# 数据时代的企业安全"观"



数字观星/郭亮(北极星)



安天网络安全冬训营第四期





## 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

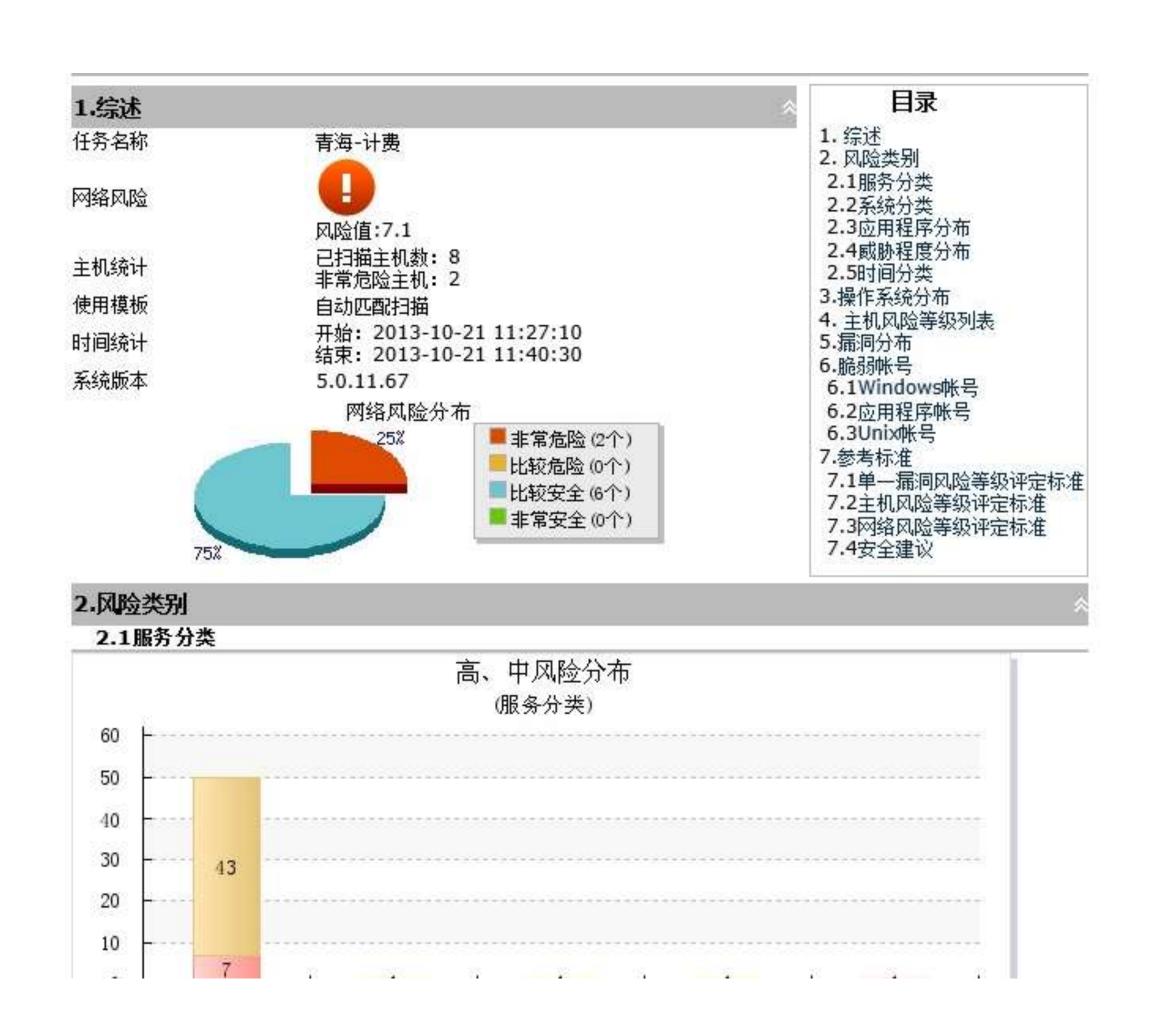
"不出事"与"能省钱"





