软安科技
SOFTWARE SAFETY

工业互联网下的
软件供应链安全

扫一扫上面的二维码图案，加我微信

徐 刚
软安科技 CEO

2021.10.22.

ABOUT US

关于我们

成都

成都市高新区

中海国际中心

上海

上海市杨浦区

光大安石中心

北京

北京市东城区

环球贸易中心

我们的愿景：

为软件安全构建基础

为数字经济保驾护航

软安科技
SOFTWARE SAFETY

2021 软安科技有限公司由新思科技、成都高新政府、社会资本及核心团队共同投资组建，2021年5月成立于成都，在上海，北京设立分公司和办事处，服务能力覆盖95%的中国领土

宏观环境 - 安全是数字经济的基石

软安科技 SOFTWARE SAFETY

信息安全作为数字经济的基石，随着我国步入数字时代的步伐而快速发展。

中国信息通信研究院发布的《中国数字经济发展白皮书》显示，2020年中国数字经济规模达到**39.2万亿元**，占GDP比重为**38.6%**，同比名义增长**9.7%**。

数字经济占GDP比重逐年提升，在国民经济中的地位进一步凸显。2020年中国数字经济占中国GDP的38.6%，较2015年的27.0%增长了**11.6%**。

离开安全的数字经济就如空中楼阁

工信部发布《网络安全产业高质量发展三年行动计划》中显示，预计2023年国内网络安全产业规模超过**2500亿元**，年复合增长率超过**15%**。

