


构建软件安全中心， 保障供应链安全

演讲人：徐帅健妮

单位名称：中国电信研究院

- 
- 01 数字时代的安全新挑战
 - 02 构建软件安全中心
 - 03 软件安全中心的实践

数字时代的安全新挑战

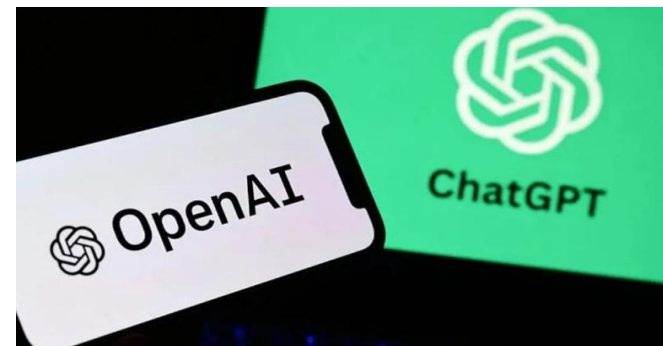
新型技术应用涌现，推动软件供应链的复杂度不断增加，针对软件供应链薄弱环节的网络攻击随之增加，受地缘政治等因素影响的断供案例频繁发生，**软件供应链成为影响数字时代软件安全的关键因素。**



- 2021年，抖音海外版TikTok的桌面平台直播软件TikTok Live Studio，因使用开源软件OBS的源代码，却未遵守GPL协议，在OBS项目组没有对抖音进行起诉维权的情况下，将桌面平台直播软件TikTok Live Studio下架。



- 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，SolarWinds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。



- 2022年，自俄乌事件爆发以来，陆续有300多家企业宣布断供俄罗斯，微软、英特尔、高通等科技巨头均宣布终止对俄服务。
- 2024年，OpenAI宣布阻止来自非支持国家和地区的API服务，其中包括中国内地、中国香港和澳门。

中国电信软件供应链安全现网问题

现网痛点：对软件引入源头的管控匮乏，对软件安全风险问题监控不足，对受影响资产的定位能力有限，治理受影响资产成本较高。

“理不清”

集团开发团队和软件资产数量庞大，涉及的业务范围广泛，在迭代和发布过程中，**尚未建立合适的软件引入机制**，导致无法理清软件的使用情况。

“看不见”

部分存量业务使用版本较低的开源组件，其中很多爆发过安全漏洞，但没有及时去更新。对于这些已知漏洞的风险隐患，**集团缺乏持续监控机制**，导致无法洞悉已有的风险隐患。

“找不到”

集团软件资产数量多，来源广，**尚未建立严格的资产管理机制**，无法快速定位受影响的软件资产，增加了溯源排查的难度，导致漏洞在供应链扩散。

“治不了”

部分省公司对漏洞影响范围以及受影响组件不够明确，缺乏成熟的治理机制，面临**缺乏软件供应链安全治理相关知识、技能和工具等问题**，导致风险缓解效率较低且手段粗犷。

