Geekbang. 极客邦科技 InfoQ

QCon 全球软件开发大会【北京站】2016

一场永不终结的猫鼠游戏

--研发安全的持续运营

苏宁易购/ 黄宙

International Software Development Conference

个人介绍

黄宙 tombook

1999
接触网络

2004
全职境外
安全渗透
技术研究

潜伏加入各类安全组织

2005
《黑客防线》
攻防实验室
最快通关奖

2007
ISO27001

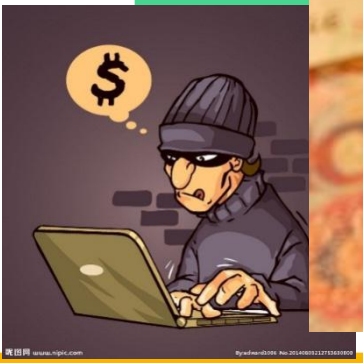
2008
中国电信

2011
IBM

2013
北理工硕士

2014
苏宁易购

“群鼠”驾到



各电商安全部门现状

1. 日常忙于**已上线**业务的“漏洞挖掘”。
2. 安全专业人员数量不足，无法承接每月研发线所有项目安全评审与项目日常安全测试。
3. 不安全新功能，不断上线。
4. 每月X-SRC**易发现**型漏洞，“烧钱”不止。

风险产生与控制

业务型

功能型

第一部分 群鼠到来祸从天降

第二部分 万众创新理论升级

第三部分 产品为本跨界创新

第四部分 大众创业能力输出

第五部分 整合资源运营为王

传统安全研发流程理论

换个姿势思考

安全扫描与测试

渗透手记

端口检测

服务检测

NGINX

ZABBIX

Serv-U

part of the SolarWinds family

社区动力 DISCUZ!

