C3安全峰会
CYBER | CLOUD | COMMUNICATION

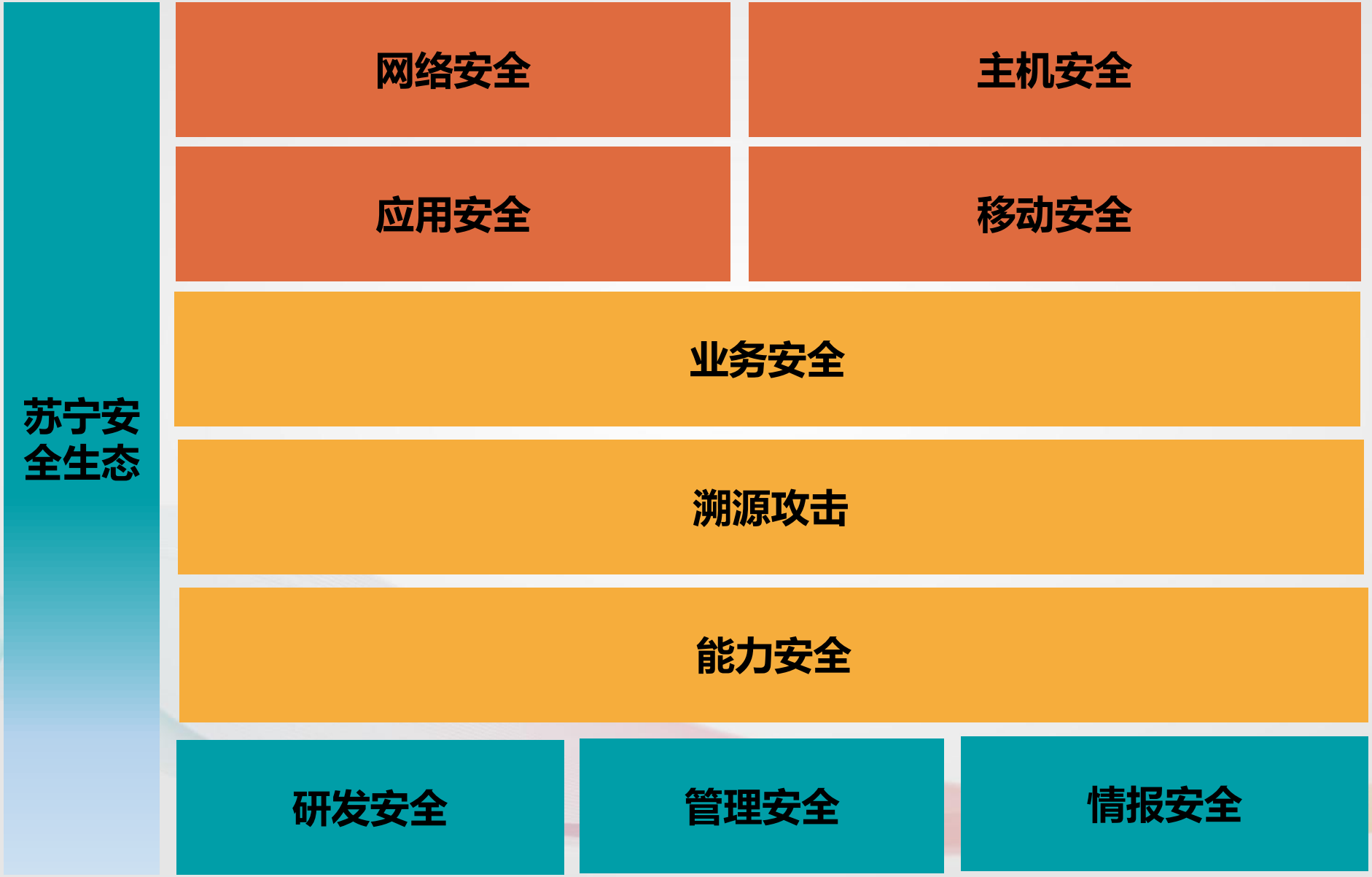
Innovation Practice
安全生态创新实践

黄宙
苏宁攻防实验室负责人

C3

目 录

苏宁安全生态



项目代号：索伦之眼

目 录

苏宁安全生态基础


2016.10
安全态势感知中心
能力意识
能力意识训练平台
2016.3
2015.10
漏洞报告中心
业务安全风险分析
2013/2016
信息情报
业务逻辑
2012/2014/2016
云安全防护
业务安全风险控制
研发流程管理
2013/2016
2015
业务资产管理
网络资产
代码功能
研发同步安全测试
2013/2016.1
2013/2016
主机安全管理
产品发布安全测试
2013/2016

