
ThreatBook
聚焦威胁 情报驱动
2018 网络安全分析与情报大会

ThreatBook

互联网企业安全建设思考与实践

2018 网络安全分析与情报大会

-- 靳晓飞--

VIPKID安全负责人

关于我

姓名：靳晓飞

公司与职位：VIPKID安全负责人、高级安全专家

网络ID：secsky

个人经历：8年安全从业经验、先后在安全公司网络攻防实验室、电商、在线教育公司从事安全研究、攻防对抗、安全体系建设等工作

从这里说起

国家

行业

个人

安全与业务的关系

安全与业务的关系			
	安全做的不好		安全做的好
公司运营与业务发展	无力应对企业面临日趋复杂的网络攻击，在网络攻防对抗中处于被动，制约公司正常运营和业务发展，成为公司发展瓶颈	VS	可主动掌控公司整体安全态势，有效控制安全风险在可接受范围内；从安全维度全面保障和支撑公司正常运营和业务快速发展
商业竞争	安全落后于竞争对手，在商业竞争中处于被动地位		安全领先于竞争对手，在商业竞争中处于主动地位
品牌形象	影响品牌形象，用户无安全感，客户流失		维护、提升品牌安全影响力和美誉度，让用户有安全感
合规与法律风险	面临监管部门处罚，严重时受到法律制裁，无法在某些领域开展业务		在满足安全合规、法律要求的同时，建立并持续运营符合公司实际情况的安全管理体系