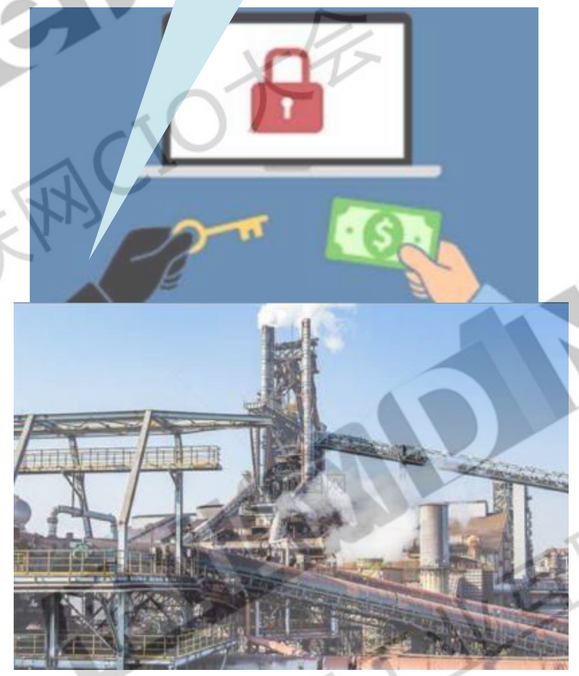
保障数字化时代的软件安全

软安科技
SOFTWARE SAFETY

软件APP泄露
个人隐私

波音787软件缺陷
导致飞机坠毁

基础设施频遭
勒索软件攻击

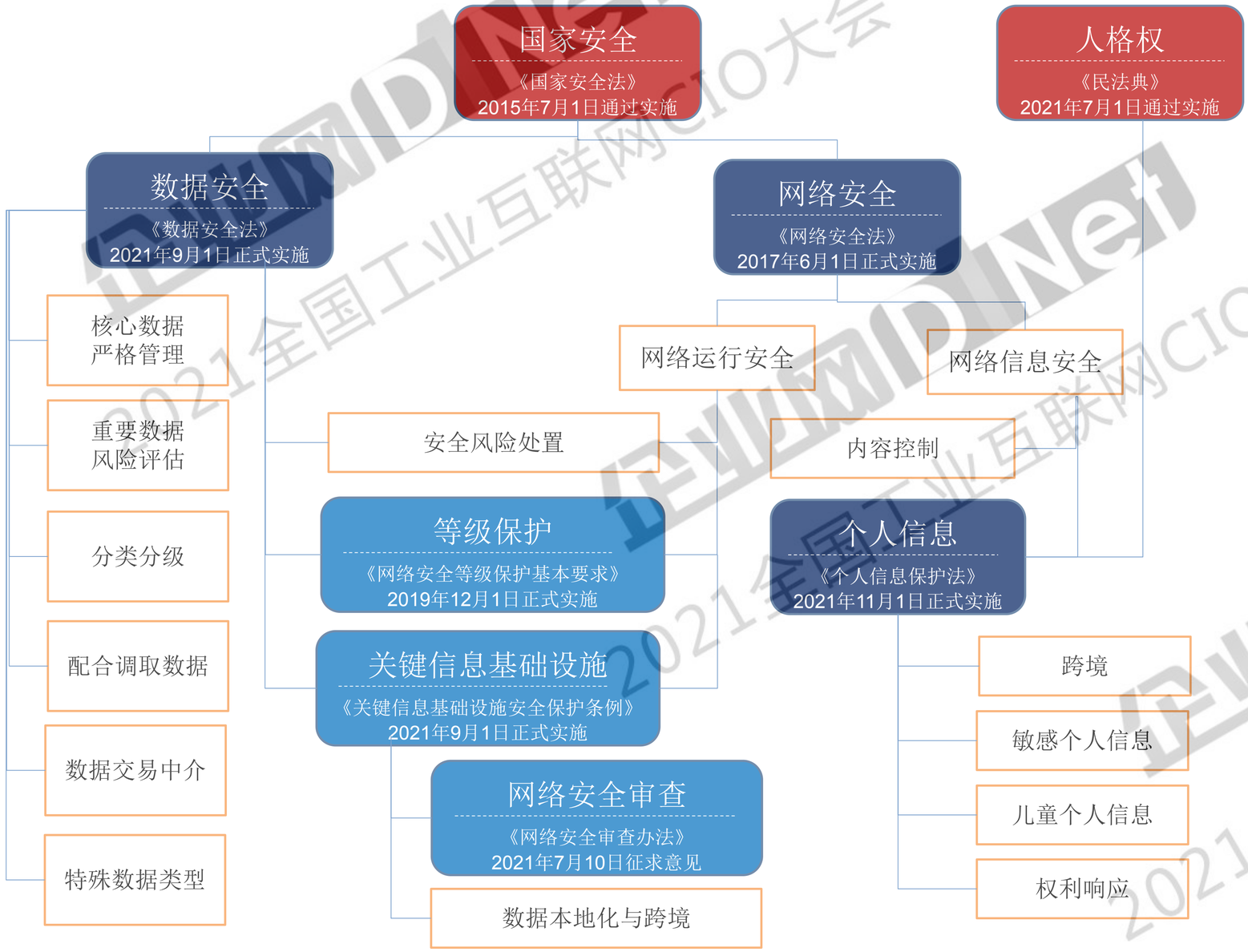


黑客通过软件设计
缺陷控制智能汽车

“软件吞噬世界”

软件安全 = 数字化时代的基础安全保障

宏观环境 - 日益完善的中国网络和数据安全法律体系



网络安全法、数据安全法等法律法规构成了中国数字规则体系，规范和促进数字经济健康发展

网络安全等保2.0标准内涵更加丰富，提出了应用安全相关要求：

✓应制定软件开发管理制度
✓应制定代码编写安全规范
✓应保证软件开发过程中对安全性进行测试
✓应检测恶意代码

行业规范要求建立健全安全机制，提出安全管理规范/技术要求：

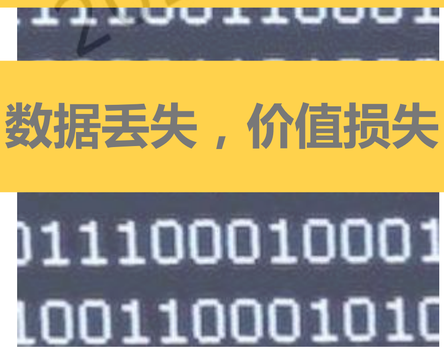
✓应对程序接口进行代码安全专项审计
✓进行源代码安全审计、渗透测试等技术检查
✓应审查代码后门，管控代码打包和发布

工业安全与传统互联网安全的差异

软安科技 SOFTWARE SAFETY

互联网安全 VS. 工业安全

	互联网安全		工业安全	
价值来源	互联网用户的数据	VS.	企业自有投资的实体	→ 实体
攻击动机	获取数据价值	VS.	破坏实体价值	→ 实体
后果影响	数据丢失，价值损失	VS.	实体长期或永久损失	→ 实体