77%的软件使用了开源组件

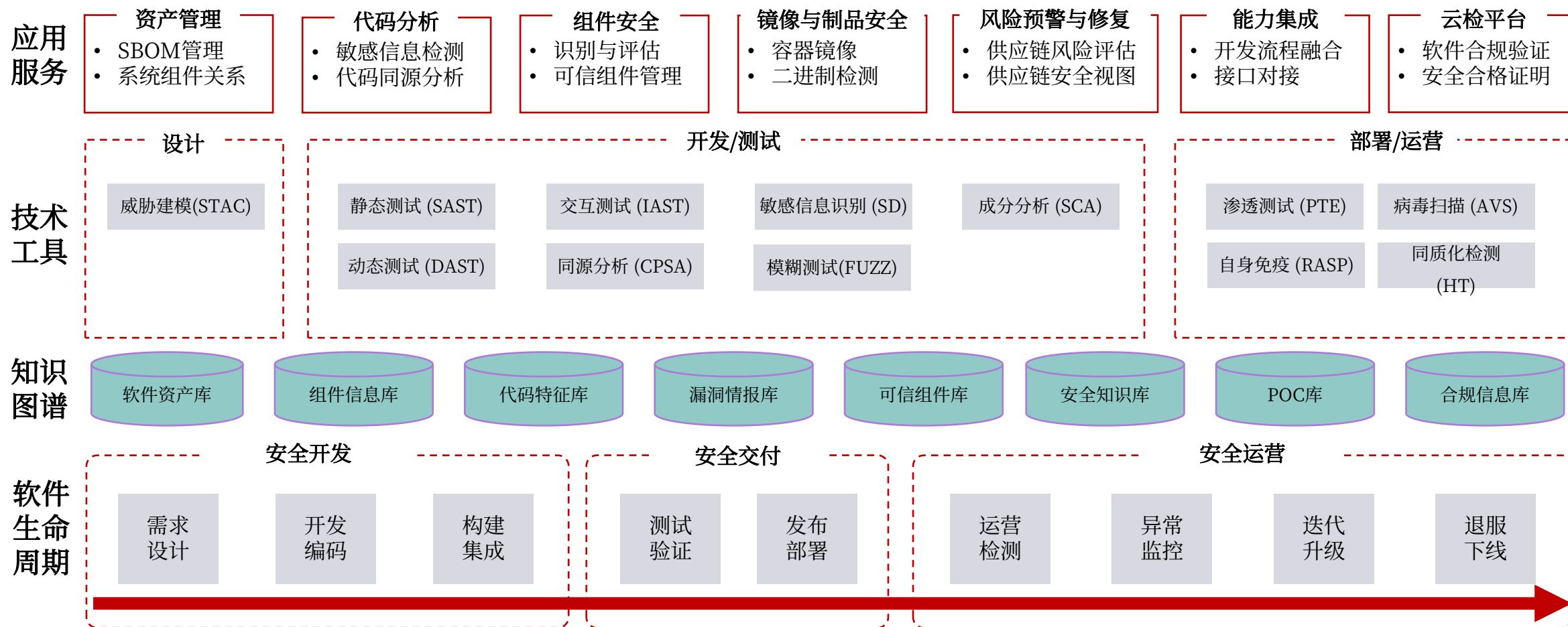
86%的自研软件中存在高危以上漏洞

57%的软件使用了高频超危风险组件

构建软件安全中心

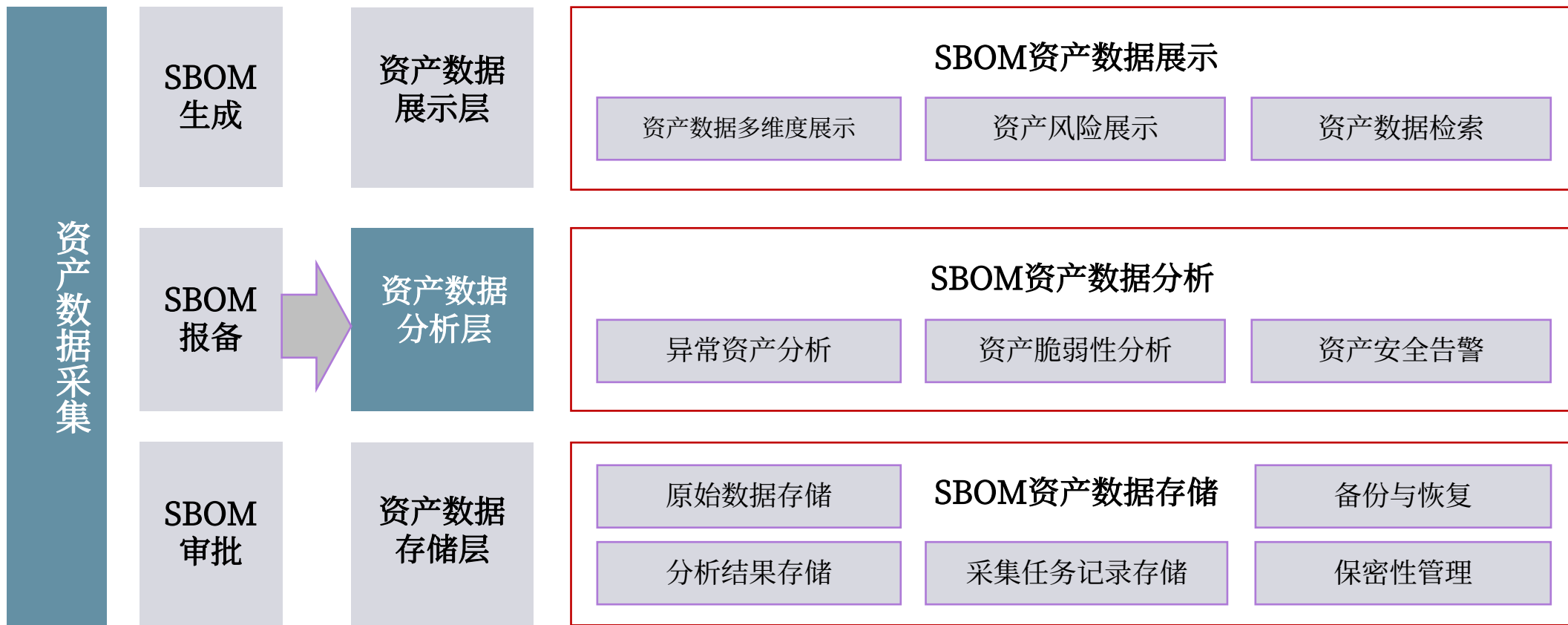
软件安全中心能力建设——能力架构

安全工具链应覆盖软件生命周期9个关键阶段



