阿里云 | 云盾先知 安全情报

企业安全团队的生存之道

王哲

宜人贷信息安全兼运维总监

先知白帽大会
开放创新 · 先知先行

议题内容简介

企业安全团队的建设过程中，不同阶段面临着不同优先级的问题，也有着不同的目标和追求。从安全的底线到更高的标准，如何有的放矢的开展安全工作、促进企业的发展、为业务保驾护航，如何更好地展现安全工作的价值、量化安全工作的产出，以及安全工作的资源分配等等，安全团队的生存之道充满了挑战与智慧……

介绍

宜人贷（NYSE: YRD）是中国在线金融服务平台，由宜信公司2012年推出。

宜人贷通过互联网、大数据等科技手段，为中国城市白领人群提供信用借款咨询服务，以及为投资者提供理财咨询服务。

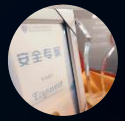
2015年12月18日宜人贷在美国纽交所成功上市，成为中国互联网金融海外上市第一股。

2016

- 创新：YISRC，行业首个安全漏洞、情报收集平台
- 合规：迎合监管，行业首批等保三级备案
- 品牌：安全品牌运营，行业独树一帜
- 领先：安全技术、安全管理体系，行业标杆

230位白帽子注册

150个安全漏洞提交



30万元漏洞奖励发放

10篇技术干货文章发表

10次外部安全会议参与

两套实时安全监控系统自研

90.1高分通过等保三级备案

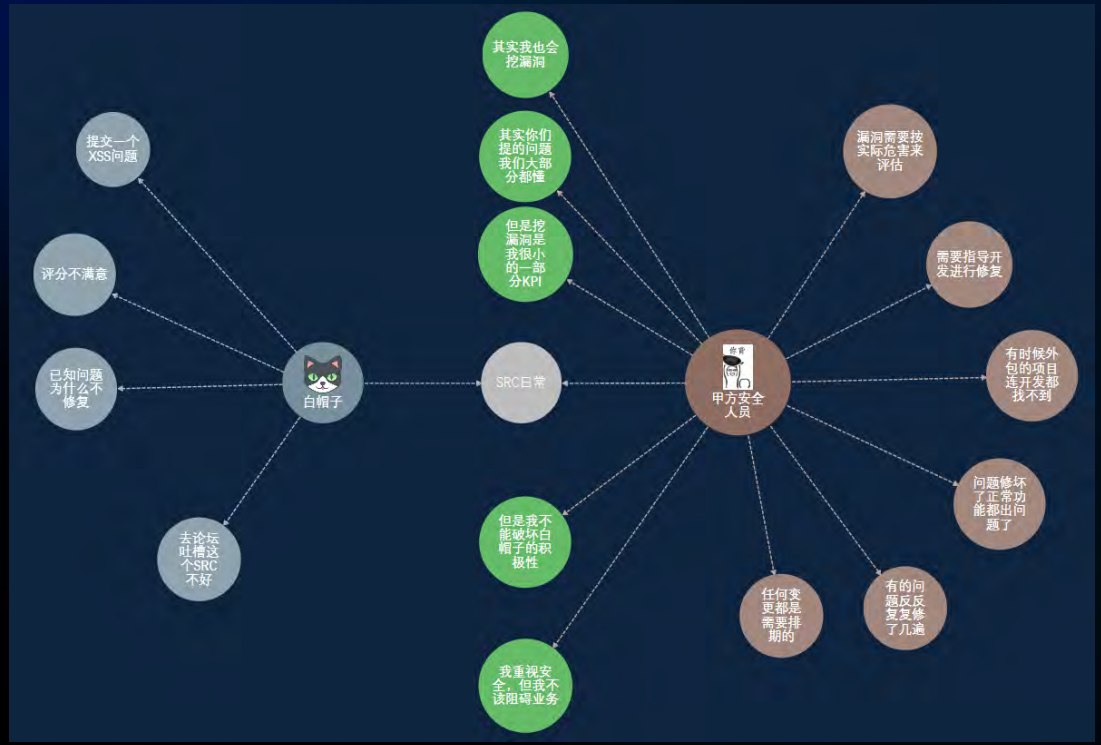
内部超过15场安全技术培训、安全意识推广

