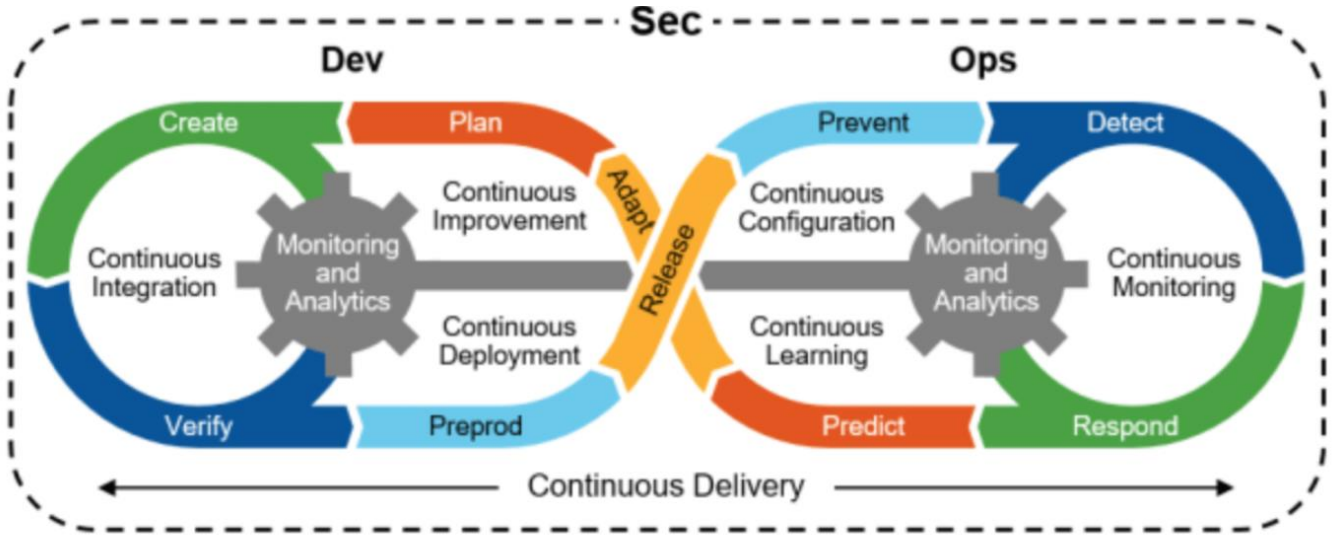
- 安全需求与设计（天璇）
- IDE安全插件
- 威胁分析
- ……

安全检测能力

- 源代码检测
- 动态分析安全测试
- 被动式应用安全测试
- 交互式分析安全测试
- 软件成分安全分析
- 镜像容器安全检测
- 安全配置检测 …

安全知识库

- 安全合规库
- 安全需求库
- 安全设计库
- 安全测试用例库
- 安全威胁库
- 漏洞/安全风险知识库
- 安全编码规范知识库 …



供应商管理：对软件供应商进行登记录入，从而进行管理，方便和资产相关联。

项目管理：对软件开发项目进行管理，使用工单插件实现工单项目和用户的查询、导入，并对项目的风险情况进行统计。

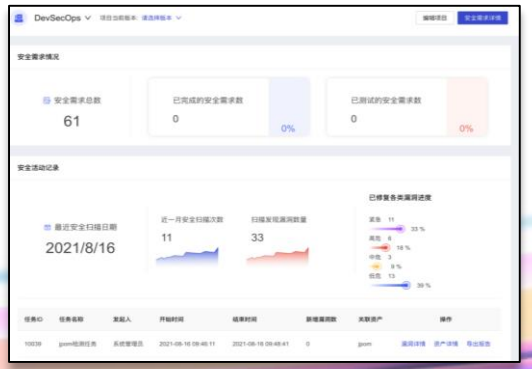
资产及第三方组件管理：管理开发项目的不同类型的资产（包括主机资产、代码资产、Web资产、App资产）以及资产依赖的第三方组件。

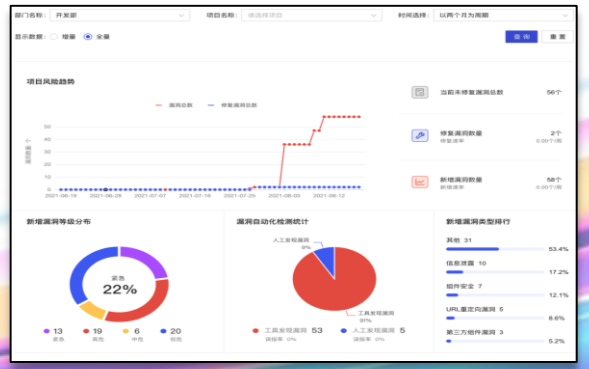
安全需求分析与设计模块：通过对网络威胁过程的分析和建模形成模板，输出针对具体功能业务的安全需求与设计，并提供相应的测试方案用于规范测试流程，解决在安全需求分析阶段的繁琐问题。

