互联网企业安全建设实践

靳晓飞　VIPKID安全中心

北京站/3.29

从这里说起

国家

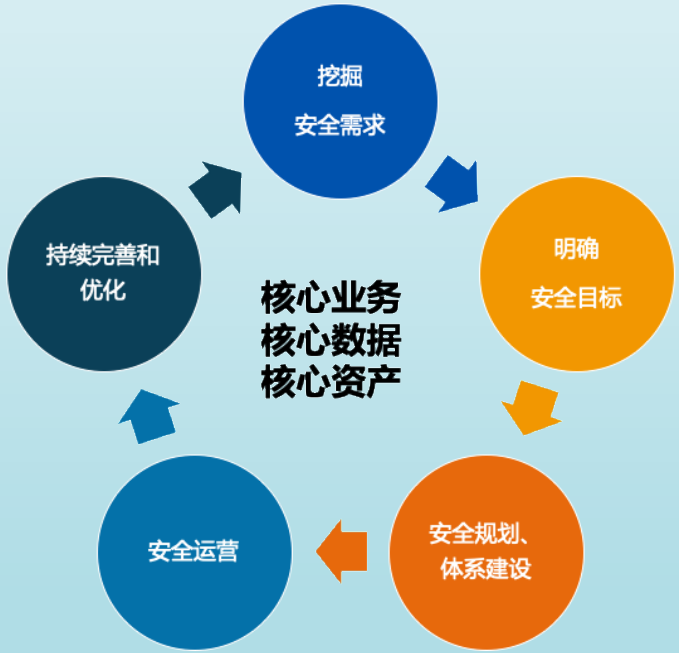
行业

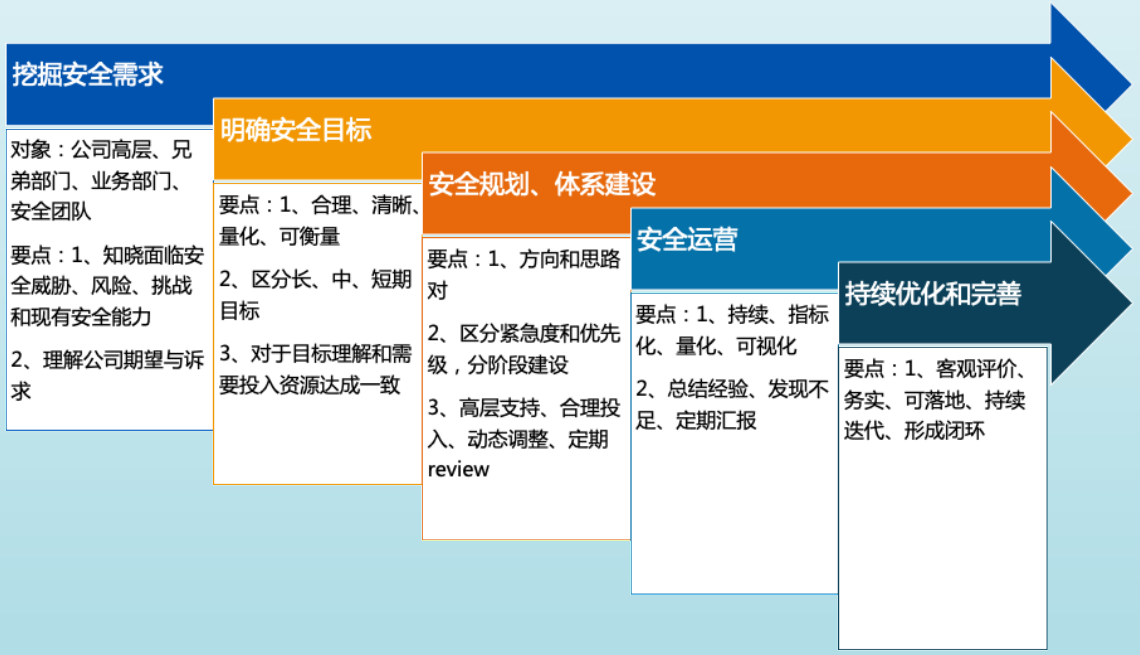
个人

互联网企业安全建设怎么做

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





互联网企业面临安全挑战分析

1、外部攻击者
2、内鬼
3、供应链
4、安全合规风险

1、窃取敏感数据
2、打击报复
3、获取目标系统权限
4、恶意勒索
5、利益驱使
6、被当作攻击跳板

1、利用系统漏洞
2、恶意扫描、探测
3、恶意爬取
4、DDOS、CC攻击
5、定向渗透攻击
6、APT
7、勒索攻击
8、利用合法权限非法获取数据

1、批量敏感数据泄露
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、市值下降、IPO受影响
5、不合规被监管机构处罚
6、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	业务安全	基础安全	人员安全	安全合规
• 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	• 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	• 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	• 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	• 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与提升

