数据时代的企业安全“观”

观星
Data Star Observatory

数字观星 / 郭亮（北极星）

PART 01

IT vs DT 安全目标

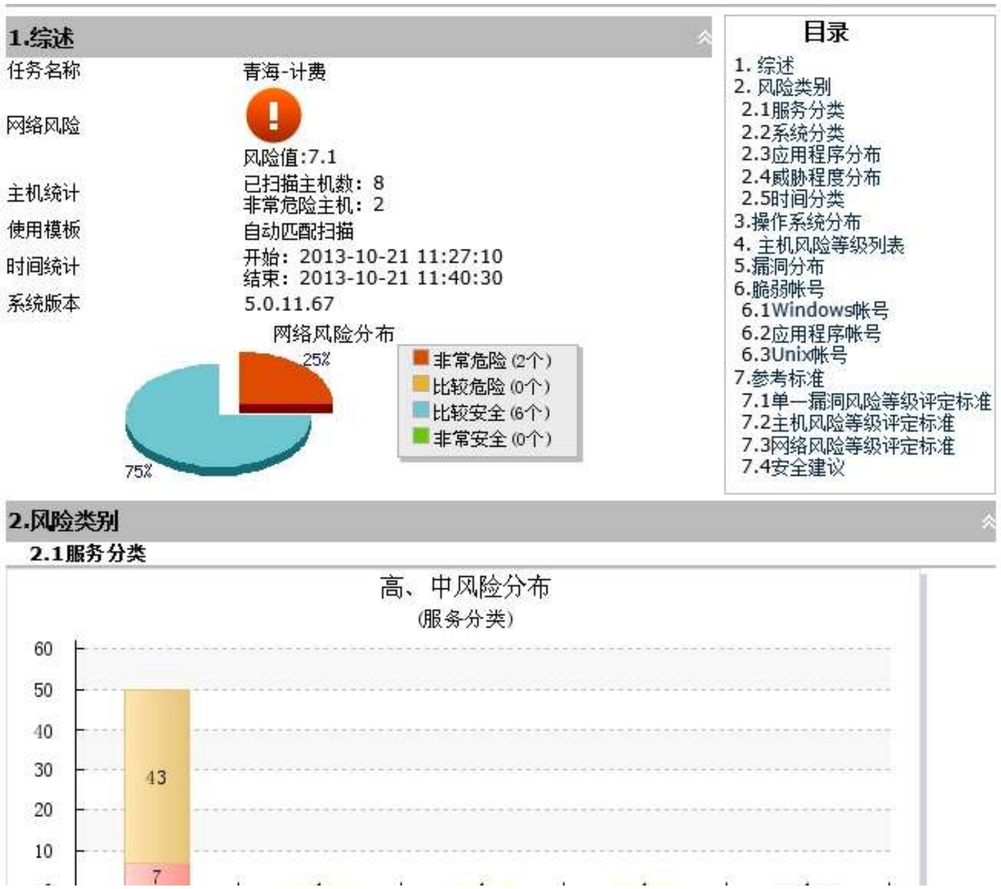
IT 和 DT 时代背景不同的安全目标

IT时代的安全目标

“不出事”与“能省钱”

IT时代的安全观

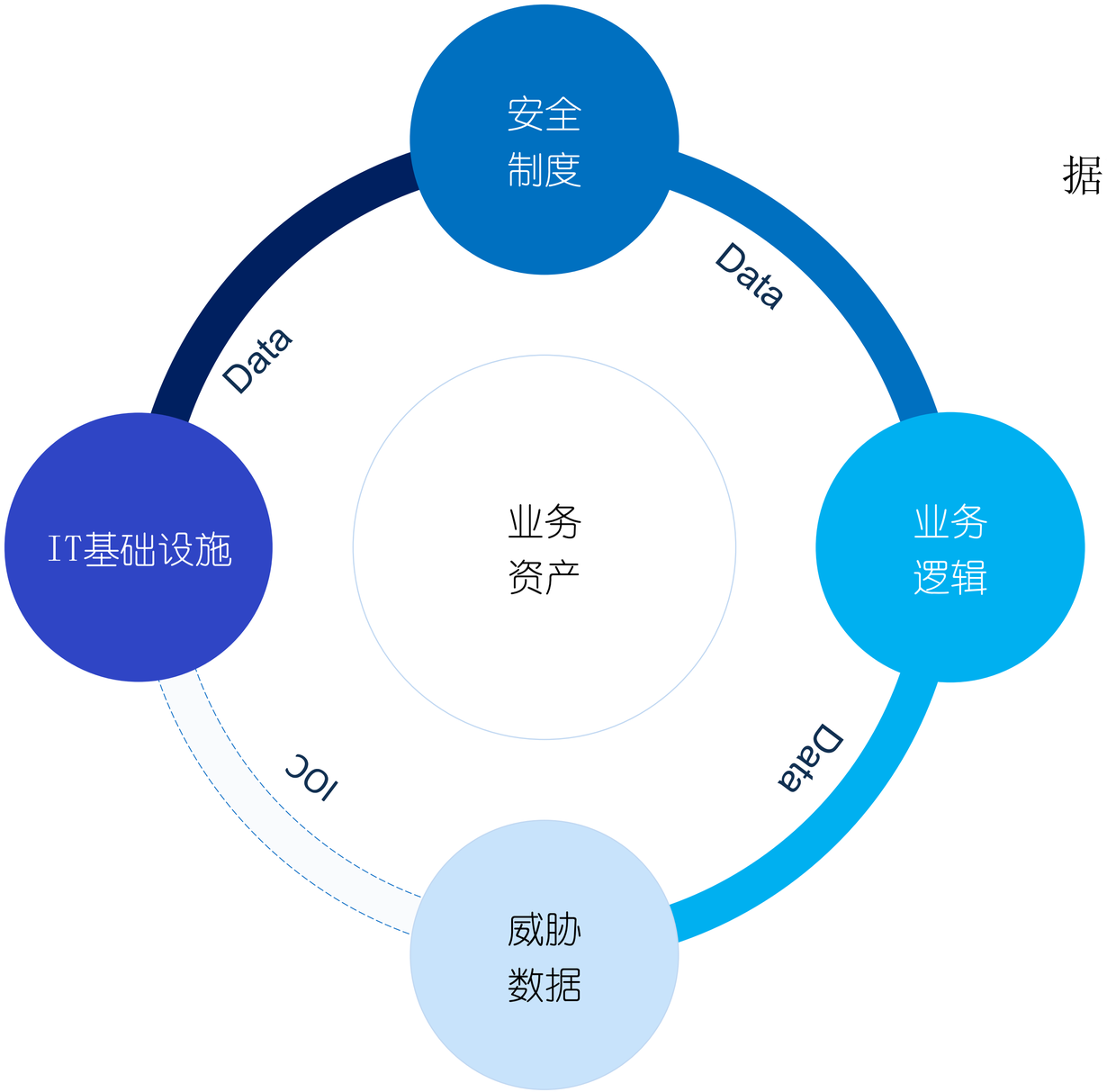
- 漏洞检测
- 立项：合规
- 采购：技术参数 & 价格；
- 管理：漏洞扫描制度；
- 技术：买漏洞扫描器；
- 运维：把漏扫和SOC对接；



DT时代的安全目标

“不出事（可度量）”与“别丢钱”