安全跑在业务前面

- 从安全维度全面保障和支撑公司业务正常运营和快速发展，领先竞争对手，在商业竞争中处于主动地位

安全与业务同步发展

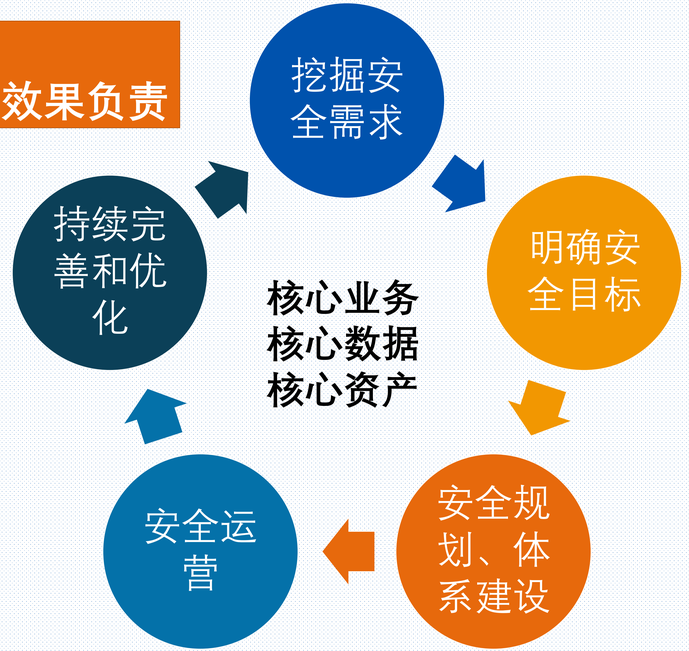
- 勉强保障和支撑公司业务正常运营和发展，大多数时候安全会充当救火队员角色

安全落后于业务发展

- 无力应对企业面临的网络攻击和无法有效控制安全风险，安全成为影响公司正常运营和业务快速增长的瓶颈和风险点

互联网企业安全建设整体思路

原则：
目标导向，对结果和效果负责



挖掘安全需求

对象：公司高层、兄弟部门、业务部门、安全团队

要点：1、知晓面临安全威胁、风险、挑战和现有安全能力

2、理解公司期望与诉求

明确安全目标

要点：1、合理、清晰、量化、可衡量

2、区分长、中、短期目标

3、对于目标理解和需要投入资源达成一致

安全规划、体系建设

要点：1、方向和思路对

2、区分紧急度和优先级，分阶段建设

3、高层支持、合理投入、动态调整、定期review

安全运营

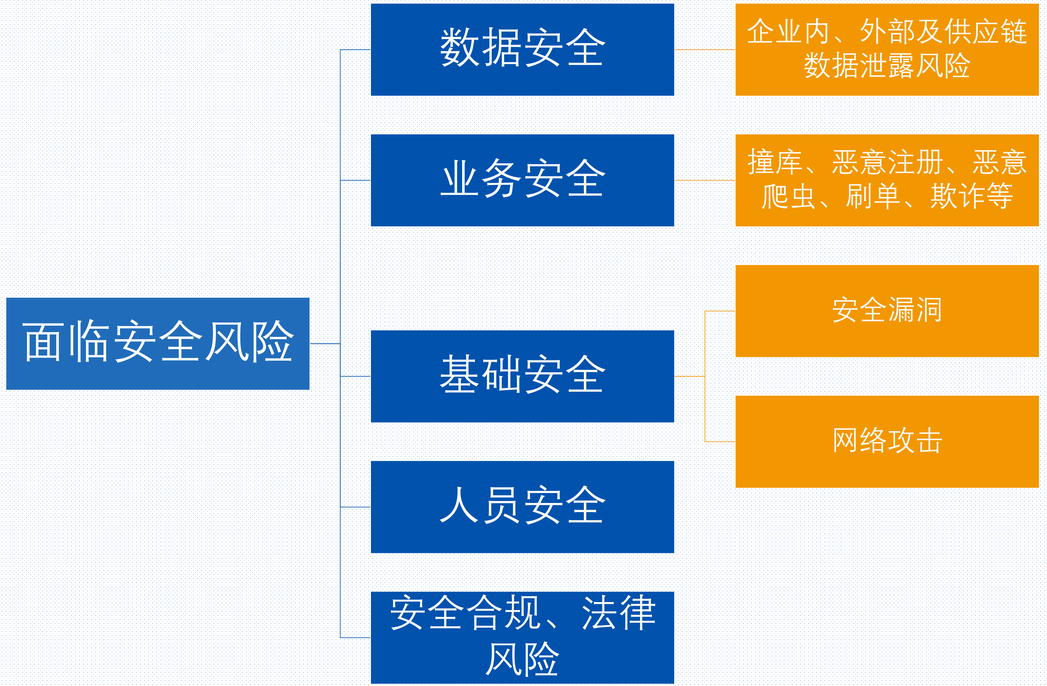
要点：1、持续、指标化、量化、可视化

2、总结经验、发现不足、定期汇报

持续优化和完善

要点：1、客观评价、务实、可落地、持续迭代、形成闭环

互联网企业面临安全风险与影响



安全风险引发的后果或影响：

1、大量机密、敏感数据被内、外恶意用户、攻击者、竞争对手、黑产获取

2、业务中断、稳定性、可用性受影响

3、PR事件，公司声誉、品牌受损，公信力下降

4、用户流失、经济损失、公司市值下降、IPO受影响

5、不合规导致被网安、监管机构处罚、无法正常开展业务、与外部合作受阻

互联网企业核心安全目标

数据安全

- 可以主动识别数据在全生命周期内和流动过程中的数据安全风险和评估出合理风险等级，并将风险控制在可接受范围内
- 具备对数据泄露事件的应急响应和溯源调查能力

业务安全

- 可以主动发现潜在业务安全风险，提供解决方案和将风险控制在可接受范围内
- 有能力支撑和应对业务正常发展和运营过程中以及业务场景变化可能带来新的业务安全风险

基础安全

- 具备主动发现主流安全漏洞和提供修复方案以及推动漏洞修复的能力
- 具备对主流网络攻击和明显异常行为的主动感知和防御能力
- 具备对安全事件应急响应和攻击溯源能力