随着工业互联网的推进，软件供应链安全变得越来越重要

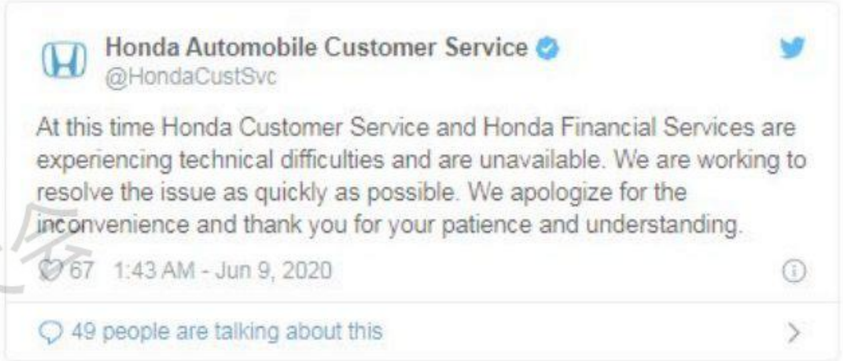
软安科技 SOFTWARE SAFETY

数字化转型，工业生产/控制系统由软件组成，工控设备的中高危漏洞占比91%，存在极大风险

本田：全球业务网络被勒索软件攻击 部分产线被迫停工

黑客眼中“香饽饽”，攻击事件频发，多家智能工厂遭遇勒索攻击

- 产线停工
- 数据泄露
- 知识产权窃取



平均每个智能工厂就有52.5个安全漏洞，一段代码就能瘫痪一座智能工厂

汽车和航空业零部件制造商Visser Precision被攻击后，其客户SpaceX、特斯拉、波音等诸多客户纷纷遭殃

Visser, a parts manufacturer for Tesla and SpaceX, confirms data breach

Zack Whittaker, Kirsten Korosec / 12:06 PM GMT+8 • March 2, 2020 Comment

制造商、供应商、集成商、服务提供商都可能存在安全隐患

- 生产厂商预留“后门”
- 基础软件商“污染”
- 工业产品漏洞
- 供应渠道劫持
- 软件升级劫持

安全左移：质量和安全的平衡

质量第一？安全是质量的关键属性，安全需要左移，从源头解决安全问题，保障软件质量

外因

监管要求陆续出台

- 《ICT 供应链风险管理标准》（NIST. SP800-161）
- 《网络安全审查办法》网络安全审查
- 等保2.0：安全规范、安全性测试、检测恶意代码
- 行业规范：安全测评、漏洞修复和加固

传统安全不足

- 无法治本：无法洞悉根源，功能全覆盖
- 修复成本：测试、上线阶段修复漏洞成本高昂

内因

软件应保证自身安全

- Gartner：75%安全攻击由软件自身漏洞造成
- NIST：92%漏洞是应用自身弱点，非网络原因

软件供应链安全

- 开源软件被大量使用
- 超8成软件项目存在已知高危开源软件漏洞
- 攻击不断左移，针对软件供应链的攻击事件频发
- 信息系统安全的底板工程

零信任：效率和安全平衡

安全妨碍生产效率？安全下的效率才是真效率，通过平台解决安全信任问题，提升真效率

工具

- CI/CD工具链本身安全
- 开源软件的高信任度
- 测试工具误报关注较多，漏报关注较少，有论文显示漏报率高达80%
- 很多企业采用多款工具共用求合集方式降低误报率，但成本太高