软件安全中心能力建设——软件资产管理

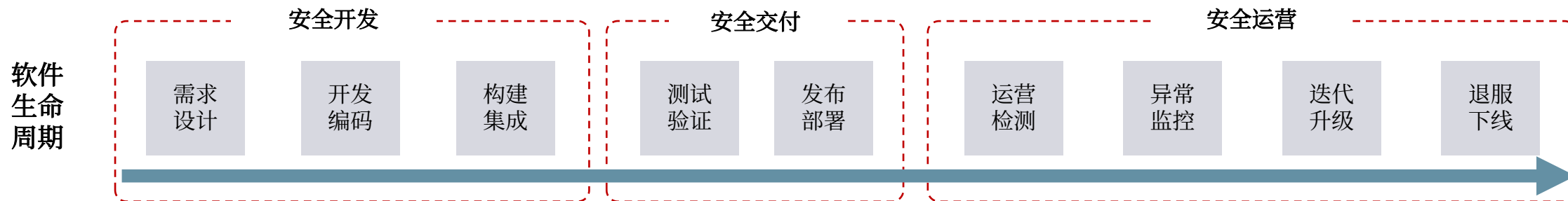
制定统一软件供应链准入标准，建立多级软件物料清单（SBOM）资产管理机制与SBOM资产管理平台，对SBOM进行有效的记录、跟踪和管理，覆盖外部采购系统及自主研发系统的软件供应链透明度问题，形成集团**全量业务统一供应链资产图谱**。