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

互联网企业整体安全视角

互联网企业基础安全体系建设框架

核心安全流程与制度

持续安全运营：安全系统与平台运营、红蓝对抗、安全监控、安全漏洞预警、威胁情报、入侵检测、安全响应、态势感知等

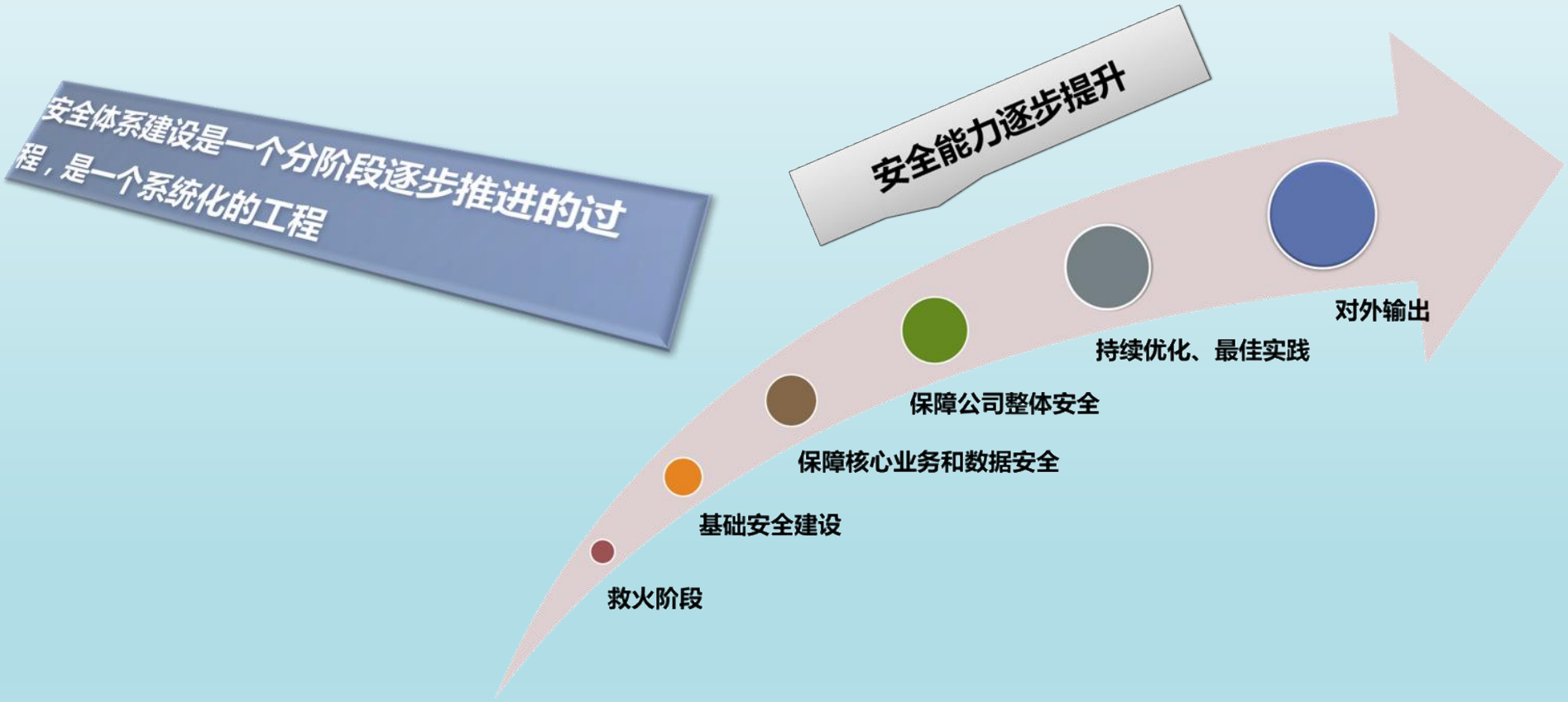
互联网企业安全建设蓝图

互联网企业安全建设如何落地实施

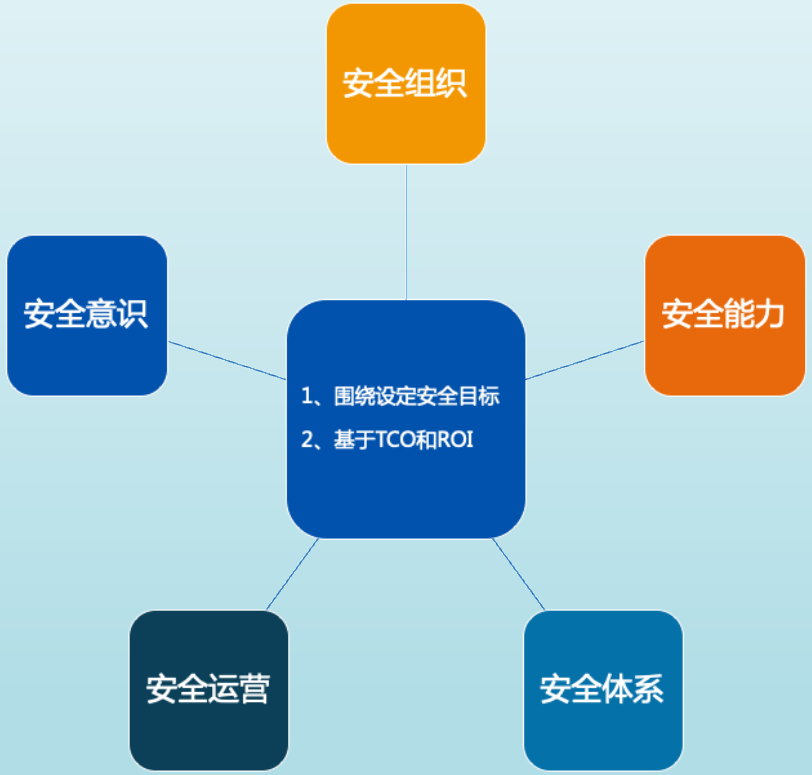
安全大类	安全子类	安全目标	实现方式
基础架构安全	物理安全	1、保障物理层面安全性	
	网络安全	1、安全域合理划分	根据业务划分不同的安全域
		2、端口安全：对公网只开放必要端口	端口开放安全管理制度
			自动化端口开放扫描，集成至自动化安全扫描平台
		3、只允许线上业务系统对公网开放	自动化域名安全评估，集成至自动化安全扫描平台
		4、传输	流量抗攻安全监测系统或服务
		5、网络	
		6、网络	
	系统安全	1、主机	
		2、主机	

安全大类	安全子类	安全目标	实现方式
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
			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、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
			安全漏洞管理规范
			WEB安全编码规范
			WEB安全设计规范
			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
		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
	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

