

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

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，如何有的放矢地开展安全工作、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



90.1高分通过等保三级备案



10篇技术干货文章发表



内部超过15场安全技术培训、安全意识推广



10次外部安全会议参与



SDLC应用安全全流程覆盖



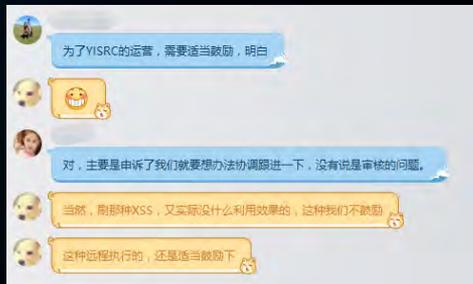
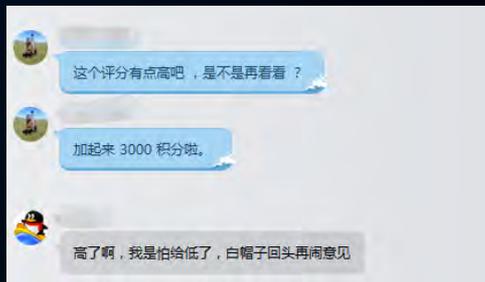
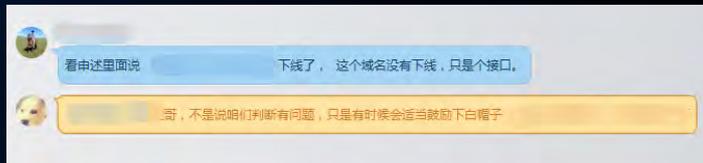
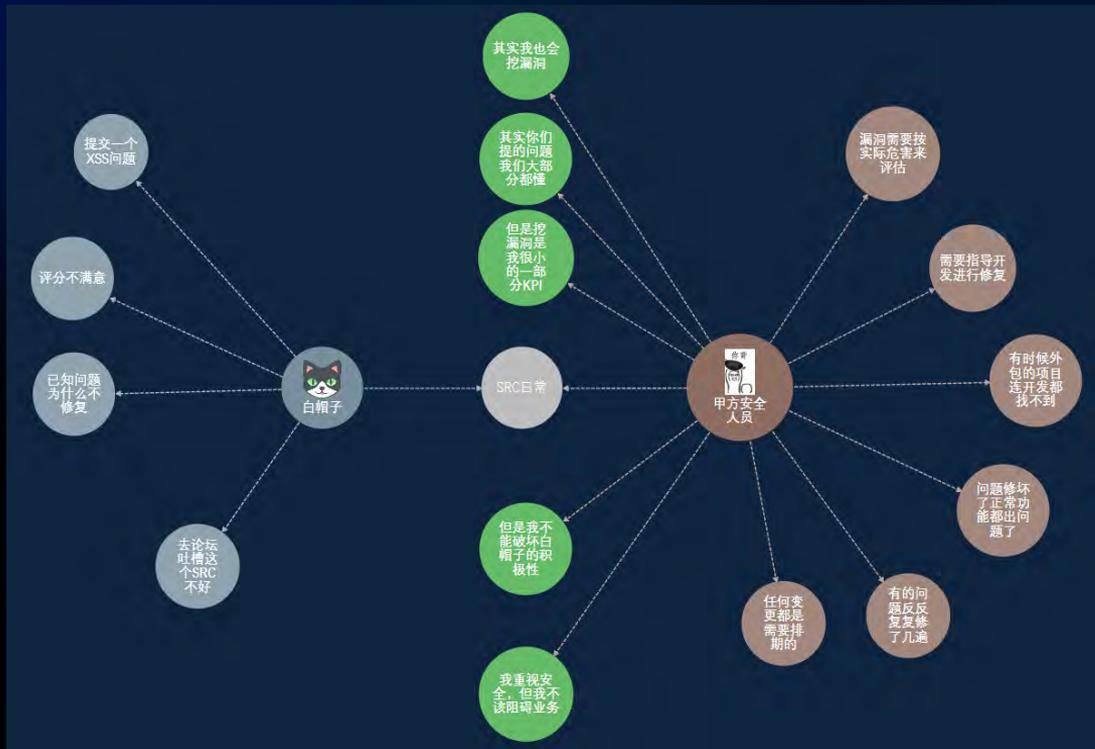
两套实时安全监控系统自研