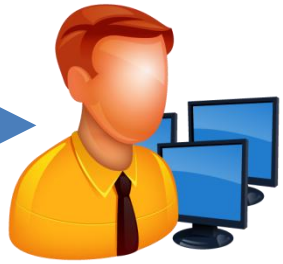
ORACLE

实施攻击

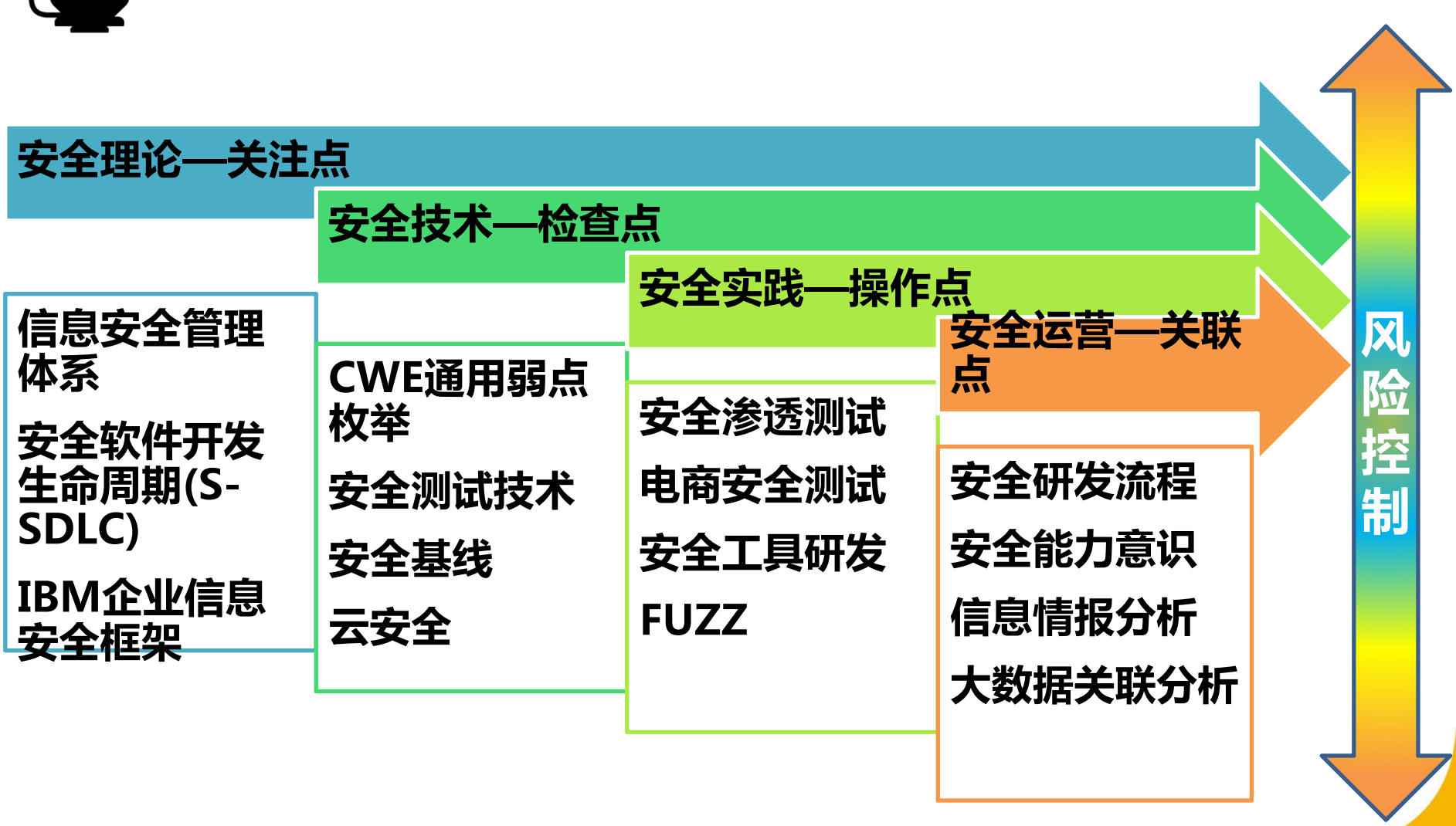
EXPLOIT DATABASE

准备攻击

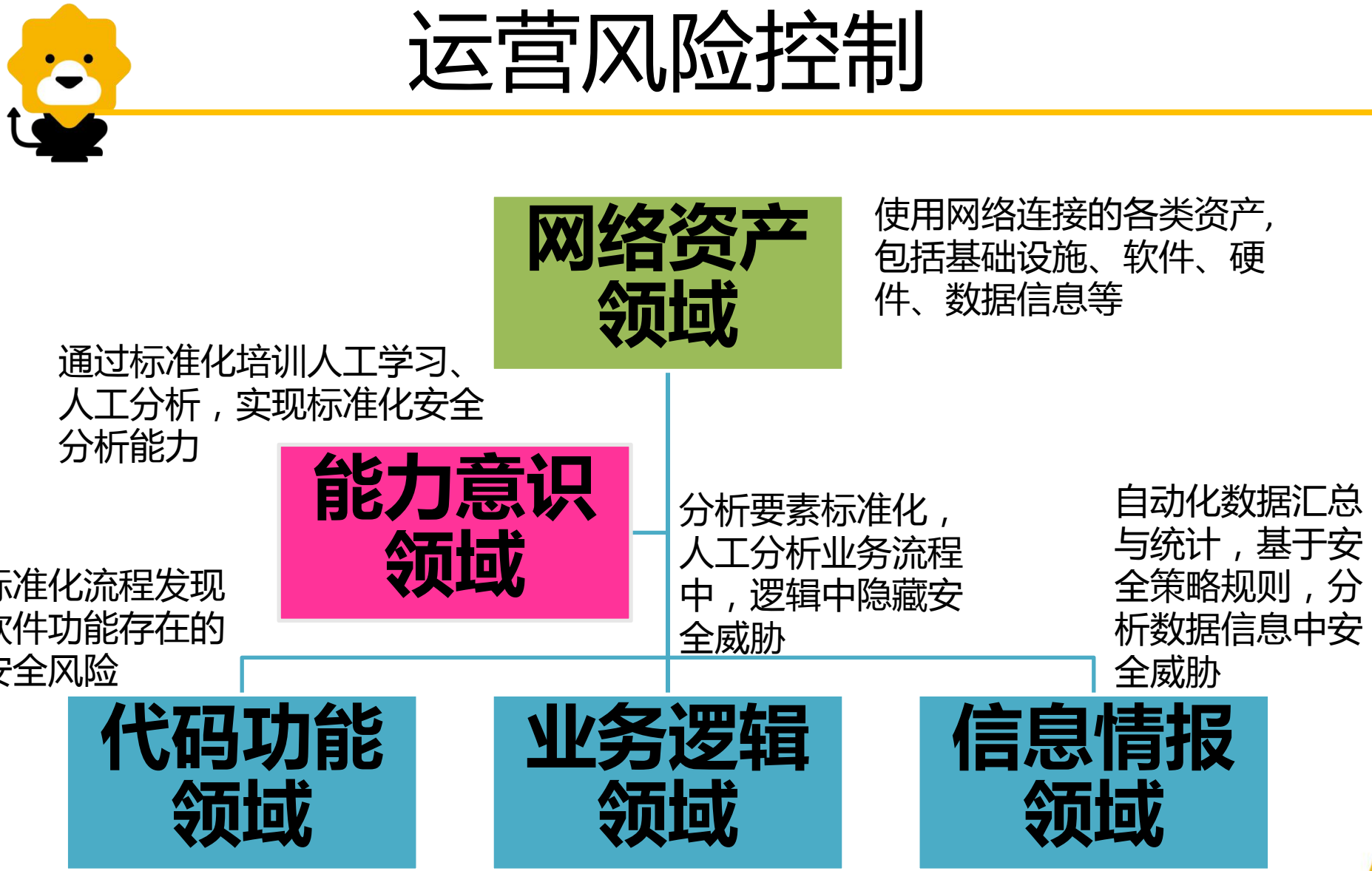
渗入内网



全流程风险控制


安全理论—关注点
安全技术—检查点
安全实践—操作点
安全运营—关联点
信息安全管理体系
安全软件开发生命周期(S-SDLC)
IBM企业信息安全框架
CWE通用弱点枚举
安全测试技术
安全基线
云安全
安全渗透测试
电商安全测试
安全工具研发
FUZZ
安全研发流程
安全能力意识
信息情报分析
大数据关联分析
风险控制

运营风险控制


网络资产领域
使用网络连接的各类资产，包括基础设施、软件、硬件、数据信息等
通过标准化培训人工学习、人工分析，实现标准化安全分析能力
能力意识领域
分析要素标准化，人工分析业务流程中，逻辑中隐藏安全威胁
自动化数据汇总与统计，基于安全策略规则，分析数据信息中安全威胁
标准化流程发现软件功能存在的安全风险
代码功能领域
业务逻辑领域
信息情报领域

产品类型跨界

安全态势感知（安全运营--分析）

	安全软件	风险控制
MS/Linux 应用软件 Redis Elasticsearch	Openvas Nmap Sql map Social Engineer Toolkit	威胁分析 风险分级 安全评估 资产分类