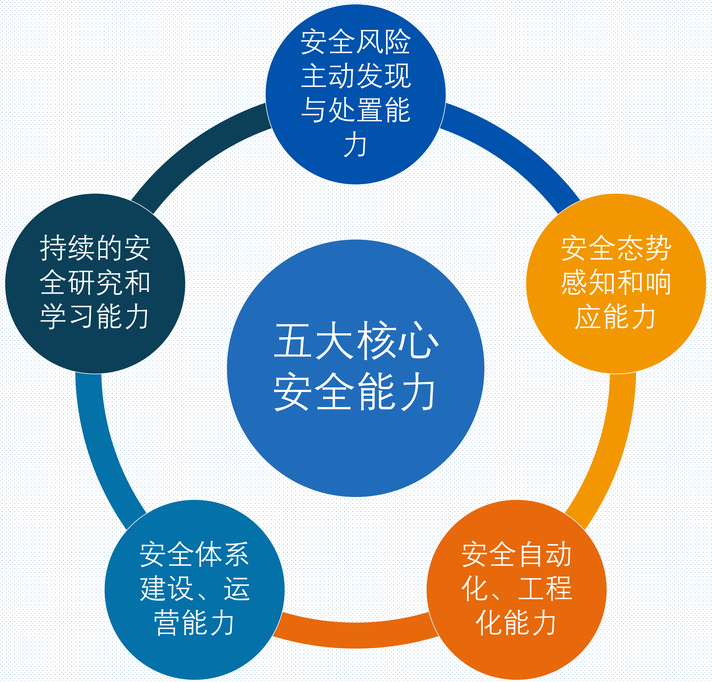
人员安全

- 让员工理解自身在公司信息安全方面的职责和义务
- 让员工具备安全意识思维和识别日常工作和生活中的常规攻击手段的能力

安全合规

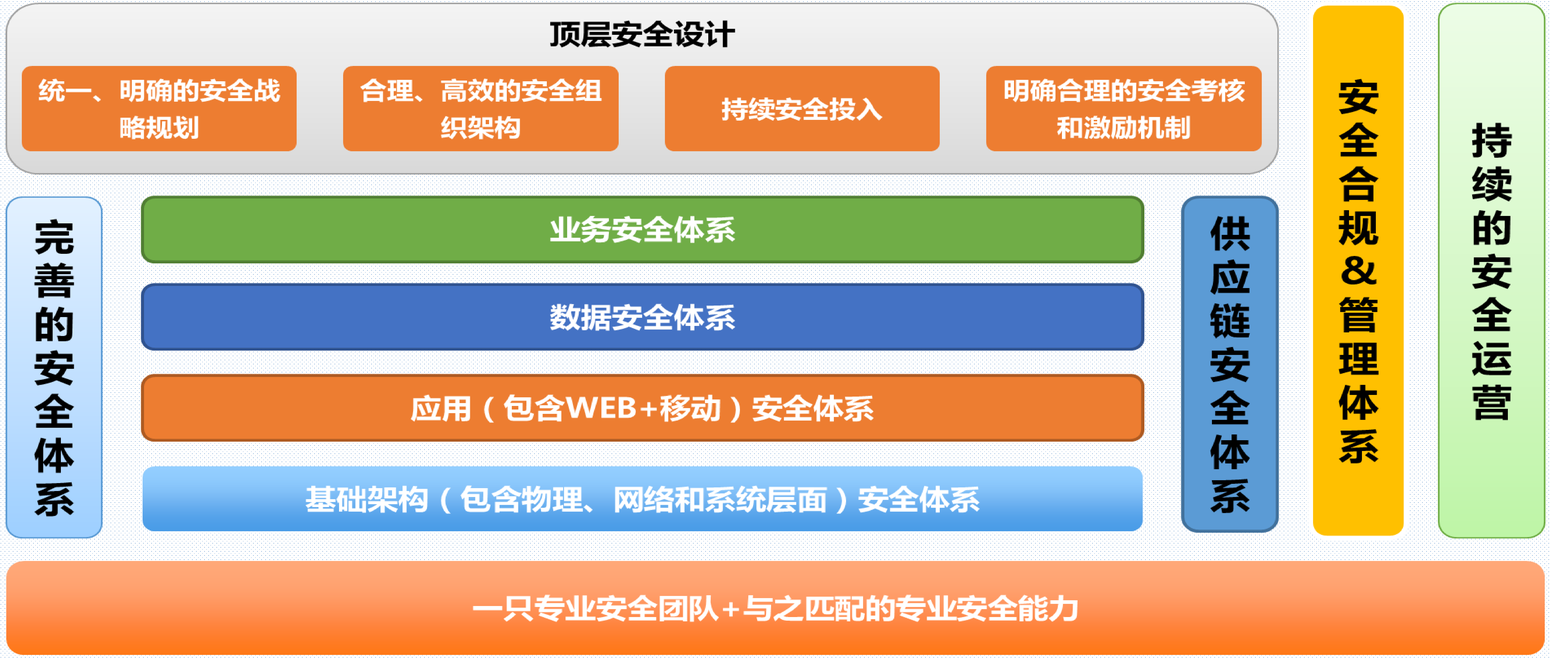
- 满足安全监管、法律要求，有效支持公司业务开展、运营和外部合作
- 在满足安全合规的基础上，构建符合公司自身特性的安全合规体系

互联网企业核心安全能力建设



- **安全风险主动发现与处置能力**
  - 主流安全风险(数据、业务、漏洞)主动发现、修复方案提供及修复推动能力
- **安全态势感知和响应能力**
  - 具备主流网络攻击、明显异常行为的主动发现和快速应急响应能力
- **安全自动化、工程化能力**
  - 自动化安全工具、系统及平台的设计和研发能力
- **安全体系建设、运营能力**
  - 具备体系化安全建设思维、视野和格局和持续安全运营能力
- **持续的安全研究、学习能力**
  - 应对新攻击、威胁、漏洞的能力

互联网企业安全蓝图


顶层安全设计
统一、明确的安全战略规划
合理、高效的安全组织架构
持续安全投入
明确合理的安全考核和激励机制
完善的安全体系
业务安全体系
数据安全体系
应用（包含WEB+移动）安全体系
基础架构（包含物理、网络和系统层面）安全体系
供应链安全体系
安全合规&管理体系
持续的安全运营
一只专业安全团队+与之匹配的专业安全能力