分阶段安全体系建设

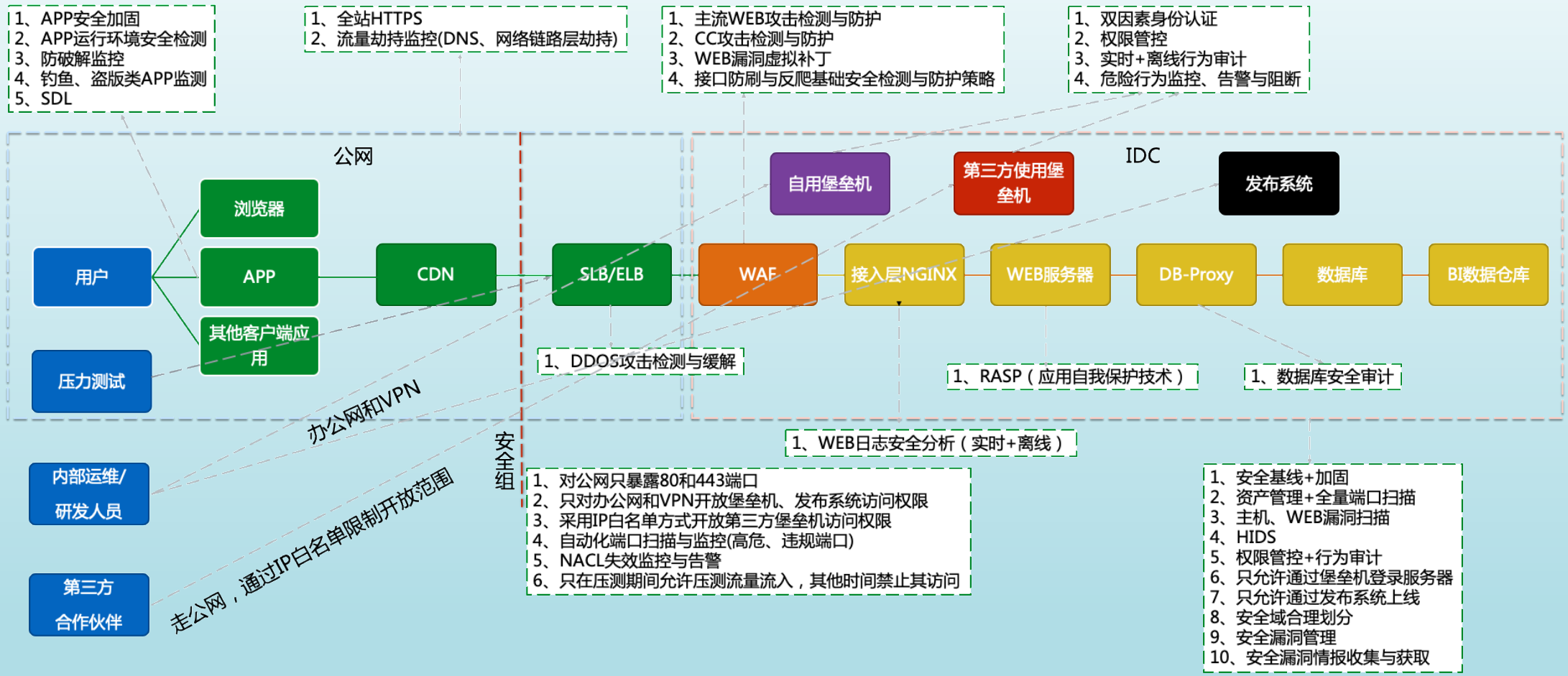

安全体系建设是一个分阶段逐步推进的过程，是一个系统化的工程
安全能力逐步提升
救火阶段
基础安全建设
保障核心业务和数据安全
保障公司整体安全
持续优化、最佳实践
对外输出

如何评价企业安全建设的效果



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

基础安全全链路纵深防御架构



API 安全监控实践

需要对哪些API进行安全监控?