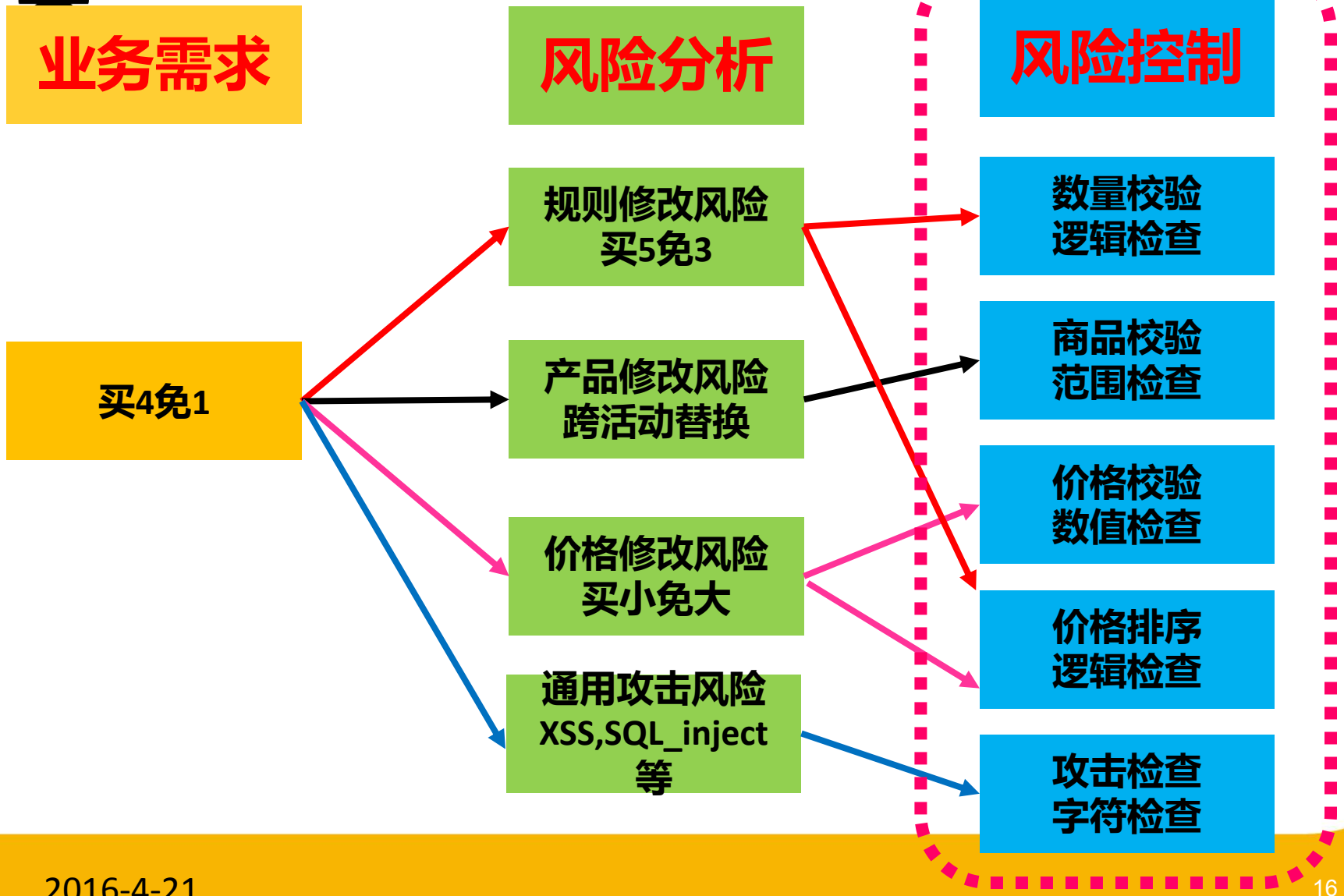
跨界安全策略（安全运营--策略）

HAproxy Hadoop Nginx Syslog Flume	Arachni Snort Nikto THC Hydra HIDS	安全管理流程 通用弱点枚举CWE 安全管理基线 安全技术基线

能力跨界—持续运营能力

软件	安全分析	安全研发
云数据	安全规则	安全关联
管理	安全职责	安全流程

全业务风险分析


业务需求
风险分析
风险控制
买4免1
规则修改风险
买5免3
产品修改风险
跨活动替换
价格修改风险
买小免大
通用攻击风险
XSS,SQL_inject
等
数量校验
逻辑检查
商品校验
范围检查
价格校验
数值检查
价格排序
逻辑检查
攻击检查
字符检查

异常访问流量

IP | 头部 | 存活 | 端口 | 版本 | 历史 | 网段

IP地址库

商业IP库
免费IP库
机房IP
CDN-IP
交换共享

请求分析： 200
UA分析 403
协议分析 500
字符规则分析 TTL
URI源分析 无响应
Accept-Language … …
Accept-Encoding
响应分析：
响应状态分析
响应字符长度分析
Server
Set-Cookie
… …

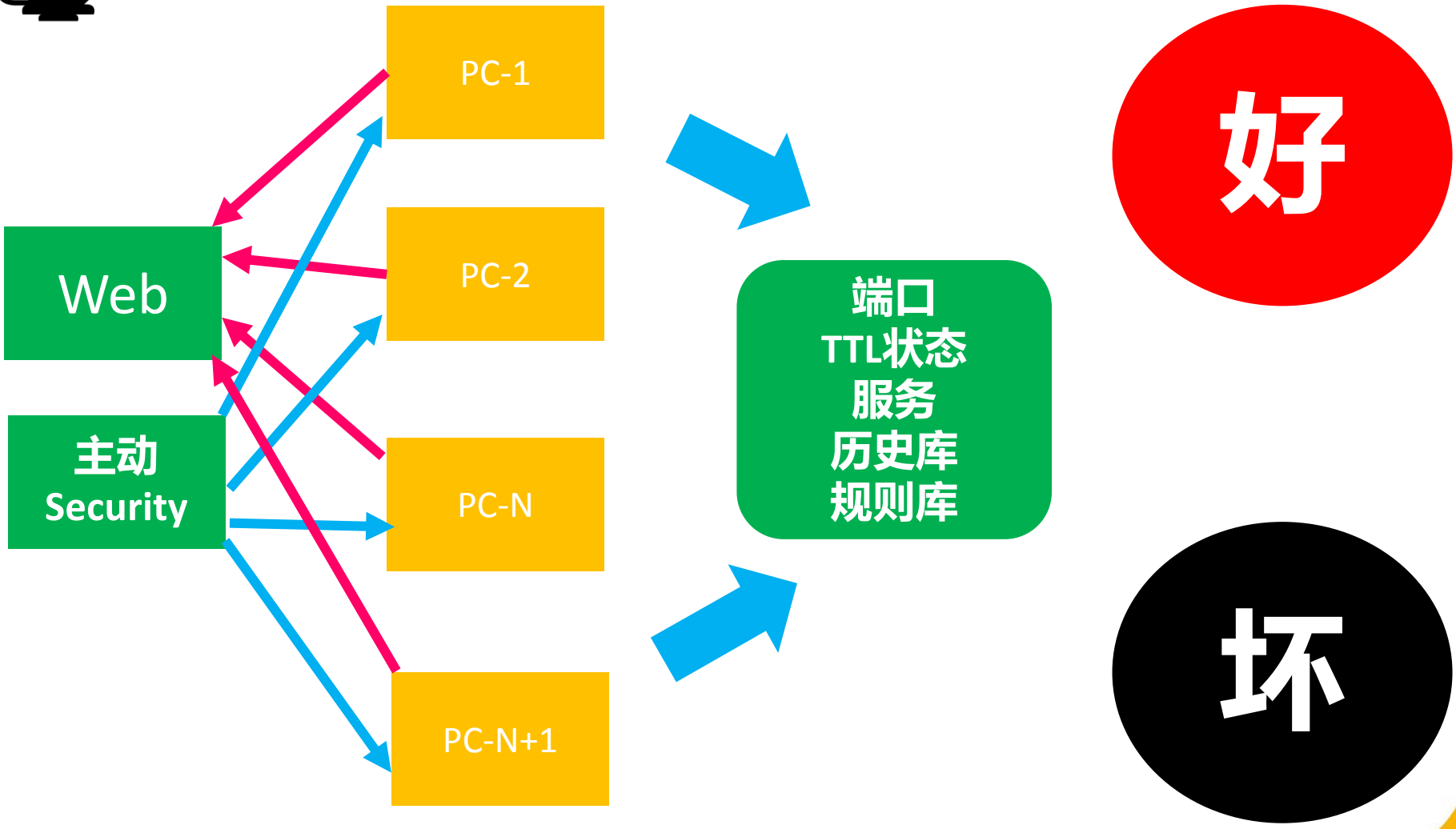
22
25
80
143
443
445
3389
5601
10000
… …

v0.1 2008.8.8
v0.2 2011.1.1
Apache 2013.3.3
Nginx 2015.6.6
Haproxy 2016.4.4
Win2008 … …
Win2010
PHPWIN
Discuz!
… …

202.13.x.x,
中国移动，
共享虚拟
主机网段，
XX租用

103.4.x.x,
中国电信，
托管主机，
南京二长
枢纽
… …

异常判断举例



接口频率策略

数据来源

1. 用户录入
2. 供应商录入
3. 本平台录入
4. 其他平台录入

数据属性

1. 公开数据
2. 私有数据
3. 混合数据

使用条件

1. 多次调用
2. 单次调用
3. 其他条件

控制策略

1. 限制频率
2. 限制时间段
3. 限制时长
4. 限制单IP
5. 限制浏览器
6. 限制会话
7. 限制账户
8. 限制IP网段
9. 限制访问顺序
10. 限制访问间隔时间
11. 其他

