成都企业信息化促进会
Chengdu Enterprise Information Promotion Association

软件安全检测分析技术服务平台

（软件检测测评-成分分析-代码审计-漏洞扫描-风险评估-开源治理）

四川CIO俱乐部、成都企业信息化促进会
中国网安成都国信安信息产业基地有限公司

1 为什么做--政策要求及面临的威胁与风险

2 怎么做？平台的功能和指标

3 成效与收益

4 终身学习：教培认证

1 为什么做--政策要求及面临的威胁与风险

2

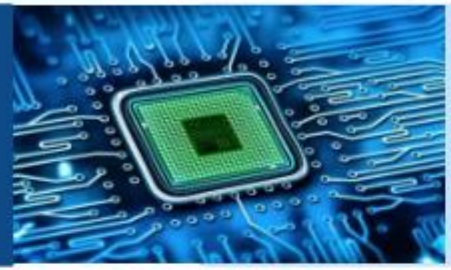
3

什么做？背景和需求（1）

软件是数字经济发展的基础，随着容器、微服务等技术的应用，以及开源软件的重复使用成为软件开发的主流形态，软件供应链风险随之呈现复杂化、多样化、隐匿化、高频化的趋势。

典型软件供应链安全风险事件

软件LD



软件LD引发的网络安全事件频发

Log4jLD让攻击者能在目标计算机上远程执行代码，这意味着他们可以窃取数据、安装恶意软件或者实施控制，全球三分之一的服务器可能受到影响。

代码复用

软件断供风险严重影响国家建设和发展

2022年8月13日，美国商务部发布EDA断供，将导致国内芯片设计领域短期内难以实现真正意义上的国产化。

软件病毒

利用高危LD造成关基设施破坏

2010年，“震网病毒”利用微软视窗操作系统的4个LD，破坏伊朗1000台提升铀浓度的离心机，以至于12年后的今天，其核战略研究依旧驻足不前。

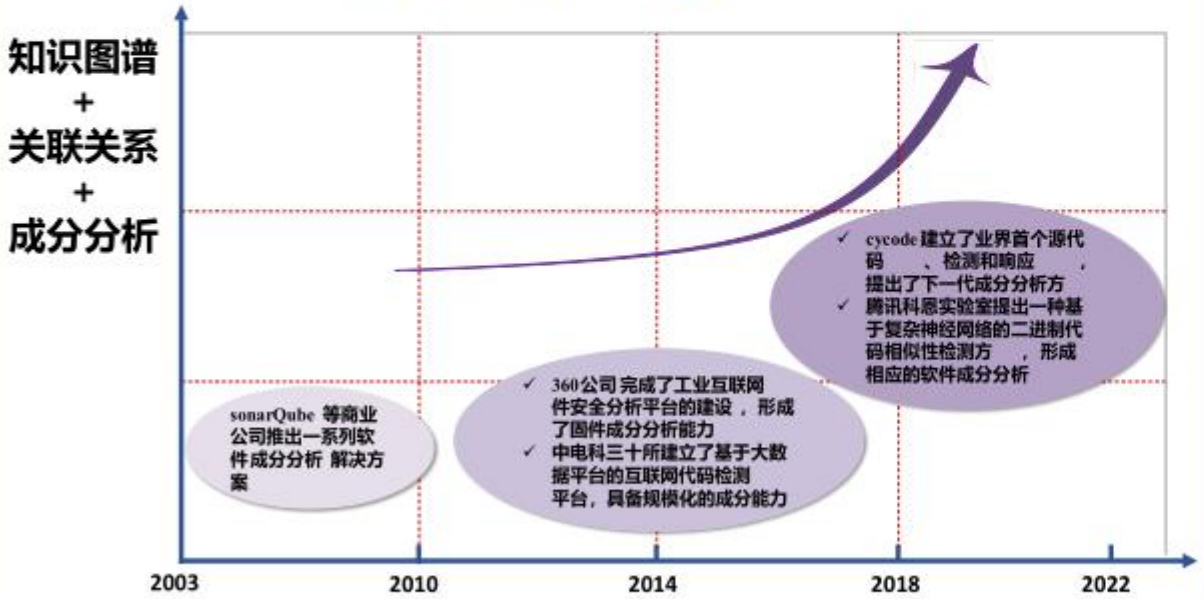
针对关基场景的软件供应链安全风险分析与检测能力亟待提升

为什么做？背景和需求（2）

软件成分分析方面

建立特定行业软件供应链知识库，基于大数据的智能成分分析技术

sonarqube　cycode　CETC



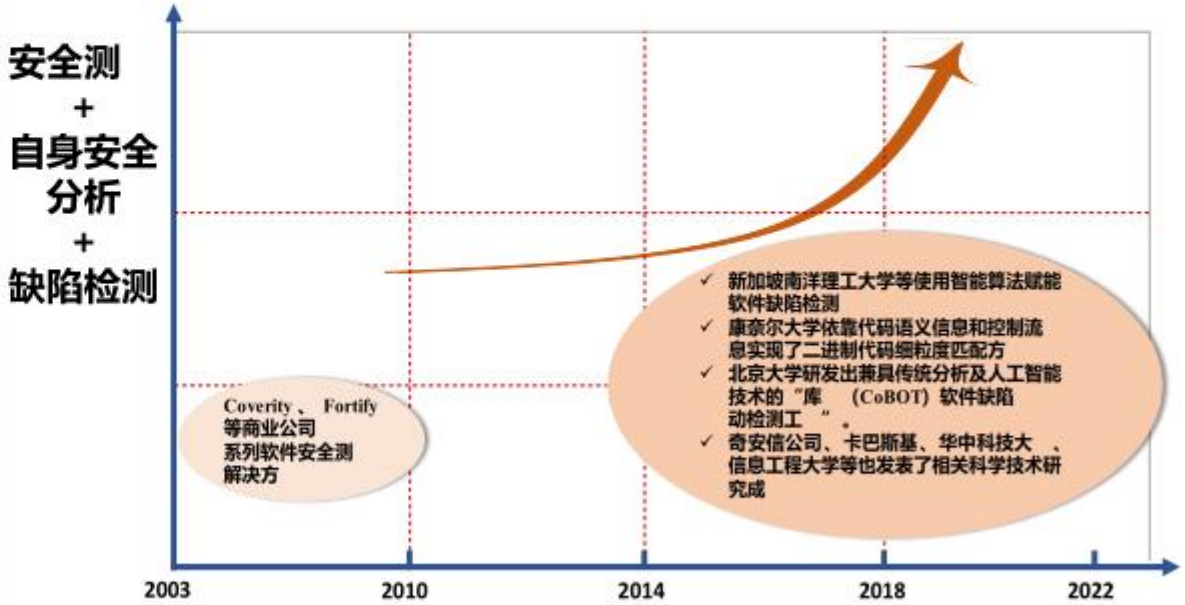
覆盖全生命周期的知识管理与表征是核心

技术向跨领域融合分析发展

软件缺陷检测方面

检测技术的深入与检测手段的多样化、智能化

coverity a higher code　奇安信　KASPERSKY



缺陷的高效检测与精准定位是核心

技术向协同化发展

为什么做？背景和需求（3）

关基场景

党政机关网站

网络服务

工控系统

国防科技工业

大型数据中心

金融系统

软件供应链全生命周期

软件设计

软件开发

软件测

软件采购

软件交付

软件部署

运维升级

目标

审查系统

检测工

安全测评

为什么做？开源软件带来的风险及分布

84%

漏洞占比

分析的1703个代码库中，84%包含至少一个公开开源漏洞。

48%

高风险漏洞

48%包含高风险漏洞。高风险漏洞是指已被主动利用、已有POC（证明漏洞存在）记录、或已被归类为远程代码执行的漏洞。

公开获取

更容易被利用

开源软件具有源代码公开易获取的优点，公开途径获取的开源代码，更容易被恶意利用。

54%

许可证冲突

有54%的代码库包含的开源代码存在许可证冲突。随着代码片段、函数、方法和可运行的部分代码引入，软件包含了更多的条款、条件及约束许可证。

91%