互联网企业安全整体视角

数据安全

- 数据安全治理
- 数据安全分析与自动化

业务安全

- 帐号安全
- 接口防刷
- 内容安全
- 反作弊、反欺诈等

基础安全

- 生产网络：物理、网络、主机、应用安全
- 办公网络：物理、网络、内部应用、终端安全

安全管理

- 安全流程、规范与制度
- 人员安全意识、文化建设

安全运营

- SRC平台
- 安全监控、响应
- 外部安全合作、交流

安全合规

- 等级保护
- ISO27001

供应链安全

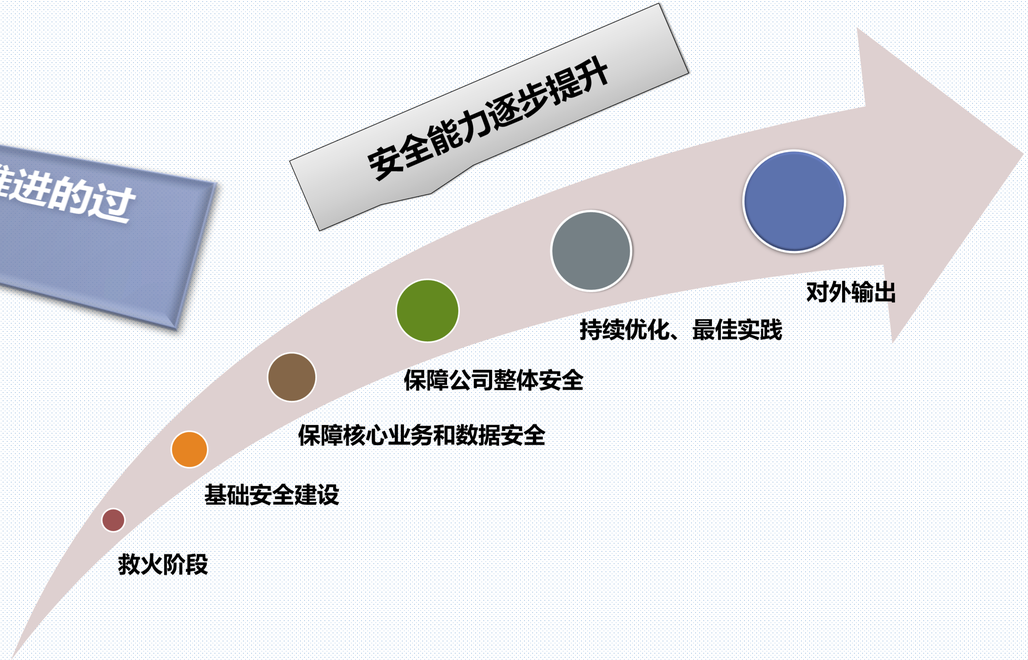
- 上下游合作伙伴安全
- 第三方采购产品安全
- 外包产品开发与人员安全

如何落地实施

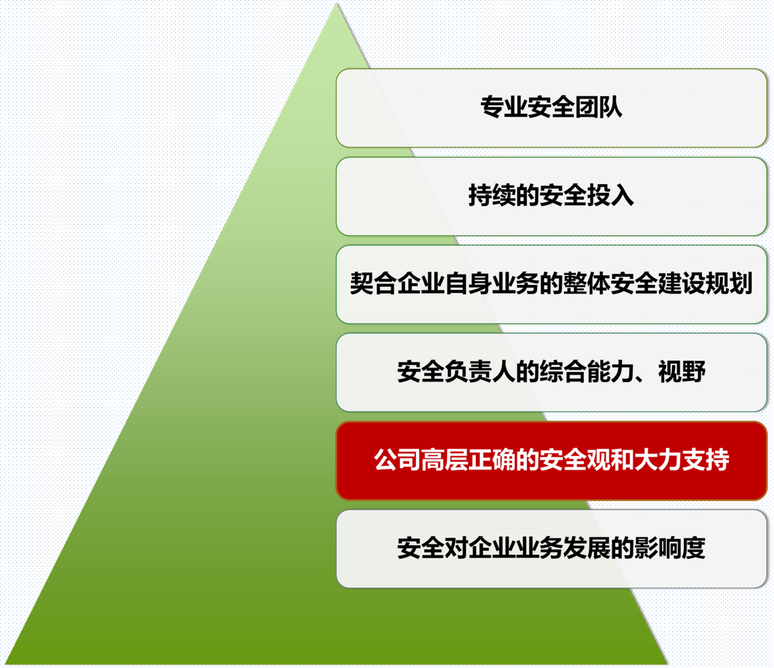
安全大类	安全子类		安全目标			实现方式	优先级	自研或第三方
基础架构安全	物理安全	1、保障物理层面安全性	应用安全	WEB安全	1、公司WEB应用业务系统定期漏洞扫描与渗透测试	WEB漏洞扫描，集成至自动化安全扫描平台		
	网络安全	1、安全域合理划分				每季度定期实施内部和外部渗透测试，输出渗透测试报告		
		2、端口安全：对公网只			2、各产品线核心业务系统强制实施SDL(安全开发流程)	VIPKID SDL(安全开发流程)推动与实施		
		3、只允许线上业务系统				安全漏洞管理规范		
		4、传输安全：保障敏感				WEB安全编码规范		
						WEB安全设计规范		
		5、网络攻击、入侵检测				项目上线前例行安全测试		
						安全漏洞管理平台		
						项目安全评审系统		
						自动化代码安全审计系统		
		6、网络设备安全加固与			3、WEB入侵检测、安全分析、安全防护、态势感知及应急响应	WAF(WEB应用防火墙)		
						WEB日志实时安全分析平台		
						WEB日志离线安全分析平台		
	系统安全	1、主机漏洞扫描、安全		移动安全	1、APP安全设计、安全测试、安全加固及安全监测	APP安全设计规范		
						APP发版前例行安全测试		
						APP自动化漏洞扫描系统		
						APP自动化安全加固系统		
						钓鱼、盗版类APP监测系统或服务		
		2、主机层面入侵检测与安全防护、态势感知				HIDS(主机入侵检测系统)		