## 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;





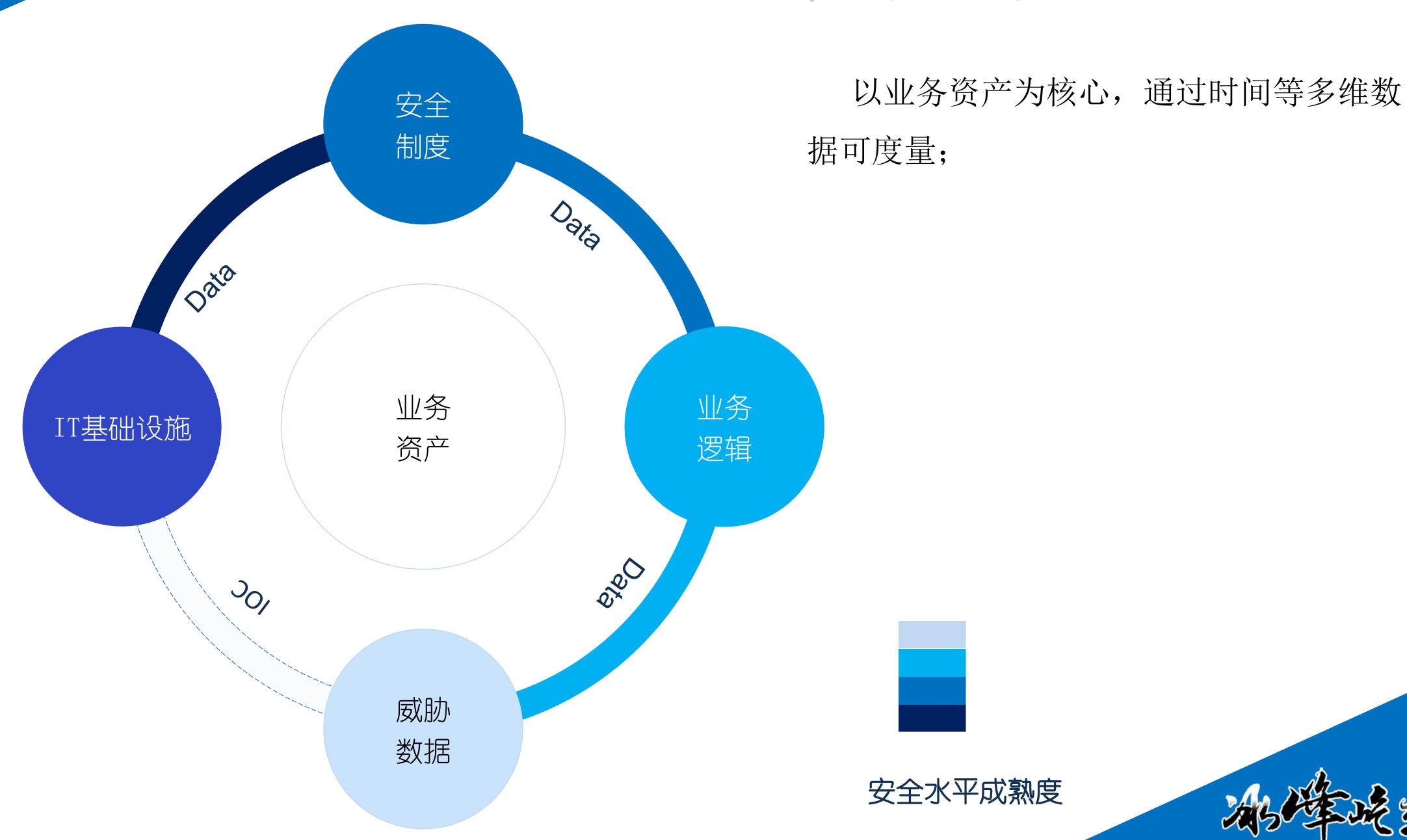
## DT时代的安全目标

"不出事(可度量)"与"别丢钱"