- 注册接口
- 登录接口
- 找回密码接口
- 订单详情接口
- 收货地址接口
- 其他所有可能会被刷的API

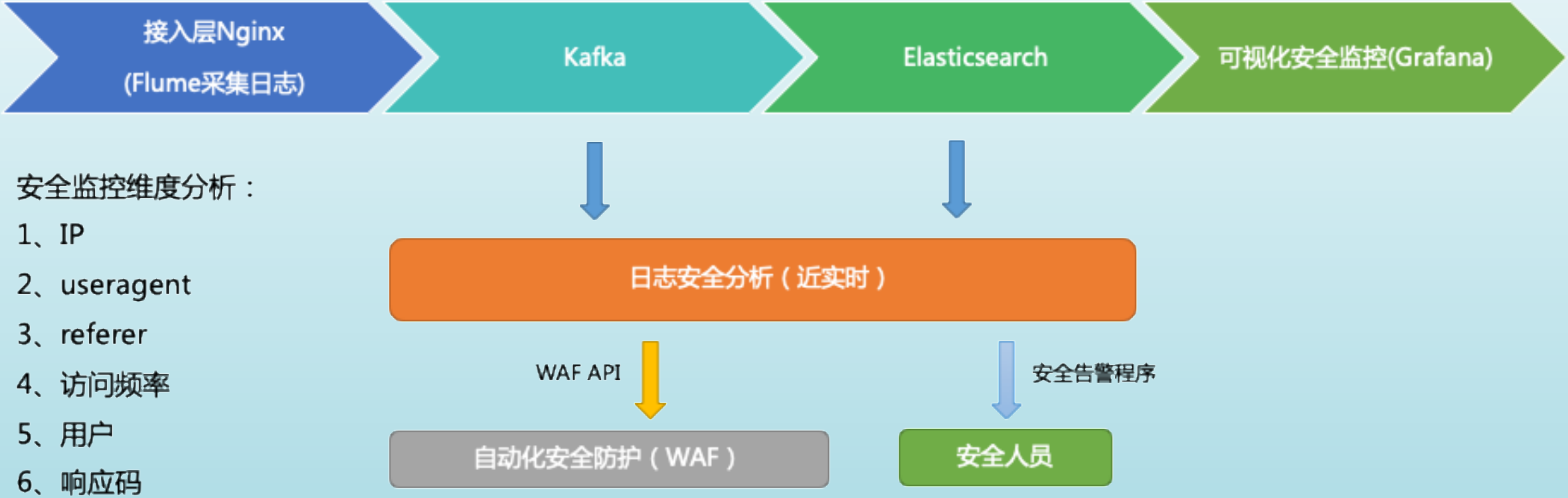
安全监控目标设定

- 具备对高风险API被刷的分钟级主动发现和感知能力，并可与安全防御系统联动，实现自动化安全防护

技术上如何实现

- 流量分析
- 日志分析

API 安全监控实践



安全监控维度分析：

1、IP

2、useragent

3、referer

4、访问频率

5、用户

6、响应码

7、其他

API 安全监控实践

```
        query: "request_method:\"POST\" AND url:\
#告警方式设置：command、email、sns
alert:
- "command"
pipe_match_json: true
command: ["/opt/weixin_alert/weixin_alert.py"]
```

触发安全策略：www-用户注册-[redacted]

攻击时间：30/Oct/2018:17:42:31 +0800

受攻击URL：/rest/parentrest/api/p[redacted]Up

Method：POST

响应码：400

攻击次数：1312

攻击者IP：122.[redacted].29

物理位置：

user_agent：Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0

Referer：https:/[redacted]%3Cfmjdjibgni

学生ID：-

已自动将此攻击IP加入WAF黑名单

```
#从elastalert获取告警详情并格式化
def format_msg():
    content = sys.stdin.read()
    #提取告警详情
    alert_content = json.loads(content[1:-2])
    # 提取告警规则名称
    rule_name = alert_content['rule_name']
    #提取攻击时间
    date_time = alert_content['time_local']
    #提取攻击次数
    attack_counts = alert_content['num_hits']
    #提取受攻击URL
    url = alert_content['url']
    #提取攻击源IP
    src_ip = alert_content['http_x_forwarded_for']
    #提取攻击者UA信息
    user_agent = alert_content['http_user_agent']
    #提取HTTP响应码
    status = alert_content['status']
    #提取referer
    referer = alert_content['http_referer']
    #提取method
    method = alert_content['request_method']
```