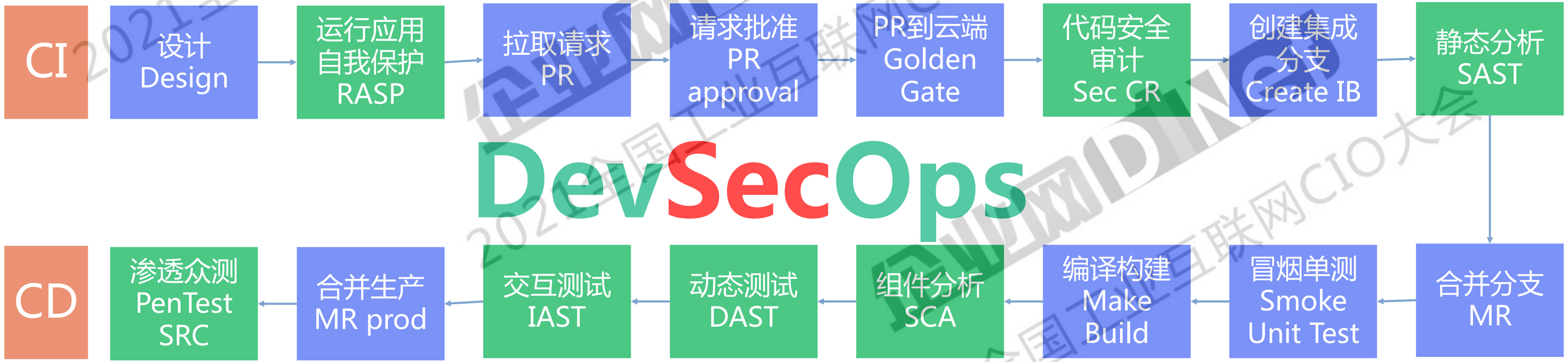
人员

- 学习每种平台工具，查看繁琐的帮助文档去扫描测试代码
- 跨语言项目包含多个开发语言，需要人工区分扫描，测试成本较大
- 业务vs开发团队vs安全团队

黄金管道：DevSecOps落地实践

软安科技 SOFTWARE SAFETY

“Golden Pipeline（黄金管道）”特指一套通过稳定的、可预期的、安全的方式自动化地进行应用持续集成/部署的软件流水线（toolchain）



DevSecOps

需要解决的问题

软安科技
SOFTWARE SAFETY

全面性

安全测试工具单一

漏洞发现能力单一

无法协同增效

有效性

处理流程难管控

管理过程难闭环

平台工具难支撑

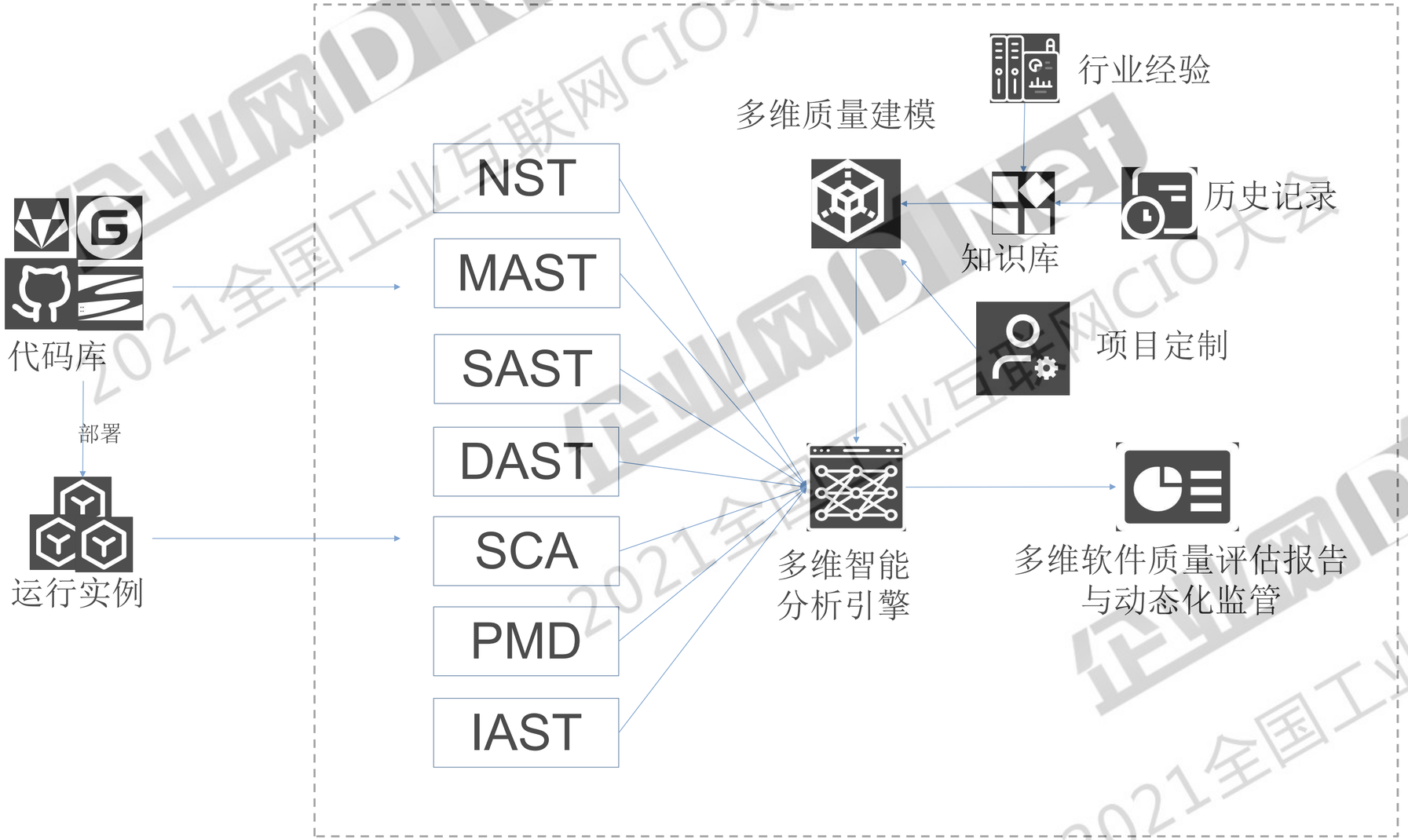
专业性

数据难以关联和利用

人员缺乏专业和效率

经验无法积累和传承

总体解决方案



全面性

平台多工具集

有效性

智能自动化任务编排

专业性

多维安全知识库