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



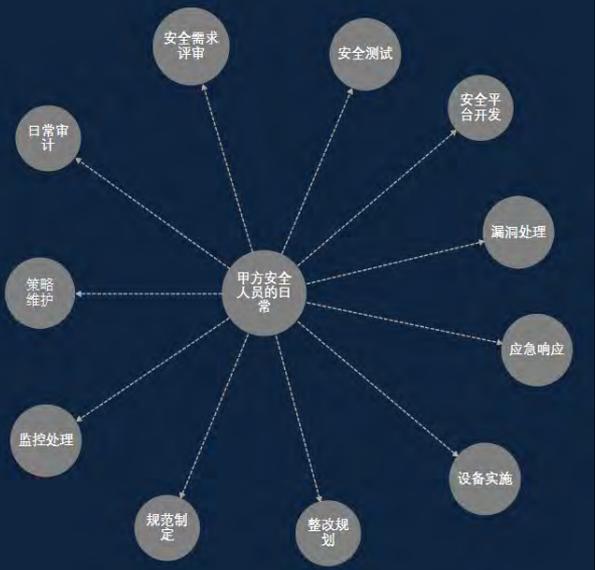
安全就会天天没事找事

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



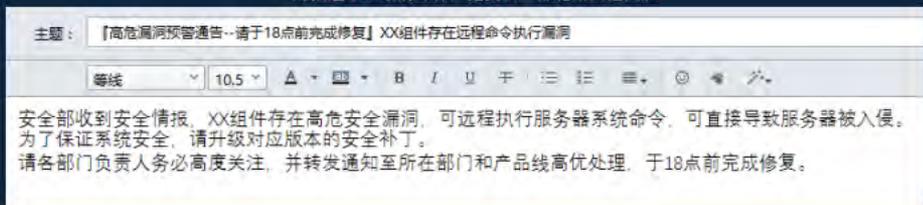
分类	任务描述	任务状态
业务安全	安全数据服务	数据服务目前已部署虚假手机号、阿里小号 204万条 (实时存活号)
	风控引擎	点选技术框架重写 替换spring-boot (进行中) 数据字典结构的定义 (进行中) 完成了"ifRule"、"TerminateRule"和名单规则, 并测试完成 (已待压测 (进行中))
	安全中心	提高资产安全性, 安全团队主导的产品, 目前还在需求阶段, (进行中)
	业务安全平台设计	业务模块拆分项目 (进行中) 业务安全平台流程制定 (进行中)
安全开发	NETSKY监控系统	重要报警发出相关逻辑 (已完成) 配置报警页面可设置多个手机号以及邮箱 (已完成)
安全技术	SDL-安全测试	渠道敏捷信创代码静态安全测试 (已完成) 生态链信创资产扫描漏洞处理 (已完成) 数据工程替代信创数据安全事件处理 (已完成) github漏洞文件处理 (已完成) 置入员工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	推进程控app加固的上线 (进行中) app渠道监控系统定期查看 (进行中)
	数据库审计项目实施	数据库安全告警需求及需求配置 (进行中)
安全管理和运营	安全审计	数据工程侧第六版本修改失误导致hadoop账户被删除。 1、 已密码LDAP绕过认证漏洞测试、修复 (已完成)
	基础安全架构&数据安全	1、 无线AP的验证测试 (进行中) 2、 评估数据工程侧报告 (已完成) 3、 起草数据工程安全标准, 启动初建 (已完成) DLP平台的维护和升级, 发现潜在的风险 (进行中)
	安全合规&安全管理	1、 数据工程前期调研报告 (已完成) 2、 出催和催款业务数据调研, 访谈催款3位, 出催1位同事 (进行中) 3、 编制《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、 FM1218二期安全专项需求对接 (已完成)
	YISRC	YISRC日常运营 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, 推广高微信及各媒体 YISRC二期需求 需求原型面设计 (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