抢购接口举例

来源	属性	条件	风险控制策略
本平台商品数据	公开	多次调用	1. 限制频率，验证码 2. 限制时间段，大促期 3. 限制时长，30分钟 4. 限制单IP，黑白名单 5. 限制浏览器，UA黑名单 6. 限制会话，登陆 7. 限制账户，黄牛账户 8. 限制IP网段，黑名单 9. 限制访问顺序，无 10. 限制访问间隔时间，1分100次

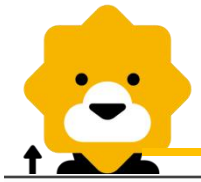
第一部分 群鼠到来祸从天降

第二部分 万众创新理论升级

第三部分 产品为本跨界创新

第四部分 大众创业能力输出

第五部分 整合资源运营为王



安全能力基石

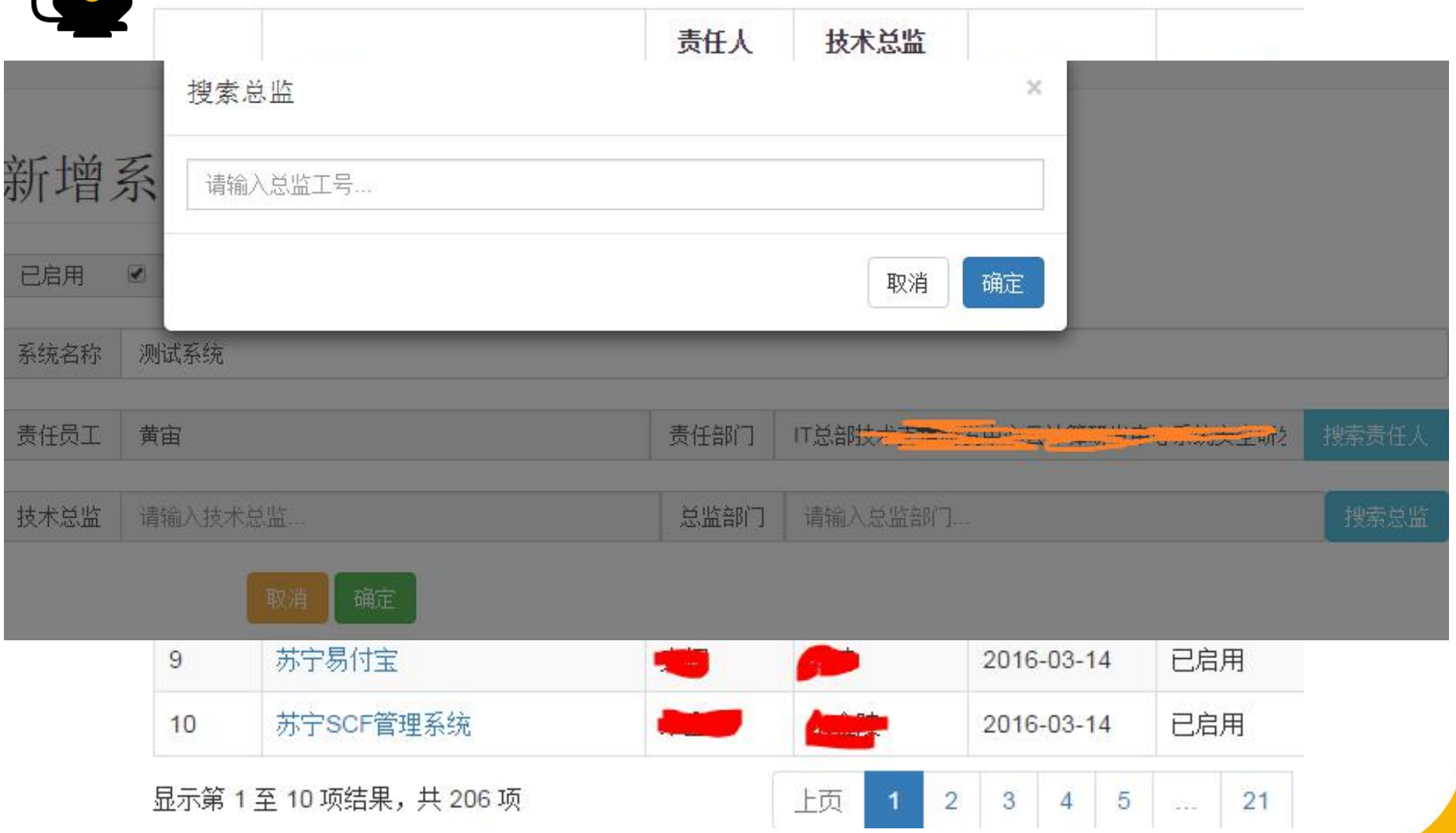
信息获取

测试名称	测试内容	使用工具	分析要求	更新人员	风险级别	说明文档
DNS	DNS查询	nslookup	暂无	黄宙	低	nslookup example.com
	DNS查询	dig	暂无	黄宙	低	dig +qr www.example.com any
	DNS查询	dig	暂无	黄宙	低	dig @ns1.example.com example.com axfr
	DNS查询	fierce.pl	暂无	黄宙	低	fierce.pl -dns example.com
port scan	Basic scans	nmap	端口检查	黄宙	低	nmap -A 192.168.50.20
	SYN scan	nmap	端口检查	黄宙	低	nmap -sS -T5 192.168.50.10
	Null scan	nmap	端口检查	黄宙	低	nmap -sN -T5 192.168.50.10
	ACK scan	nmap	端口检查	黄宙	低	nmap -sA -T5 192.168.50.10
	Shifting blame	nmap	端口检查	黄宙	低	nmap -v -O -Pn -n 192.168.50.10
	指定扫描	nmap	端口检查	黄宙	低	nmap -p 23,53,80,1780,5000 -Pn -sI 192 192.168.1.111
snmp检测	简单网管协议信息探测	snmpenum.pl	暂无	黄宙	低	snmpenum.pl 192.168.121.252 public lin myFW.txt
SSL	SSL检查	TLSSLed.sh	暂无	黄宙	低	TLSSLed.sh www.suning.com 443
IDS	IDS测试	hping2	暂无	黄宙	低	hping2 -S --fast 192.168.1.100
SMTP	SMTP测试		暂无	黄宙	低	nmap -sS -sV -O 192.168.1.1
VPN	VPN测试	ike-scan	识别是否存在VPN服务	黄宙	低	ike-scan -AM 192.168.1.1