理论基础

基于日志的挖掘安全未知漏洞的方法和系统 审中-实审

申请号：201510026904.6 申请日：2015-01-19

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求资源信息进行分析清洗；S4、对所述服务器域名和用户请求资源信息进行未知漏洞分析与挖掘。本发明的技术方案可以通过对日志数据正向过滤与安全漏洞攻击特征逆向排除，实现挖掘利用漏洞攻击发现，降低安全漏洞挖掘成本，提高了挖掘未知漏洞效率。

申请人： 苏宁云商集团股份有限公司

地址： 210042 江苏省南京市玄武区苏宁大道1号15楼

发明(设计)人： 黄宙

主分类号： H04L29/06(2006.01)I

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

目 录

苏宁安全生态“十戒”

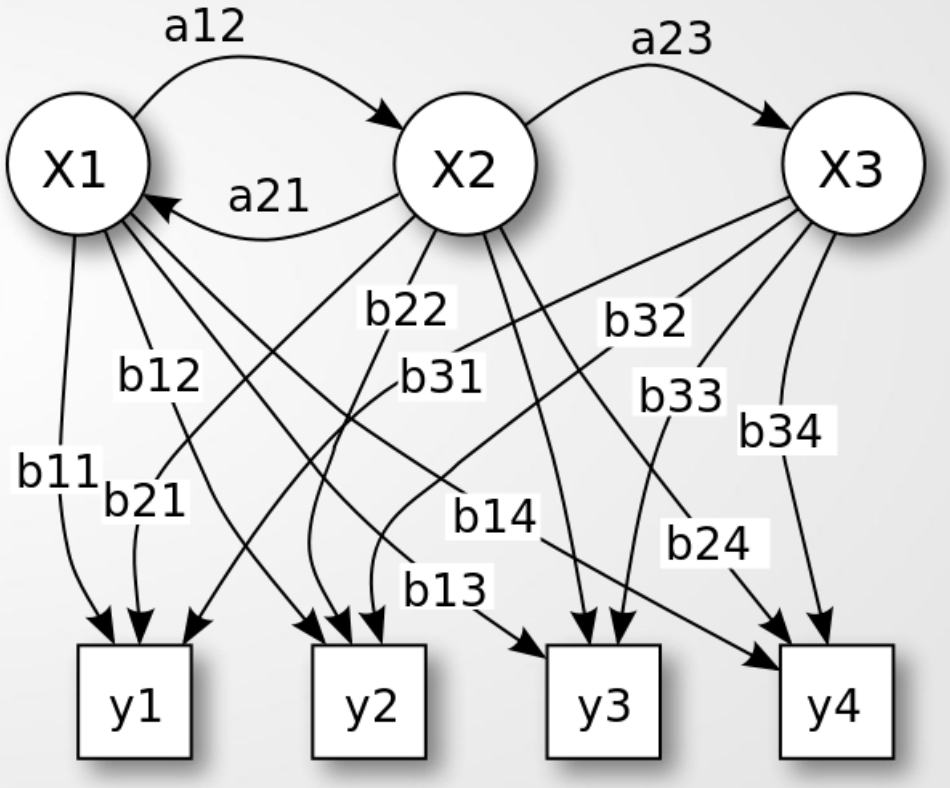

业务安全
网络安全
主机安全
情报安全
研发安全
管理安全
溯源攻击
能力安全
移动安全
应用安全
高级
高级
高级
中级
中级
初级
初级
中级
初级
高级
高级
初级
初级