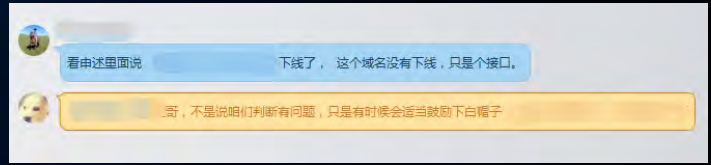
SDLC应用安全全流程覆盖

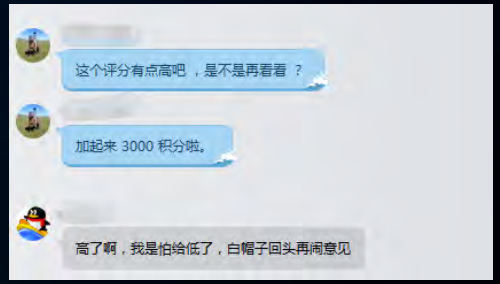
Topics

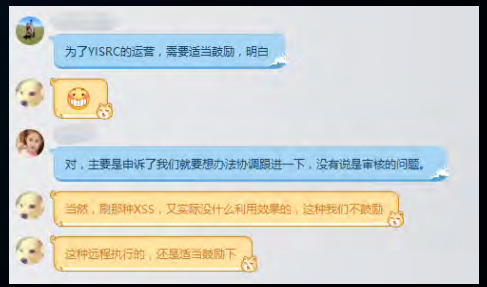
- 甲方安全人员的日常
- 安全工作中的用户体验
- 安全工作的数据化运营
- 安全能力产品化的探索
- 以数据安全风险为核心

甲方安全人员的日常


甲方安全人员
白帽子
SRC日常
提交一个XSS问题
评分不满意
已知问题为什么不修复
去论坛吐槽这个SRC不好
其实我也会挖漏洞
其实你们提的问题我们大部分都懂
但是挖漏洞是我很小的一部分KPI
但是我不能破坏白帽子的积极性
我重视安全，但我不该阻碍业务
任何变更都是需要排期的
有的问题反反复复修了几遍
问题修坏了正常功能都出问题了
有时候外包的项目连开发都找不到
需要指导开发进行修复
漏洞需要按实际危害来评估


看申述里面说
下线了，这个域名没有下线，只是个接口。
哥，不是说咱们判断有问题，只是有时候会适当鼓励下白帽子


这个评分有点高吧，是不是再看看？
加起来 3000 积分啦。
高了啊，我是怕给低了，白帽子回头再闹意见


为了YISRC的运营，需要适当鼓励，明白
对，主要是申诉了我们就要想办法协调跟进一下，没有说是审核的问题。
当然，刚那种XSS，又实际没什么利用效果的，这种我们不鼓励
这种远程执行的，还是适当鼓励下