版本缺乏维护

有91%的代码库含有在过去两年中没有发生任何开发活动的开源组件，包括：过时的、没有功能升级、代码优化和安全问题修复。

- 新思科技的《2023开源安全和风险分析报告》中指出，在2022年审查的1,703个代码库中，有**96%**包含开源代码，在所有的被测代码库中，**76%**为开源代码库，其中**84%**的代码库包含至少一个已知开源漏洞，有**48%**包含高风险漏洞，**91%**的代码库包含两年内未更新的组件，有**54%**的代码库包含的开源代码存在许可证冲突。

- 数据来源：新思科技《2023年开源安全和风险分析》

为什么要做？政策合规要求：安全可靠测评

- 财政部会同工业和信息化部研究起草了《通用服务器政府采购需求标准（征求意见稿）》《一体式计算机政府采购需求标准（征求意见稿）》《便携式计算机政府采购需求标准（征求意见稿）》《台式计算机政府采购需求标准（征求意见稿）》《操作系统政府采购需求标准（征求意见稿）》《数据库政府采购需求标准（征求意见稿）》《工作站政府采购需求标准（征求意见稿）》于2023年8月4日及7日向社会公开征求意见。
- 硬件整机产品，均要求其搭载的CPU、操作系统等核心部件必须为通过安全可靠测评标准的产品；针对基础软件产品，同样要求其必须为通过安全可靠测评标准的产品，且要求其兼容ARM、LoongArch、MIPS、SW64、x86等多种架构的CPU平台

实施单位

- 中国信息安全测评中心（国测中心）
- 国家保密科技评测中心
- 依据标准：安全可靠测评工作指南（试行）
- 面向计算机终端和服务器搭载的中央处理器（CPU）、操作系统以及数据库等基础软硬件产品，通过对产品及其研发单位的核心技术、安全保障、**持续发展**等方面开展评估
- 评定产品的**安全性和可持续性**，实现对产品研发设计、生产制造、**供应保障**、售后维护等全生命周期安全可靠性的综合度量和客观评价。

送测产品

- 设计、开发、生产等关键环节在中国境内完成的情况，以及实施必要的安全防护措施的情况；
- 遵守中华人民共和国知识产权相关法律法规、行业标准规范的情况，履行开源许可协议、授权许可合同的要求的情况；
- 不存在未声明功能和已知安全风险的情况；
- 安全风险防护能力的情况；
- 供应链安全性和持续稳定性的情况；
- 服务保障安全性、持续稳定性和可追溯性的情况。

送测单位

- 具备相关的运营、研发、管理、服务等资质的情况；
- 实施知识产权保护及管理的情况；
- 对核心数据、重要数据进行保护的情况；
- **供应链服务的情况或风险；**
- 具备与送测产品研发设计、生产制造、供应保障、售后维护相匹配的人员队伍的情况；
- 具备产品定制开发能力，能够基于自身产品构建产业生态，保持生态开放性、透明性，满足各种应用场景需求的情况；
- 具备**漏洞响应等能力与管理机制**的情况。

什么要做？建设的必要性

软件已经成为支撑社会正常运转的基本元素，软件行业的蓬勃发展得益于大范围的分工合作以及由此产生的软件供应链，其中开源软件在软件供应链体系中扮演着重要角色。针对开源软件供应链的安全攻击事件一直呈快速增长态势，造成的危害也越来越严重。因此，为降低开源软件安全合规风险，提升软件供应链安全公共服务水平，建设开源治理技术公共服务平台非常必要。