漏洞管理：在研发过程中引入安全检测能力，同时引入第三方风险组件库，通过定时性或周期性的安全扫描任务来检测漏洞并在漏洞库中统一管理。

集成工具：具备IDE插件、CI接口等。

知识库：具备各类知识库信息及安恒信息安全开发工具（SDK）、应用编程接口、使用指南。

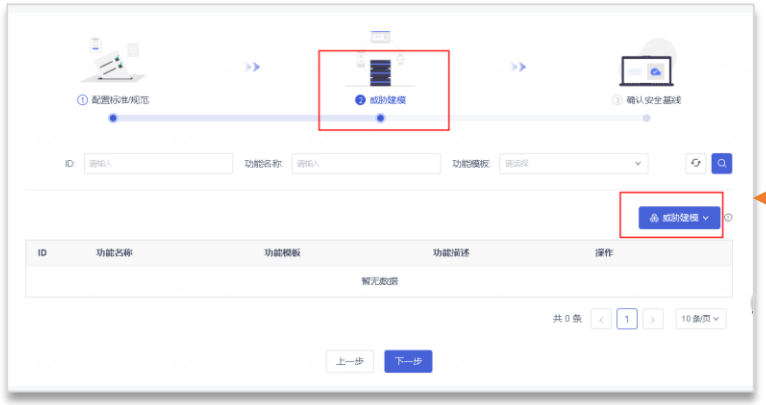




供应链威胁建模分析系统

CNIS 云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

■ **威胁建模平台**，根据实际项目背景、业务场景，输出**威胁清单、安全需求清单、安全需求测试用例**，解决威胁建模过程复杂、缺少安全专家、缺少安全测试人员和安全测试用例等问题。



威胁建模知识库具有最佳实践，等同于大量的威胁建模专家知识，根据建模历史不断丰富和沉淀，积累专家经验，复用正确的思路。

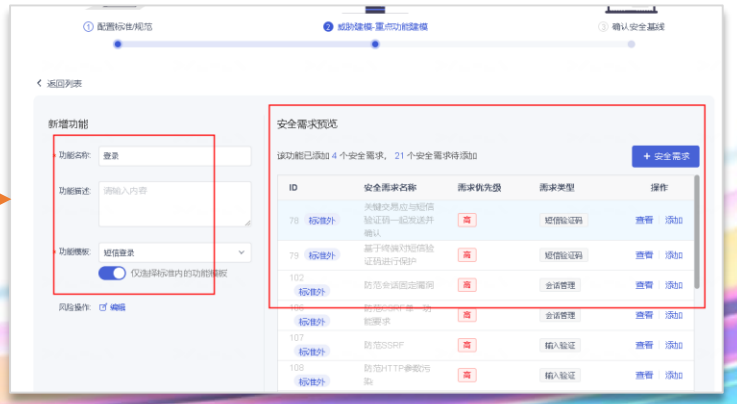
项目 → 问卷调查 → 威胁建模

威胁建模 → 批量功能建模
威胁建模 → 功能需求文档建模
威胁建模 → 核心功能建模

批量功能建模 → 输出安全基线
功能需求文档建模 → 输出安全基线
核心功能建模 → 输出安全基线

输出安全基线 → 开发部门
输出安全基线 → 测试部门

- 基于**业务场景**的轻量级的威胁建模工具进行威胁建模，下沉到具体业务功能或者接口，提供与安全需求对应的安全开发SDK，输出**准确的安全基线**；
- **10+ 项**业界领先的合规标准、可扩展的安全需求知识库
- 支持对接**Gitlab、Zentao、Jira**等工单系统，灵活调整基础模版，规范的安全需求变更和评审流程、权限管理
- **多维度**导出安全需求研发文档和测试文档
- 联动安全检测工具，实现**DevSecOps自动闭环**



运行时应用“防火墙”RASP

运行时应用自我保护RASP这一概念由Gartner于2012年提出， 是一种新型应用安全保护技术，它将主动防御能力“注入”到应用程序中，可以通过分析应用程序的行为和该行为的上下文，实时检测和阻断安全攻击，保护其不受恶意输入或行为的影响，使应用程序具备自我保护能力。