甲方安全人员的日常

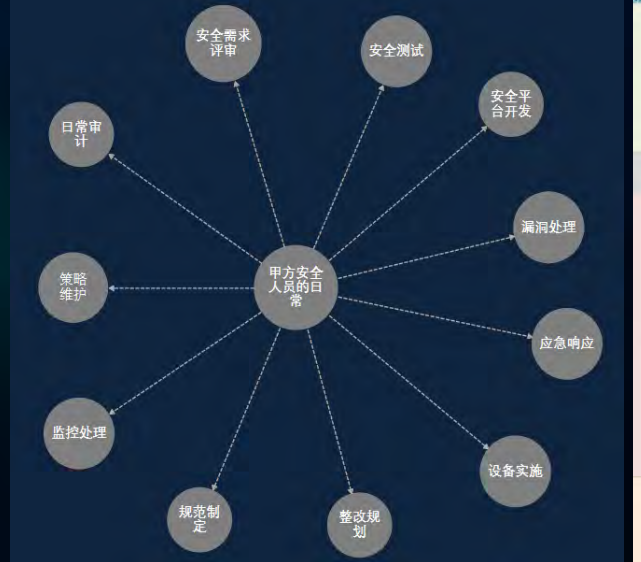
安全就会天天没事找事

又往电脑装监控

又误拦截了

安全阻碍了业务发展

别出去吹牛X了，都被日站了



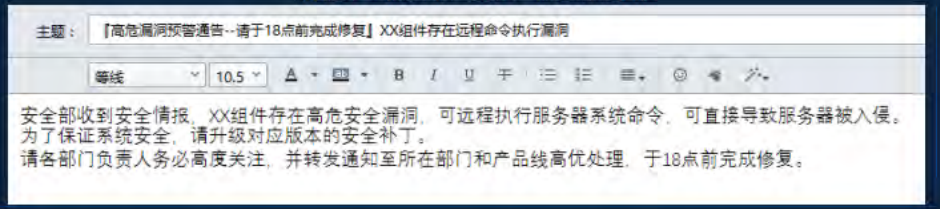
分类	任务描述	具体任务
业务安全	安全数据服务	数据服务目前已积累虚假手机号、阿里小号、204万条（实时在线号）
	风控引擎	库里技术框架重写，替换spring-boot（进行中） 数据实体结构的定义（进行中） 完成了"IFRule"、"TerminateRule"和各单规则，并测试完成（已完成） 待压测（进行中）
	安全中心	提高用户安全性，安全团队主导的产品，目前还在需求阶段。（进行中）
	业务安全平台设计	业务模块拆分项目（进行中） 业务安全平台流程制定（进行中）
安全开发	NETSKY监控系统	重写报警发送相关逻辑（已完成） 报警标准调优bug修复（已完成） 编辑策略页面可设置多个手机号以及邮箱（已完成）
安全技术	SDLC-安全测试	渠道极速轻借验证码登录安全测试（已完成） 卡联邮箱注册进行测试和漏洞完成（已完成） 数据工程邮代码泄露安全事件处理（已完成） github监控文件处理（已完成） 宜人贷主站安全问题修复测试（已完成）
	安全平台开发	安全申请-安全测试以及需求审计申请、产品原型设计（进行中）
	APP安全加固项目	推进借款app加固的上线（进行中） app渠道监测系统定期查看（进行中）
	数据库审计项目实施	数据库安全告警场景及需求配置（进行中）
	安全审计	数据工程邮离六脚本修改失误导致hadoop账户被删除。
		1、[redacted]它密码LDAP统过认证漏洞测试、修复（已完
安全管理和运营	基础安全架构&数据安全	补充[redacted]5无线AP的验证测试（进行中） 评审数据工程调研报告（已完成） 起草数据使用安全标准、完成初稿（已完成） DLP平台的维护和分析，发现潜在的风险（进行中）
	安全合规&安全管理	1、数据工程部调研报告（已完成） 2、出借和借款业务部数据调研、访谈借款3位、出借1位同事（进行中） 3、编写《设备账号及权限管理指引》，收集多个系统现有安全、运维角色及权限进行整理（进行中） 4、FM1218安全小课堂（已完成） 5、FM1218二期安全专栏需求对接（已完成）
	YISRC	YISRC日常运营 YISRC日常处理、公众号维护、漏洞跟进审核及订单处理、申诉处理等 各安全媒体及src相关合作事宜跟进（进行中） 各安全媒体企业号申请完成 本月安全技术文章一篇，推广至微信及各媒体 YISRC二期需求 需求原型图设计（进行中）
	安全公益项目	计划调整（进行中）

安全工作中的用户体验

漏洞修复通告

做法1：别人一脸懵X

一封描述不清晰的邮件，把责任全部抛给其他团队



做法2：大家合作愉快

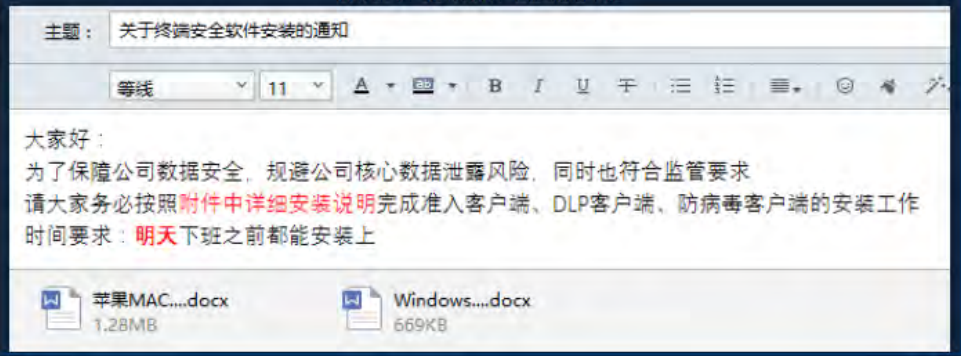
- 邮件通知
  - 漏洞说明
  - 复现说明
  - 确定明确受影响主机或服务
    - CMDB资产筛选
    - Ansible批量确认
  - 评估修复方案
    - 修复方式
      - IP访问限制
      - WAF加对应特征
      - 升级补丁
    - 修复周期
    - 可能存在的修复风险
- 漏洞修复过程中的支持
- 组织复测
- 确认漏洞修复工作结果