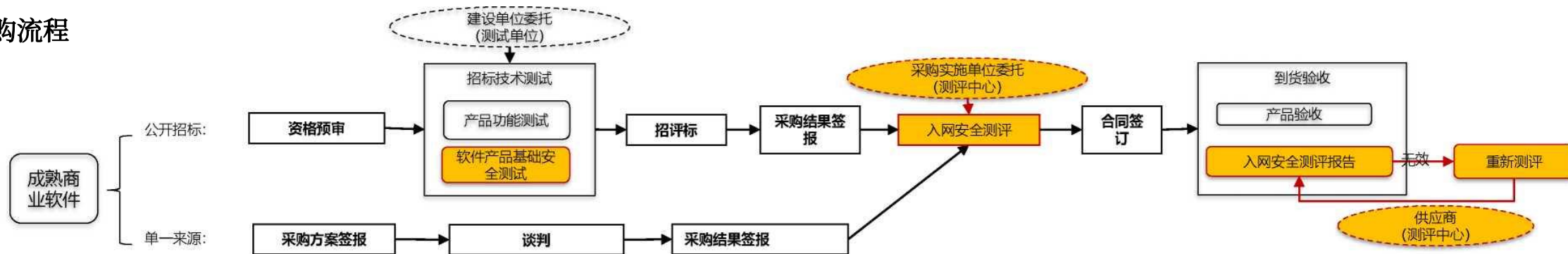
软件安全中心能力建设——软件安全检测

提供软件开发、交付、运营阶段全生命周期多维度安全检测能力，全面保障自研、商采、合作、开源软件供应链安全，有效强化软件资产安全管控。

自研流程

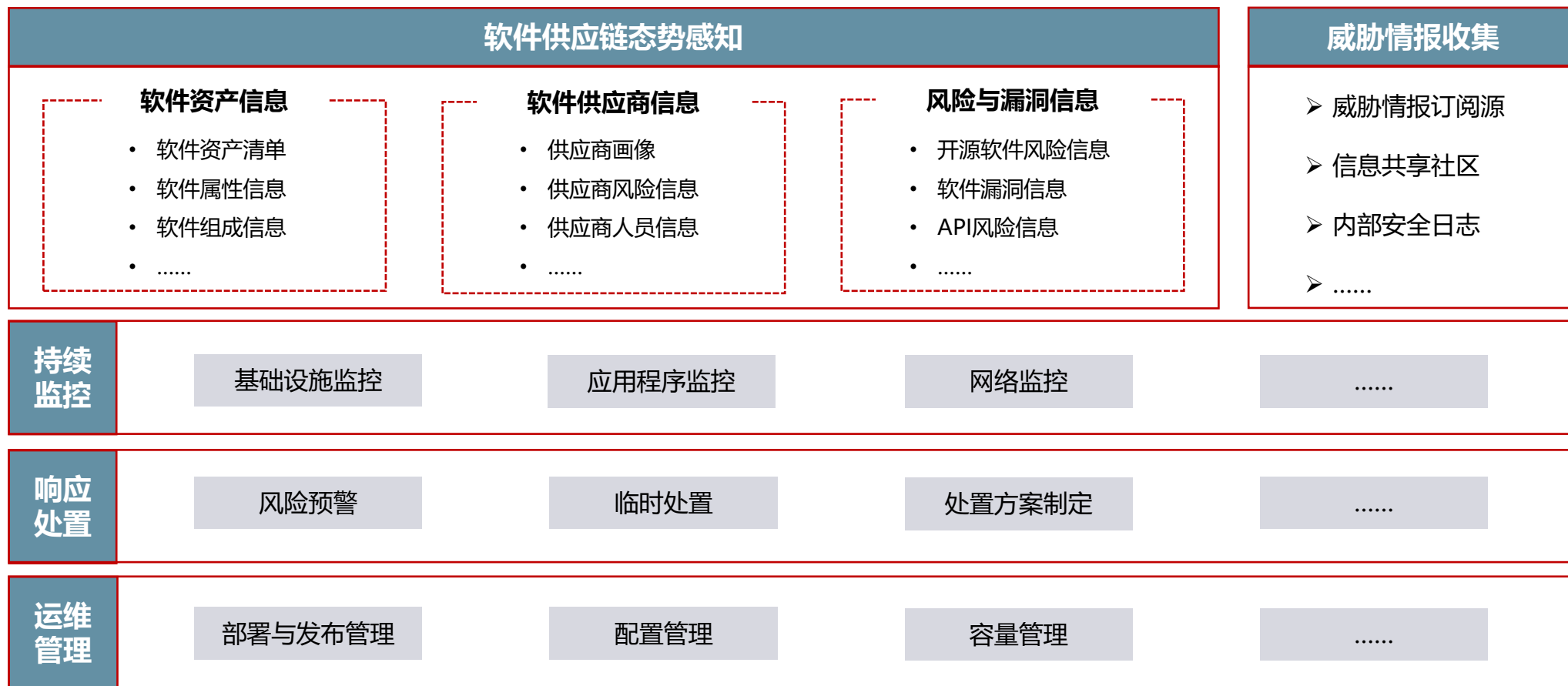