平台多工具集成架构

软安科技 SOFTWARE SAFETY

标准规范与质量控制

安全技术体系

管理工具：JIRA、禅道、redmine、TAPD、……

分析监管：项目质量分析、团队质量评估、风险趋势分析、热点漏洞监控、高危风险管控

测试报告 多维智能分析

任务调度：任务智能规划、任务智能调度、分布式执行器、动态任务流水线、多语言环境支持、多包管理组件适配

扫描工具：NST、MAST、SAST、DAST、SCA、IAST、PMD

知识库：ATT&CK、CWE、CVW、OWSAP、CNNVD、行业规范、历史经验

智能自动化任务编排

用户

流水线模版定义

配置管理

任务管理

编排引擎

工具管理

配置 → 编译 → 扫描 → 打包 → 部署

项目应用业务影响度评估 → 代码库地址 → 检测策略 → 任务规划策略

智能动态任务规划

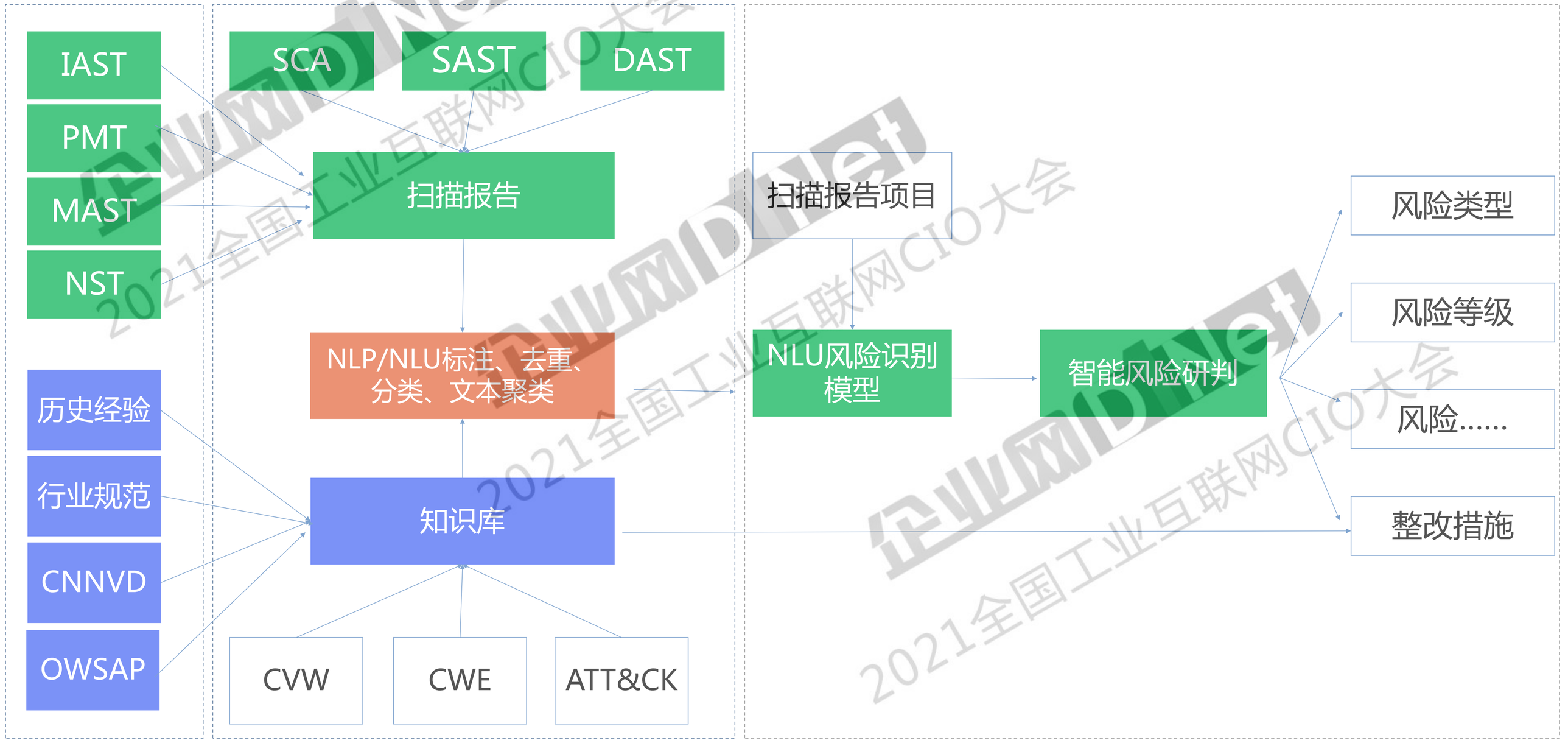
路由策略 → 串行并行 → 执行频率 → 子任务 → 异常策略

行业经验　规则库　智能搭配动态巡检　知识库　安全规范