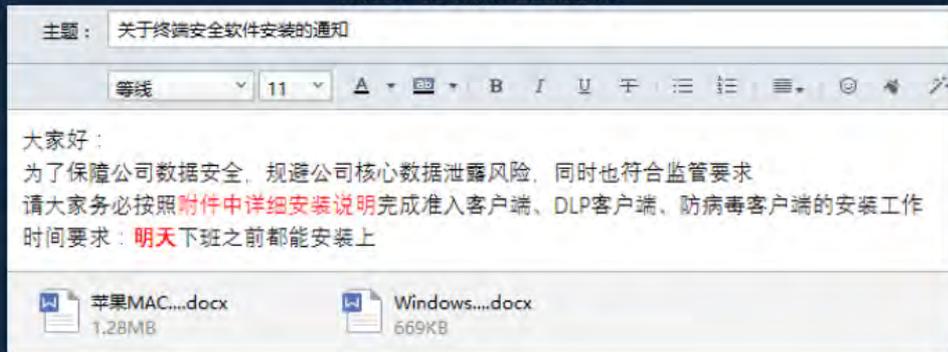


安全工作中的用户体验

终端安全的实施

做法1：怨声载道

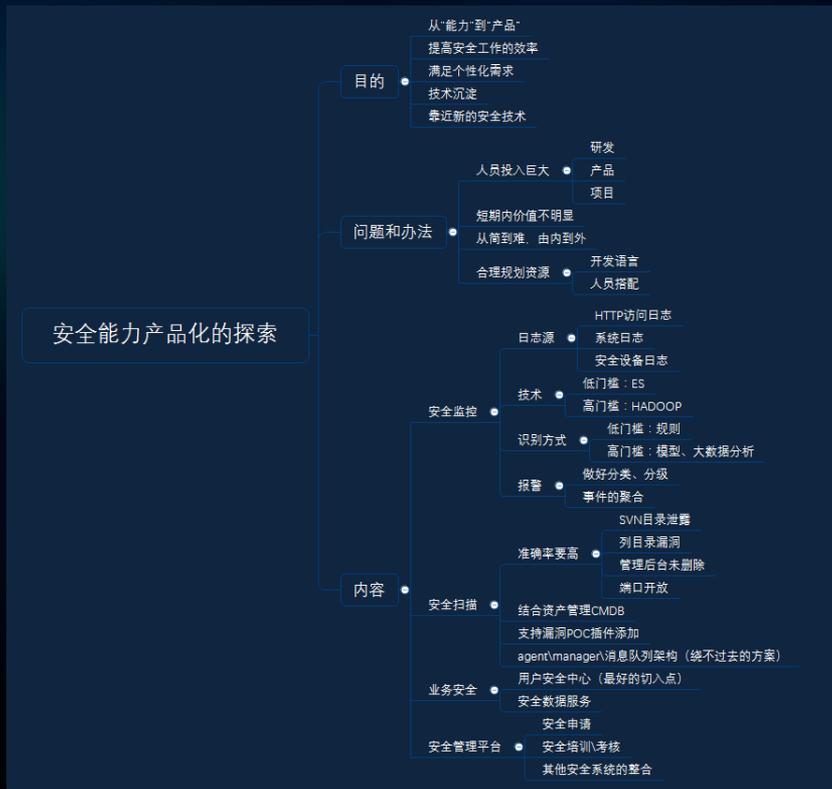
只有命令，没有支持，风险预估不足



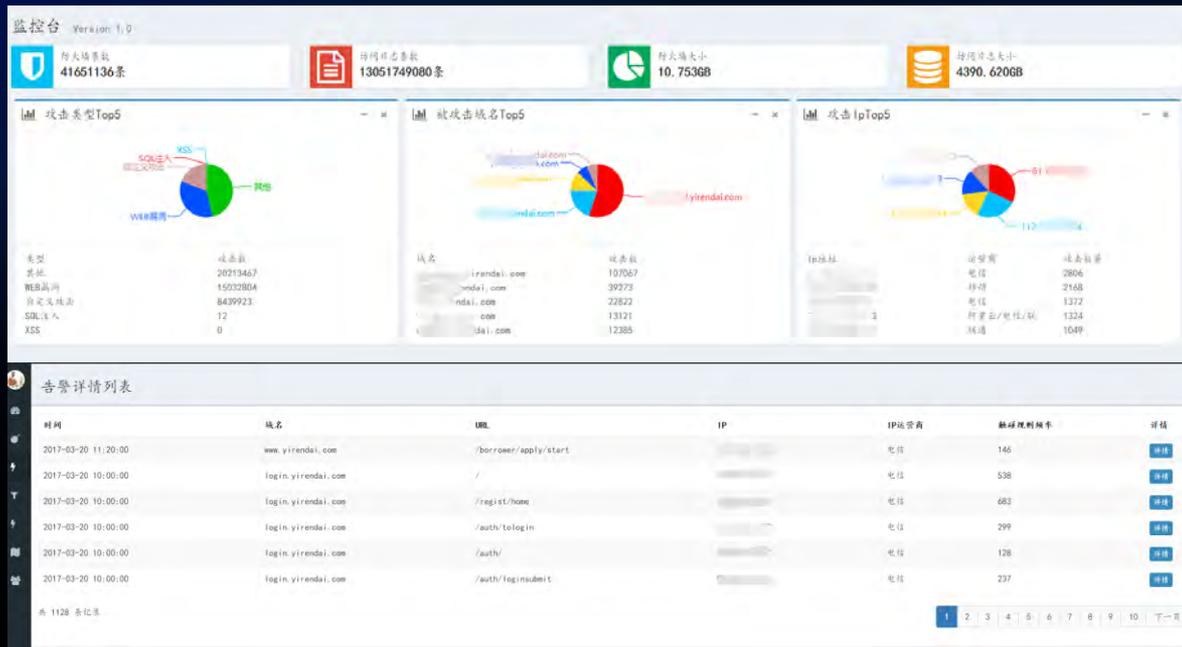
做法2：大家相互理解

- 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

安全能力产品化的探索



安全能力产品化的探索



宜人统一安全平台

漏洞管理平台

安全自服的平台

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

告警地图

告警详情

告警ID	告警名称	域名	URL	IP	告警内容
...	HTTP 403 Unauthorized	yirendai.com	/borrower/apply/start
...	HTTP 403 Forbidden	yirendai.com	/
...	HTTP 403 Forbidden	yirendai.com	/regist/home
...	HTTP 403 Forbidden	yirendai.com	/auth/login
...	HTTP 403 Forbidden	yirendai.com	/auth/
...	HTTP 403 Forbidden	yirendai.com	/auth/loginsubmit

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		