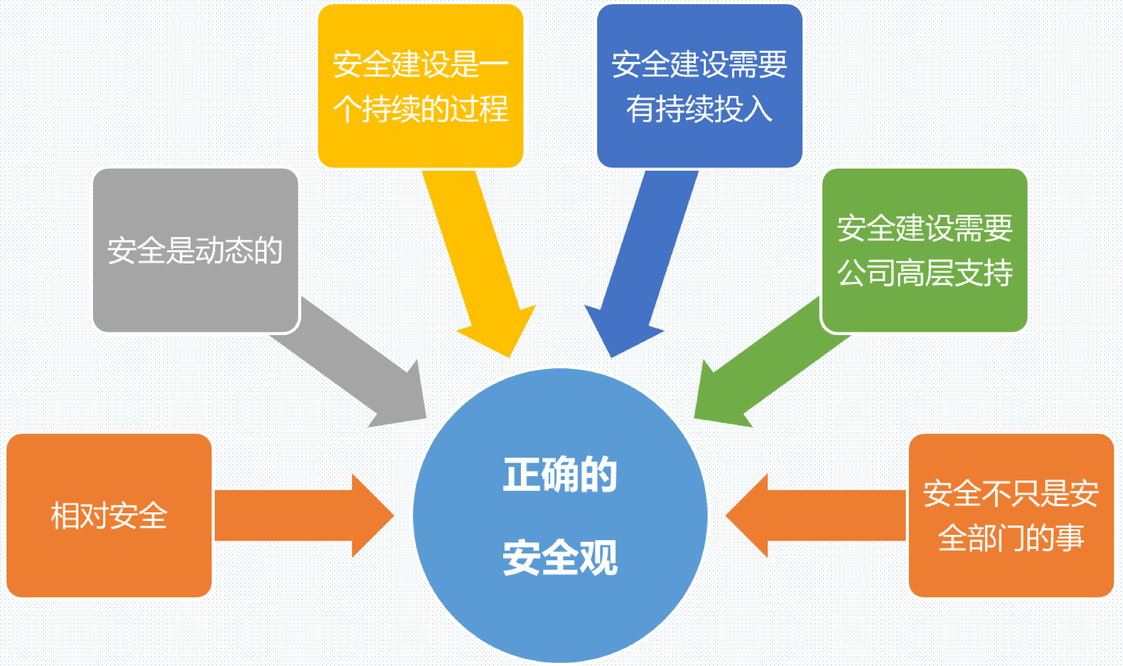
分阶段安全体系建设

安全体系建设是一个分阶段逐步推进的过程，是一个系统化的工程

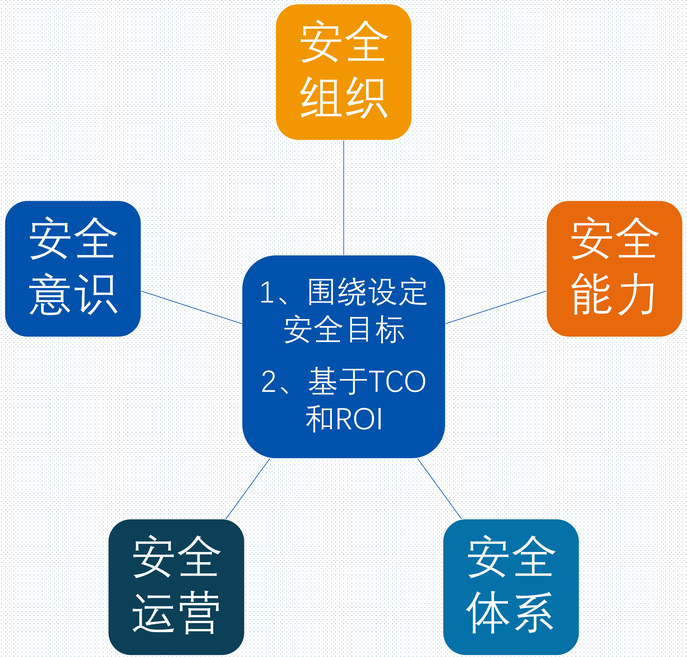


做好安全建设的必要条件



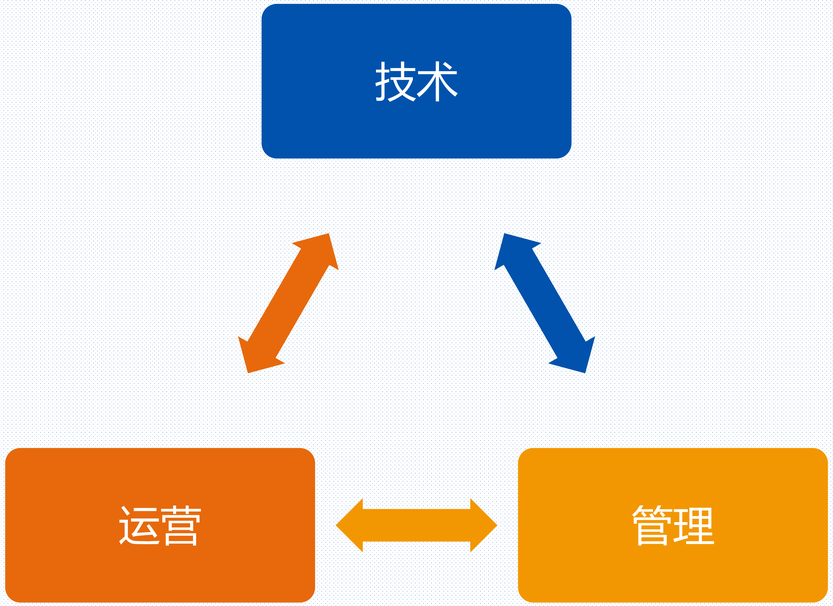


如何衡量安全建设的效果



编号	评价方面	评价指标(参考)
1	**安全组织**	1、安全团队规模；2、团队角色构成和分布；3、部门层级；4、安全负责人职级和汇报对象
2	**安全能力**	1、安全风险主动发现和处置能力；2、安全态势感知和响应能力；3、安全自动化、工程化能力、4、安全体系建设、运营能力；5、持续的安全研究和学习能力
3	**安全体系**	1、安全体系的合理性和完整性
4	**安全运营**	1、是否实现持续运营；2、是否设定运营指标及指标是否合理、明确；3、运营指标是否可量化和可视化；4、运营指标设定和实现粒度；5、是否有运营指标考核标准及标准是否落地执行