2000年2000年第四期

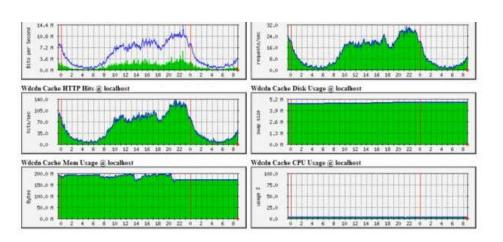


## 数据时代的安全观





### 10月31日 14:00分



### 出口拥塞

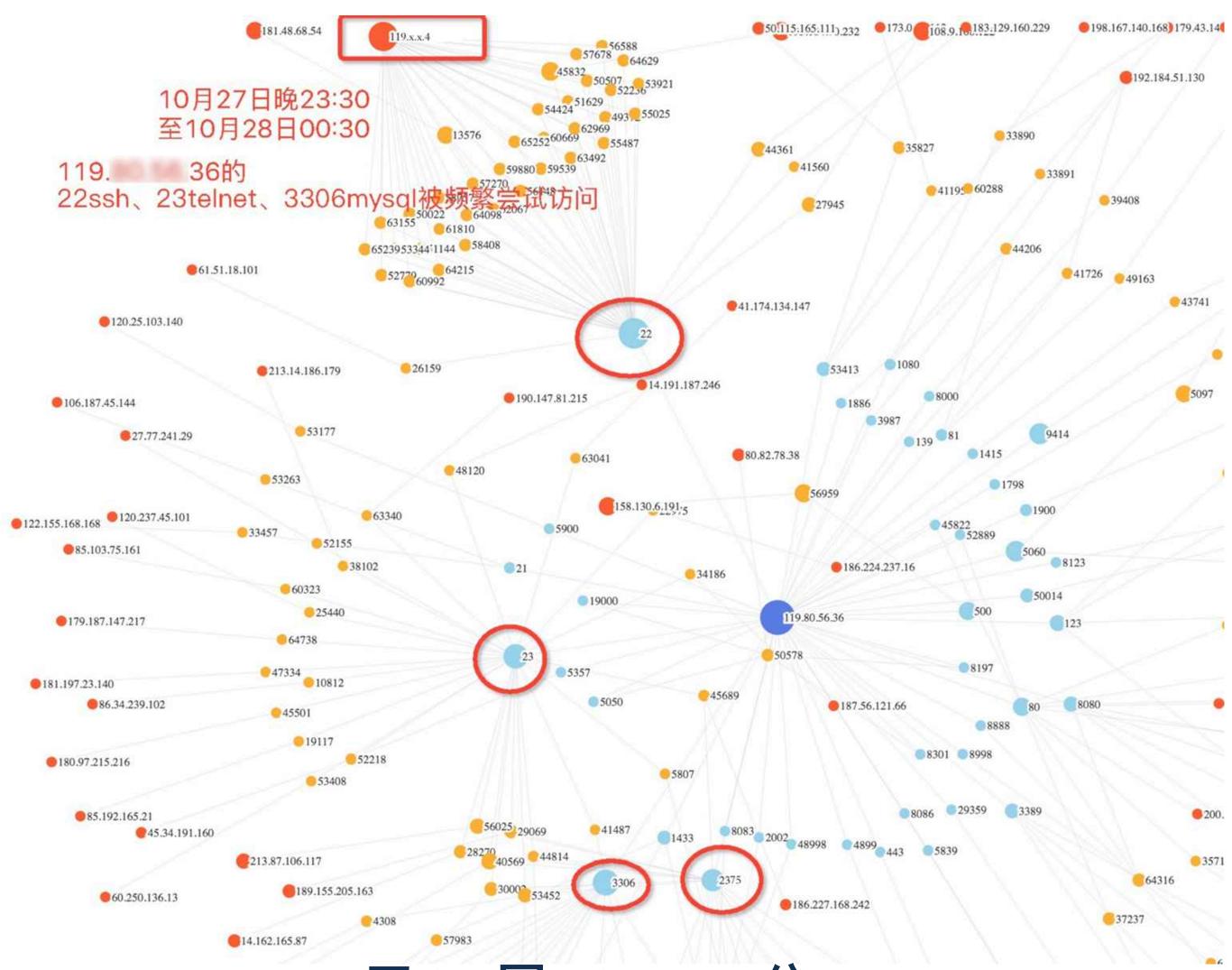
由内向外

119. x. x. 36





119. x. x. 4 119. x. x. 36



Port:

22

23

3306

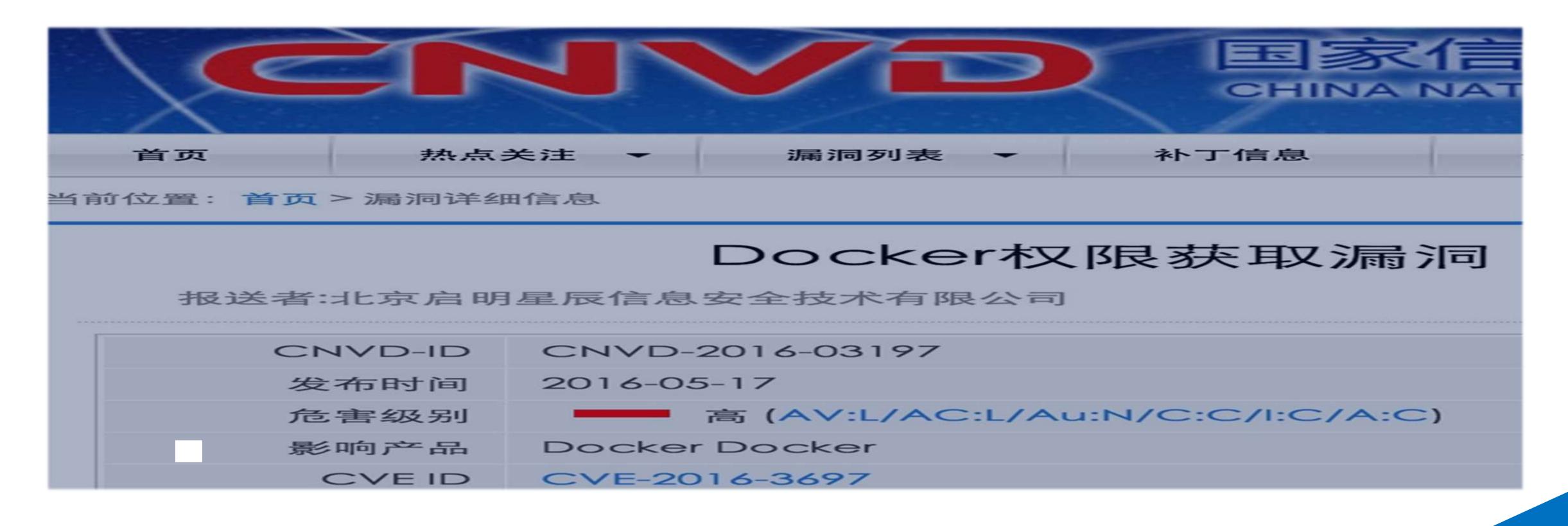
2375





### 10月27日 23:30分

2375: Docker



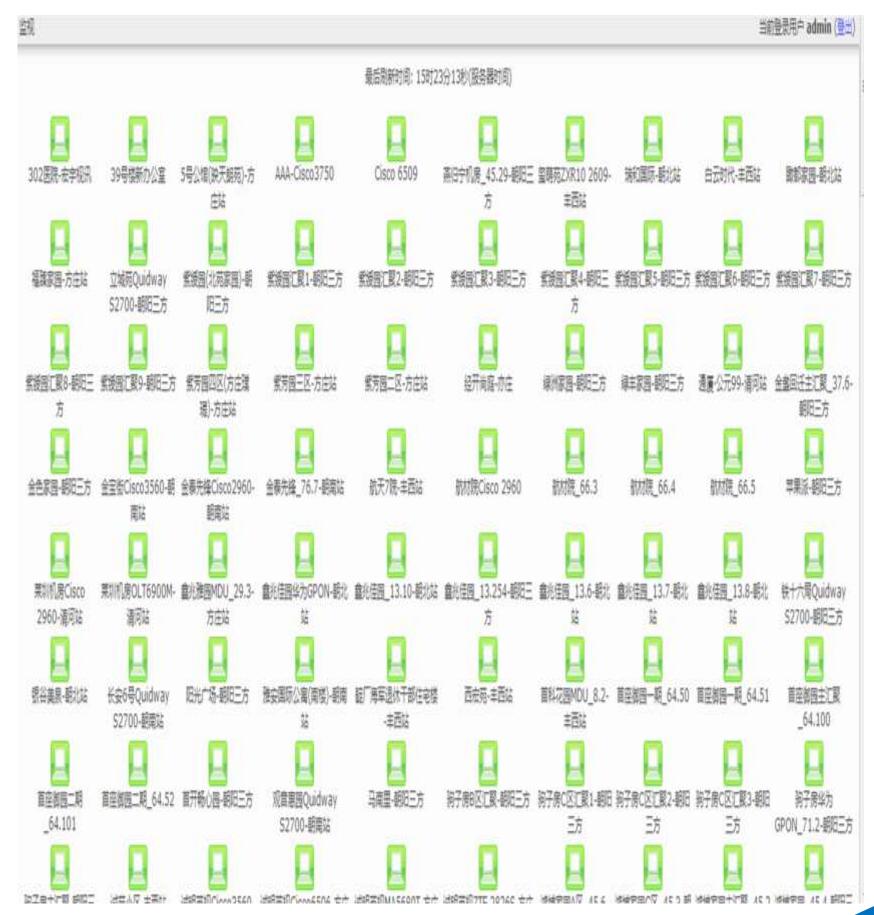
2016年5月17日 CVE-2016-3697





### IP: 119. x. x. X / 24-98台服务器







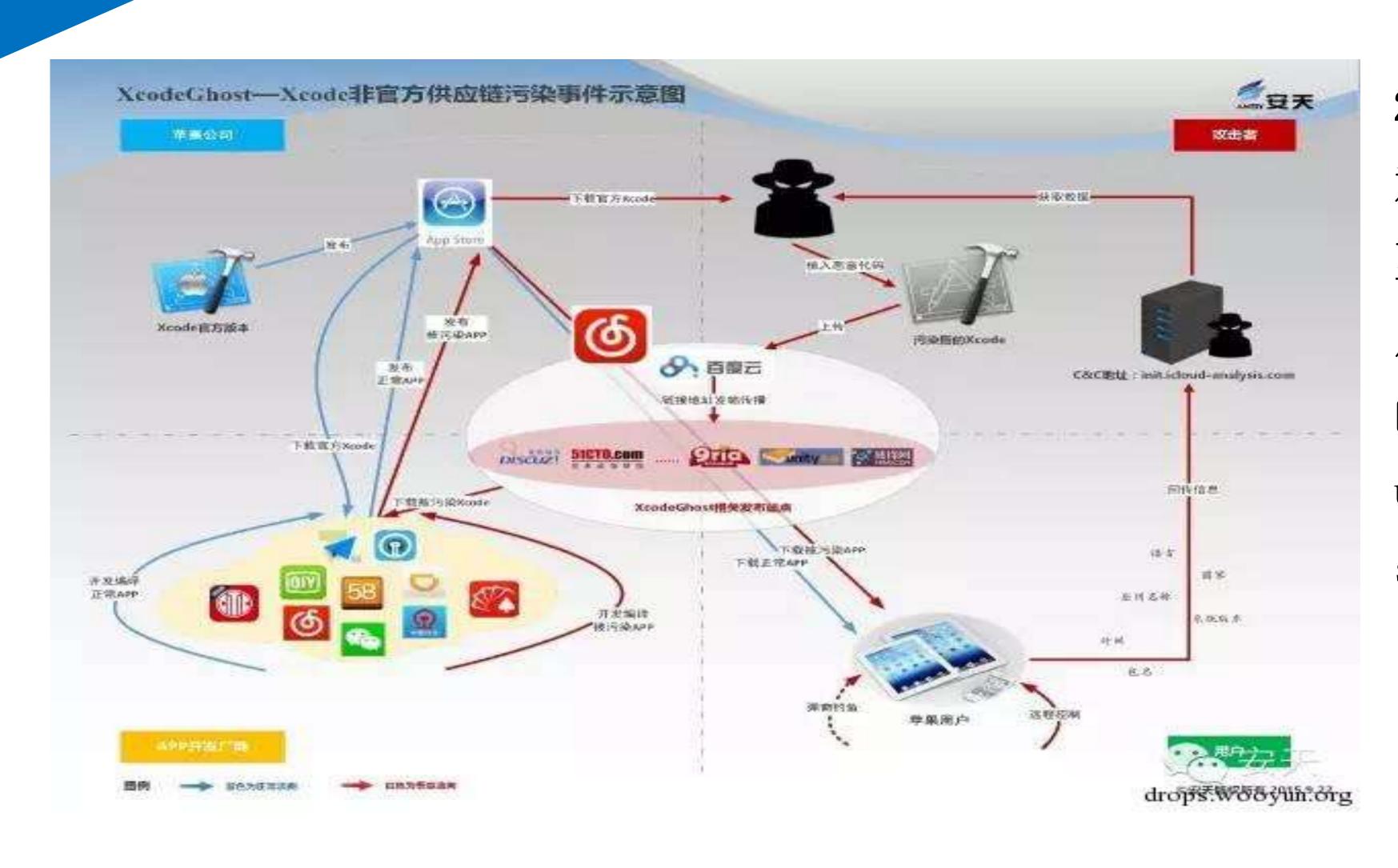


## 时间观

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.h tml	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.ce eger.com/foru m/read.php?ti d=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-43 267	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.51ct o.com/thread- 1149738-1.ht ml	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.h tml	coderfun 安元 rops.wooyun.or