		羊毛党		
		手机验证平台		
		阿里小号		
		老赖用户		
		贷款中介		
	手机号归属地	第三方风险数据		
		数据部黑名单		
		风控黑名单		
		盗刷		
		欺诈用户		
		出情高危区域		
IP地址	手工录入			
	代理IP			
	攻击IP			
	僵尸IP			
	欺诈用户			
	第三方风险数据			
IP地址归属地	数据部黑名单			
	风控黑名单			
	盗刷			
	出情高危区域			
	借款高危区域			
	手工录入			
用户ID	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			
身份证号	风控黑名单			
	风控黑名单			
	盗刷			
	欺诈用户			
	手工录入			
	羊毛党			
设备ID	老赖用户			
	贷款中介			
	第三方风险数据			
	数据部黑名单			
	风控黑名单			
	风控黑名单			

业务安全平台

🔍

数据主页

安全数据服务

标签/数据设置

接入设置

用户安全中心

用户安全

安全预警

反欺诈预警

反欺诈数据

反欺诈SDK埋点

反欺诈规则引擎

反欺诈预警中心

设备指纹

设备图谱

业务安全规则引擎

规则引擎管理

今日异常数据

99 条

比上周上涨11%

用户安全数据预警

75 条

比上周上涨8%

安全数据

129

比上周

1 安全数据服务通过安全部门收集高危用户、高危设备等信息及第三方黑灰数据，并对收集的信息做分类、标签标识、对特殊数据增加规则处理及维护，为查人贷各业务部门提供可靠准确，大数据量的数据支持，为业务方提供高效高价值数据服务。