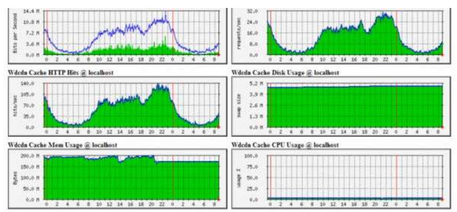
数据时代的安全观



以业务资产为核心，通过时间等多维数据可度量；

安全水平成熟度

10月31日 14:00分

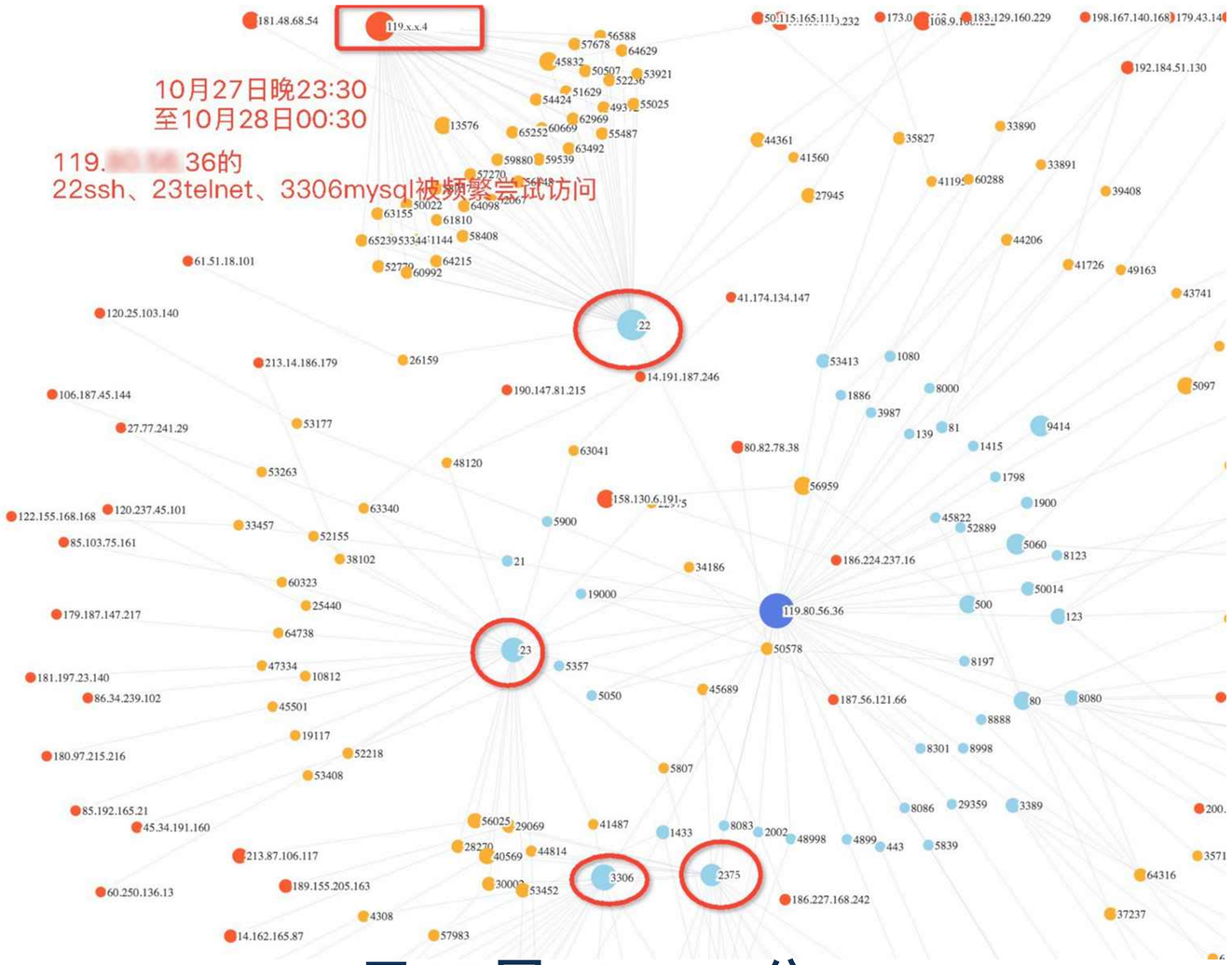


出口拥塞

由内向外

119. x. x. 36

119. x. x. 36 → 119. x. x. 4



Port：
22
23
3306
2375

10月27日 23:30分

10月27日 23:30分

2375：Docker

CNVD 国家信 CHINA NAT

首页 | 热点关注 | 漏洞列表 | 补丁信息

当前位置： 首页 > 漏洞详细信息

Docker权限获取漏洞

报送者:北京启明星辰信息安全技术有限公司

CNVD-ID	CNVD-2016-03197
发布时间	2016-05-17
危害级别	高 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Docker Docker
CVE ID	CVE-2016-3697

2016年5月17日
CVE－2016-3697

IP：119. x. x. X / 24—98台服务器

PART 02

时间观

时间因素影响的安全价值

XcodeGhost

2015年9月19日爆出，植入恶意代码的Xcode由攻击者上传至百度云网盘，然后通过国内几个知名论坛发布传播，传播的论坛包括：威锋网论坛、unity圣典、9ria论坛和swiftmi。

最早发布是在“unity圣典”，进行传播的时间为2015年3月16日。

站点名称	站点说明	发帖时间	标题	网址	发帖 ID
威锋网	国内知名 iPhone 社区	2012-12-29 13:17 最后编辑时间 2015-6-15 09:41	Xcode 最全版本下载，Xcode7 以及 Xcode6 全系列	http://bbs.feng.com/read-htm-tid-5711821.html	lmznet
unity 圣典	Unity3D 中文技术交流社区	2015-03-16 11:49 最后编辑时间 2015-3-23 18:12	最全 Xcode 各版本网盘超快下载！！【求加精】	http://game.ceeger.com/forum/read.php?tid=204961-1-1.html	coderfun
9ria 论坛	游戏开发者社区	2015-03-24 16:55	Xcode 最全版本下载	http://bbs.9ria.com/thread-43267	linuxFans
51CTO 论坛（百度快照地址）	中国领先的 IT 技术网站	2015-04-09 18:56 最后编辑时间 2015-7-1 14:07	Xcode 6、Xcode 7 全系列，百度网盘下载地址	http://bbs.51cto.com/thread-1149738-1.html	jrl568
威锋网	国内知名 iPhone 社区	2015-06-15 09:43	Xcode 最全版本下载，Xcode 7 以及 Xcode 6 系列等	http://bbs.feng.com/read-htm-tid-9581633.html	coderfun


盘古
PANGU TEAM
XcodeGhost
病毒感染统计报告
截止日期2015年09月22号 18:00
染毒应用比例
经过651,713次的扫描，我们的云端染毒应用库中已经积累4469条记录，共涉及3414个不同应用（某些应用有多个版本被感染）由此估计苹果商店中可能还有更多的染毒应用尚未被发现。尽管部分染毒应用已从苹果商店下架，但仍有大量染毒应用继续在苹果商店销售。
已扫描总数
651713
染毒应用总数
4469