提高软件安全可靠水平

通过管理和控制开源软安，**确保开源风险可控**，提高软件的安全性和可靠性

提高企业软件产品项目交付效率

与开发业务结合进行开源软件管理，可以在项目论证、设计、实施过程中**监控开源风险**，及时整治，保障交付通过率

增强合规性/降低法律风险

平台通过提供许可证**审计、合规性检查**等功能，帮助企业确保其使用开源软件的行为符合法律法规要求，降低法律风险

降低软件企业运行成本

平台提供**无偿的开源治理技术服务**，降低由于开展开源治理工作为企业带来的管理成本

保障新质生产力发展

通过平台提高开源软件应用的安全性和合规性，保障**新一代信息技术产品软件生态发展**

1

2 怎么做？平台的功能和指标

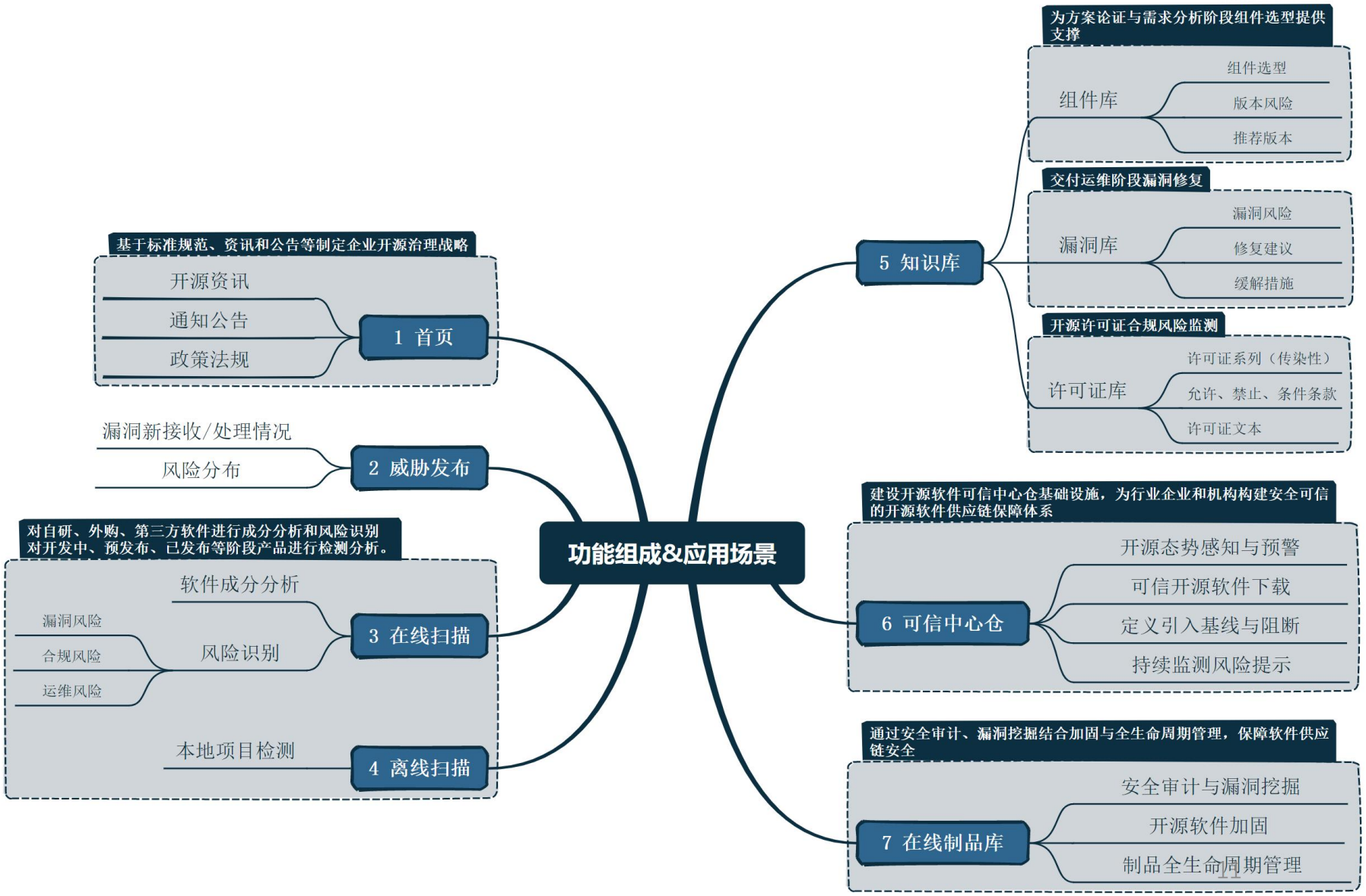
3

我们这样做--平台建设内容（1）

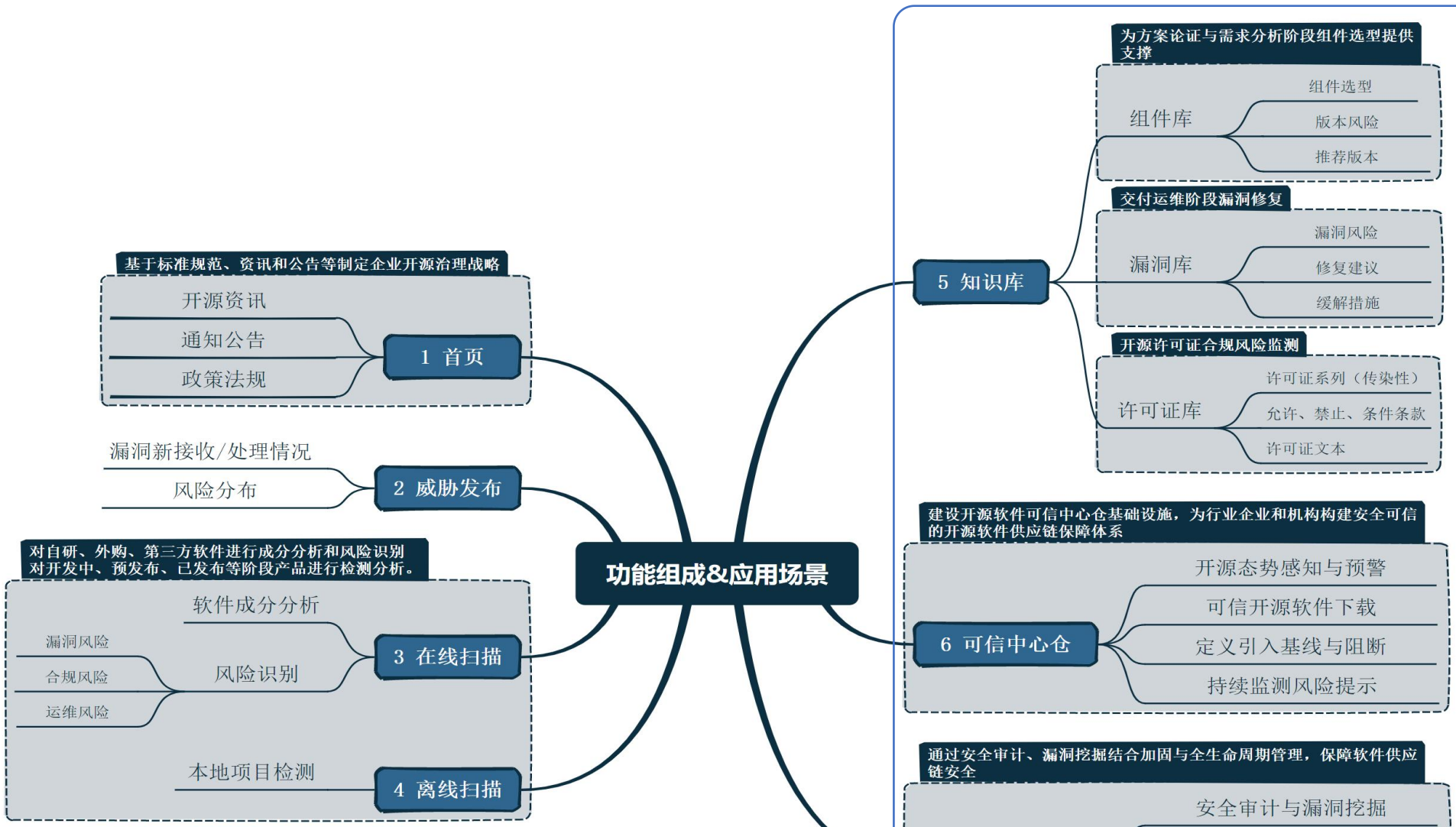
1、用户访问的首要入口，展示开源资讯、通知公告、政策法规等核心信息，以满足用户对开源治理技术信息的获取需求。