安全工作中的用户体验

终端安全的实施

做法1：怒声载道

只有命令，没有支持，风险预估不足

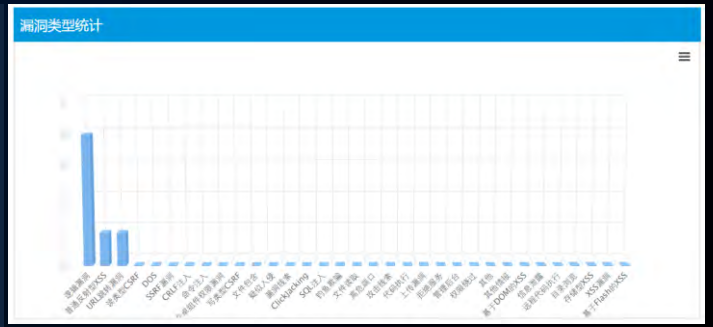


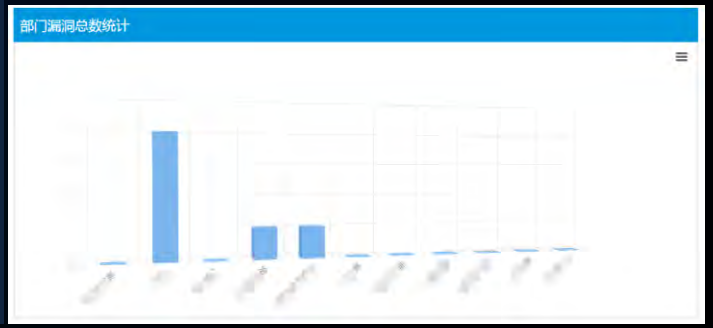
做法2：大家相互理解

- 配套宣传
  - 安全意识推广
  - 内部安全规范推广
- VIP员工支持
  - 整理出各部门负责人的LIST
  - 1对1完成安装支持
- 提前和IT桌面人员沟通
  - 发生问题时的预案
  - 支持的响应时间

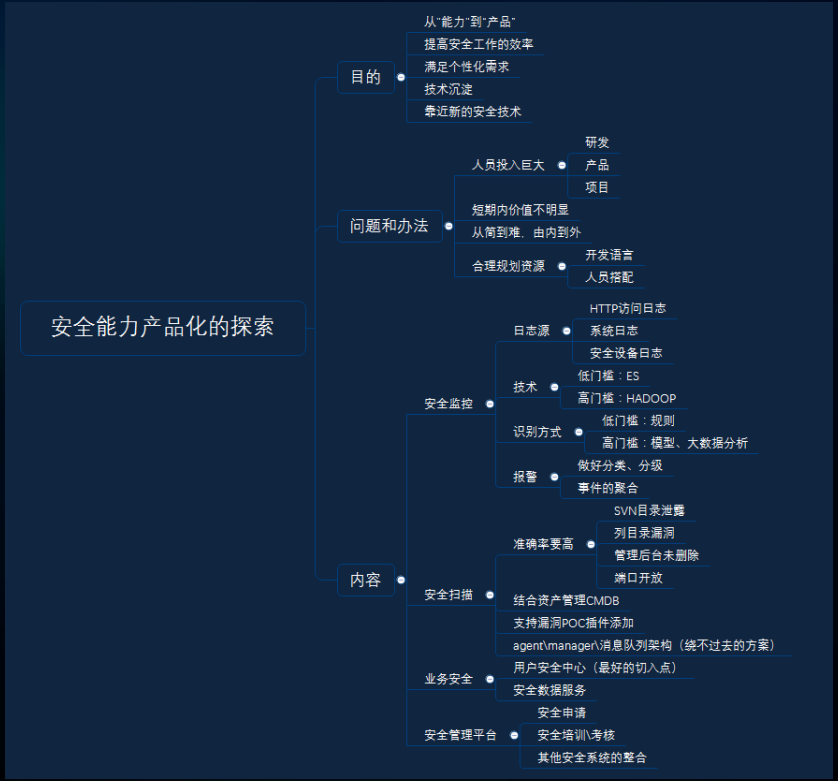
安全工作的数据化运营


安全工作的数据化运营
作用
量化安全工作的产出
和CXO沟通的桥梁
错误：给CXO汇报某个漏洞的详细原理分析
这不是CXO需要关心的问题
认为安全负责人缺乏全局掌控能力
正确：给CXO汇报安全工作的数据
目前企业所处的安全形势
安全工作解决和缓解了多少安全问题
安全工作未来的重心
评估投入和产出
内容
安全事件监控和拦截
防火墙
WAF
IDS
其他告警数
安全审计
GITHUB代码泄露
内部数据泄露违规
账号审计
操作审计
日志审计
安全参与的项目和评审数
安全测试支持
安全需求评审
漏洞
发现和解决安全漏洞数
内部测试发现
外部收集和通报
漏洞的修复率、关闭率
漏洞的分布统计
安全培训
安全意识
安全技能
数量
覆盖率