设备感染比例估计
在651,713次的终端扫描中，检出感染比例57%，未感染比例43%
说明
检测工具不收集除安装应用列表之外的任何用户和设备信息，因此无法区分同一设备发出的多次扫描请求，上述比例仅能粗略反应设备的感染比例，仅供参考。
检出感染比例57%
检出未感染比例43%

4天后，2015年9月22日。

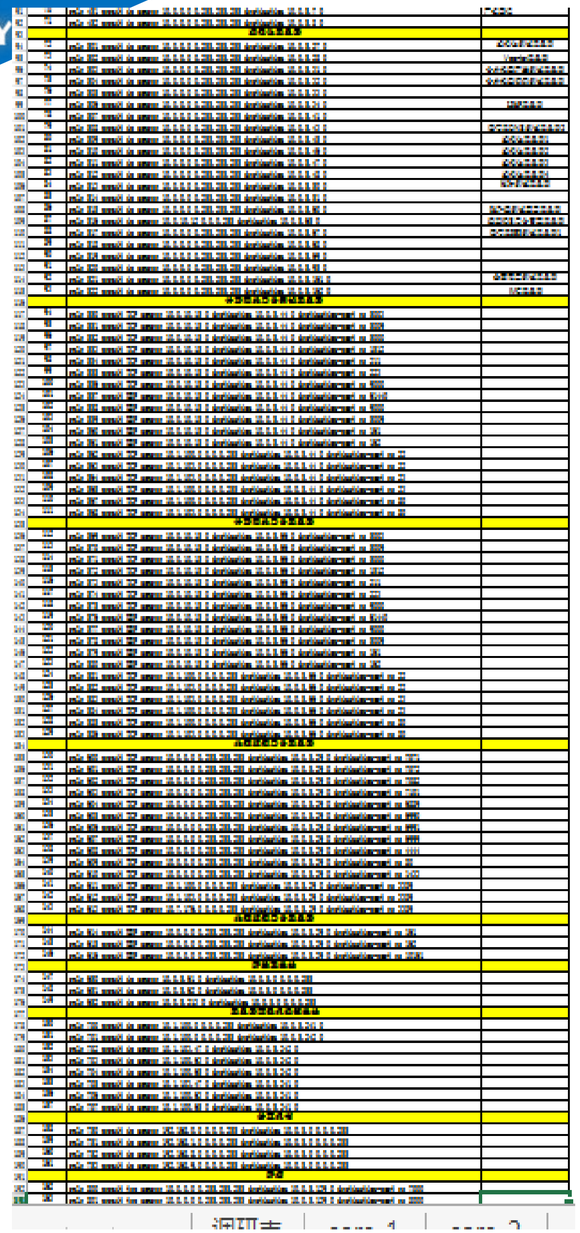
“置若罔闻”是最可怕的安全观

PART 03

可视分析观

可视分析给安全一个“观”点

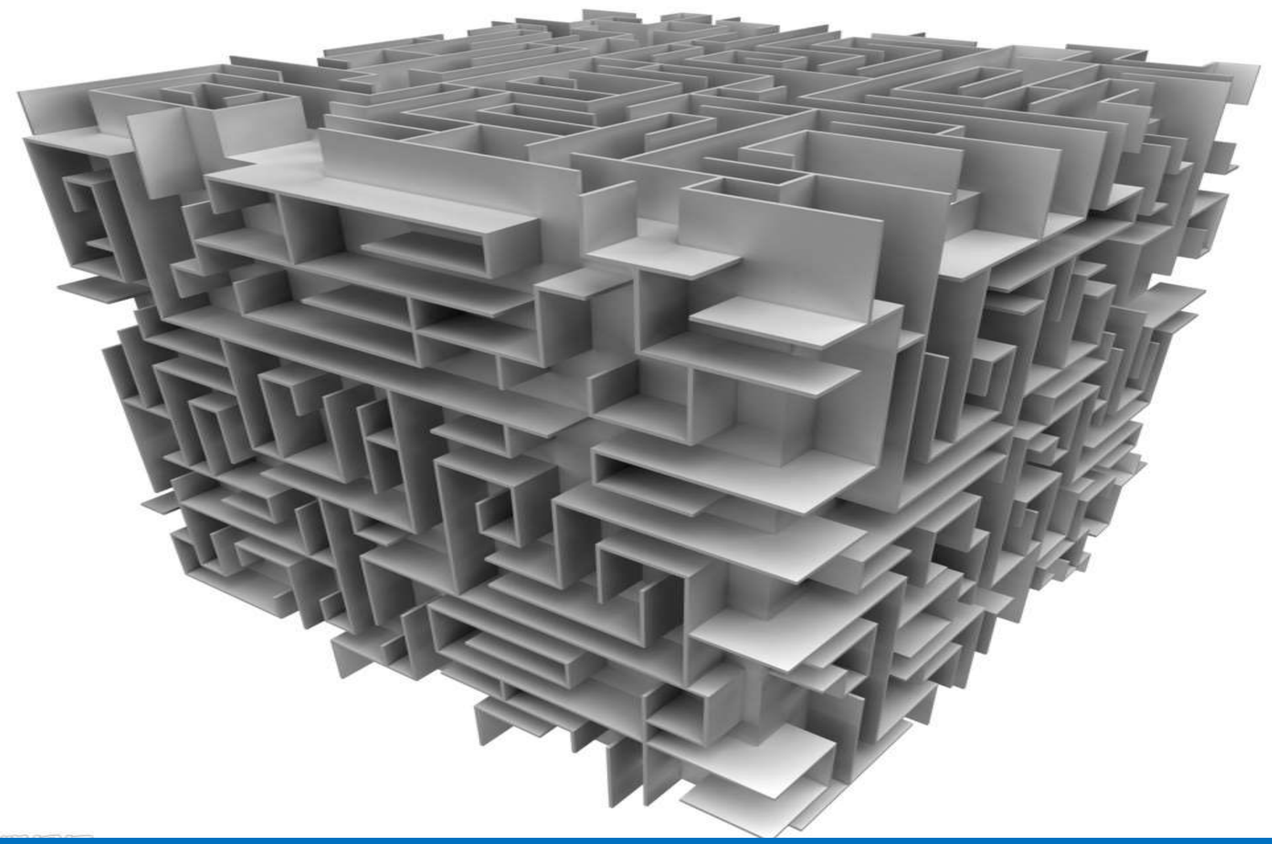
数据规律-防火墙



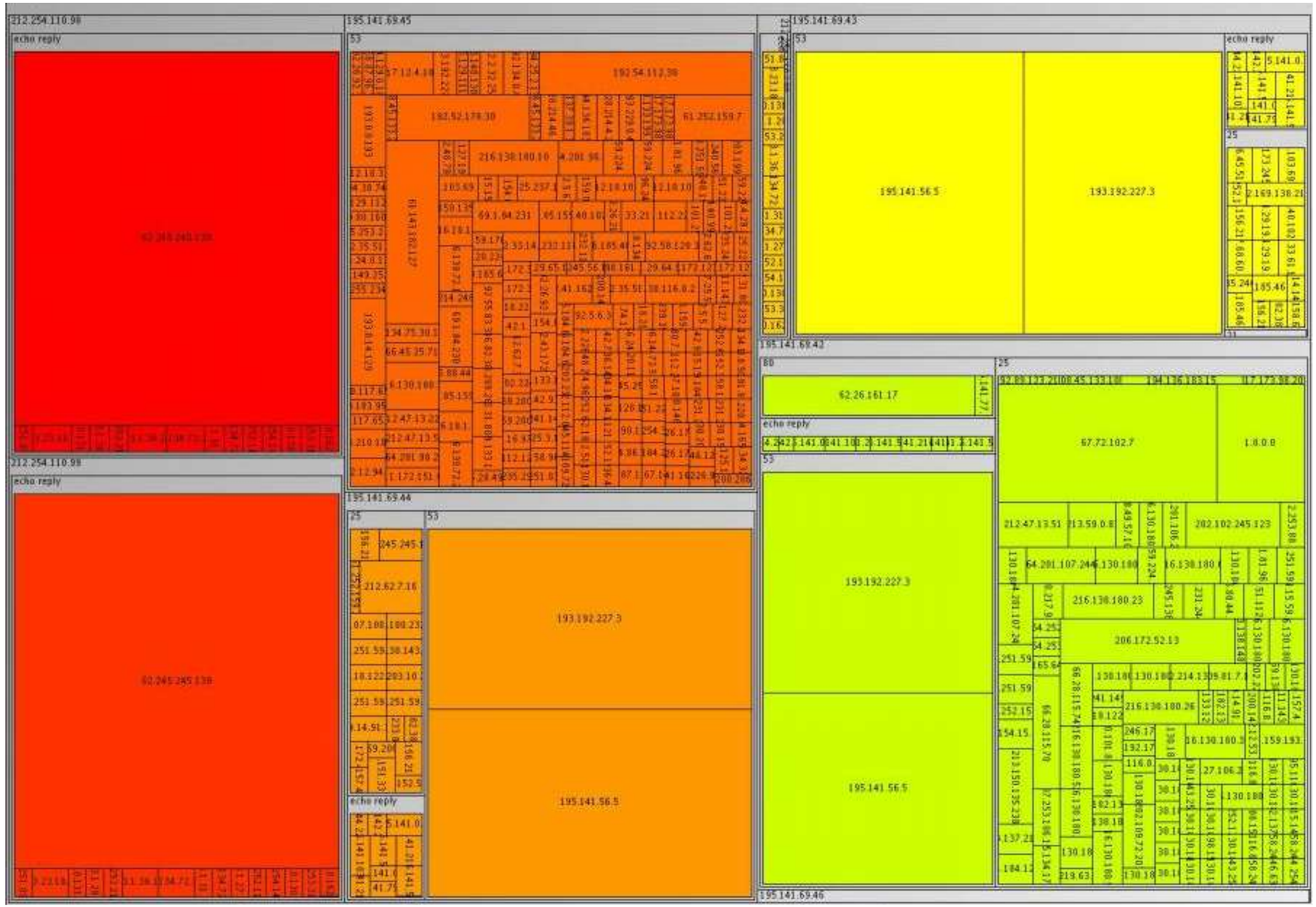
缩放比例 X 10%

防火墙访问控制规则统计表

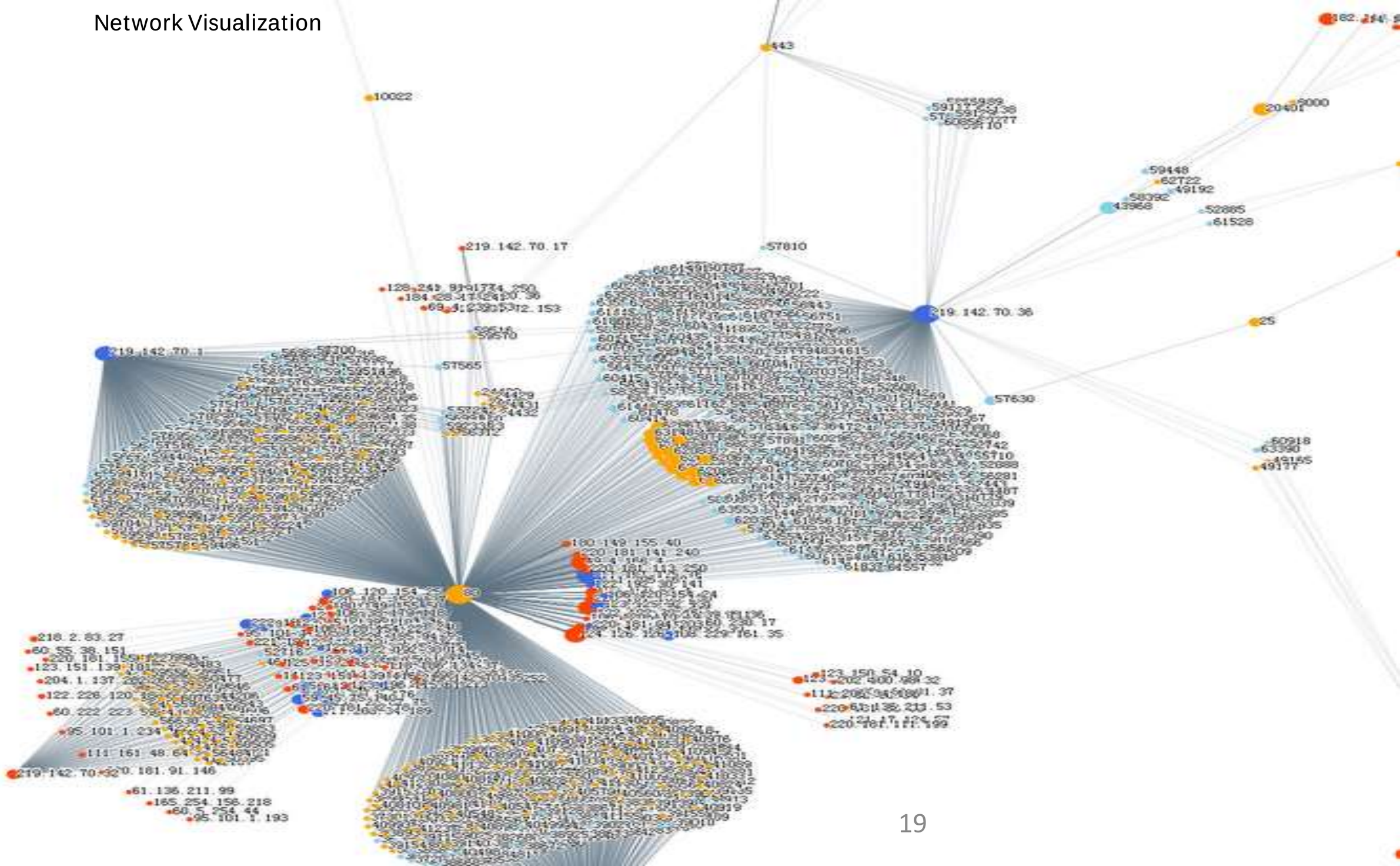
IP类型	序号	IPv4地址	是否存在	操作系统	用途	开启的服务	*访问限制	*备注
例1	/	1.1.1.1	是	Centos 6.0	web服务器	http:8080 https	只允许集团内网使用	
例2	/	2.2.2.0/24	是	/	xx部	/	只允许2.2.2.86访问互联网	
单个IP	1	10.0.2.1		windows	DHCP服务器		允许10.0.2.1到any目的端口53(tcp/udp)	
	2	10.0.2.5		windows	杀毒补丁		禁止10.0.2.5访问10.24.0.0/14 允许10.0.2.5访问任意目的	谁访问谁
	3	10.0.2.11		windows	OA系统备份服务器		允许10.0.2.11访问任意目的	谁访问谁
	4	10.0.2.234			临时访问公网使用			
	5	10.0.2.235						
	6	10.0.2.236						
	7	10.0.5.200			信息情报系统服务器访问公网出口地址			
	8	10.0.250.250						
	9	10.0.252.1		windows	集团老网站	80	开启POP3、SMTP、DOMAIN端口/只允许6080端口访问/只允许内网80端口访问	6080端口被访问？ 80端口谁访问谁
	10	10.0.252.2		隶属10.0.252.1服务器	站点	80		
	11	10.0.252.3			站点	80	只允许80端口访问	
	12	10.0.252.4			站点	80	只允许80端口访问	
	13	10.0.252.5			站点	80	只允许80端口访问	
	14	10.0.252.6			站点	80	只允许806端口访问	
	15	10.0.252.10			站点	80	只允许80端口访问/只允许内网3389端口访问、TELNET、FTP、开启22端口	