2、威胁发布功能可查看近期漏洞披露信息，以表格和仪表板的形式展示威胁情报，通过该系统用户可以及时了解到开源软件的安全威胁信息，以便采取相应的措施保障自身的信息安全。

3、在线/离线扫描，以在线或离线的方式支持用户进行开源成分分析，支持源代码、二进制及容器镜像等多种介质形态的分析识别。



我们这样做--平台建设内容（2）



5、知识库收录各官网、开源社区、商业漏洞库等渠道1000w+开源项目，收录了共24w+漏洞，兼容了NVD、CNVD、CNNVD等。同时，知识库覆盖2700余种许可证并归纳各类许可证条款。支撑平台的安全合规检测

2、面向软件行业提供开源软件可信中心仓基础设施，保障企业引入开源软件的安全可信。

3、根据安全审计结果，提供针对性的安全加固建议，帮助用户修复漏洞并提升开源软件安全性。

技术优势和特色：强大知识库+AI和与可操作性：源代码分离

知识库涵盖 1100万+ 开源组件信息，包含 22万+ CVE漏洞信息、11万+ CNVD漏洞信息、22万+ CNNVD漏洞信息，同时提供2600+ 开源许可证信息。平台通过**AI大模型算法**提供知识库检索入口，能够**快速定位安全的开源软件，减少准入升本**。

- 1100万+个开源组件
- 2.62亿+个开源项目版本
- 2600+许可证协议
- 组件来源保障精准数据
- 300T在线知识库
- AI数据运营流程
- 每小时更新在线数据

漏洞列表　　风险等级　超危

漏洞编号	漏洞名称	风险等级	披露时间	利用难度
CVE-2016-1901	cgit 整数溢出漏洞	超危	2016-01-20	困难
CVE-2016-1928	SAP HANA XS引擎缓冲区溢出漏洞	超危	2016-01-20	困难
CVE-2015-8617	PHP 格式化字符串漏洞	超危	2016-01-19	一般
CVE-2016-1903	PHP'gdImageRotateInterpolated'函数安全漏洞	超危	2016-01-19	困难
CVE-2016-1142	Seeds acmailer 操作系统命令注入漏洞	超危	2016-01-16	困难
CVE-2016-1909	Fortinet FortiOS 权限许可和访问控制漏洞	超危	2016-01-15	一般
CVE-2015-6314	Cisco Wireless LAN Controller 授权问题漏洞	超危	2016-01-15	困难
CVE-2015-6323	Cisco Identity Services Engine Software 授权问题漏洞	超危	2016-01-15	困难
CVE-2016-0856	Advantech WebAccess 基于栈的缓冲区错误漏洞	超危	2016-01-15	困难
CVE-2016-0854	Advantech WebAccess 任意文件上传漏洞	超危	2016-01-15	简单
CVE-2016-0859	Advantech WebAccess Kernel服务整数溢出漏洞	超危	2016-01-15	困难
CVE-2016-0857	Advantech WebAccess 基于堆的缓冲区溢出漏洞	超危	2016-01-15	困难
CVE-2016-0945	多款Adobe产品缓冲区溢出漏洞	超危	2016-01-14	困难