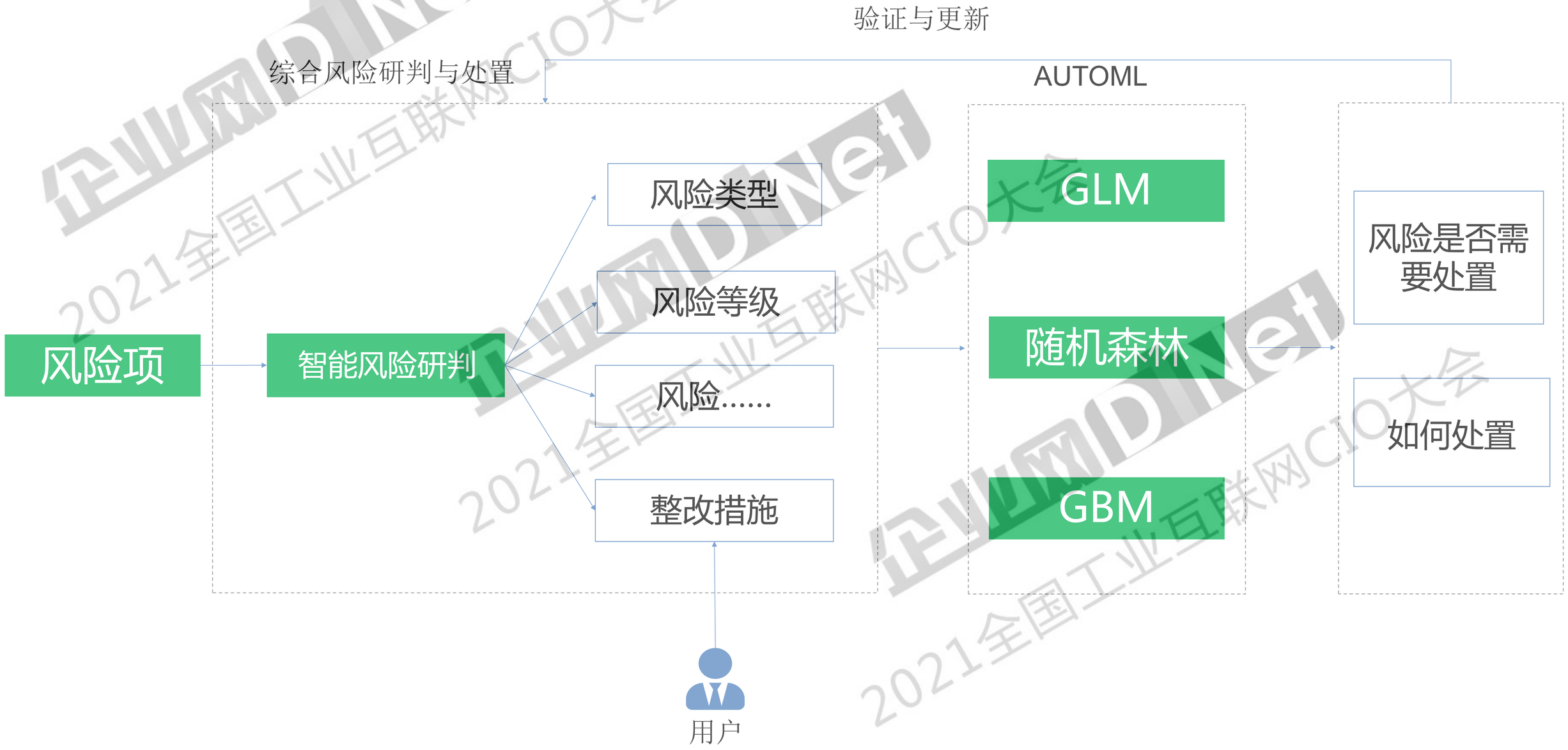
NST　MAST　SAST　DAST　IAST　SCA　PMD

动态调度 → 执行器 → 工具调用 → 扫描工具 → 报告输出 → 消息队列 → 智能分析 → 数据展示

知识库-NLP/NLU在风险识别中的实践



多维安全知识库-风险误报与处置方案预测



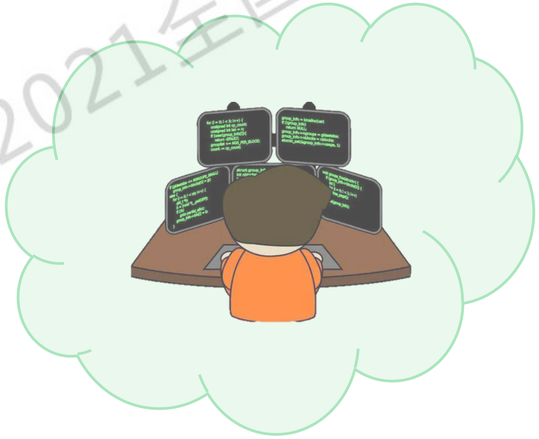
多维安全知识库-多维数据分析展示

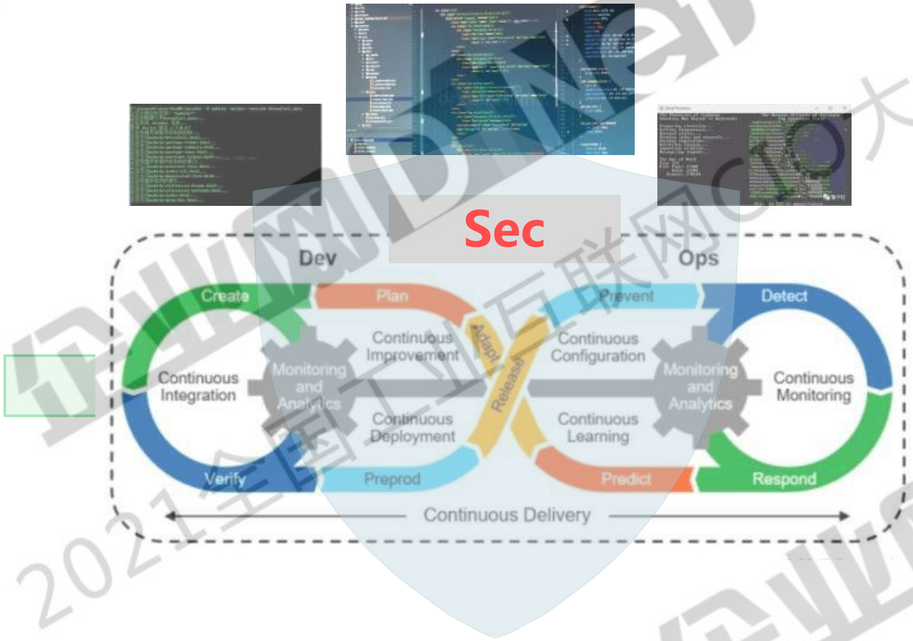
软安科技 SOFTWARE SAFETY

角色	场景	指标
开发人员	MISRA 报告	项目缺陷分布
测试人员	CVSS 报告	缺陷类型/等级分布
安全审计人员	CERT 报告（C、JAVA）	人员缺陷分布/缺陷密度
项目经理	OWASP 十大网络安全风险报告	逾期未处理分布
产品经理	移动 OWASP 十大安全风险报告	缺陷趋势
管理层	PCI DSS 报告	重要缺陷密度
……	GJB报告 （8114、5369）	……