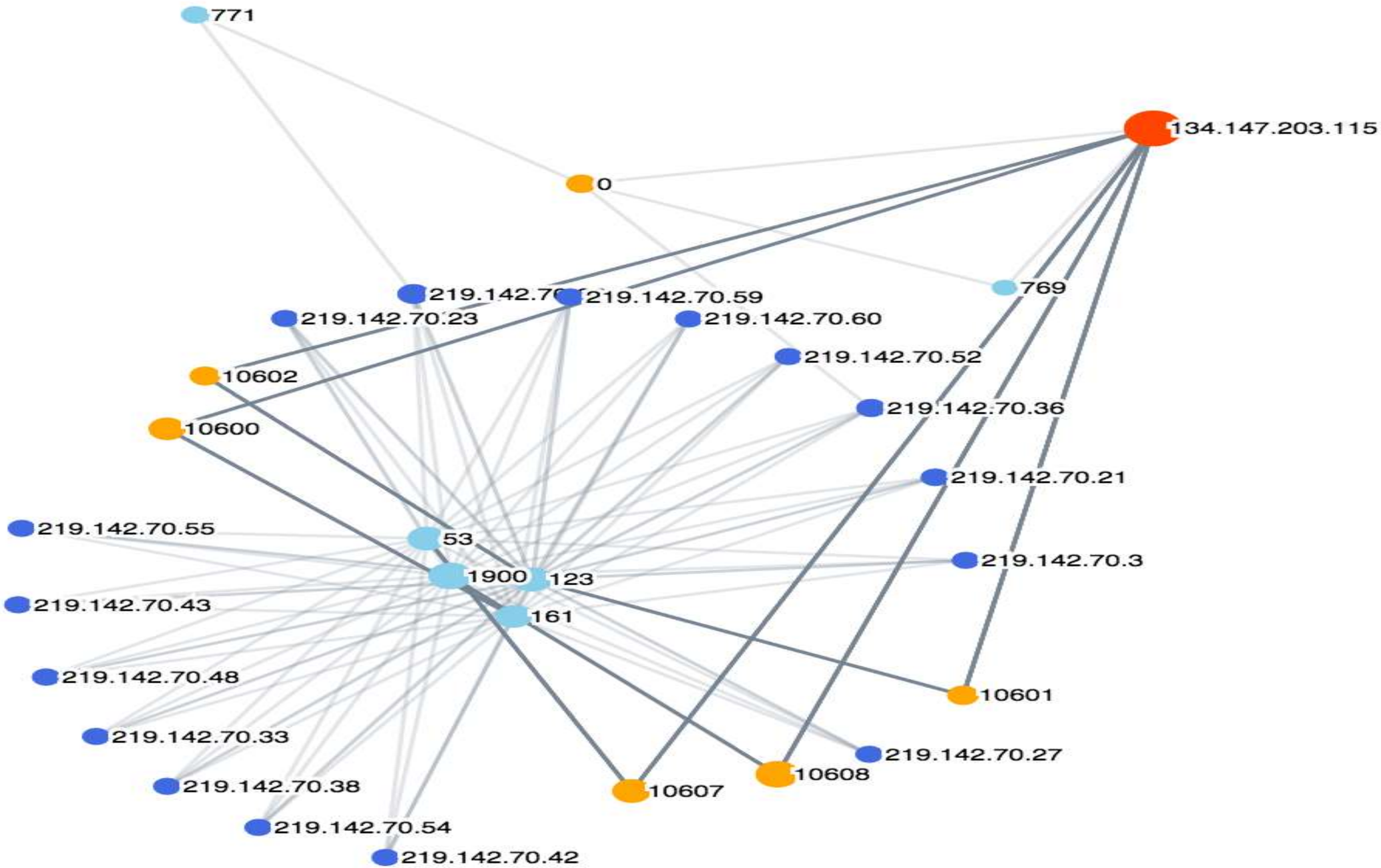
防火墙数据体现的业务规律



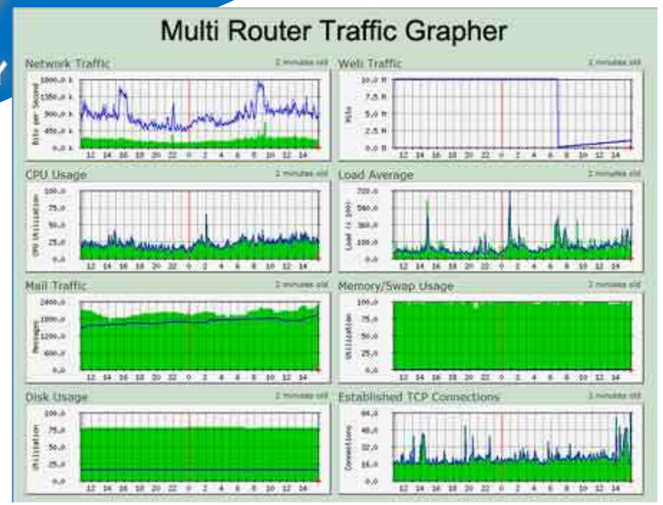
Network Visualization

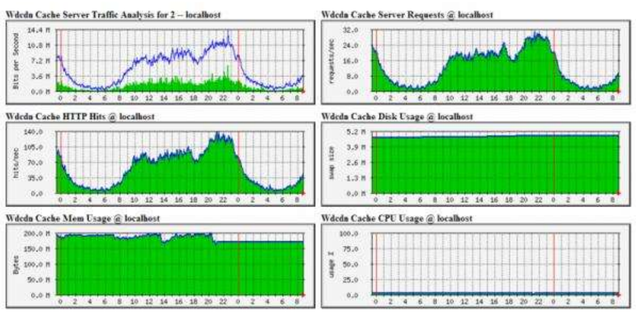


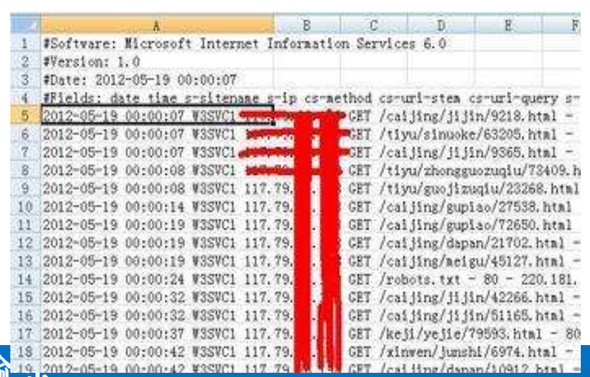
Network Visualization



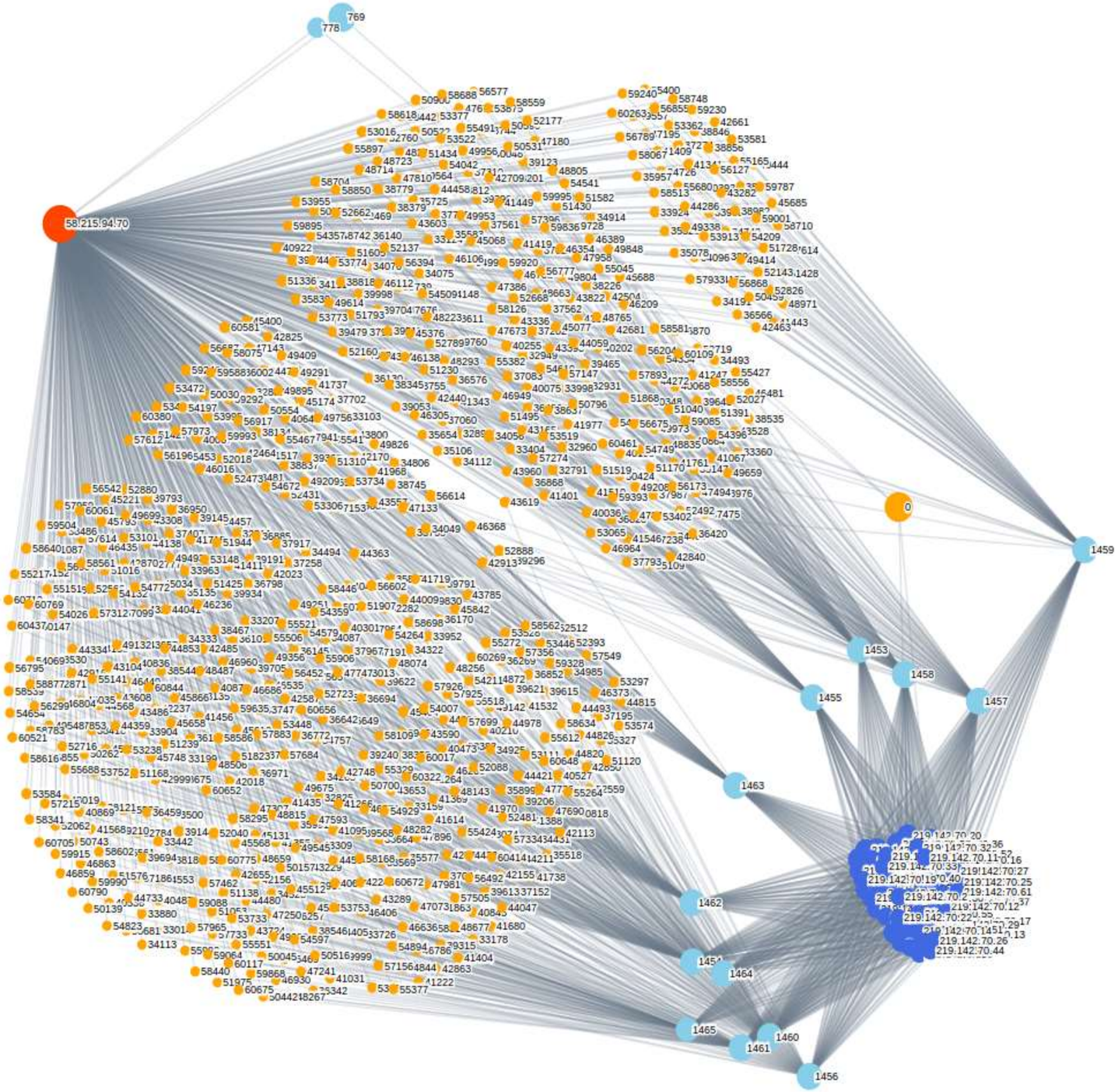
Network Visualization







```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2012-05-19 00:00:07
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-
2012-05-19 00:00:07 W3SVC1 [redacted] GET /caijing/jijin/9218.html -
2012-05-19 00:00:07 W3SVC1 [redacted] GET /tiyu/sinuoke/63205.html -
2012-05-19 00:00:07 W3SVC1 [redacted] GET /caijing/jijin/9365.html -
2012-05-19 00:00:08 W3SVC1 [redacted] GET /tiyu/zhongguozuqiu/73409.h
2012-05-19 00:00:08 W3SVC1 117.79. [redacted] GET /tiyu/guojizuqiu/23268.html
2012-05-19 00:00:14 W3SVC1 117.79. [redacted] GET /caijing/gupiao/27538.html
2012-05-19 00:00:19 W3SVC1 117.79. [redacted] GET /caijing/gupiao/72650.html
2012-05-19 00:00:19 W3SVC1 117.79. [redacted] GET /caijing/dapan/21702.html -
2012-05-19 00:00:19 W3SVC1 117.79. [redacted] GET /caijing/neigu/45127.html -
2012-05-19 00:00:24 W3SVC1 117.79. [redacted] GET /robots.txt - 80 - 220.181.
2012-05-19 00:00:32 W3SVC1 117.79. [redacted] GET /caijing/jijin/42266.html -
2012-05-19 00:00:32 W3SVC1 117.79. [redacted] GET /caijing/jijin/51165.html -
2012-05-19 00:00:37 W3SVC1 117.79. [redacted] GET /keji/yejie/79593.html - 80
2012-05-19 00:00:42 W3SVC1 117.79. [redacted] GET /xinwen/junshi/6974.html -
2012-05-19 00:00:42 W3SVC1 117.79. [redacted] GET /caijing/dapan/10912.html -
```