我们这样做-平台功能和技术指标

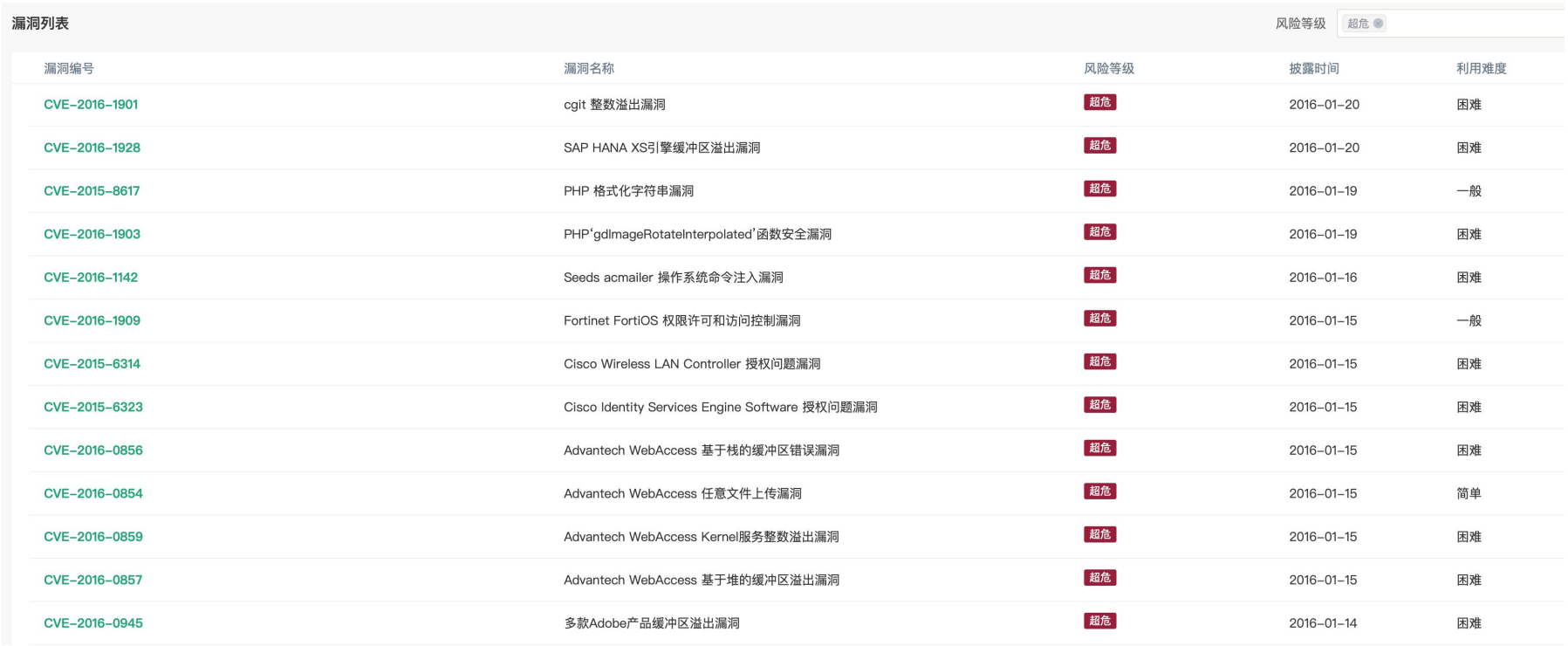
- 强大的知识库为基础
- 与源代码隔离
- 检测能力
- 开/自研率分析
- 许可证冲突
- 强大的项目管理能力
- 许可证兼容
- 自定义风险等级
- 漏洞状态修改
- 修改记录保存
- 版本比对
- 二进制检测

- 广泛的覆盖的语言：多达18种开发语言
- 25类包管理器：Maven、Gradle、Lerna
- 多种扫描方式：依赖检测：20+类型包管理器检测
- C/C++项目检测：Linux--GCC/G++、ARM GCC/G++
- 开源资产管理
- 软件成分分析管理
- 代码克隆检测
- 漏洞检测
- 策略管理
- 私服管理
- 大项目检测
- 任务管理
- 漏洞管理

我们这样做的技术来自哪里？平台强大的知识库

知识库涵盖 1100万+ 开源组件信息，包含 22万+ CVE漏洞信息、11万+ CNVD漏洞信息、22万+ CNNVD漏洞信息，同时提供2600+ 开源许可证信息。平台提供知识库检索入口，能够快速定位安全的开源软件，减少准入升本。

- 1100万+个开源组件
- 2.62亿+个开源项目版本
- 2600+许可证协议
- 组件来源保障精准数据
- 300T在线知识库
- AI数据运营流程
- 每小时更新在线数据



漏洞列表

风险等级 超危

漏洞编号	漏洞名称	风险等级	披露时间	利用难度
CVE-2016-1901	cgit 整数溢出漏洞	超危	2016-01-20	困难
CVE-2016-1928	SAP HANA XS引擎缓冲区溢出漏洞	超危	2016-01-20	困难
CVE-2015-8617	PHP 格式化字符串漏洞	超危	2016-01-19	一般
CVE-2016-1903	PHP'gdImageRotateInterpolated'函数安全漏洞	超危	2016-01-19	困难
CVE-2016-1142	Seeds acmailer 操作系统命令注入漏洞	超危	2016-01-16	困难
CVE-2016-1909	Fortinet FortiOS 权限许可和访问控制漏洞	超危	2016-01-15	一般
CVE-2015-6314	Cisco Wireless LAN Controller 授权问题漏洞	超危	2016-01-15	困难
CVE-2015-6323	Cisco Identity Services Engine Software 授权问题漏洞	超危	2016-01-15	困难
CVE-2016-0856	Advantech WebAccess 基于栈的缓冲区错误漏洞	超危	2016-01-15	困难
CVE-2016-0854	Advantech WebAccess 任意文件上传漏洞	超危	2016-01-15	简单
CVE-2016-0859	Advantech WebAccess Kernel服务整数溢出漏洞	超危	2016-01-15	困难
CVE-2016-0857	Advantech WebAccess 基于堆的缓冲区溢出漏洞	超危	2016-01-15	困难
CVE-2016-0945	多款Adobe产品缓冲区溢出漏洞	超危	2016-01-14	困难

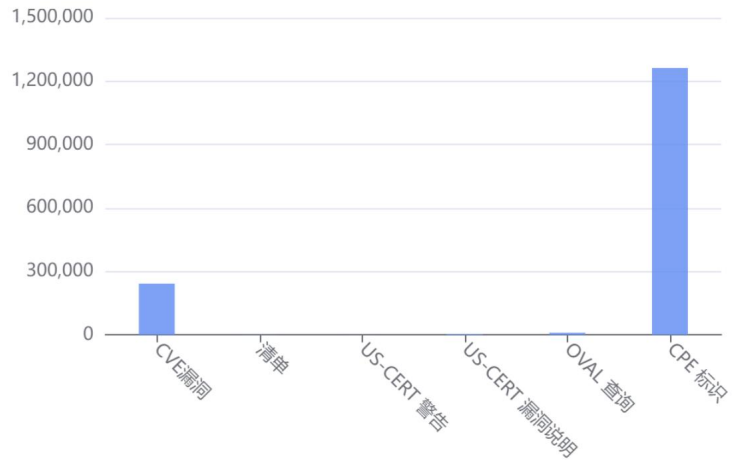
软件安全检测分析技术平台- -威胁发布

CVE状态计数

总计	已收到	等待分析
242623	22	4035

分析中	已修复	已拒绝
113	93943	14008

NVD构成



CVSS V3 分数分布

风险等级	漏洞数量
严重	23018
高危	60927
中危	59886
低危	2528

接受和处理的CVE

时间段	最新收到	最新分析	收到后修改	重新分析后修改
今日	91	5	0	0
本周	91	5	0	0
本月	2465	178	0	64
上月	2749	1310	0	746