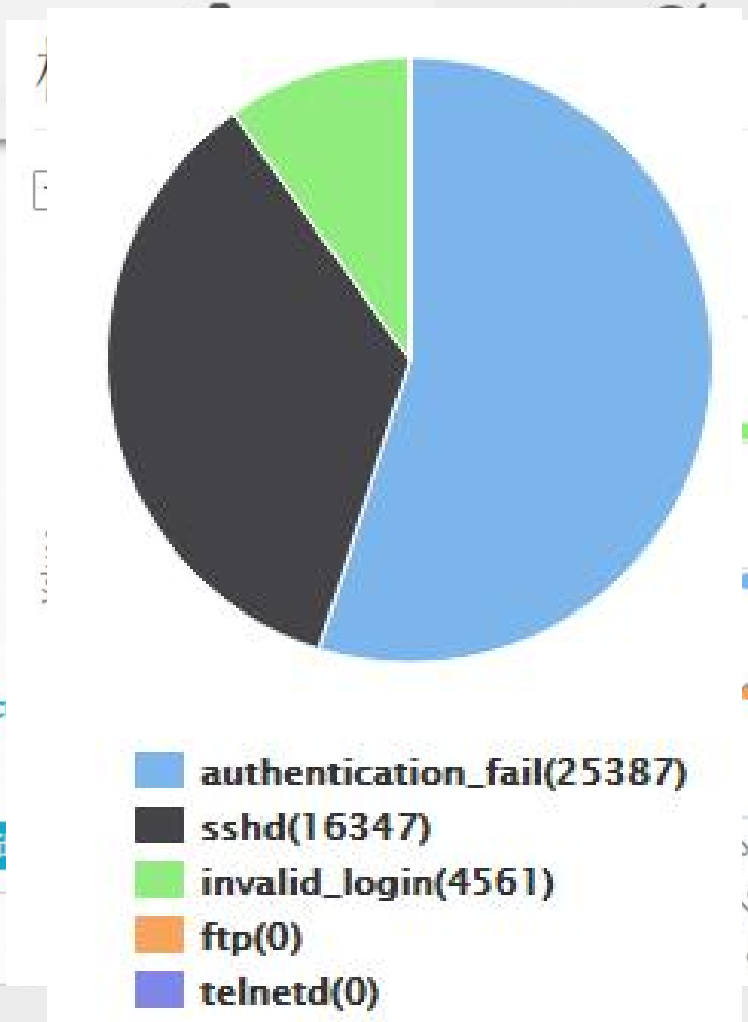
	审核系统事件	手工+脚本工具	成功，失败	黄宙	高
防病毒软件	安装防病毒软件	手工+脚本工具	是	黄宙	很高

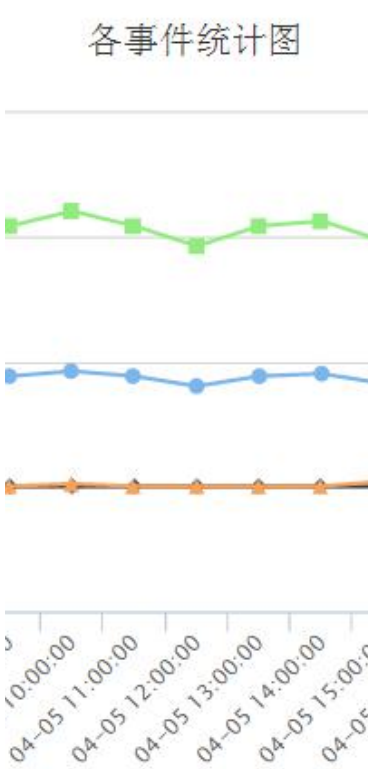
产品

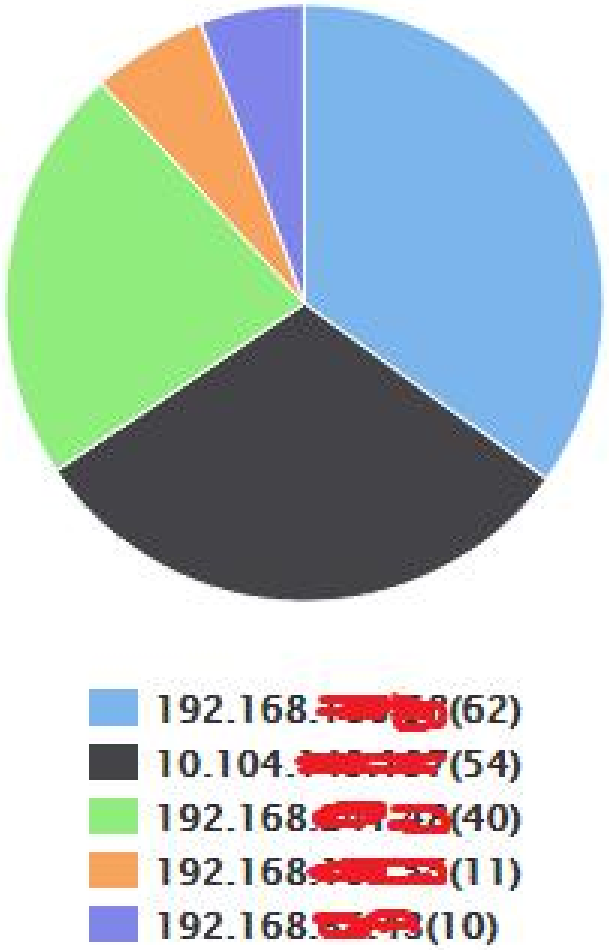
业务系统资产管理


责任人
技术总监
搜索总监
请输入总监工号...
取消
确定
新增系
已启用
系统名称
测试系统
责任员工
黄宙
责任部门
搜索责任人
技术总监
请输入技术总监...
总监部门
请输入总监部门...
搜索总监
取消
确定
9
苏宁易付宝
2016-03-14
已启用
10
苏宁SCF管理系统
2016-03-14
已启用
显示第 1 至 10 项结果，共 206 项
上页
1
2
3
4
5
...
21

主机安全管理


authentication_fail(25387)
sshd(16347)
invalid_login(4561)
ftp(0)
telnetd(0)


各事件统计图
04-05 11:00:00
04-05 12:00:00
04-05 13:00:00
04-05 14:00:00

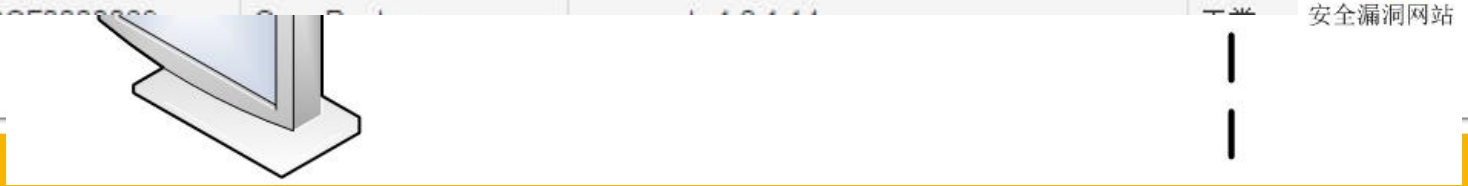

(62)
(54)
(40)
(11)
(10)

软件安全风险管理

操作系统	创建时间	CPU	内存	磁盘
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	2C	1G	52.04G
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	4C	2G	104.05G
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	4C	2G	104.05G
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	2C	1G	52.04G
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	8C	4G	108.05G
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	2C	1G	52.04G
Red Hat Enterprise Linux Server 5.5 (64 Bit)	2014-07-02 21:05:19.0	16C	8G	106.05G