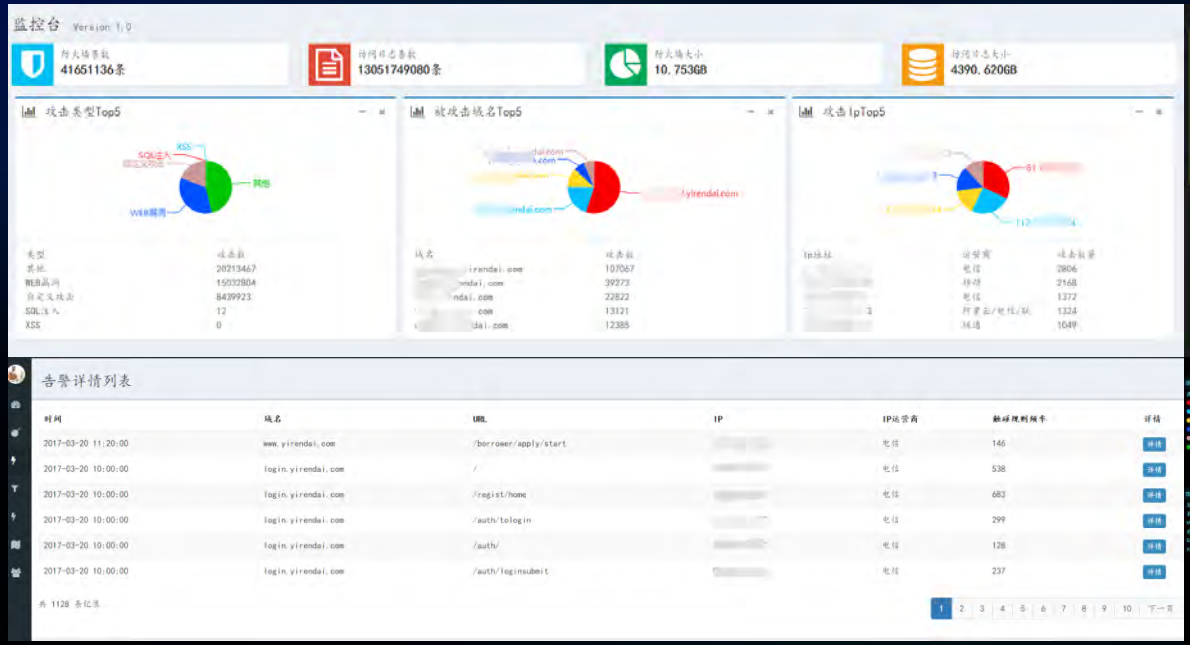

漏洞类型统计

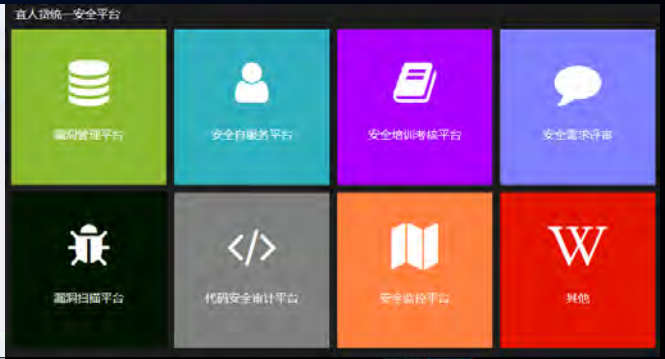

部门漏洞总数统计

安全能力产品化的探索


安全能力产品化的探索
目的
从"能力"到"产品"
提高安全工作的效率
满足个性化需求
技术沉淀
靠近新的安全技术
问题和办法
人员投入巨大
研发
产品
项目
短期内价值不明显
从简到难，由内到外
合理规划资源
开发语言
人员搭配
内容
安全监控
日志源
HTTP访问日志
系统日志
安全设备日志
技术
低门槛：ES
高门槛：HADOOP
识别方式
低门槛：规则
高门槛：模型、大数据分析
报警
做好分类、分级
事件的聚合
安全扫描
准确率要高
SVN目录泄露
列目录漏洞
管理后台未删除
端口开放
结合资产管理CMDB
支持漏洞POC插件添加
agent\manager\消息队列架构（绕不过去的方案）
业务安全
用户安全中心（最好的切入点）
安全数据服务
安全管理平台
安全申请
安全培训\考核
其他安全系统的整合

安全能力产品化的探索


监控台 Version: 1.0
防火墙事数
41651136条
待阿日志事数
13051749080条
防火墙大小
10.753GB
待阿日志大小
4390.620GB
攻击类型Top5
被攻击域名Top5
攻击IpTop5
告警详情列表
时间
域名
URL
IP
IP运营商
触发规则频率
详情