CVSS V2 分数分布

风险等级	漏洞数量
高危	56837
中危	104170
低危	19074

软件安全检测分析技术平台-创新点

平台通过整合多种服务方式，优化服务模式。平台为中小型企业提供**快速高质量的成分分析**服务，客户可根据软件检测情况或私有化部署的试用效果，灵活选择是否继续采用其他专业服务。相较于传统服务形式，服务内容更为专业，且性价比更高，能够更好地满足客户的多样化需求。

结合开源治理行业实践经验，为信息产业搭建一个汇集“地方政府、高校、企业、行业、机构”等综合力量的开源软件安全合规保障生态，构建统一的开源软件安全合规制度建设、知识库建立、分析、评估、升级维护、咨询服务及人才培养体系。

建立可信中央仓，对开源软件的引入源头进行安全管理，能够帮助企业和机构对开源软件的引入进行决策、掌握开源软件使用情况、了解待引入开源软件的风险状态、在引入后及时获知风险变化，从而将高风险开源软件挡在门外，并实现更加主动的开源治理。

1

2

3 成效与收益

这样做了好处和收益？平台的价值和效益

构建高水平软件检测服务，推动地区软件和信息产业高质量发展

响应国家“供应链安全”政策，推进国家安全体系和能力现代化

构建软件安全开发生命周期产业链，完善软件产业链结构

打造高品质营商环境，助力企业健康发展

加强软件供应链安全与网络安全创新，促进数字化转型

平台的应用场景

方案论证与需求分析

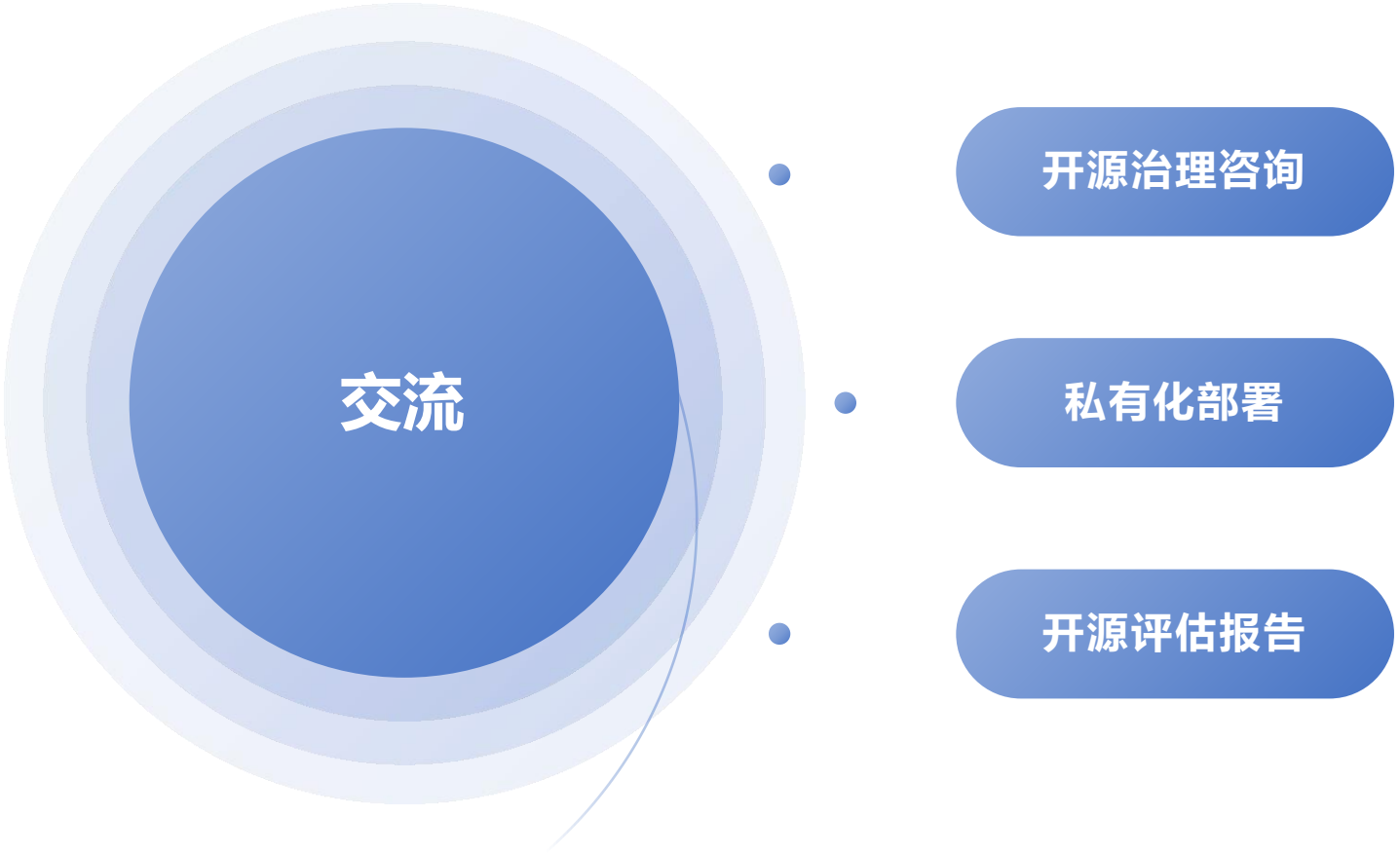
- 组件选型
  - 官方发布确认
  - 安全风险分析
  - 合规风险分析
  - 运维风险分析