	……	

软安科技，为中国软件安全贡献力量

基于自主研发“金刚”平台，以DevSecOps为抓手，提供软件开发全生命周期安全整体解决方案。





生态产品 + “金刚”软件安全质量平台 + **运营服务**

“金刚”软件安全质量平台

软安科技
SOFTWARE SAFETY

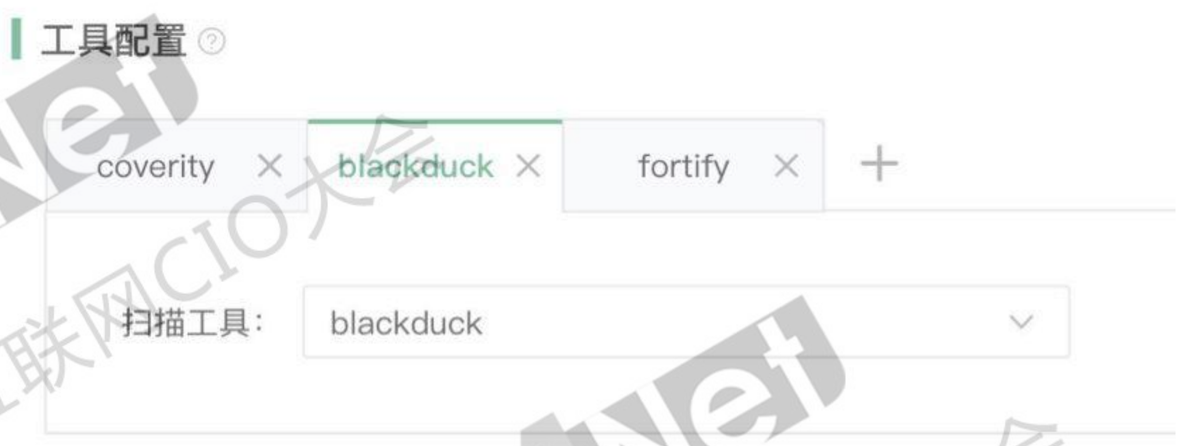
“金刚”软件安全质量平台，是软安科技面向软件开发全生命周期所研发的安全管控平台，用以赋能软件研发企业，在软件需求的复杂度越来越高、交付速度越来越快、定制比例普遍增多情况下，可以有效的保障软件产品安全水平。

1. 多维报告中心，获得软件安全的综合分析结果和完整风险视图。
2. 智适应安全任务集成编排，智能、自动工具链接入。
3. 高兼容性的生态产品整合能力，支持接入国内外主流代码安全工具产品。
4. 智能升级的知识库，可根据历史数据和行业经验持续优化分析能力
5. SaaS 化运营，可兼容市面主流云平台，可以在私有云环境部署和管理。
6. 提供API 接口，可以与企业内部敏捷开发平台实现无缝整合