采购流程



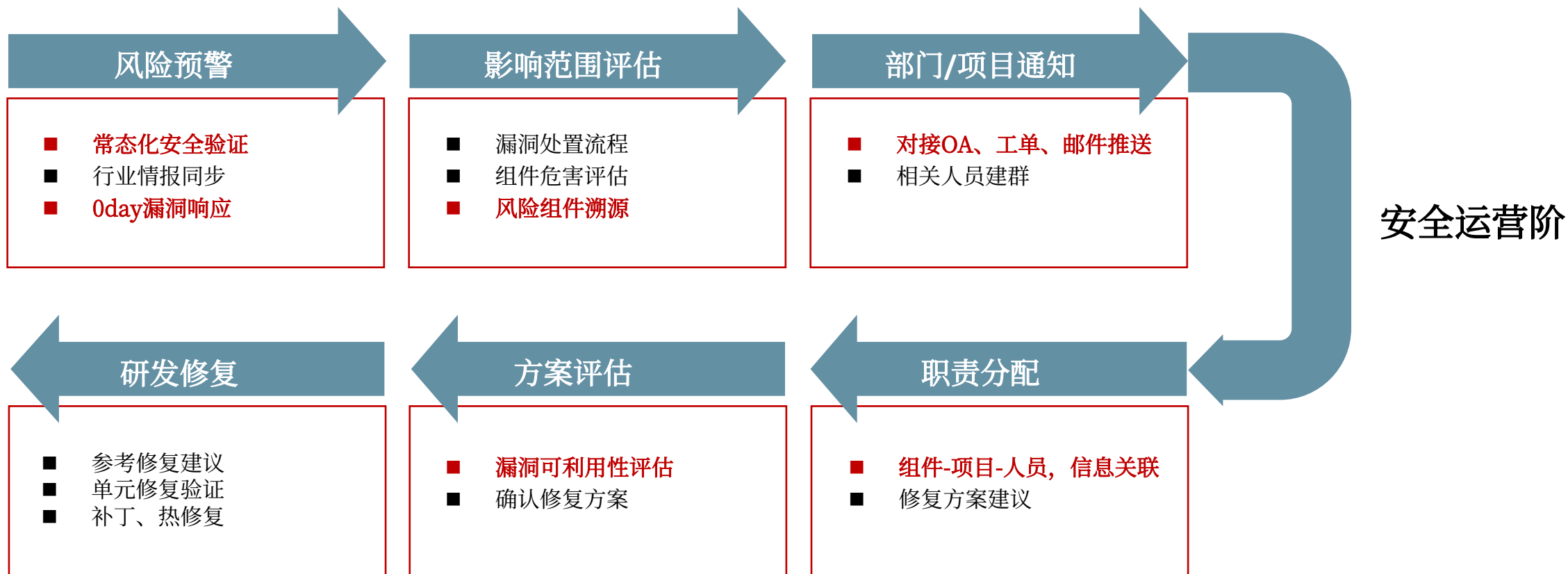
软件安全中心能力建设——软件供应链监测治理

全面监控软件供应链的安全态势并建立有效的威胁情报获取途径，形成面向软件供应链安全的**持续监控、响应处置和数据管理能力**，控制和消除安全事件所带来的安全威胁和不良影响。