直人猫统一安全平台
漏洞管理平台
安全自服务平台
安全培训考核平台
安全需求评审
漏洞扫描平台
代码安全审计平台
安全监控平台
其他

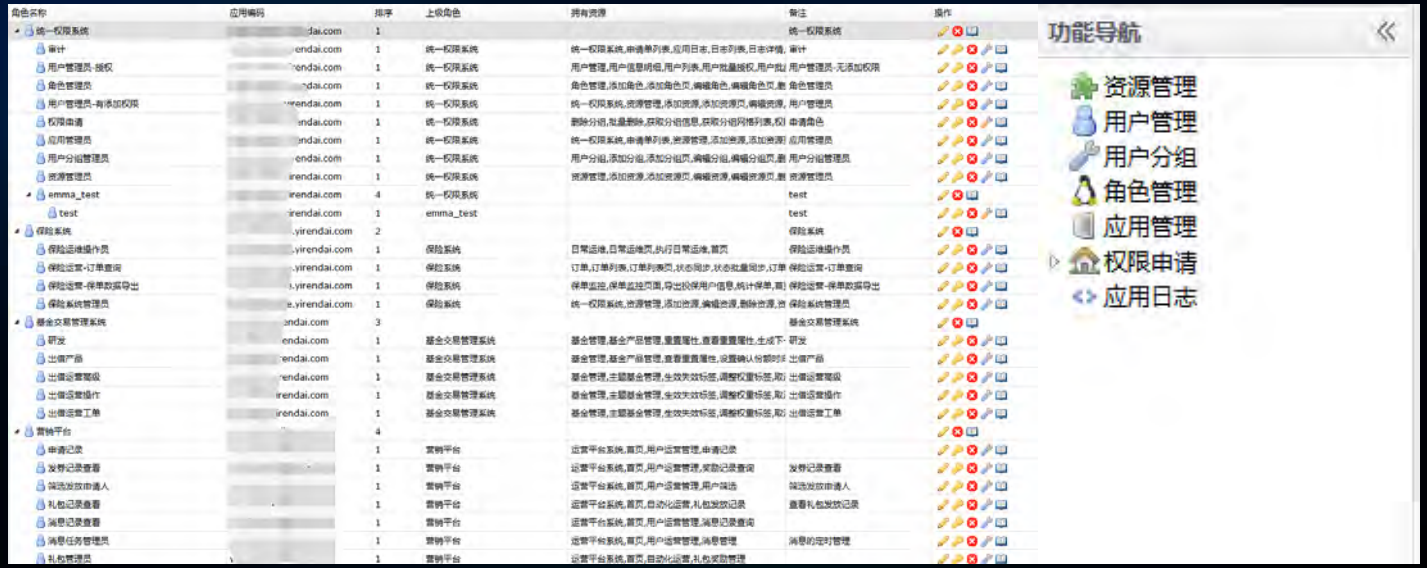
安全能力产品化的探索

功能	数据类型	数据标签	对应数据库ID	设置时间
数据服务	手机号	手工录入		记录各标签标记时间、取消时间、标记次数记录各条数据的录入时间、取消时间、录入次数
		羊毛党		
		手机接码平台		
		阿里小号		
		老赖用户		
		贷款中介		
		第三方风险数据		
		数据部黑名单		
		风控灰名单		
		盗刷		
		欺诈用户		
	手机号归属地	凹借高危区域		
		借款高危区域		
	IP地址	手工录入		
		代理IP		
		攻击IP		
		肉鸡IP		
		欺诈用户		
		第三方风险数据		
		数据部黑名单		
		风控灰名单		
		盗刷		
		羊毛党		
	IP地址归属地	凹借高危区域		
		借款高危区域		
	用户ID	手工录入		
		羊毛党		
		老赖用户		
		贷款中介		
		第三方风险数据		
		数据部黑名单		
		盗刷		
		风控灰名单		
		欺诈用户		
	身份证号	手工录入		
		羊毛党		
		老赖用户		
		贷款中介		
		第三方风险数据		
		数据部黑名单		
		风控灰名单		
		盗刷		
		欺诈用户		
	设备ID	手工录入		
		羊毛党		
		老赖用户		
		贷款中介		
		第三方风险数据		
		数据部黑名单		
		风控灰名单		