平台多工具集成

静态代码分析**Coverity**配置：

软件组成分析**blackduck**配置：



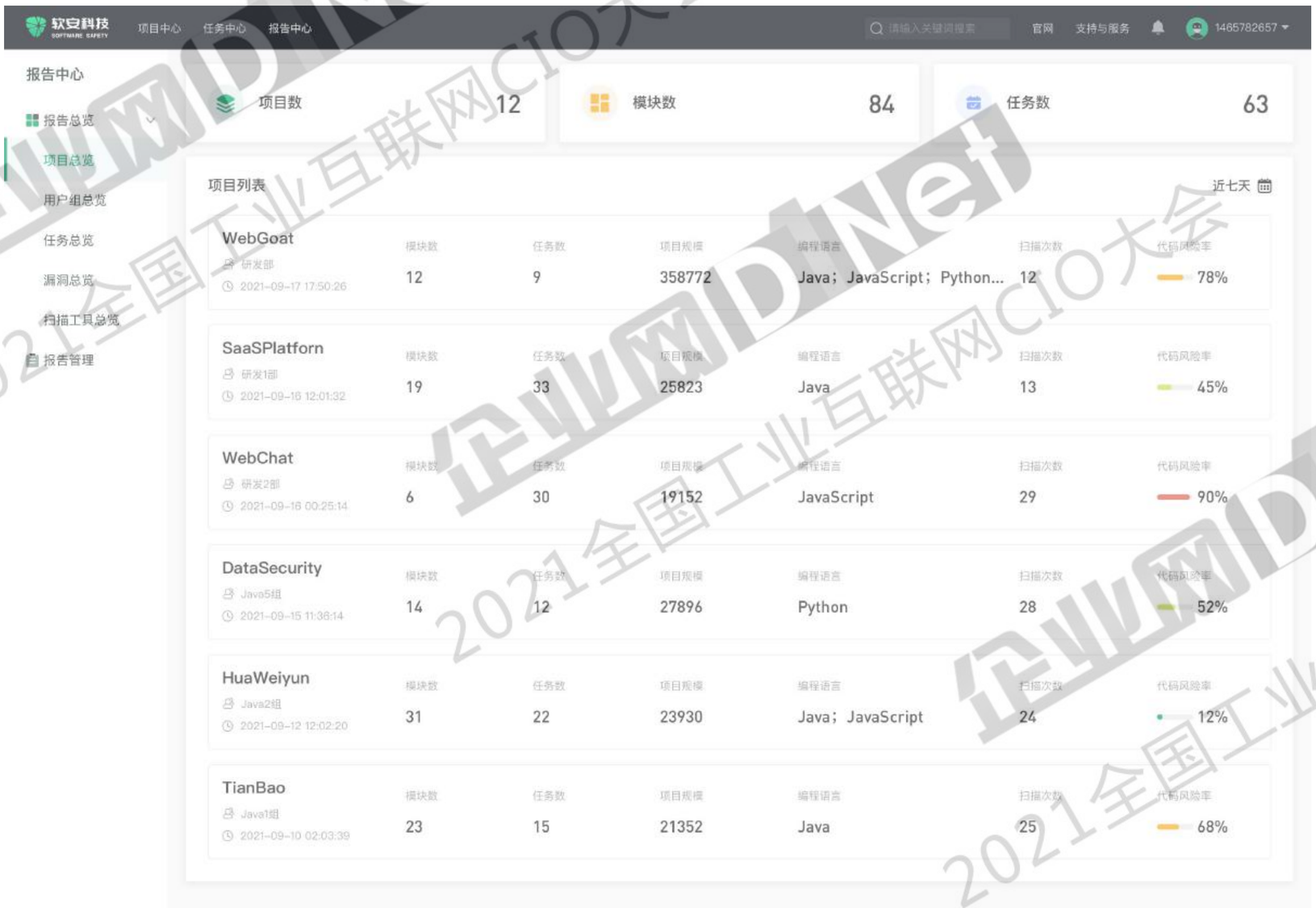
扫描结果展示：

流水线任务编排

问题报告

数据分析-团队效率

数据分析-项目安全质量



实施前后对比

以某企业为例，实施该解决方案后，在保持原有开发效率前提下，以更低的成本获得了更高的软件安全性

安全
提升

质量

- 软件缺陷漏报率显著下降
- 多维软件安全知识库提升整体安全短板

成本
下降

成本

- 灵活的测试工具定制能力省去了大量采购成本
- 大大节省后期漏洞修补成本

效能
提升

效能

- 测试人员节省80%的安全测试工作量
- 对接开发IDE和缺陷跟踪工具，提升相关干系人处理效率

实施前后对比

对比方面	实施前	实施后
应用开发生命周期管理	➢沟通效率低 ➢通知不及时 ➢制度难落实	➢安全规范形式化描述，效率高 ➢系统自动邮件通知 ➢所有过程数据记录在案
应用安全漏洞修复	➢定位/响应时间长 ➢整改不彻底、不了了之 ➢同样的问题反复发生 ➢上线后发现的安全漏洞占比较高	➢定位更加精准、修复更加快捷 ➢强化问题跟踪，确保彻底整改 ➢避免问题再次发生 ➢上线后发现的安全漏洞占比显著降低
安全与开发团队协作	➢手工填表单，格式多样 ➢重复填写基础信息 ➢会议评审或者邮件评审	➢自动带出已知信息，效率高 ➢同样的信息只填一次 ➢线上评审，有据可查
安全漏洞管理	➢无风险评估 ➢手工分拣发给相关责任人，难跟踪 ➢漏洞价值随时间、人员而流逝	➢CARTA，持续应用风险威胁评估 ➢发现到修复闭环跟踪监控 ➢积累工具数据，沉淀分析报告

源于软件安全能力，助力数字安全未来

软安科技
SOFTWARE SAFETY

软件安全质量

数据安全管理

专业安全服务

智慧安全运营

THANKS

谢谢！

Steven Xu

上海 浦东新区

扫一扫上面的二维码图案，加我微信