5	**安全意识**	1、知晓和理解公司对其在信息安全方面的职责和义务要求员工数占比；2、单位时间内因人员安全意识薄弱导致安全事件和安全违规事件数量和占比

安全漏洞管理平台建设实践



VIP KID 安全漏洞管理平台

首页　漏洞列表　漏洞

当前位置： 安全漏洞管理平台 >> 首页

最新提交

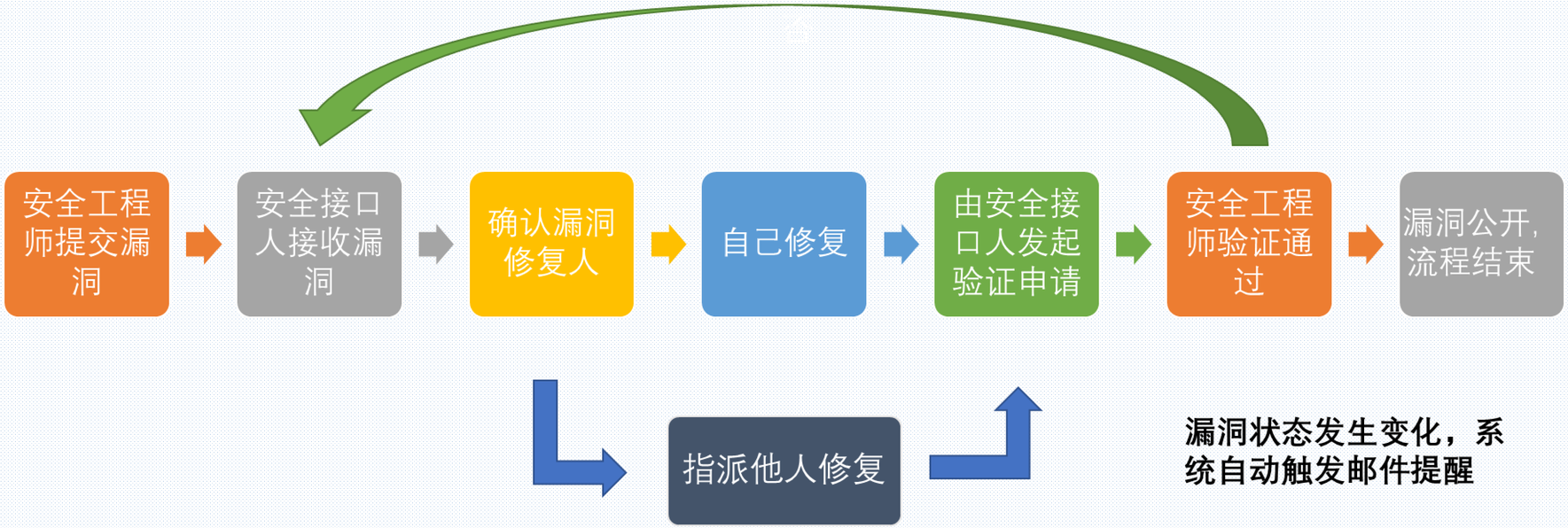
漏洞编号	提交时间
SEC-VD-201808-015	2018-08-23 14:14:36
SEC-VD-201808-014	2018-08-23 11:52:13
SEC-VD-201808-013	2018-08-23 11:47:59
SEC-VD-201808-012	2018-08-23 11:42:35
SEC-VD-201808-011	2018-08-22 11:44:04