以数据安全风险为核心

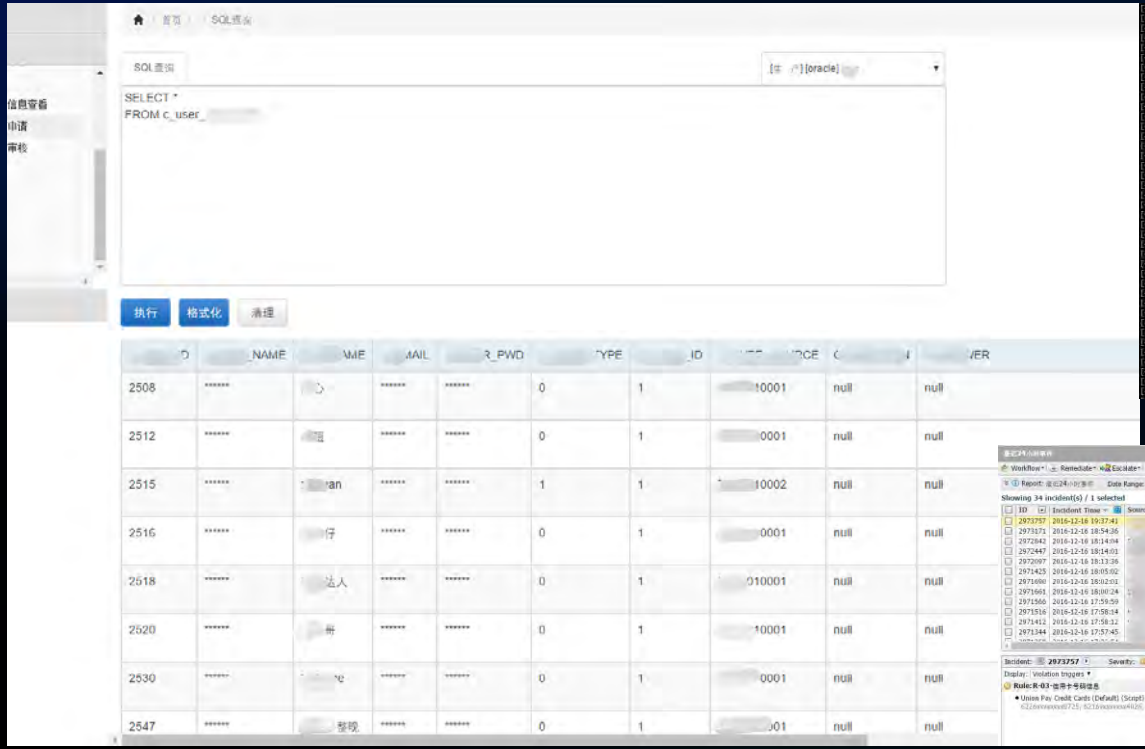

以数据安全风险为核心
明确
数据分类分级
数据出口
数据流向
数据安全整体策略
威胁建模
内容
统一权限管理
登录
资源权限
统一数据库查询系统
数据加密、掩码
更新维护敏感字段
系统对接
客服
跨部门对接
DLP
终端
网关
审计
数据库审计
数据查询、操作审计
管理系统操作审计