PART 04

数据规律观

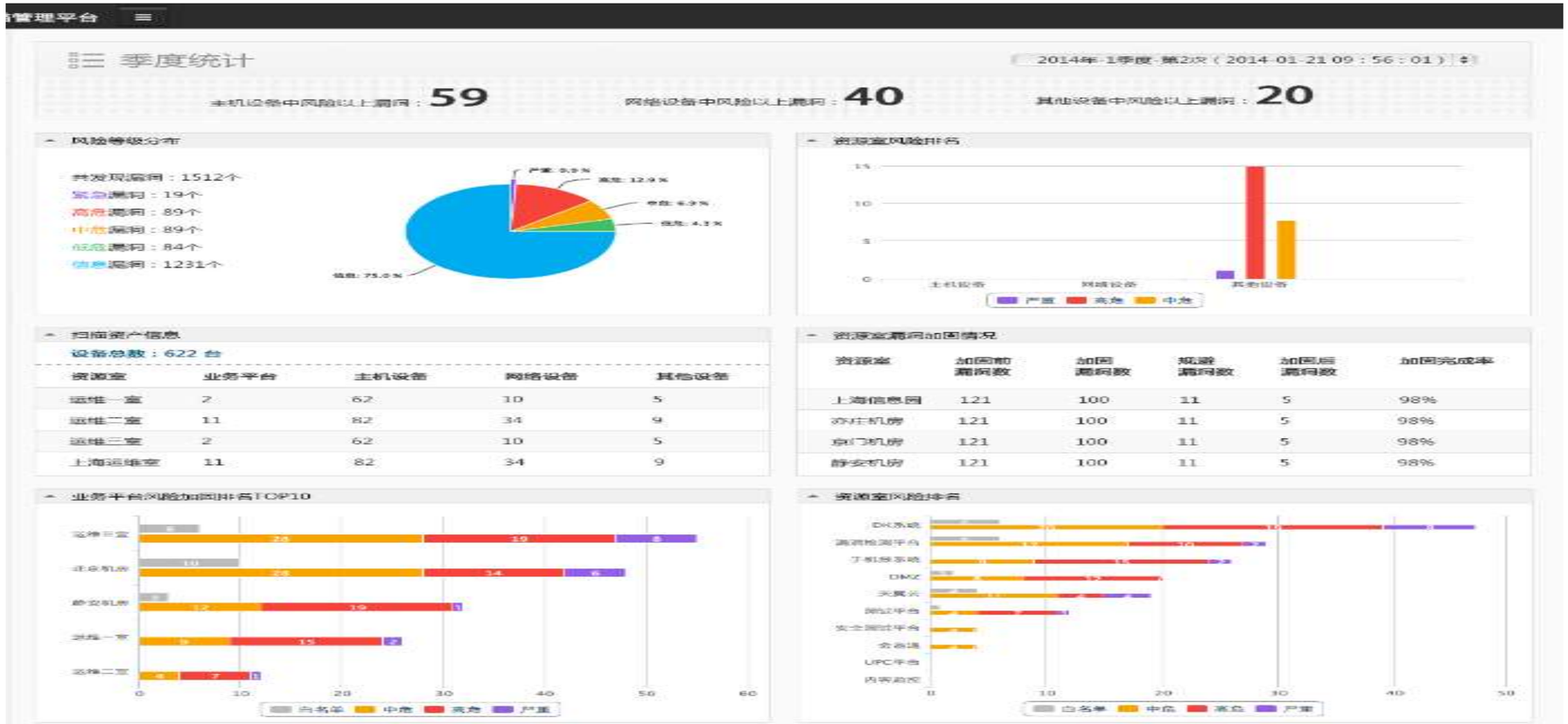
多维度的数据应用，发现规律

安全数据在企业落地的价值三足：

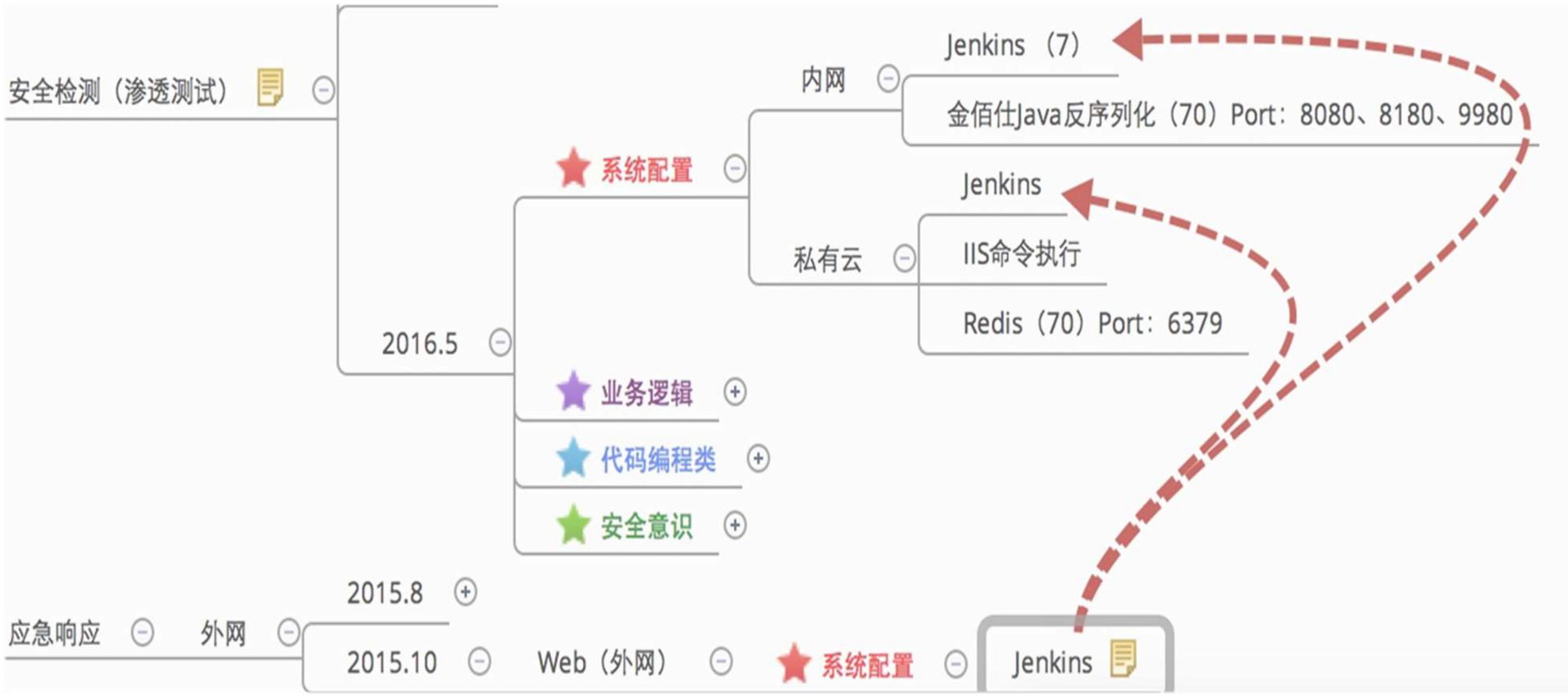
“资产”

“责任”