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

6 5 1 7 1 3

染毒应用总数

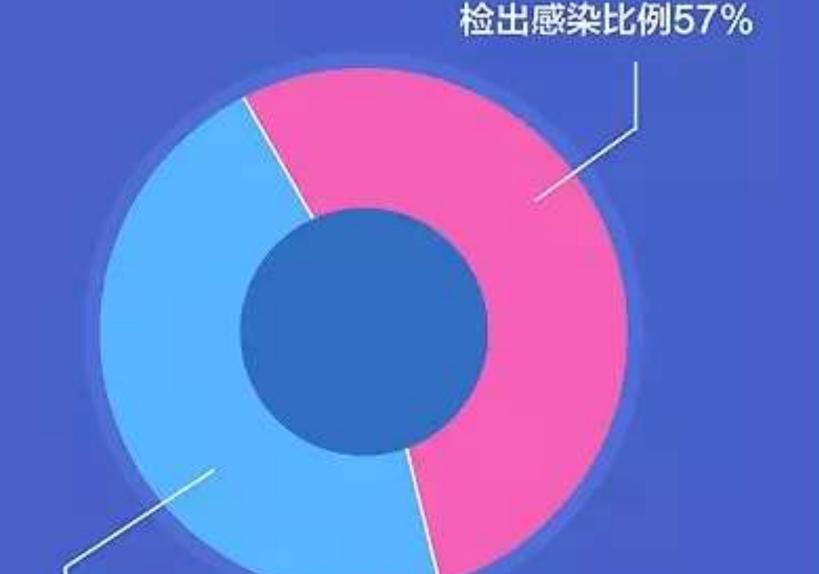
4 4 6 9

#### 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







## 可视分析观

可视分析给安全一个"观"点



## 数据规律-防火墙

ŀ	-	rais di mani in mano il 11111 201 201 201 destination il 1111 1 rais di mani in mano il 1111 1201 201 destination il 1111 1	Feet
۱	-	rais Sil consil de server 18.0.0.0.20.20.20.00 destination 18.0.0.7.0	200200000
-		rais SC count in come 11.1.1.1.1.28.28.28 decision 11.1.1.21	VerteXA2
_	-	rale 82 armili de arme 2.1.1.1 1.20.20.20 destinados 2.1.1.2 1	ORGANISM AND ADDRESS.
_	1	rado 201 servidi de senero 30.0.0.0 0.230.230.230 destinados 30.0.0.22 0	ONCERENCE
ŀ		nds ES entil in man (1.110.138.38.38 indication (1.11.2)	
١	-	rado 100 mendo de sensos 10, 0, 0, 0, 0 (1, 10), 100, 100 destinacións 10, 0, 0, 0, 0, 0 (1, 1), 10	DEPTAR
H	•	rain till ment til menn 11.1.1.1.1.21.21.21 deritarion 11.1.1.0.1	DC0001890340
		rado 100 mendo de marco 10.0.0.0 0.000.000.000 destinados 10.0.0.0 0	20022430
		rain 120 maril de marco (2.1.1.0 1.33.33.33) destinados (2.1.1.6 )	200424.00
L	-	rele III medi in man II. 1.1.1 1.30.30.30 indication II. 1.1.4 ()	20042430
ŀ	- 2	nds 12 mm2 in man (I.1.1.) 1.31.31.31 indication (I.1.1.4.)	200,0404
H	-	rado ED completo comerce (E. E. E. S. E. SEL SEL SEL SEL CONTRACTOR (E. E. E. E. E. S.	
r		puls 122 march de marco 12.0.0.0 0.231.231.231 destinación 12.0.0.00 0	0.0000000000000000000000000000000000000
		rate 10 march to march 10.0 to 0.0 to	SECURE OF SECURE
		refer \$2" words for many \$2,0,0,0 0,300,300,300 destination \$2,0,0,0 0	DOMESTIC STREET, ST.
ŀ	-	rais \$2 area in many \$1.1.1.0 1.30.30.30 desiration \$1.1.1.0 0	
ŀ	-	rado 100 mendo de amero 10.0.0.0 0.000.000 destinados 10.0.0.00 0 rado 100 mendo de amero 10.0.0.0 0.000.000.000 destinados 10.0.0.00 0	_
r		min 121 mm/2 in secure 10.0.0.0 0.200.200.200 designation 10.0.0.000	72-6-4-00 med ex
	-	rado 122 mendi de marco 18, 0, 0, 0 (18, 200, 200, 200 destinación 18, 0, 0, 0 (18, 0)	MESSAS
	_	#BEADS#EELS	
ŀ	-	rale III armid III armin II. L. II. I destination II. L. II. I destination and in IIII	
۱	-	rais SC const TD comes 10.0 to 30 destination 10.0.0 to 0 destination on 5000 rais SC const TD comes 10.0 to 30 destination 10.0.0 to 0 destination on 5000	<del></del>
۲	-	rate SC error CP error (E.C.) (C.C.) is defination (E.C.) of Contractor-rank or SSS rate SC error CP error (E.C.) (C.C.) is defination (E.C.) of Contractor-rank or SSC	+
٦	•	rain 194 arrait 177 array 18.1.18.19 ( destination 18.1.1.4) ( destination and as 20.	
		refer this expect TO proces (0.0, 0.0) is developation (0.0, 0.0) is developation-rand on (0.0)	