23	SVR0004958	192.168.[redacted]	[redacted]		DB2 v9.7.0.4	知识管理系统(SNKM)
24	SVR0005316	192.168.[redacted]	inter[redacted]		WAS 6.1.0.33 x86	知识管理系统(SNKM)

-用色管理
-功能管理

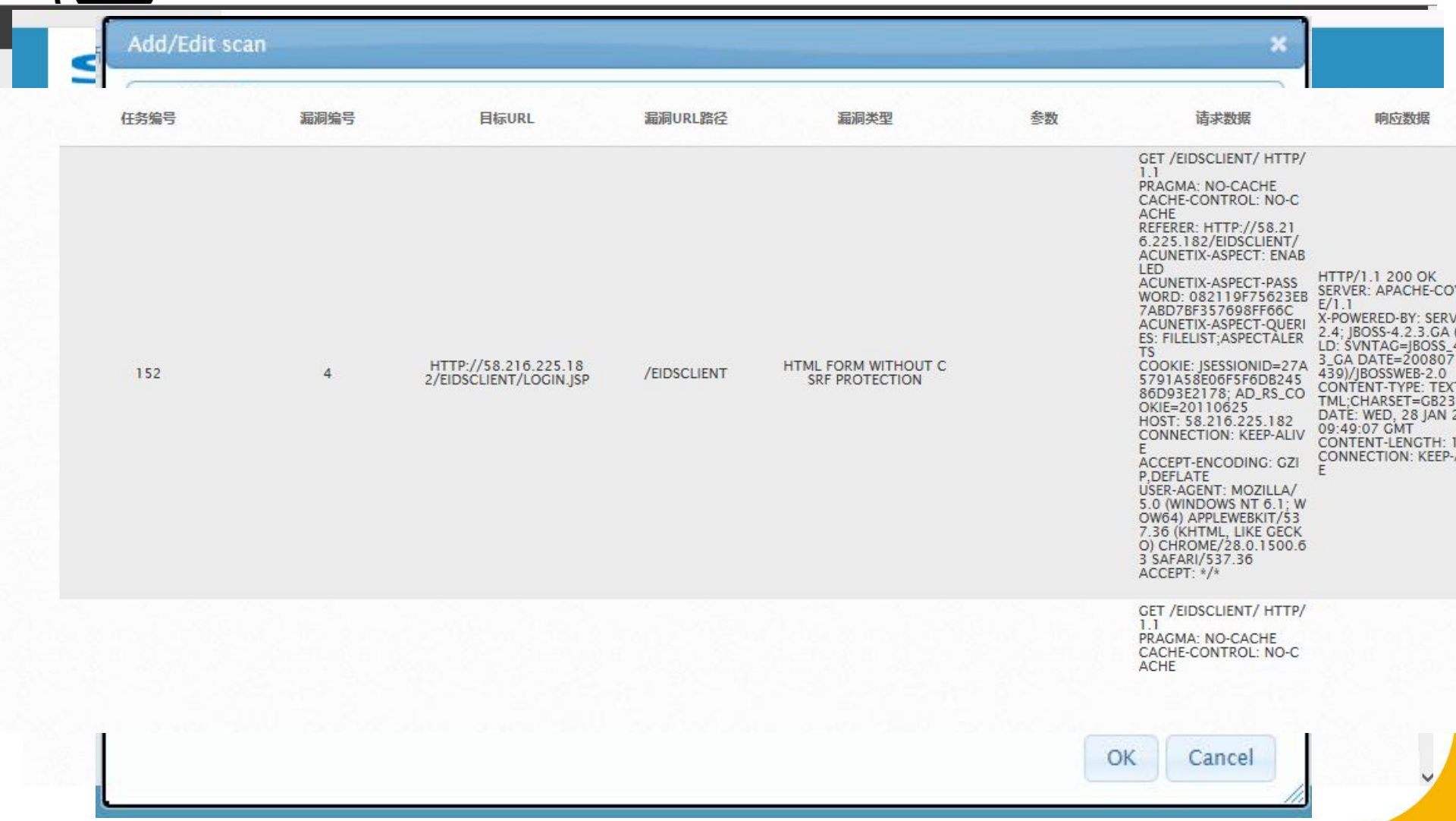


安全漏洞网站

云安全防护


首页
266
接入waf系统数量
View Details
383
接入waf域名数量
View Details
PPTV.com
本周拦截CC攻击总数
20855619
接入系统
我的拦截
恶意拦截
CC拦截
攻击排名
攻击网站url Top5
1
http://www.suning.com/
299
接入waf策略数量
View Details
1086
下发次数
View Details
5678954次

老版本--Web安全检测


Add/Edit scan
任务编号
漏洞编号
目标URL
漏洞URL路径
漏洞类型
参数
请求数据
响应数据
152
4
HTTP://58.216.225.182/EIDSCLIENT/LOGIN.JSP
/EIDSCLIENT
HTML FORM WITHOUT CSRF PROTECTION
GET /EIDSCLIENT/ HTTP/1.1
PRAGMA: NO-CACHE
CACHE-CONTROL: NO-CACHE
REFERER: HTTP://58.216.225.182/EIDSCLIENT/
ACUNETIX-ASPECT: ENABLED
ACUNETIX-ASPECT-PASSWORD: 082119F75623EB7ABD7BF357698FF66C
ACUNETIX-ASPECT-QUERIES: FILELIST;ASPECTALERTS
COOKIE: JSESSIONID=27A5791A58E06F5F6DB24586D93E2178; AD_RS_COOKIE=20110625
HOST: 58.216.225.182
CONNECTION: KEEP-ALIVE
ACCEPT-ENCODING: GZIP,DEFLATE
USER-AGENT: MOZILLA/5.0 (WINDOWS NT 6.1; WOW64) APPLEWEBKIT/537.36 (KHTML, LIKE GECKO) CHROME/28.0.1500.63 SAFARI/537.36
ACCEPT: */*
HTTP/1.1 200 OK
SERVER: APACHE-CO
E/1.1
X-POWERED-BY: SERV
2.4; JBOSS-4.2.3.GA
LD: SVNTAG=JBOSS_4
3_GA DATE=200807
439)/JBOSSWEB-2.0
CONTENT-TYPE: TEX
TML;CHARSET=GB23
DATE: WED, 28 JAN 2
09:49:07 GMT
CONTENT-LENGTH:
CONNECTION: KEEP-A
E
GET /EIDSCLIENT/ HTTP/1.1
PRAGMA: NO-CACHE
CACHE-CONTROL: NO-CACHE
OK
Cancel