2 流程图

```

graph LR
    subgraph Security_Department [安全部门]
        A[数据收集  
1.用户ID  
2.身份信息  
3.IP地址  
4.设备ID  
5.银行卡号] --> B[数据分发/标签]
        B --> C[处理规则/监控日志]
        C --> B
    end
    subgraph Business_Department [各业务部门]
        D[数据识别/标记] --> E[风险处理/监控]
        E --> F[有风险  
优化服务]
        G[用户、设备、IP、手机...] --> D
        H[业务量/活动推广] --> I[风险处理/监控]
        I --> J[精准服务]
        J --> K[用户]
    end
    A -- http 使用场景一 --> D
    C -- http 使用场景二 --> D
    D --> E
    H --> I
    
```

先知白帽大会

开放创新·先知先行

以数据安全风险为核心



以数据安全风险为核心

角色名称	应用编码	排序	上级角色	拥有资源	备注	操作
统一权限系统	sa.com	1			统一权限系统	
审计	rendai.com	1	统一权限系统	统一权限系统,申请单列表,应用日志,日志列表,日志详情,审计		
用户管理员-授权	rendai.com	1	统一权限系统	用户管理,用户信息增修,用户列表,用户批量授权,用户分配,用户管理,无添加权限		
角色管理	rendai.com	1	统一权限系统	角色管理,添加角色,添加角色页,编辑角色,编辑角色页,角色管理页		
用户管理员-有添加权限	rendai.com	1	统一权限系统	统一权限系统,资源管理,添加资源,添加资源页,编辑资源,用户管理页		
权限申请	rendai.com	1	统一权限系统	删除分组,批量删除,获取分组信息,获取分组详情列表,应用角色		
应用管理	rendai.com	1	统一权限系统	统一权限系统,申请单列表,资源管理,添加资源,添加资源页	应用管理页	
用户分组管理员	rendai.com	1	统一权限系统	用户分组,添加分组,添加分组页,编辑分组,编辑分组页,用户分组管理页		
资源管理	rendai.com	1	统一权限系统	资源管理,添加资源,添加资源页,编辑资源,编辑资源页,资源管理页		
emma_test	rendai.com	4	统一权限系统		test	
test	rendai.com	1	emma_test		test	
保险系统	yirendai.com	2			保险系统	
保险运营操作	yirendai.com	1	保险系统	日常运营,日常运营页,外行日常运营,首页	保险运营操作	
保险运营-订单查询	yirendai.com	1	保险系统	订单,订单列表,订单列表页,状态同步,状态批量同步,订单,保险运营-订单查询		
保险运营-保单数据导出	yirendai.com	1	保险系统	保单监控,保单监控页,导出投保用户信息,统计保单,保单,保险运营-保单数据导出		
保险系统管理	yirendai.com	1	保险系统	统一权限系统,资源管理,添加资源,编辑资源,删除资源,资源管理	保险系统管理页	
基金交易系统	rendai.com	3			基金交易系统	
研究	rendai.com	1	基金交易系统	基金管理,基金产品管理,基金属性,查看基金属性,生成下-研究		
出账产品	rendai.com	1	基金交易系统	基金管理,基金产品管理,查看基金属性,设置确认份额,出账产品		
出账运营高级	rendai.com	1	基金交易系统	基金管理,主题基金管理,生效无效标签,调整权重标签,取回出账运营高级		
出账运营操作	rendai.com	1	基金交易系统	基金管理,主题基金管理,生效无效标签,调整权重标签,取回出账运营操作		
出账运营工具	rendai.com	1	基金交易系统	基金管理,主题基金管理,生效无效标签,调整权重标签,取回出账运营工具		
营销平台		4				
申请记录	rendai.com	1	营销平台	运营平台系统,首页,用户运营管理,申请记录		
发帖记录查看	rendai.com	1	营销平台	运营平台系统,首页,用户运营管理,发帖记录查看	发帖记录查看	
筛选发帖申请人	rendai.com	1	营销平台	运营平台系统,首页,用户运营管理,用户筛选	筛选发帖申请人	
礼包记录查看	rendai.com	1	营销平台	运营平台系统,首页,用户运营管理,礼包发放记录	查看礼包发放记录	
消息记录查看	rendai.com	1	营销平台	运营平台系统,首页,用户运营管理,消息记录查看		
消息任务管理	rendai.com	1	营销平台	运营平台系统,首页,用户运营管理,消息管理	消息的定时管理	
礼包管理	rendai.com	1	营销平台	运营平台系统,首页,礼包运营,礼包发放管理		