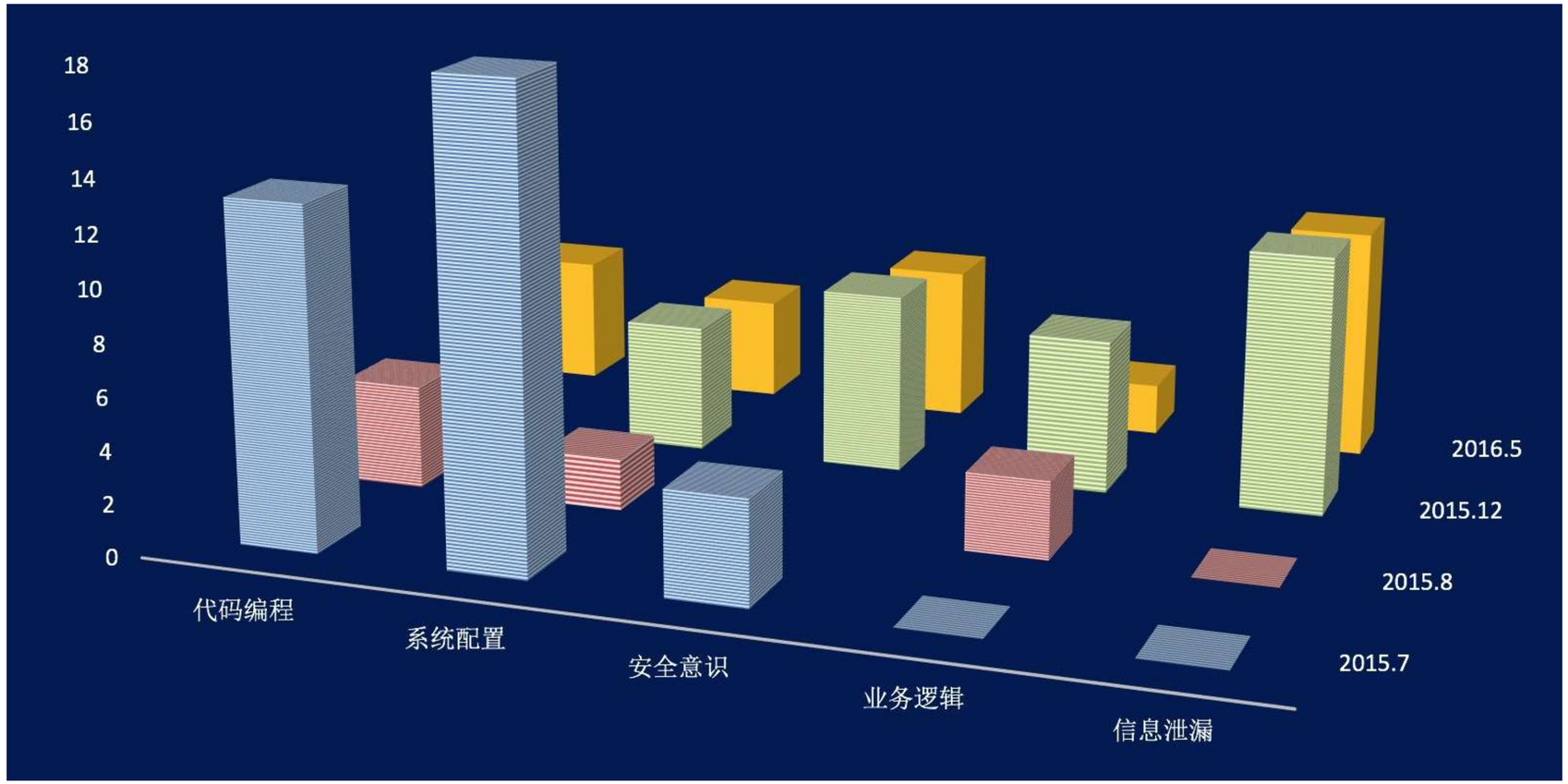
“流程”



时间发现的“责任”

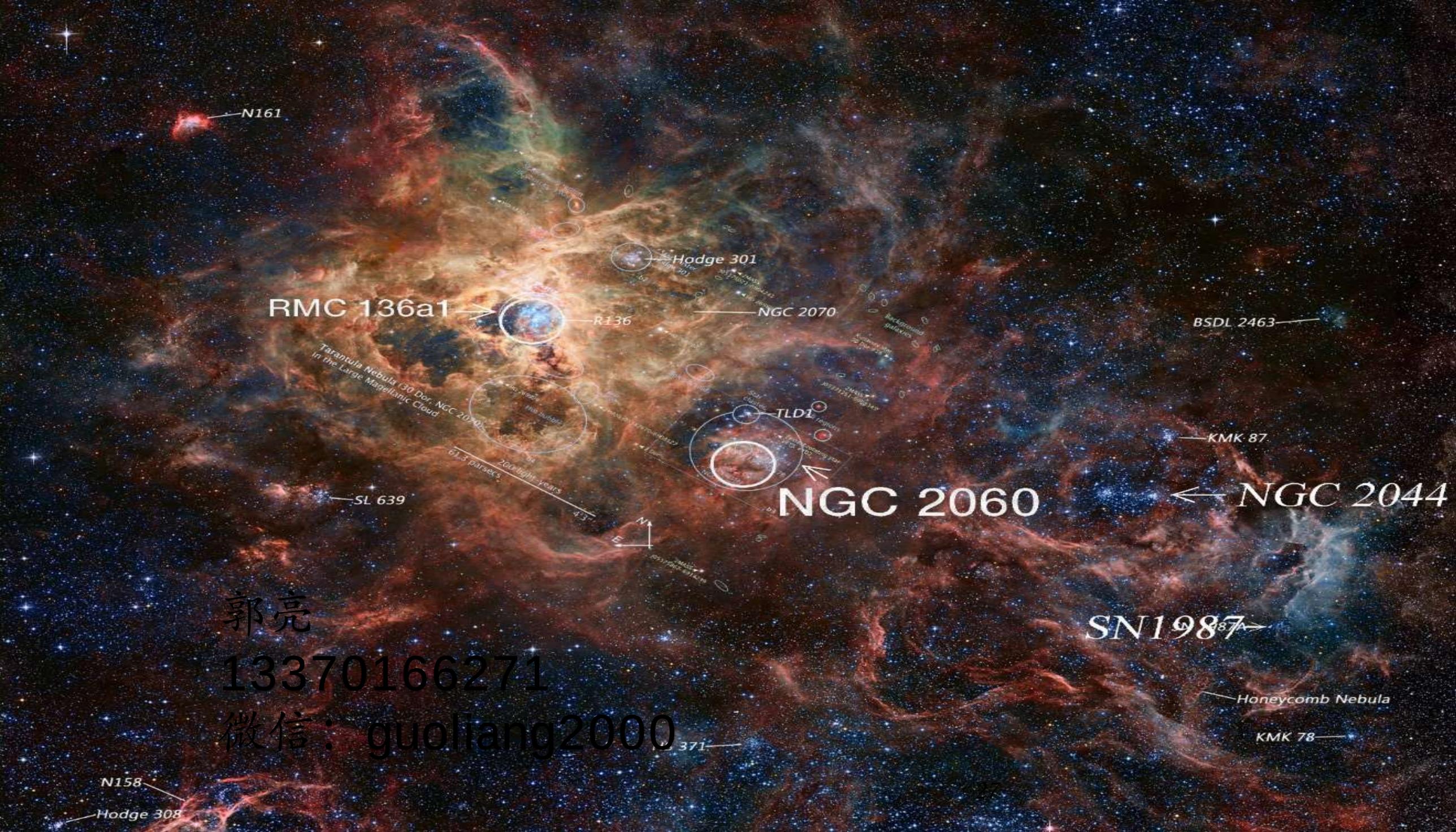

安全检测（渗透测试）
2016.5
系统配置
内网
Jenkins（7）
金佰仕Java反序列化（70）Port：8080、8180、9980
私有云
Jenkins
IIS命令执行
Redis（70）Port：6379
业务逻辑
代码编程类
安全意识
2015.8
应急响应
外网
2015.10
Web（外网）
系统配置
Jenkins

数据规律，指引价值


18
16
14
12
10
8
6
4
2
0
代码编程
系统配置
安全意识
业务逻辑
信息泄漏
2016.5
2015.12
2015.8
2015.7

数据时代的企业安全观，在管理、技术、流程之外

- “多”数据
- “重”资产
- “用”时间
- “立”信誉



谢谢聆听

THANK YOU FOR YOUR ATTENTION