研发同步安全测试

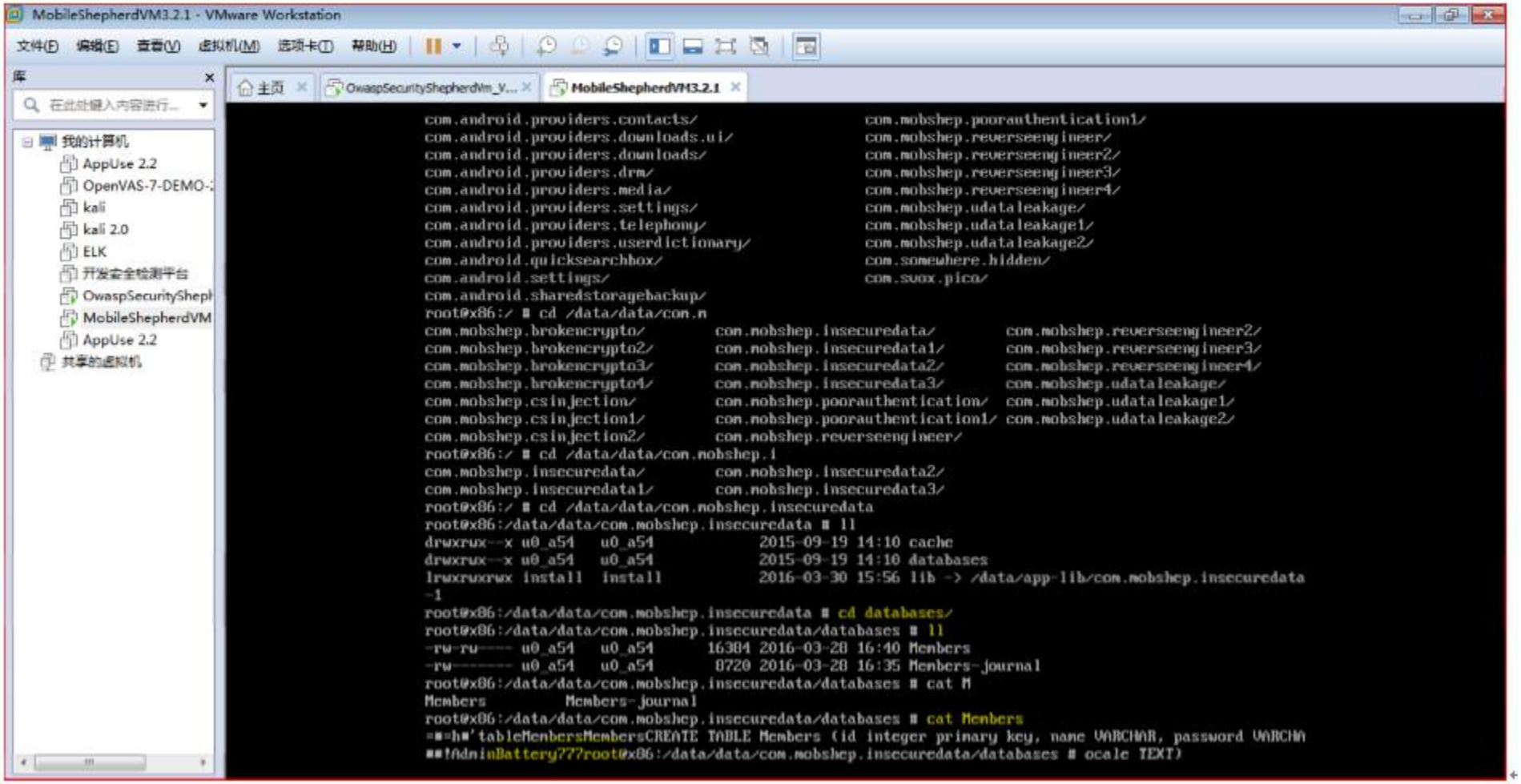

自动化测试
安全测试
BETA
稳定性测试
深度遍历测试
测试报告
个人中心
黄宙
注销
安全测试添加网站
网站验证
网站验证方法
1. 请点击下载验证文件，获取验证文件
2. 将验证文件放置于你所配置网站(www.suning.com)的根目录下
3. 确认地址www.suning.com/test-verify-acf18a2731fea33f4ec6a15c25904a610e14f4fe959e6f40.txt可以访问
执行描述:
请简要说明本次任务，可以为空,长度不能超过100!
开始扫描

产品发布安全测试


持续交付平台
重要通知:亲爱的用户，为提升用户体验、提高发布
系统空间
苏宁安全渗透测试平台(SSPTP)
系统
团队
代码库
分支
持续集成
发布包
打包配置
系统环境
MQ连接
安全扫描
【安全扫描申请】
*扫描URL:
http://
用户名:
密码:
*计划扫描时间:

能力意识训练平台

4、访问其目录下的/database 目录，并查看目录类的文件。



通关值 Battery777

安全流程管理


漏洞审核
禁用漏洞
删
审核通过
审核不通过
重复漏洞
正在解决中...
状态: 已审核通过
是否禁用: 已启用
上一条
下一
所属系统
漏洞类型
危害等级
漏洞积分
漏洞域名
提交人昵称
苏宁易付宝
Web安全漏洞-cookie设置不当
低危漏洞
10
pay.suning.com
kakak
责任人工号
责任人姓名
责任人boss工号
责任人boss姓名
审核人工号
审核人姓名
提交时间
更新时间
审核时间
审核备注
不奖励积分说明
解决人工号
2016-04-12 17:38:39.0
2016-04-13 09:24:43.0
2016-04-13 09:24:43
解决人姓名
解决备注
解决时间
重复漏洞id
附加备注
0
无
134525]