L	-	rale 100 ments 127 ments 10.0.10.10 i destination 10.0.0 ii destination and in 1000	
H	-	rade SE constit DP comes 10.0.10.10 0 destination 10.0.1.10 0 destination and as 6000 color of the constitution and as 6000 color of the constitution and as 6000 color of the	
۲		ndo 30 ente 30 ente 3.1.1.3.3 decidades 3.1.1.4 decidades 4.1.5 decidades	+
ľ		nde 20 mars 27 mars 20.0 2 d destination 20.0 2 d destination 20.0 2 d	
Ĺ		nde 100 marie 25 marie 20.0 20 destantion 20.0 2 destantion and as 20	
ŀ	-	nde SC mark III mans 3.1.35.1.1.1.35 knihodia 3.1.1.4 i knihodiavani m.Z	
ŀ	-	rado (80 mend) (32 menes (8.1 M), 0.0.0.0.00 destination (8.0.0.0) destination-ment es (2) rado (84 mend) (32 menes (8.1 M), 0.0.0.0.00 destination (8.0.0.0) destination-ment es (2)	+
ŀ		ndo 30 entil 17 ente 3 1 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	+
ľ	-	rele M. march 17 march 18.1 (20.0 1.1.1.2) derféention (2.1.1.4) à derféention-mart en 20	
Į		mile (60 mmile 12) mmm (0.1.10), 0.0.0.101 (methodox (0.0.0.0) (methodox-mat in 2)	
Ļ		*50AD02A5	
ŀ		rain 30 march 170 march 18.0.10.0 Continuous 18.0.10 Continuous 18.0.1	
t	-	nic III and IV new 1.1.1.1 (defeate 1.1.1.0) integrate a 100	
ľ		rate SC words SD grove \$1.0 to 3 deptember \$1.0.0 0 deptember on \$10.	
I	23	rain 17 area 17 area 2.1.2.2 ( defende 2.1.2.6 ) defendered a 22	
L	-	nde Di sendi IV sense II. II. II i destantas II. I. II i destantas varia (	
ŀ		rain III sensi III sense II. I. II. II i deritarian II. I. II i deritarianen iz 500 rain III sensi III sense II. I. II. II i deritarian II. I. II i deritarian iz 500	
H	-	rain III sensi III sense II. I. II. II deritarian II. I. II deritarian III. III deritarian est e 1000 rain III sensi III sense II. I. II. II deritarian II. I. II deritarian III. III deritarian III. III deritarian	
r		print ST count ES press (0.0 to 0 destination (0.0.0 to destination out to 000)	
I		rely \$15 march \$25 march \$1,0,0,0 0 destination \$1,0,0 % destination and as \$10.	
ŀ	2	nie III annii IV anna II.I.I.I i definite II.I.I ii definiterant a II	
ŀ		raio III, centil III cente III 1 III 0 1.0.1.23 destination II.0.1.9 destination and com- raio III centil III cente III.1.10.0.1.0.1.23 destination II.0.1.9 destination and co	-
r	- 13	rain III mentil III mener III i III. I I I I I I I I I I I I I I	
I		ede Sti erecti IV erece St. 1 30.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	
Ļ	_	rele III med IV men 2.1.32.01.1.1.33 deddedde 2.1.1.9 0 deddeddwynd e 2	
ŀ	-	eds III and IV near II   II   I   I   I   I   I   I   I	
r	235	ndo 60 maril 37 maril 3.0.0.0.0.30.30.30 deplaction 3.0.0.31 deplactment in 370	
	200	rale Mil mende TV menne 18.0.0.0.000.000.000 deplication 18.0.0.000 deplication and no 1973	