漏洞列表

请选择　在这里输入内容

漏洞编号	提交时间	漏洞名称	漏洞等级	漏洞作者	漏洞状态	安全接口人
SEC-VD-201808-015	2018-08-23 14:14:36	[redacted]	低危	[redacted]	待修复	[redacted]
SEC-VD-201808-014	2018-08-23 11:52:13	[redacted]	低危	[redacted]	待修复	[redacted]
SEC-VD-201808-013	2018-08-23 11:47:59	[redacted]	中危	[redacted]	待修复	[redacted]
SEC-VD-201808-012	2018-08-23 11:42:35	[redacted]	高危	[redacted]	待修复	[redacted]
SEC-VD-201808-011	2018-08-22 11:44:04	[redacted]	中危	[redacted]	待修复	[redacted]
SEC-VD-201808-010	2018-08-[redacted]	[redacted]	低危	[redacted]	待修复	[redacted]
SEC-VD-201808-009	2018-08-[redacted]:43	[redacted]	中危	[redacted]	待修复	[redacted]
SEC-VD-201808-008	2018-08-[redacted]6:51	[redacted]	中危	[redacted]	待修复	[redacted]
SEC-VD-201808-007	2018-08-[redacted]38	[redacted]	中危	[redacted]	待修复	[redacted]
SEC-VD-201808-006	2018-08-1[redacted]4	[redacted]	低危	[redacted]	待修复	[redacted]

漏洞修复流转图：



漏洞状态发生变化，系统自动触发邮件提醒

五大核心功能模块

资产管理	漏洞管理	漏洞态势	用户中心	安全知识库
核心功能： 1、资产列表 2、添加、编辑、删除资产 3、资产关联安全接口人、所属业务线或团队	核心功能： 1、漏洞提交 2、漏洞列表、搜索 3、漏洞等级管理 4、漏洞来源管理 5、漏洞类型管理 6、漏洞提醒管理(状态变化提醒、延期提醒)	核心功能： 1、漏洞数量趋势 2、漏洞状态、等级、来源、类型分布 3、漏洞修复率 4、安全工程师发现漏洞数统计与趋势分析	核心功能： 1、角色管理 2、用户管理 3、权限管理 4、个人中心	核心功能： 1、主流安全漏洞介绍与修复方案 2、记录、分享和沉淀VIPKID的安全经验

安全漏洞管理平台建设实践

漏洞管理部分细节设计：

漏洞提交

- 必填项：漏洞标题、受影响系统、漏洞类型、漏洞等级、漏洞来源、漏洞描述、漏洞危害、漏洞详情、漏洞修复方案
- 系统自动对应：漏洞编号、漏洞接口人、漏洞修复时长、对应漏洞知识库链接
- 小细节：受影响系统快速定位、支持拖拽上传图片、截图、漏洞提交预览、临时查看链接

漏洞编号

- 生成及命名规则：SEC-VD-年月-当月第几个漏洞
- 漏洞编号的意义：通过漏洞编号即可快速了解当月漏洞总数及当前漏洞为当月第几个漏洞；例如SEC-VD-201808-007，就代表2018年8月第7个漏洞

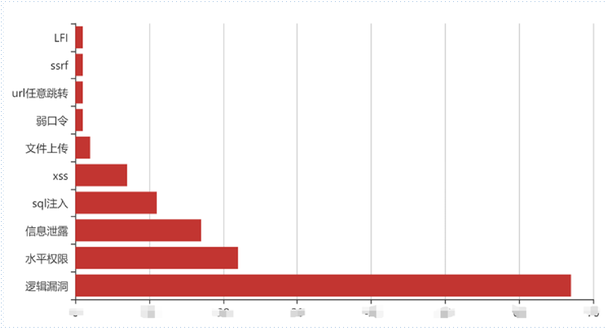
漏洞提醒

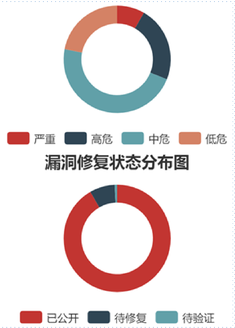
- 漏洞状态变化提醒：漏洞状态发生变化自动触发邮件或其他方式提醒
- 漏洞延期提醒：系统自动扫描延期修复漏洞，自动给对应安全工程师、安全接口人及其部门负责人发送邮件或其他方式提醒