统一权限的管理、审计

以数据安全风险为核心

SQL 查询

SELECT * FROM c_user

执行 格式化 清理

ID	NAME	NAME	MAIL	R_PWD	TYPE	ID	TYPE	FORCE	C	I	VER
2508	*****	心	*****	*****	0	1	10001		NULL		NULL
2512	*****	理	*****	*****	0	1	10001		NULL		NULL
2515	*****	an	*****	*****	1	1	10002		NULL		NULL
2516	*****	仔	*****	*****	0	1	10001		NULL		NULL
2518	*****	达人	*****	*****	0	1	101001		NULL		NULL
2520	*****	井	*****	*****	0	1	10001		NULL		NULL
2530	*****	吧	*****	*****	0	1	10001		NULL		NULL
2547	*****	警呀	*****	*****	0	1	1001		NULL		NULL

```

[+] db_name randa | db_id 1140-as17-005006634579 | table ydy | user | column_name mobile | data 1556 | 4600
[+] db_name randa | db_id 591 | 1140-as17-005006634579 | table ydy | r | column_name mobile | data 1581039 | 5
[+] db_name | db_id 591 | 1140-as17-005006634579 | table srv_user | user_name telephone | data 1312003294 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name C | data 52270018 | 800989324
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name F | data 1845050000 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name ID | data 2322311982 | 81267
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name MOBILE_NO | data 1363 | 7310
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name BANK_ACCOUNT_NO | data 227065173040286633 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name IDCARD | data 2200291979 | 24345
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name PHONE | data 134856644 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name TELEPHONE | data 3702501844 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name TELEPHONE | data 00043050 | 6446451952634649392
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name IDCARD | data 44072 | 9305023516
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name ALIPAY_ACCOUNT | data 158 | 45257
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name CONTACT_PHONE1 | data 150 | 7181
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name CONTACT_PHONE2 | data 139 | 7269
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name CONTACT_PHONE3 | data 165 | 1881
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name CONTACT_PHONE4 | data 158 | 257
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name CONTACT_PHONE5 | data 180 | 11
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name TELEPHONE | data 1501039 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name OPEN_CONTACTER1 | data 11 | 3678
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name OPEN_CONTACTER2 | data 11 | 4424
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name OPEN_CONTACTER3 | data 10 | 3917
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name OPEN_CONTACTER4 | data 10 | 1295
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name OPEN_CONTACTER5 | data 10 | 7079
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name PHONE | data 10385 | 303
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | overdue | column_name IDCARD | data 198403220017 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | overdue | column_name TELEPHONE | data 12269117 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name ID_CARD | data 45451198 | 2421
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name SUPERSEDE_MOBILE | data 1 | 37011
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name BANK_ACCOUNT_NO | data 227065173040286633 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name ID_NO | data 50023519846 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | ser | column_name user_login_name | data 1342 | 3508
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name period | data 300000 | 26069
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name bank_card | data 6222 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name mobile | data 12 |
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name bank_card | data 622 | 4004210220190
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name idcard_no | data 3623 | 8305183513
[+] db_name | db_id 591 | 1140-as17-005006634579 | table ts_a1a_sav | column_name | data 4232 |
    
```