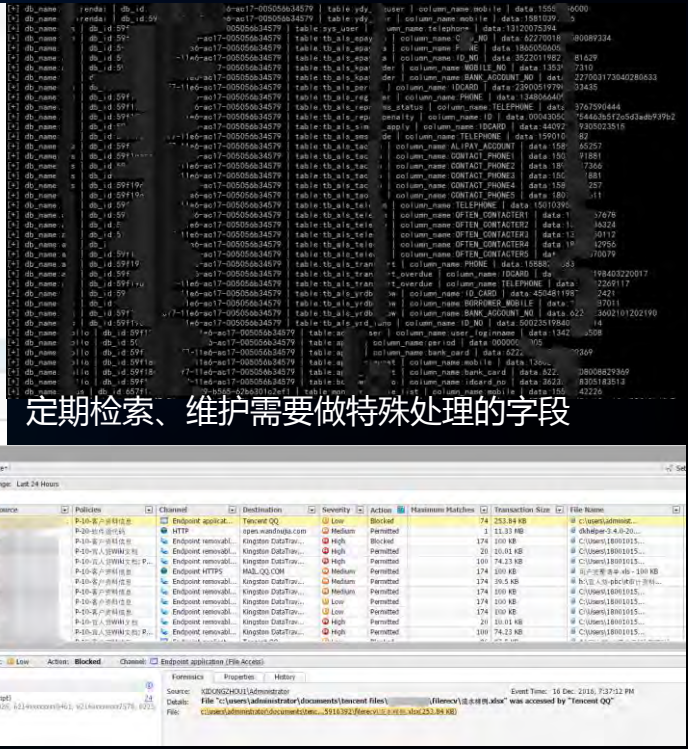
以数据安全风险为核心



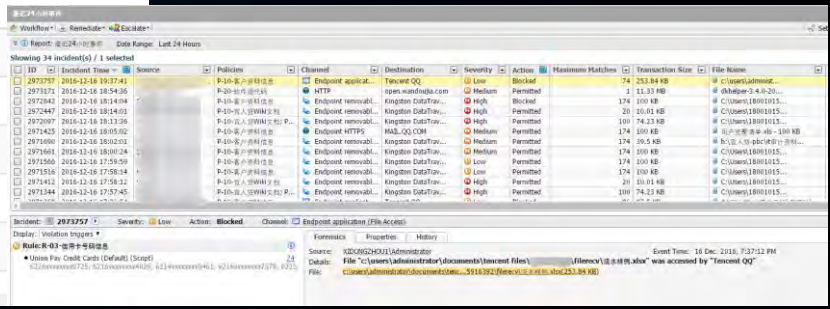
统一权限的管理、审计

以数据安全风险为核心

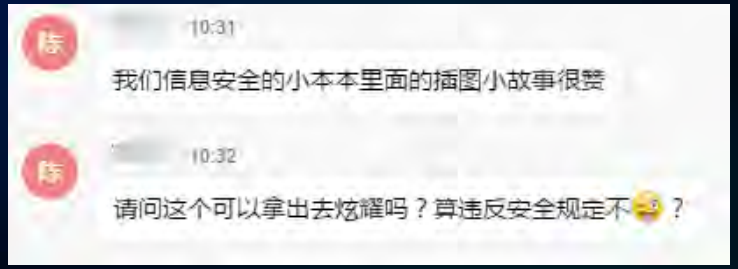




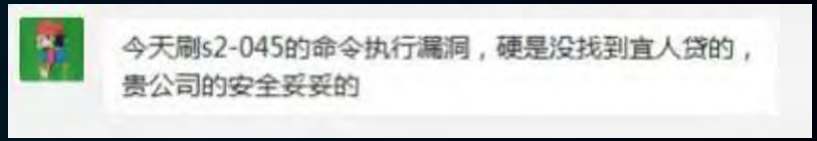
定期检索、维护需要做特殊处理的字段

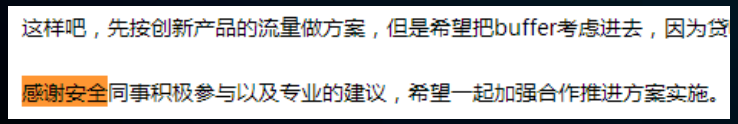


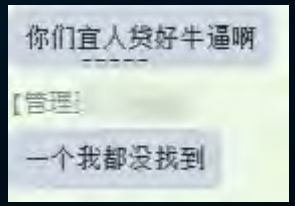
世界其实还是美好的

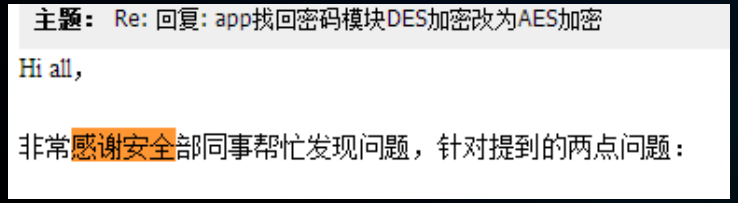

陈
10:31
我们信息安全的小本本里面的插图小故事很赞
陈
10:32
请问这个可以拿出去炫耀吗？算违反安全规定不？

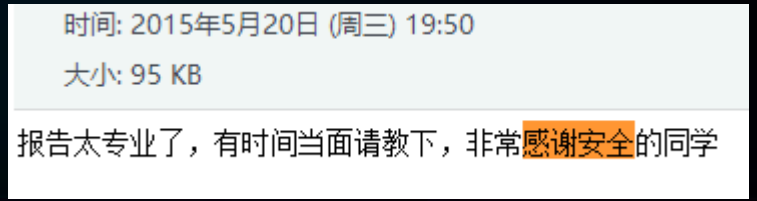

积分体系二期V2.2-8.9.docx (244 KB)
各位好，
非常感谢安全组的同事下午前来参加评审会，并给积分体系的安全性提供了宝贵建议。


今天刷s2-045的命令执行漏洞，硬是没找到宜人贷的，
贵公司的安全妥妥的


这样吧，先按创新产品的流量做方案，但是希望把buffer考虑进去，因为贷
感谢安全同事积极参与以及专业的建议，希望一起加强合作推进方案实施。


你们宜人贷好牛逼啊
[管理]
一个我都没找到


主题： Re: 回复: app找回密码模块DES加密改为AES加密
Hi all，
非常感谢安全部同事帮忙发现问题，针对提到的两点问题：


时间: 2015年5月20日 (周三) 19:50
大小: 95 KB
报告太专业了，有时间当面请教下，非常感谢安全的同学

选择信息安全工作，就代表了一份责任、一份使命、一份坚守，用自己的力量为企业保驾护航就是我们的价值所在