安世加

Face the challenge,Embrace the best practice

EISS-2021
企业信息安全峰会

深圳站|2021.10.15

平安DevSevOps之“道”与“术”

平安科技信息安全运营团队

王治纲

1 痛点与挑战

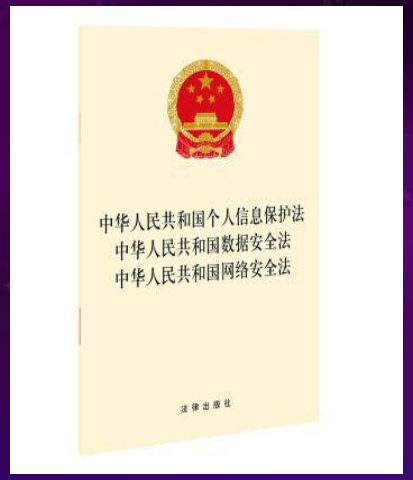
2 “明道”与“炼术”

3 On the road

外部环境因素

技术标准

律法



监管

威胁

新技术

内部环境因素

工具
- 集成
- 系统架构
- 误报率
- 漏报率

效率
- 时效
- 容量
- 周期
- 流程

体量
- 下属公司
- 团队组织
- 应用数量
- 语言类型

价值
- 业务价值
- 投入产出
- 企业文化

1

痛点与挑战

2

“明道”与“炼术”