开发与集成测试

- SBOM持续监测
  - 安全风险监测
  - 合规风险监测
- 黑名单组件感知
  - 风险预警
  - 漏洞修复建议

交付及运维

- 交付SBOM清单
  - 安全风险监测
  - 合规风险监测
  - 漏洞缓解措施
  - 漏洞修复建议


交流
开源治理咨询
私有化部署
开源评估报告

软件安全检测平台-服务方式服务方式(toB 和 to G)

- TO-G端：
- ✓ ToG端-1-企业和政府客户：建立软件测试测评公共服务平台；
- ✓ ToG端-2-与生态合作共建更多的产业链：形成专业和独立代码检测和审计服务；
- TO-B端：
- ToB端-1：私有化部署平台建设—安装建设软硬系统平台；
- ToB端-2：账号模式（全功能），按时间结算；
- ToB端-3：账号模式（部分功能），按时间结算；
- ToB端-4：项目报告/份（代码行数量）；
- ToB端-5：项目报告/份+盖章（风险评估/CCRC安全审计/CMA/CNAS）模式；
- ToB端-6：项目报告/份+专家技术咨询（按时间/项目）+线下其他工具模式；
- 其他方式。

软件安全检测分析技术平台-平台演示

- VPN登录方法一：
- 1、使用浏览器访问https://58.246.36.122:8443/
- 2、输入账户密码即可完成登录。

- 供应链安全软件测试公共服务平台
- 访问地址：http://172.20.201.221/home/index

测试报告演示：报告

1

2

4　终身学习：教培认证

成都企业信息化促进会
Chengdu Enterprise Information Promotion Association
Enterprise Qualification

高新技术企业

成都市企业技术中心

CMMI3认证

军用实验室认证

质量管理体系ISO9001认证

CNAS西南工程软件测评中心

成都市重大产业技术平台（信息安全）

中国信息安全测评中心CISP培训认证

工信部教育考试中心授权机构

四川省经信厅“智改数转”合格服务供应商

企业资质及政府授牌

- ◆国家科技部 “国家（西部）信息安全成果产业化基地”
- ◆国家工信部 “工业和信息技术人才培训基地”
- ◆四川组织部 “四川省信息安全人才培训基地”
- ◆四川人社厅 “四川省专业技术人员继续教育基地”
- ◆四川保密局 “四川省国家保密局保密培训基地”
- ◆成都市政府 “中国软件名城人才基地”
- ◆成都人社局 “成都市专业技术人员继续教育基地”
- ◆成都人社局 “成都市高技能人才培训基地”
- ◆成都高新区 “成都市软件人才培训基地”
- ◆四川教育厅 “现代学徒制试点单位”
- ◆四川人社厅 “第三方职业技能等级认定单位”
- ◆成都人社局 “职业技能等级认定试点企业”
- ◆成都人社局 “成都市重点群体技能培训机构”
- ◆成都人社局 “成都市劳务品牌培训机构”
- ◆成都退役军人事务局“成都市退役士兵定点培训机构”
- ◆成都蓉漂人才发展学院信息安全人才培训基地

- 教育部“2020网络空间安全产学合作育人优秀案例”一等奖
- 中国国防邮电职工技术协会“新时代工匠学院”
- 国家信息安全评测中心“注册信息安全人员培训机构”
- 中华总工会“第七届全国职工职业技能大赛”支撑单位
- 成都市总工会“成都市百万职工技能大赛”支撑单位
- 教育部“2023年产学合作协同育人”项目
- 教育部“2024年供需对接就业育人”项目
- 成都市 “职业技能等级认定试点单位”
- 成都市 “成都市职业技能定点培训机构”
- 四川省 “第三方职业技能等级认定单位”
- 成都市 “成都市重点群体技能培训机构”
- 成都市 “成都市劳务品牌培训机构”
- 成都退役军人事务局“成都市退役士兵定点培训机构”
- 四川省计算机学会理事单位
- 四川省物联网联盟常务理事单位
- 四川省软件行业协会会员单位
- 四川省软件和信息技术服务业协会会员单位
- 成都市外包行业协会会员单位
- 成都电子信息行业协会会员单位
- 成都电子商务企业协会会员单位
- 成都市软件行业协会人才服务中心
- 成都物联网联盟常务理事单位
- 成都服务贸易协会理事单位
- 中国信息产业商会信息安全产业分会会员单位
- 四川省网信人才发展促进会会员单位

职业技能培训

面向企业核心需求岗位
精准培养精准输送

政企培训

重点就业帮扶群体培训
企业在职员工培训

认证培训

工信部教育与考试中心
中国信息安全测评中心
职业技能等级认定

竞赛服务

全国总工会职工竞赛
成渝双城百万职工竞赛
竞赛支撑

工业和信息化部教育与考试中心

01

程序设计
网络安全

中国信息安全测评中心

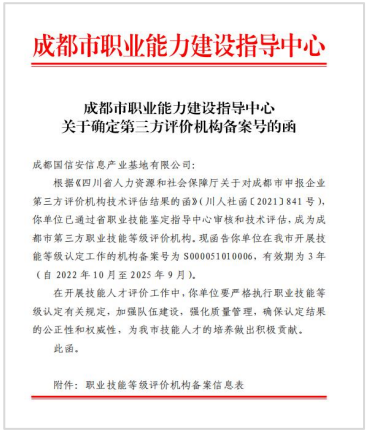
02

CISP
CISP-PTE

职业技能等级认定

03

网络安全
程序设计



成都市职业能力建设指导中心

成都市职业能力建设指导中心
关于确定第三方评价机构备案号的函

成都国信安信息产业基地有限公司：

根据《四川省人力资源和社会保障厅关于对成都市申报企业第三方评价机构技术评估结果的函》（川人社函〔2021〕841号），你单位已通过省职业技能鉴定指导中心审核和技术评估，成为成都市第三方职业技能等级评价机构。现函告你单位在我市开展技能等级认定工作的机构备案号为S000051010006，有效期为3年（自2022年10月至2025年9月）。