定期检索、维护需要做特殊处理的字段

WorkSpace | 2016-12-16 16:37:41

Showing 34 incident(s) / 1 selected

ID	Incident Time	Source	Channel	Destination	Severity	Action	Maximun Matches	Transaction Size	File Name
2971797	2016-12-16 16:37:41	P3-攻击-网络钓鱼	Endpoint application	Twitter QQ	Low	Blocked	74	253.94 KB	C:\Users\administrator\...
2971825	2016-12-16 16:54:36	P3-攻击-网络钓鱼	HTTP	www.vandorlab.com	Medium	Permitted	2	111.37 KB	C:\Users\administrator\...
2972043	2016-12-16 18:14:04	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	High	Blocked	174	100 KB	C:\Users\18801015\...
2972447	2016-12-16 18:14:01	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	High	Permitted	28	103.4 KB	C:\Users\18801015\...
2972607	2016-12-16 18:13:28	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	High	Permitted	101	74.13 KB	C:\Users\18801015\...
2973425	2016-12-16 18:05:02	P3-攻击-网络钓鱼	Endpoint HTTPS	MAL_QQ.COM	Medium	Permitted	174	100 KB	C:\Users\18801015\...
2973680	2016-12-16 18:02:52	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	Medium	Permitted	174	100 KB	C:\Users\18801015\...
2973665	2016-12-16 18:00:24	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	Medium	Permitted	174	100 KB	C:\Users\18801015\...
2973560	2016-12-16 17:59:59	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	Low	Permitted	174	100 KB	C:\Users\18801015\...
2973516	2016-12-16 17:58:14	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	Low	Permitted	174	100 KB	C:\Users\18801015\...
2973412	2016-12-16 17:58:12	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	High	Permitted	20	61.4 KB	C:\Users\18801015\...
2973344	2016-12-16 17:57:45	P3-攻击-网络钓鱼	Endpoint removable	Kingston DataTraveler	High	Permitted	101	74.13 KB	C:\Users\18801015\...

Incident: 2971757 | Severity: Low | Action: Blocked | Channel: Endpoint application (Dns-Access)

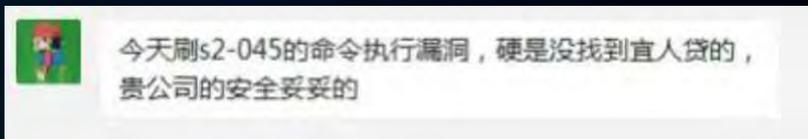
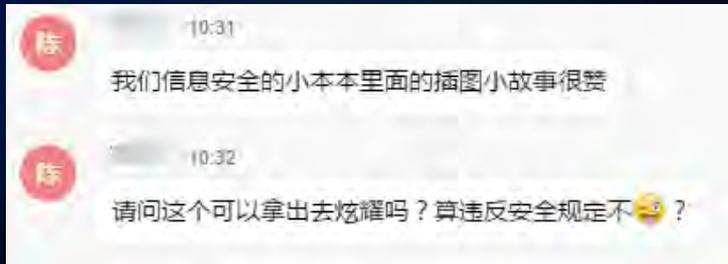
Display: Validation Progress | Summary: Unseen Pay Credit Cards (Default) (Scope)

Source: XECONG24531\administrator | Event Time: 16 Dec 2016 17:37:01 PM

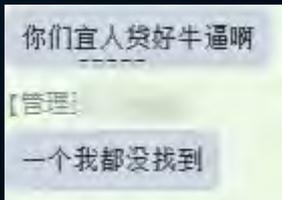
Details: File "C:\Users\administrator\documents\incident Files" (file) "该文件被打开" was accessed by "eventest QQ"

File: C:\Users\administrator\documents\20161216\eventest QQ\253.94 KB

世界其实还是美好的



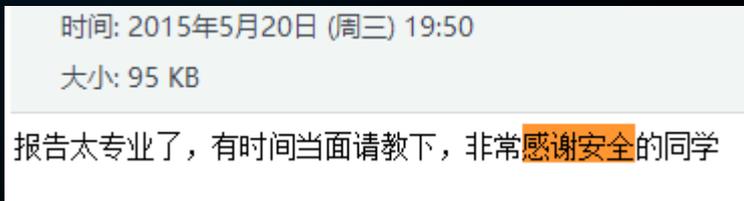
这样吧，先按创新产品的流量做方案，但是希望把buffer考虑进去，因为贷
感谢安全同事积极参与以及专业的建议，希望一起加强合作推进方案实施。



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：



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



风雨同舟 坚持不懈