3

On the road

平安DSO之道：一个中心、三大要素

专业的事情交给专业的人来做？ OR 安全靠大家，人人都爱TA？

围绕人、管理、技术进行安全赋能，
全方位、持续性提升整体安全水平

平安之术：八种武器

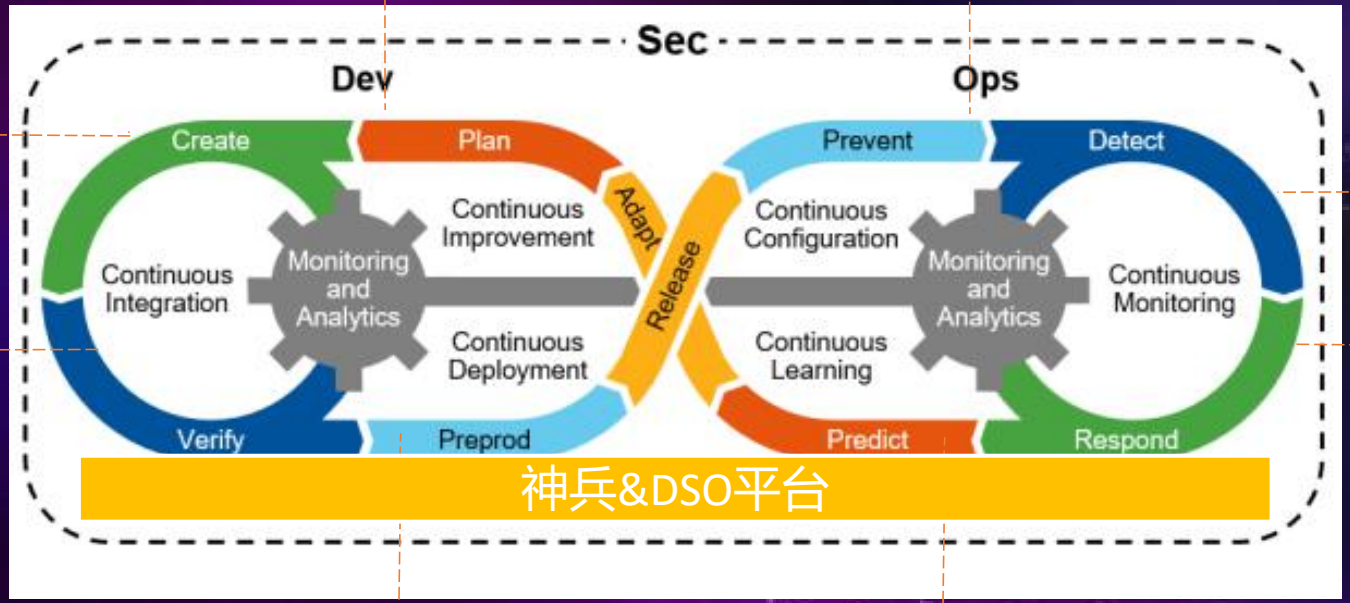
工具链建设

安全编码规范
源代码静态扫描
开源组件扫描
安全组件库

安全规范要求
安全需求&设计评审
威胁建模
安全培训平台

WAF
DDOS
NGFW

RASP
蓝军渗透
态势感知



黑盒安全扫描
灰盒安全扫描
Fuzz安全测试
App扫描
安全测试案例库

安全门禁
主机漏洞扫描
容器安全扫描

威胁情报
漏洞预警

应急响应平台

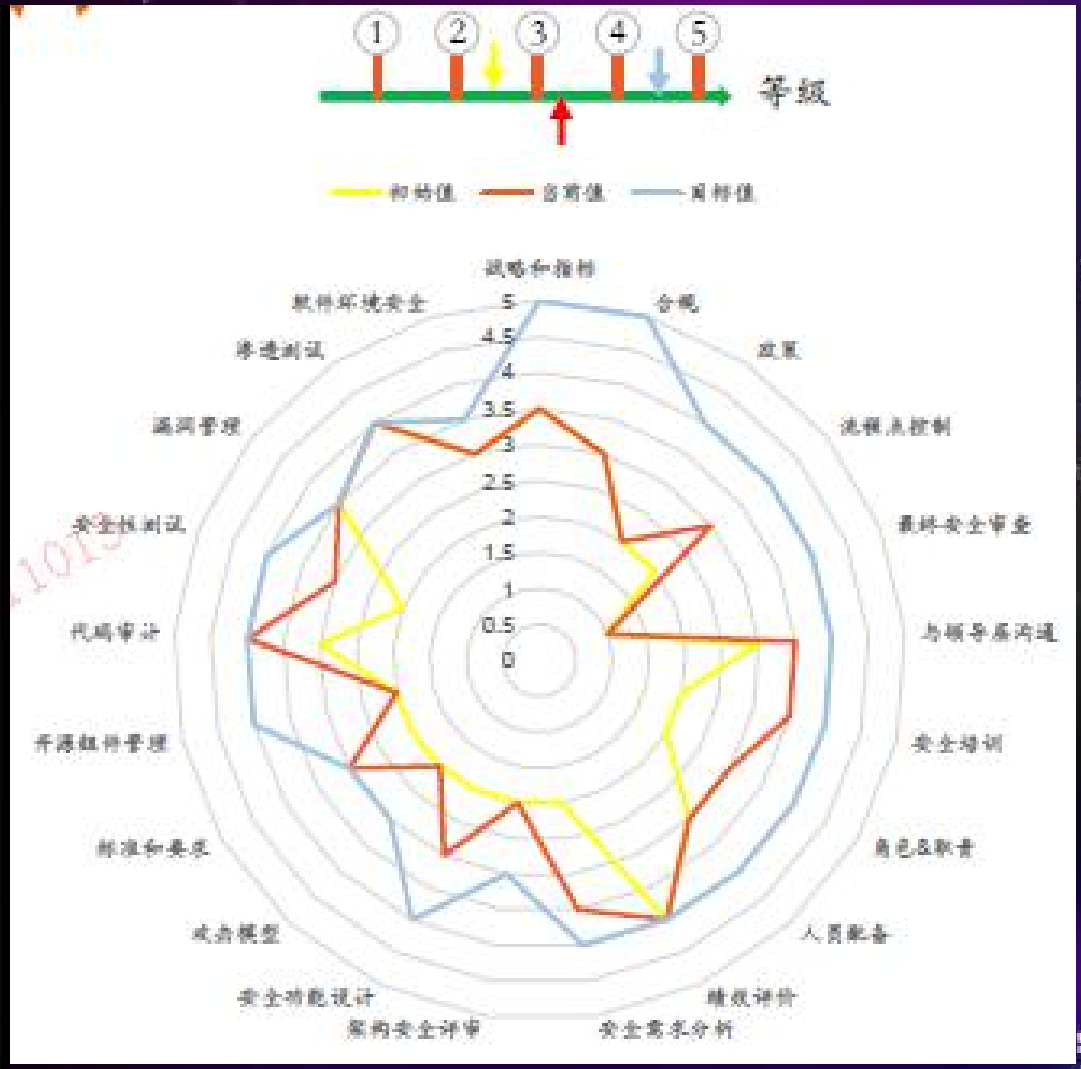
组织架构

协同部门安全职能

- **研发管理部**
- **运维管理部**
- 项目管理部
- 风险管理部
- 法务部
- ……

成熟度评估

领域	子域
组织与计划	战略和指标
	合规
	政策
	流程检查点控制
	最终安全审查
	与领导层/相关方沟通
	安全培训与意识教育
	角色&职责
	人员配备
	绩效评价
开发与实现	软件安全需求分析
	架构安全评审
	安全功能和设计
	攻击模型
	标准和要求
	开源组件管理
验证与测试	代码审计
	安全性测试
部署与响应	漏洞管理
	渗透测试
	软件环境安全