在开展技能人才评价工作中，你单位要严格执行职业技能等级认定有关规定，加强队伍建设，强化质量管理，确保认定结果的公正性和权威性，为我市技能人才的培养做出积极贡献。

此函。

附件：职业技能等级评价机构备案信息表

附件

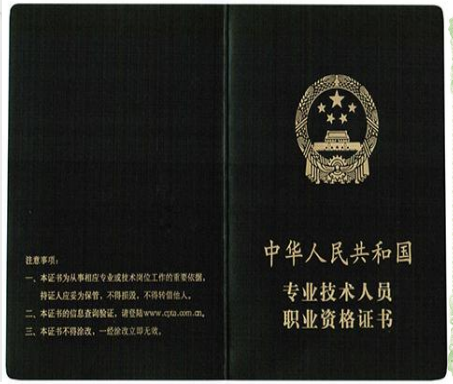
职业技能等级评价机构备案信息表

单位名称	成都国信安信息产业基地有限公司			
机构备案号	S000051010006			
统一社会信用代码	91510100743007815Q			
注册地址	成都高新区云华路333号			
办公地址	成都高新区云华路333号			
法定代表人	李恺			
认定职业（工种）等级范围	职业名称	职业编码	工种名称	认定等级
	网络与信息安全管理员	4-04-04-02	网络安全管理员	4、3、2、1
	网络与信息安全管理员	4-04-04-02	信息安全管理员	4、3、2、1
	网络与信息安全管理员	4-04-04-02	互联网信息审核员	4、3、2、1
	计算机程序设计员	4-04-05-01		5、4、3
	计算机及外部设备装配调试员	6-25-03-00	计算机整机装配调试员	5、4、3、2、1
	计算机及外部设备装配调试员	6-25-03-00	计算机零部件装配调试员	5、4、3、2、1
	计算机及外部设备装配调试员	6-25-03-00	计算机外部设备装配调试员	5、4、3、2、1
	计算机及外部设备装配调试员	6-25-03-00	计算机网络设备装配调试员	5、4、3、2、1

注：开展职业技能等级认定职业（工种）范围以技能人才评价工作网职业技能等级评价机构公示查询系统公示信息为准。

◆ 软考职称类：

	计算机软件	计算机网络	计算机应用技术	信息系统	信息服务
高级资格	信息系统项目管理师　系统分析师　系统架构设计师　网络规划设计师　系统规划与管理师				
中级资格	软件评测师 软件设计师 软件过程能力评估师	网络工程师	多媒体应用设计师 嵌入式系统设计师 计算机辅助设计师 电子商务设计师	系统集成项目管理工程师 信息系统监理师 信息安全工程师 数据库系统工程师 信息系统管理工程师	计算机硬件工程师 信息技术支持工程师
初级资格	程序员	网络管理员	多媒体应用制作技术员 电子商务技术员	信息系统运行管理员	网页制作员 信息处理技术员



◆ 职业技术类：

- 程序设计师（初中高）
- 渗透测试工程师（初中高）
- 安全运维工程师（初中高）
- 网络安全架构师（初中高）
- 移动安全工程师（初中高）
- 软件测试工程师（初中高）
- 人工智能应用工程师（初中高）

机构	序号	证书专业名称	序号	证书专业名称
工业与信息化部教育与考试中心	1	弱电系统工程师	2	弱电系统集成项目经理
	3	安防系统工程师	4	安防系统集成项目经理
	5	智能化系统工程师	6	智能化系统集成项目经理
	7	IT运维工程师	8	智慧家居系统工程师
	9	网络工程师	10	网络信息安全工程师
	11	电气工程师	12	信息系统运维管理工程师
	13	物联网应用工程师	14	数据恢复工程师
	15	信息安全管理	16	数据库工程师
	17	机电一体化工程师	18	渗透测试工程师
	19	网络安全架构师	20	移动安全工程师
	21	硬件维修工程师	22	大数据分析师
	23	硬件技术维护工程师	24	软件技术开发工程师
	25	安全运维工程师	26	软件工程师
	27	智能建筑弱电应用工程	28	智能建筑弱电系统项目管理师
	29	智能楼宇工程师	30	综合布线工程师
	31	数据中心（机房）运维管理工程师	32	智能建筑弱电工程师
	33	数据中心（机房）规划设计工程师	34	安全防范工程师
	35	智能家居系统工程师	36	智能建筑弱电系统设计师
	37	5G网络优化工程师	38	楼宇自控工程师
	39	信息系统集成管理	40	网络工程管理
	41	JAVA软件工程师	42	档案信息化管理师
	43	程序设计师	44	网络营销师
	45	物联网技术	46	软件测试技术
	47	平面设计师	48	室内设计师
	49	财务信息化应用	50	ERP财务应用师
	51	舞台灯光（高级）	52	音响工程（高级）
	53	照明设计（高级）	54	手机维修工程师
	55	工业机器人技术	56	人工智能应用工程师

认证培训--中国信息安全测评中心(CISP)专业

- [CISE（注册信息安全工程师）：从事信息安全技术领域:信息系统安全集成、安全技术测试、安全加固和安全运维等。
- [CISO（注册信息安全管理人员）：负责信息安全管理：信息安全风险评估、总体规划编制、策略制度制定和监督落实等。
- [CISP-PTE（渗透测试工程师）：专注于渗透测试技术，包括渗透测试、漏洞挖掘、安全评估等。
- [CISP-A（注册信息系统审计师）：信息系统审计和信息安全风险评估工作、知识和技能。
- [CISD（注册信息安全开发人员）：专注于软件开发过程中的信息安全问题，包括应用安全等。
- [CISP-PTS（注册渗透测试专家）：主要从事高级渗透测试工作，包括漏洞研究、代码分析、最新网络安全动态跟踪等。
- [CISP-IRE（注册应急响应工程师）：负责网络安全事件的应急响应和处置。
- [CISP-IRS（注册应急响应专家）：专注于高级应急响应分析及规划管理，包括网络安全事件溯源分析、应急处理方案制定等。
- [CISP-CTE（密码技术专家）：掌握密码学基础理论、密码法律法规、密码应用等知识，服务于党政机关、关基设施等领域。
- [CISP-F（电子数据取证专业人员）：专注于电子数据取证技术，包括电子证据的收集、分析和呈现等。
- [CISP-Cloud（云计算安全认证）：专注于云计算安全领域，适合云计算平台的安全管理人员和云安全产品开发者等。
- [CISP-ICS（工业控制系统安全认证）：专注于工业控制系统安全领域

(CISP)学生专属区

请各位领导和专家批评指正