第一部分 群鼠到来祸从天降

第二部分 万众创新理论升级

第三部分 产品为本跨界创新

第四部分 大众创业能力输出

第五部分 整合资源运营为王

安全能力整合

2016.10

安全态势感知中心

2015.10

漏洞报告中心

2012/2014/2016

云安全防护

2015

业务资产管理

主机安全管理

2013/2016

2016-4-21

2016.3

能力意识训练平台

2013/2016

业务安全风险分析

2013/2016

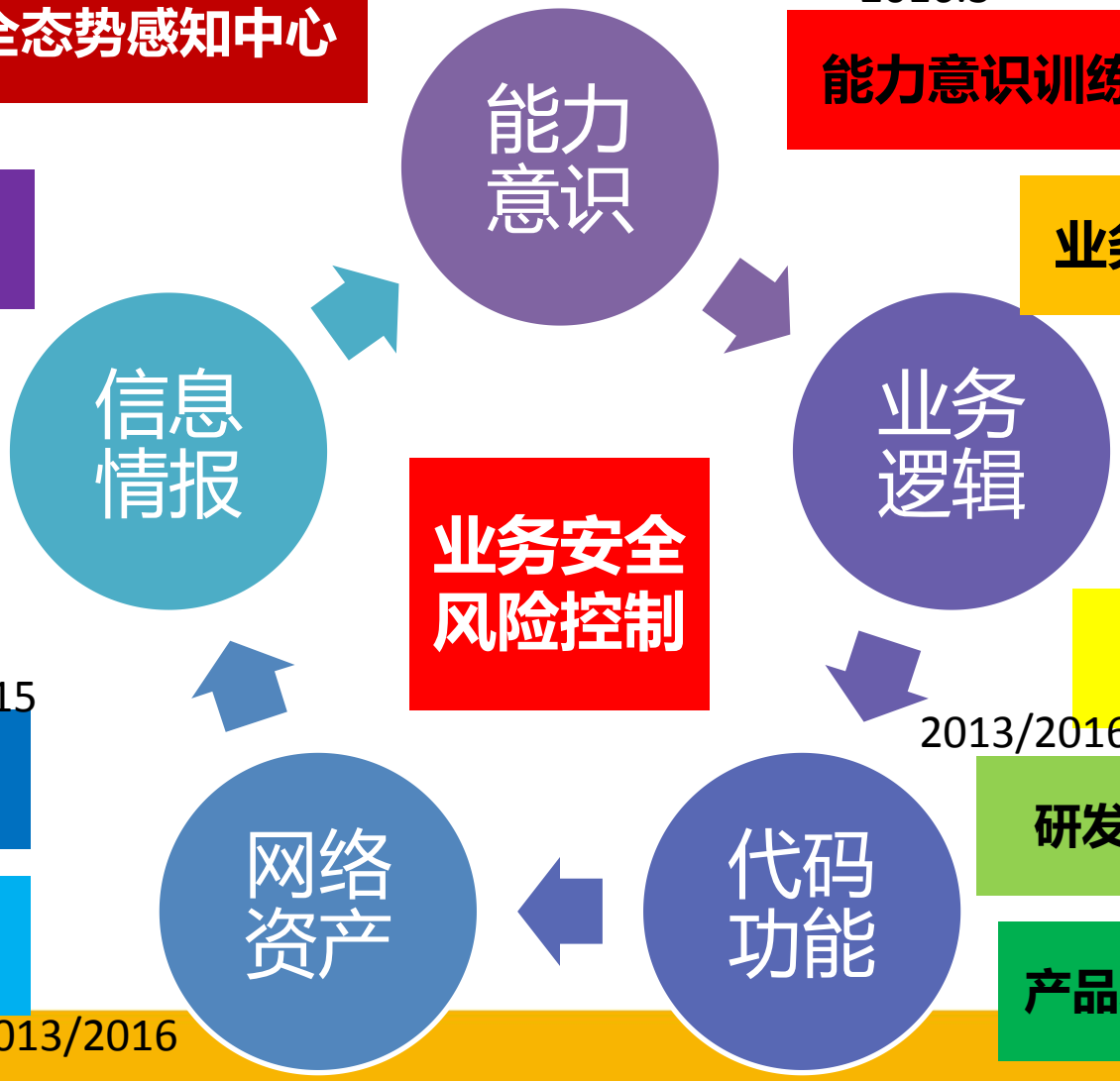
研发流程管理

2013/2016.1

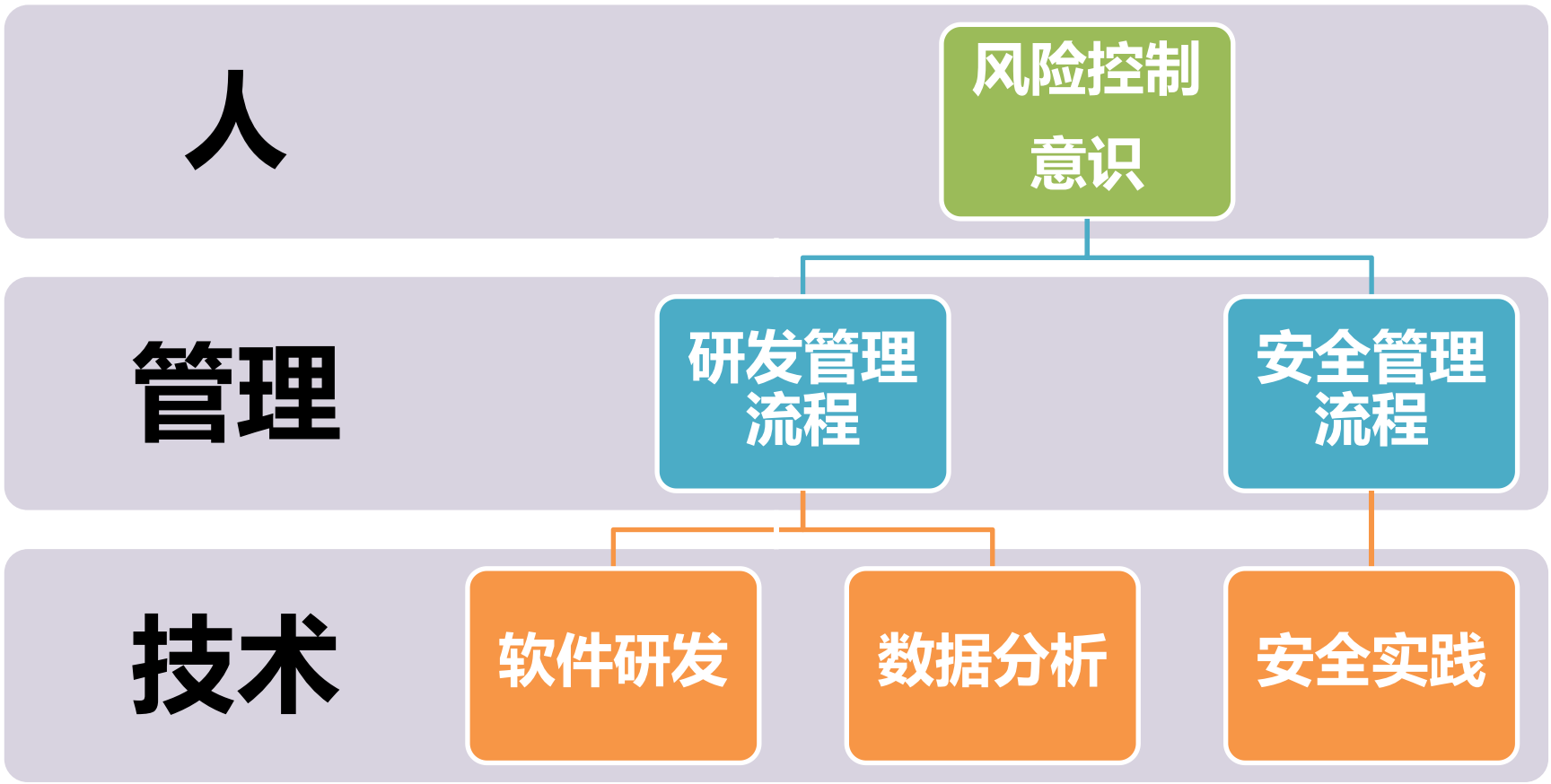
研发同步安全测试

产品发布安全测试

2013/2016



安全意识整合



持续运营研发安全

已建 **在建** **待建**

已建	已建	在建	待建
能力意识训练	社工泄漏风险分析	移动APP安全	
研发流程管理	漏洞报告中心	业务安全风险分析	
研发同步安全测试	云安全防护	潜在威胁探索	安全风险态势感知中心
产品发布安全测试	主机风险管理	业务资产管理	
软件安全风险分析	网络架构风险分析		

一场永不**终结**的猫鼠游戏

Geekbang 极客邦科技 InfoQ

THANKS!