培训体系

线下培训

线上知鸟课程

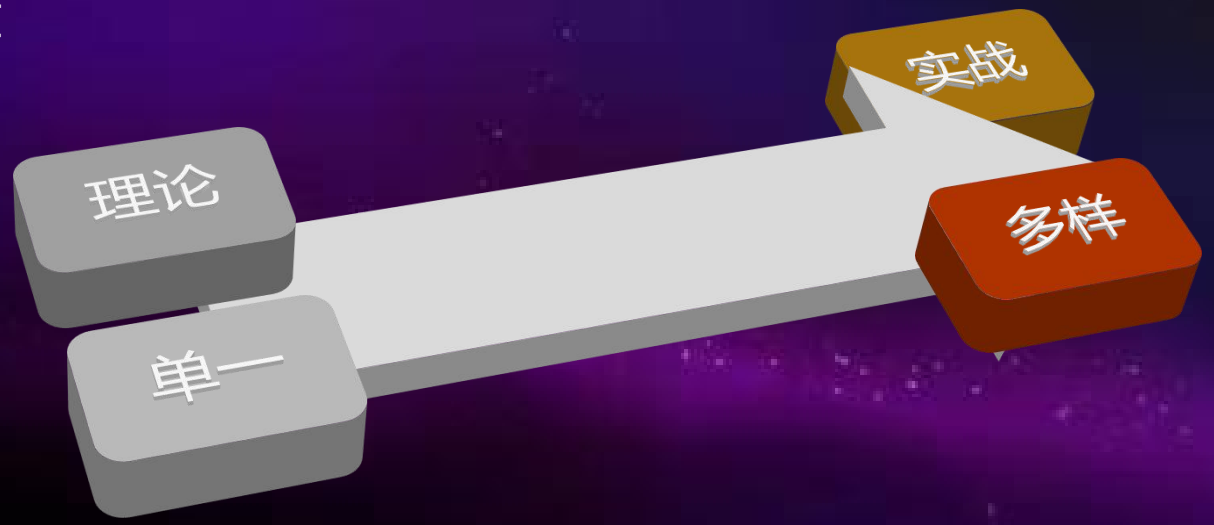
Sec2know

银河钓鱼平台

银河零号（靶场）

在线文档库

邮件宣导



智能应答

1

痛点与挑战

2

“明道”与“炼术”

3

On the road

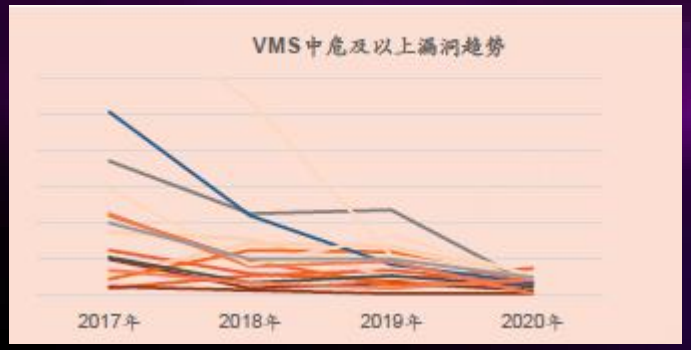
成效

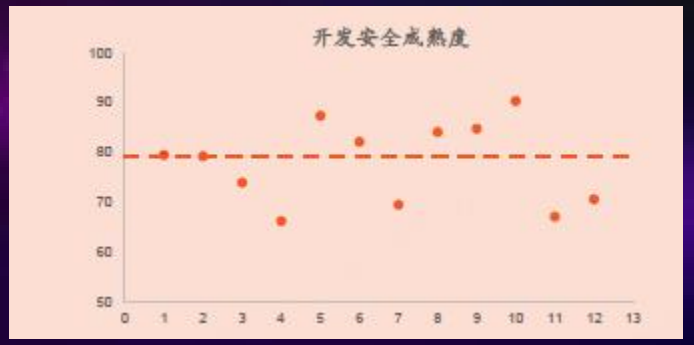
上线前扫描覆盖27家专业公司，??k个应用系统，日均扫描量约??W，平均扫描时长不超过9.4分钟

目前漏洞扫描总共覆盖25家专业公司，总计扫描数量为???w台主机，日均扫描量约为??w台主机。

全集团整体线上漏洞数量下降率达到72.75%

集团安全成熟度逐步登上“已管理”级，并向“可优化”级迈进





未来的方向

智能化：用户画像、问题溯源、精准赋能

自动化：数据可视化、特殊流程优化

平台化：工具的持续优化

Thanks!

专注于网络安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站:
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加