安全经验与算法（HMM）

说了很多，往往一句话解决问题。

XX，你说的方法，有点像XX模型？

隐马尔可夫模型
Hidden Markov Model

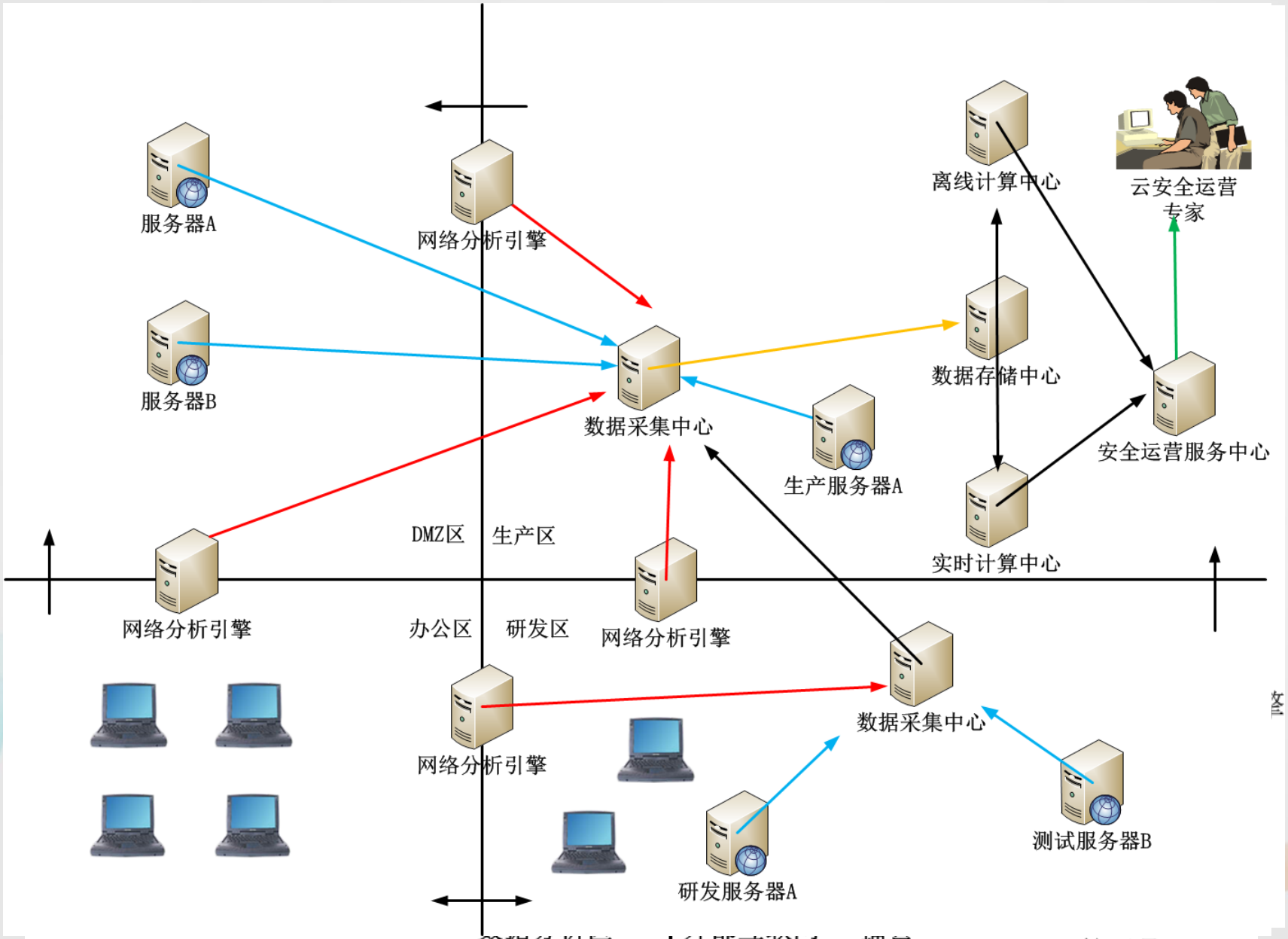


目 录

平台架构

- Spark
- Spark Streaming
- Hbase
- Flume
- Kafka
- Mysql
- Nginx
- Redis
- Sqoop
- … …

适应场景路线



开放云服务

私有云服务

公有云服务

混合云服务

业务安全——业务之戒

C3安全峰会
CYBER | CLOUD | COMMUNICATION

场景列表 > 0001

请输入URI关键字过滤

规则ID	域名	URL	规则	状态	规则属性	准确性	附加规则
7001000164	my.suning.com	/wap/addrInput0.do	参数名:addrNum, 参数类型:A...	停用	正常 异常	精确 模糊	编辑
7001000165	my.suning.com	/ajax/getCommonHorizontalMenu.do	参数名:_t,参数类型:A,最大长度...	停用	正常 异常	精确 模糊	编辑
7001000166	my.suning.com	/ajax/getCommonVerticalMenu.do	参数名:_t,参数类型:A,最大长度...	停用	正常 异常	精确 模糊	编辑
7001000167	my.suning.com	/wap/addrInput0.do	参数名:addrNum,	停用	正常 异常	精确 模糊	编辑