漏洞态势部分细节设计：

多维度漏洞态势监控与分析

漏洞数量&趋势 | 漏洞状态分布 | 漏洞类型分布 | 漏洞等级分布 | 漏洞来源分布 | 漏洞修复率 | 安全工程师发现漏洞数&趋势





安全漏洞管理平台建设实践

用户中心部分细节设计：

角色管理

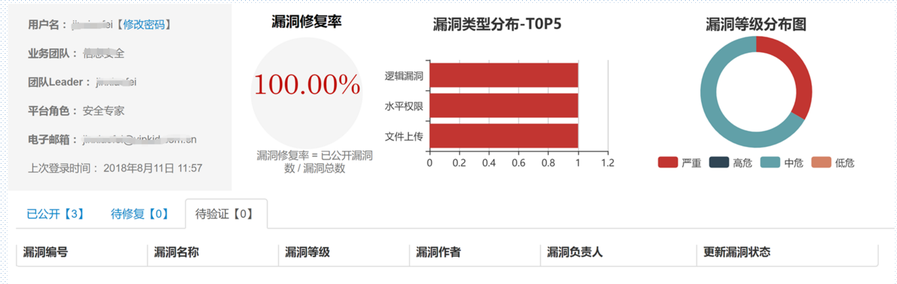
- 五种角色：安全专家、安全接口人、部门负责人、普通用户、管理员

权限管理

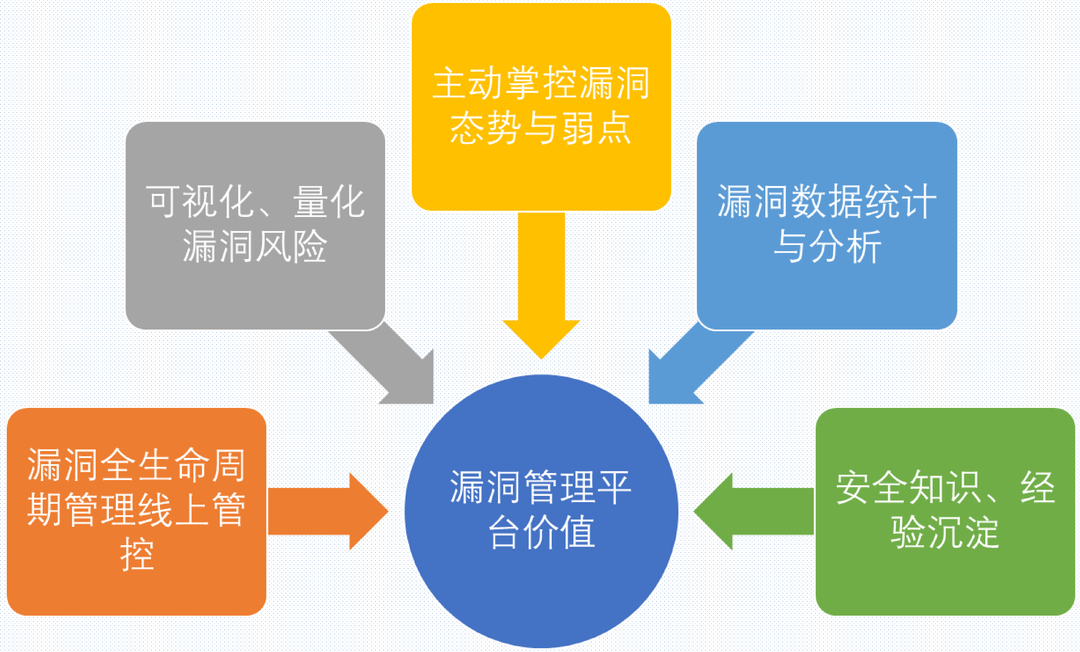
- 安全专家：提交、管理漏洞
- 安全接口人：查看、管理自己负责业务系统的漏洞
- 部门负责人：查看负责部门的所有漏洞
- 普通用户：只允许查看已修复公开的漏洞
- 管理员：拥有最高权限

个人中心

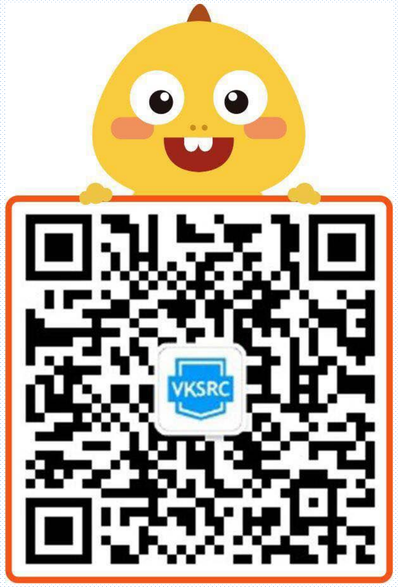
- 安全专家：可查看、维护自己提交的所有安全漏洞及对应的漏洞态势
- 安全接口人&部门负责人：可查看、维护自己负责所有漏洞以及对应的漏洞态势



安全漏洞管理平台建设实践



写在最后




ThreatBook
感谢您的观看
2018 网络安全分析与情报大会