软件安全中心能力建设——风险修复分析

通过软件成分分析、全量软件资产管理，打造安全风险预警机制。对资产信息变更进行有效的记录、跟踪和管理，**针对新发漏洞能快速定位业务系统，及时修复，降低系统风险。**

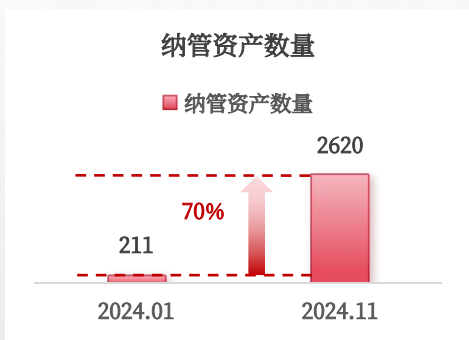


软件安全中心的实践

内部治理成效

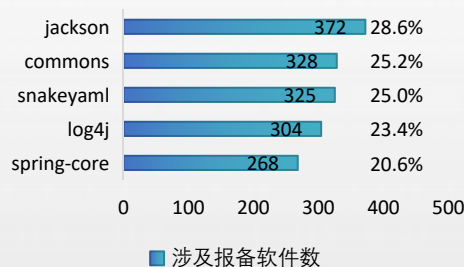
软件安全中心通过**软件物料清单（SBOM）管理**、**软件成分分析**、**供应链风险监测**、**风险修复分析**等核心能力，有效解决企业软件供应链安全治理**“理不清”**、**“看不见”**、**“找不到”**、**“治不了”**的难题。

- **问题1：“理不清”**；对集团重要资产缺乏统筹。
- **解决：基于SBOM的资产治理**



软件供应链安全管理平台已覆盖**100%的内部单位**，纳管**80%的集团重要软件资产**。

- **问题2：“看不见”**；对软件供应链存在风险缺乏识别能力。
- **解决：软件成分分析**



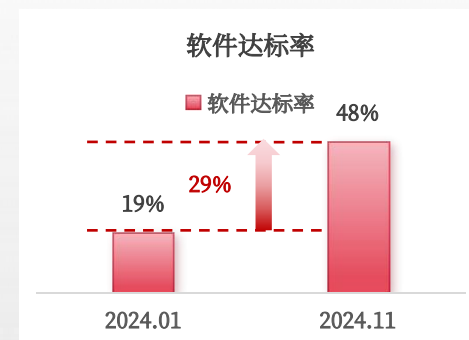
摸清影响软件资产安全的**高频超危开源组件**

- **问题3：“找不到”**；遭遇软件供应链事件时无法快速响应。
- **解决：供应链监测治理体系**



排查、监测各软件资产**安全达标情况**

- **问题4：“治不了”**；缺乏有效的管理平台、整改能力。
- **解决：风险修复分析**



软件安全达标率共提高**29个百分点**

项目连续两年荣获**中国国际大数据博览会领先科技成果奖**。

外部成果认可

社会影响

- **标准建设：**行业联合，建设《电信和互联网软件供应链安全》系列行业标准，牵头其中3项关键标准；
- **推广实践：**开展SBOM试点工作，推广软件供应链安全治理体系；
- **对外赋能：**进入公安三所供应链安全能力中心推荐分析工具清单；推动社区软件供应链能力中心建设；
- **情报共享：**举办论坛、沙龙，搭建先进治理经验交流渠道，提升中国电信软件供应链安全治理影响力。



奖项荣誉

- “2024年数博会领先科技成果奖”
- “2023年数博会领先科技成果奖”
- “网络安全国家标准20周年优秀实践案例三等奖”
- “2022年IDC CSO 全球网络安全峰会（中国站）Top20 项目”
- “2021年通信行业企业管理现代化创新成果三等奖” 等



科研成果

- 授权专利24项
- 核心期刊/EI论文8篇，其中SCI论文2篇
- 软著15项
- CCSA行业标准6项
- IEEE标准2项
- ITU-T标准2项

THANK YOU!