Github安全监控实践

VIPKID安全中心自研github安全监控系统开源啦

VIPKID安全中心 VIPKID安全应急响应中心 2018-12-19

系统简介

Github Monitor是由VIPKID安全中心打造的一套用于主动监控github敏感信息泄露的系统。利用该系统可主动、及时发现企业敏感数据通过github泄露的情况。

系统亮点

- 分钟级监控
- 简单且灵活的任务配置
- 邮件提醒
- github token管理
- Docker一键部署
- 运行十分稳定
- 大方、简洁的UI，用户体验好

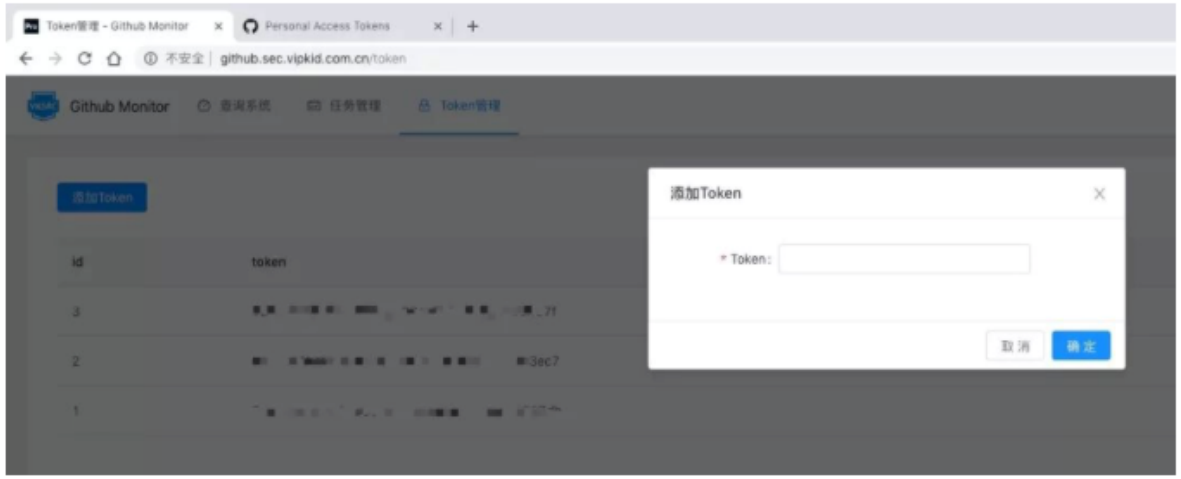
使用手册

1.添加Token

Github Monitor使用Github REST API v3接口进行搜索，所以需要预先配置Token进行认证。

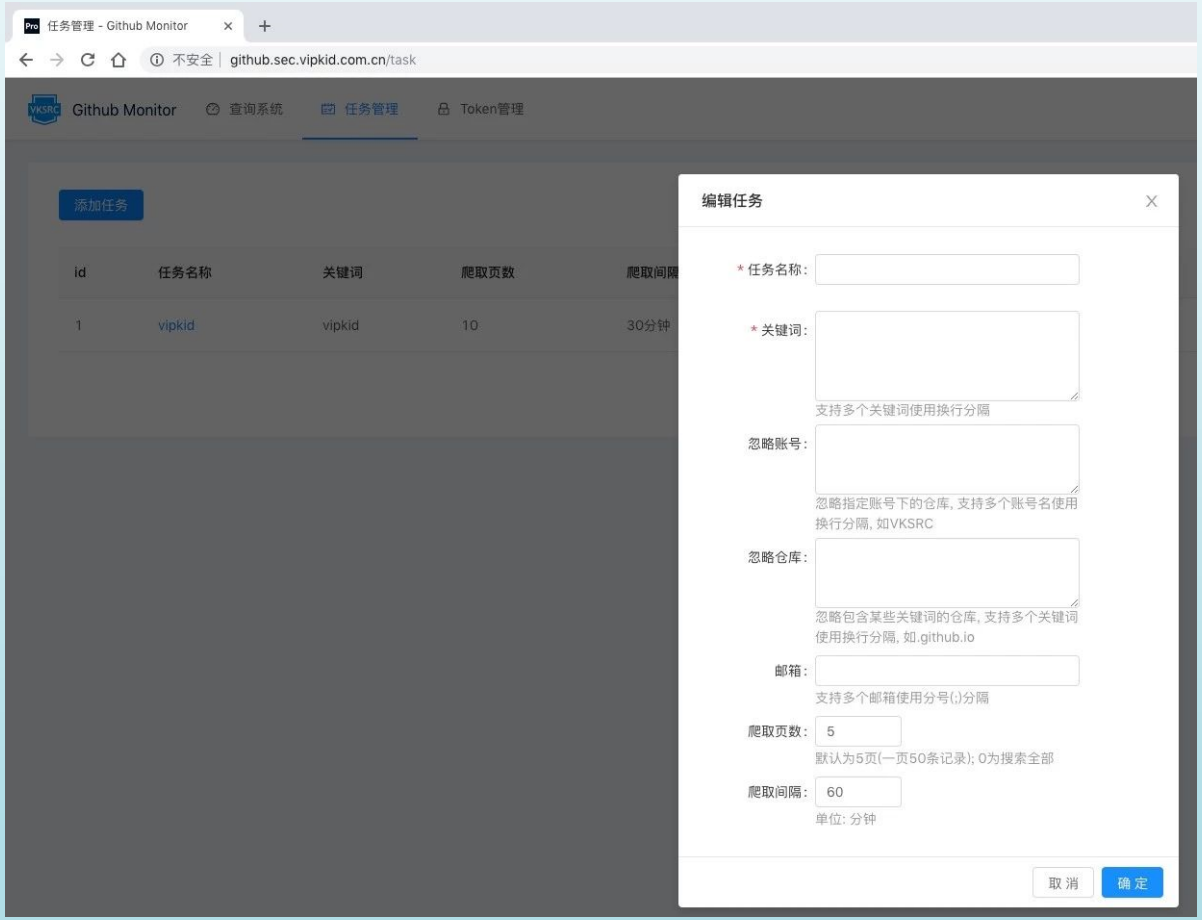
首先登录Github，然后进入Token配置页面创建Token。

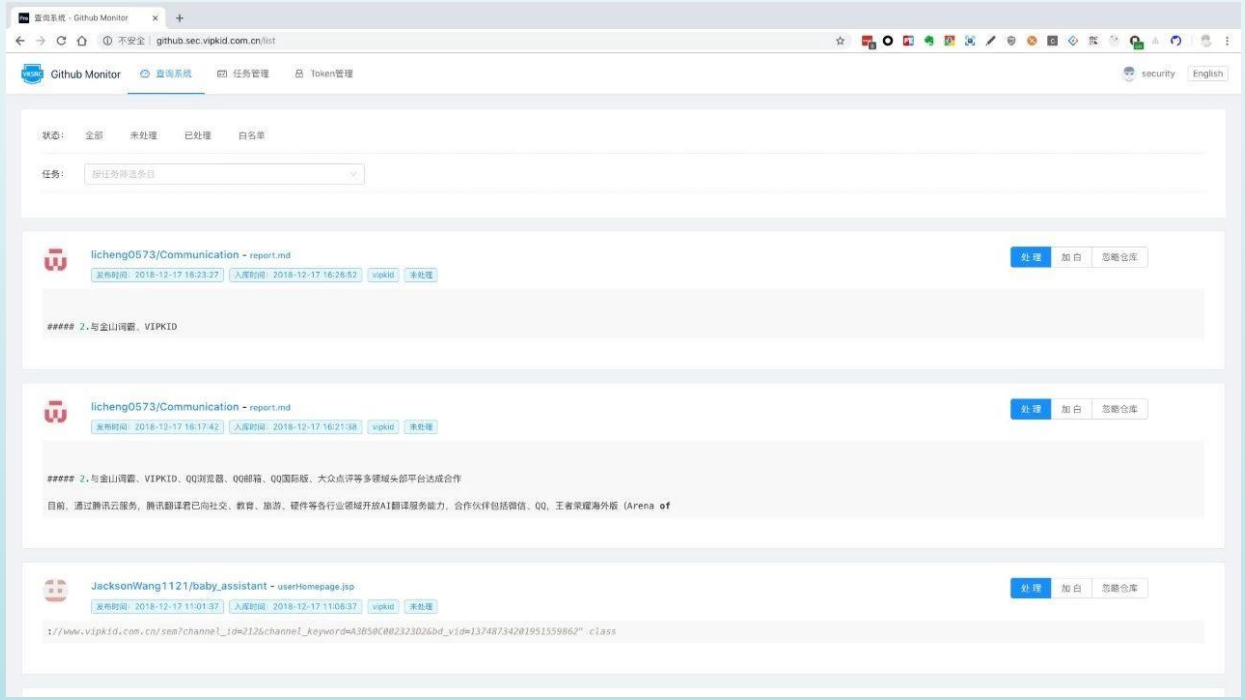
随后把Token添加到Github Monitor中。