代码注入

RASP技术通过在应用程序运行时的进程中注入特定的保护代码，以实现实时监控和保护。

安全检测和拦截

RASP技术使用各种安全检测机制，如行为分析、规则引擎、机器学习等，对应用程序的行为进行实时监测和分析。当检测到异常行为或潜在攻击时立即采取拦截、告警等措施。

组件漏洞修复热补丁

可以自动下发组件漏洞修复热补丁，实现对组件风险的代码级加固防御，

代码上下文感知

RASP技术具有上下文感知能力，基于行为来精准识别攻击，能够分析请求、参数、调用栈、执行流程等信息，并提供受到攻击影响的相关代码调用堆栈。

实时保护

RASP技术能够实时响应和保护应用程序，对抗各种威胁和攻击。它可以防御常见的漏洞利用，如SQL注入、跨站脚本攻击、代码注入等，以及未知的攻击形式。

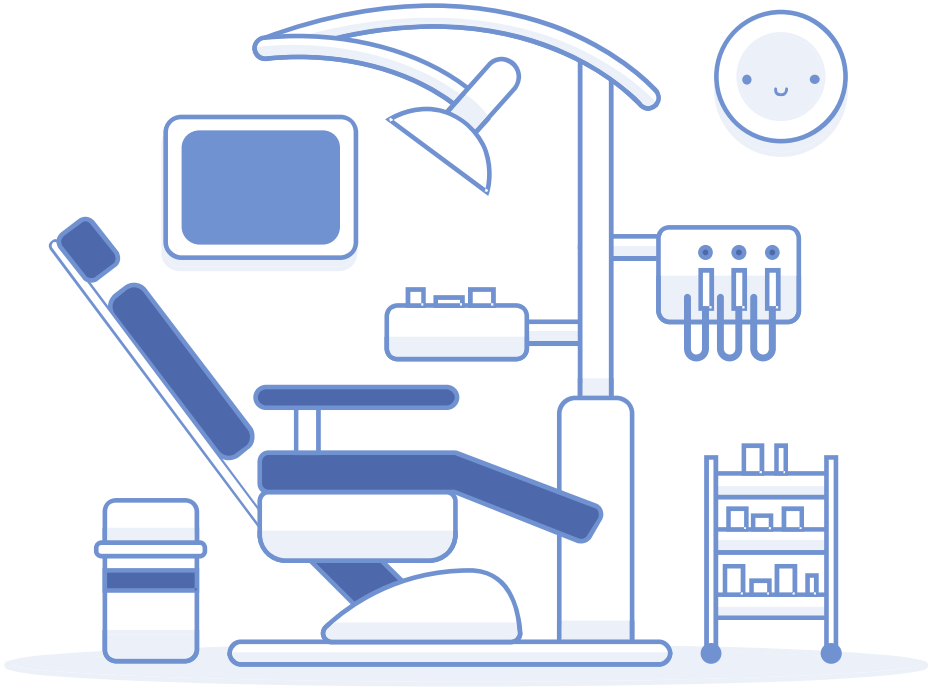
日志和报告

RASP技术可以生成详细的日志和报告，这些日志和报告可以用于安全审计、威胁分析和应急响应等方面。

04 关键新技术应用

软件供应链安全挑战

做**安全难**，
做**软件供应链安全管理更难**！



“亡羊补牢”不可取

软件供应链应用的安全手段往往在运维阶段介入，时间滞后，导致**漏洞发现晚**，研发人员对软件的**修复成本高**

安全左移难落地

软件开发流程缺乏**管理、技术、自动化工具**支撑，软件供应链安全规范管理**落地困难**

第三方应用难理清

软件供应商在开发过程中多**使用开源软件**，**仅交付制品的方式**导致安全性极不可控，未知开源软件带来巨大安全隐患

工具多误报高难治理

开发安全**工具种类多**，单点工具“各自为战”，工具**使用繁琐、误报高、运营成本大**，导致日常扫描结果无人把关

痛点难点“全解决”：AI +

CNIS 云网基础设施安全国家工程研究中心 National Engineering Research Center of Cloud and Network Infrastructure Security

恒脑AI，助力软件供应链安全平台，4 大核心能力实现，解放人力

AI+降低安全需求分析与设计活动成本

结合AI能力，**4个步骤**快速对研发需求文档进行**智能分析，大幅提升安全需求分析准确性**，降低对安全人员的依赖度，帮助研发人员理解、实现安全需求与安全设计。

IDE插件全方位辅助研发人员安全编码

结合AI能力，开发**全新IDE插件**，通过**安全漏洞与代码质量分析、代码片段释义、自动化编码**等核心功能，辅助研发人员进行安全编码。

恒脑

白盒误报和漏洞优先级判别引擎

结合AI能力，从漏洞分类标准、业务类型、利用可能性、资产重要程度、威胁严重程度等多维度对安全漏洞进行**智能评级，辅助研判**安全漏洞是否误报。

多工具漏洞去重提升修复效率

结合AI能力，打造多**工具漏洞去重模型**，对多款开源、商业化工具扫描结果，进行**集成和去重审计**，目前测试同类型检测工具漏洞去重**有效率最高可达90%。**

软件供应链安全体系成果

■ 软件供应链安全方案，建立基于软件全生命周期的可信供应链安全管理体系与机制，能够解决运营商企业在应对供应链安全风险时面临的技术挑战。

软件供应链安全

单点 → **全面**

在软件行业近年的不断技术迭代与产业发展中，逐步形成了复杂多元产品组合、技术体系融合、开发供应消费一体化的产业趋势。大量的新技术的引入，要求对软件风险防护的范围从单一产品上升到整个供应链层面，软件供应链安全风险贯穿软件产品整个生命周期，**安全视角从单点转向全面。**

总体效益价值

- **软件供应商透明化、增强软件可见性**
- **完善软件供应链安全商用风险管理，使用技术检测手段代替人工作业以实现降本增效**
- **减少发生安全事件时因供应链上游信息交互响应迟缓导致的影响面扩大**
- **提升多软件供应商安全管理效率，避免因供应商基数大而产生的管理、沟通成本激增**

谢 谢