溯源攻击——溯源之戒

攻击来源

#	城市
3235	Beijing
2118	Guangzhou
1930	Hangzhou
1559	Meizhou
1430	Nanjing
1387	Chengdu
1227	Shanghai
1009	Shenzhen

攻击类型

#	攻击类型
32177	CC_Attack
95	XSS_Attack
57	CommExec_Attack
9	FileIn_Attack
4	SQL_Attack

实时攻击列表

攻击时间	攻击者IP	攻击者所在地	被攻击应用/IP	攻击类型	攻击端口
00:02:02.353	42.94.66.56	Lanzhou, China	dt.suning.com	CC_Attack	80
00:02:02.351	112.225.211.122	Qingdao, China	passport.suning.com	CC_Attack	80
00:02:01.311	140.237.98.68	Yong'an, China	reg.suning.com	CC_Attack	80
00:02:00.991	122.238.216.240	Wenzhou, China	reg.suning.com	CC_Attack	80
00:02:00.555	113.250.191.15	Chongqing, China	aq.suning.com	CC_Attack	80
00:02:00.145	224.235.69.167	Wuhan, China	reg.suning.com	CC_Attack	80
00:01:59.785	119.0.0.24	Jagdaqi, China	cart.suning.com	CC_Attack	80
00:01:59.471	110.53.145.89	Changsha, China	reg.suning.com	CC_Attack	80

研发安全——研发之戒

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Web应用安全评估系统

- 任务
  - 任务列表
  - 蛙测列表
- 漏洞
- 管理

蛙测任务列表

序号	扫描url
1	http://[redacted]/sec-scan/tracker/scan/
2	http://[redacted]/sec-scan/tracker/
3	http://[redacted].com/
4	http://[redacted]sec-scan/tracker/
5	http://api.bing.com/qsml.aspx?query=http%3A%2F%2F[redacted] maxwidth=32765&rowheight=21§ionHeight=210&FORM

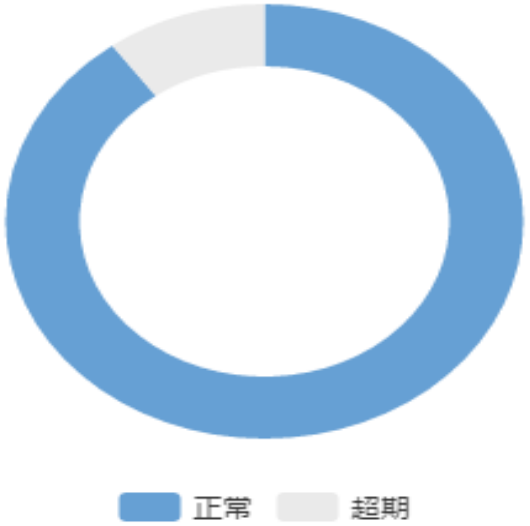
能力安全与管理安全

C3安全峰会
CYBER | CLOUD | COMMUNICATION

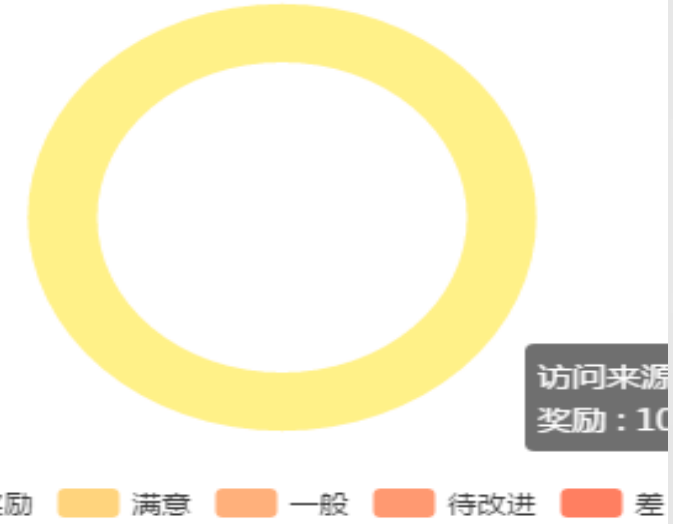
服务统计

渗透安全工程师 全部 | 年份 2017 | 统计类型 按季度 | 选项 第一季度

完成质量



用户评估



序号	系统名称	开始时间	完成时间	超期情况	评分	评语
1	决策分析平台	2017-03-01 00:00:00	2017-03-11 00:00:00	正常	5	
2	[redacted]红包系统 [redacted]	2017-01-07 00:00:00	2017-01-09 00:00:00	正常	5	好
3	snfs	2017-02-15 00:00:00	2017-02-18 00:00:00	正常	5	

目 录

未来规划

C3安全峰会
CYBER | CLOUD | COMMUNICATION

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

攻击预警

攻击 | 规则库

规则自动发送 勾选后产生的规则会自动的发送给waf平台

	规则序号	拦截IP	拦截时段	域名
	1	112.80.230.69	9:00 -21:00	[redacted]

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You

C3