Github API有次数限制，1分钟最多请求30次，为了提高爬取速度，Github Monitor支持添加多个Token。

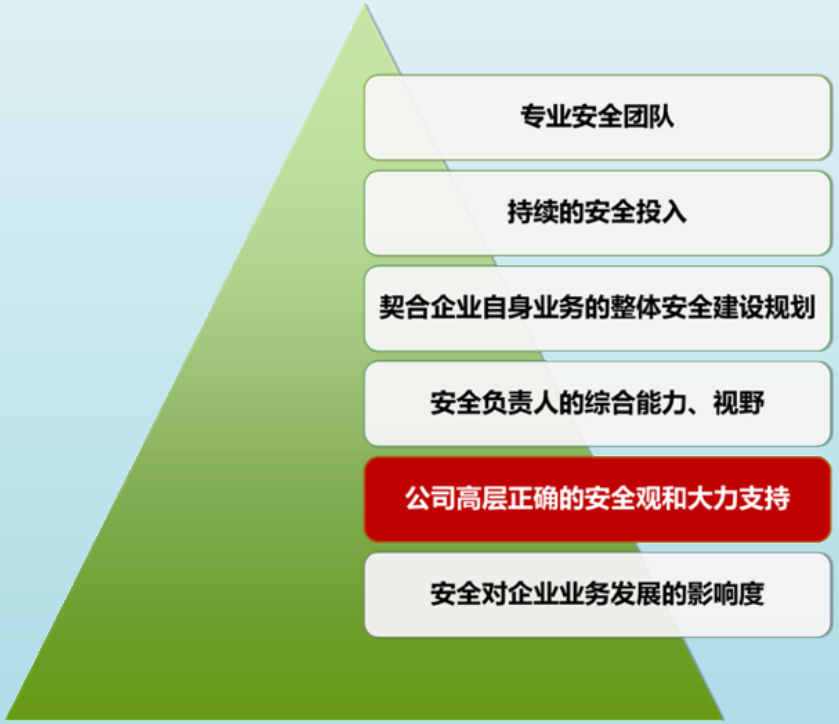
Github安全监控实践





项目地址：https://github.com/VKSRC/Github-Monitor

做好企业安全建设的必要条件



写在最后

“未知攻，焉知防”，网络攻防对抗本质上是人与人之间的较量，在安全建设和安全运营过程中企业安全人员不能仅限于被动防御，还需要积极转变思路，以攻击者视角来看待和审视安全风险，做到攻防兼备，化被动为主动。

Thanks