L	- 22	rain 60 march 50 march 10.0.0.0.00.00.00.00 deployed to 10.0.0.00 deployed on 100	
Ĺ	-	nde SD vendi TV vene (E. 1.1.1.1.38.38.38 deddedde (E. 1.1.3.1 deddedderend er TS)	
ŀ	-	rais (6) const TD comes (0.0.0.0.100.000.000 depleation (0.0.0.0.000) depleation and as (60) rais (60) const TD comes (0.0.0.0.000.000.000 depleation (0.0.0.000) depleation and as (60)	
۲		rain 60 area 17 area (0.0.0.0.00.00.00.00 protection (0.0.0.0.0.00 protection of the	+
ľ		nde SC march 37 march 3.1.1.1.1.33.33.33 depletion 3.1.1.3.1 depletionment or SSS	
Ĺ	_	rain 80 maril 37 marin 10.0.0.0 0.30.30.30 deploation 10.0.0.3 0 deploation and a 466	
ŀ	-	nde 60 mail 17 mars 11.1.1.1.131.31.31 destaction 11.1.1.3.1 destaction at 11.1.3.1 destact	
H	-	rado 600 cerció 727 cerces 10.0.0.0.0.000.200.200 destinación 10.0.0.200 destinación cerció en 1000 cedo 600 cerció 727 cerces 10.0.000.000.200 destinación 10.0.0.200 destinación cerción 10.000.200 destinación	+
r	- 10	rado (CC merci) (CC marco (C. ), (C. ) (C. ), (C. )	
ľ	100	rele 82 meet 27 maar 18.1.7%   8.1.1.38 deritaation 18.1.1.38   deritaation and as 223	
Ĺ	410	AGREDALIS	
ŀ	- 100	erio dei serati CP anno 18.0.0.0.000.000.000 destination 18.0.0.00 destination ent es 180 erio 600 anno 180 anno 18.0.0.0.000.000.000 destination 18.0.0.00 destination ent es 180	<del></del>
r		nds 60 mail 27 mail 2.1.1.1.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2	+
ľ		71110	
Ĺ	- 8	rain 60 menti de senor 3.11 6.0 destinados 3.110 1.113	
ŀ	- 10	nds 80 and in some 2.110 I indication 2.11111123	
١	-111	rais SC count in some \$1.1.1.20 I desiration \$1.1.1.1.1.1.20 EASTERNATION	
۴		nds (00 erect) to seem 10.1.00.0 0.0.0.00 destourting 10.0.1.00 0	
١		min Til menti de mene (I. 1.00.) I. 1.1.20 destantion (I. 1.1.20 )	
Ĺ	-	rado (10 ment) de senso (0.1 00. C ) destandos (0.1 1 00. C	
ŀ	-	ede TO med in some \$1.100.00 (indication \$1.11.00)	<del></del>
ŀ	-	rate (D) contil de como (E. L. M. M. ) destinados (E. E. L. M. ) este (D) contil de como (E. L. M. C. ) destinados (E. E. L. M. )	_
۲	-	ndo 10 mail de mare 2.1.20.0 i destantas 2.1.20.0	+
ľ	•	rate III mentil de maner II. L. III. III i destination II. L. L. C. C.	
		9244	
F		nde 110 maril de marie 30, 30, 51, 51, 51, 521 destinados 33, 51, 51, 51, 521	
ŀ		nds 10 anni de mans 30 30 10 11 1 11 20 destinada 20 11 1 1 1 1 20	+
ŀ		rado (10 centr) de centre (10 100.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	+
۱		7-0	
۴		rds 20 and in our 2.1.1.1.2.20.20.20 detaction 2.1.1.20 I defeationed in 1980	
H	- 1	refer this entail for severe 10.0.0.0 t.20.20.20 destination 10.0.0.12 Continutionment of 2000	

14	10 10.0.232.2		- 15 / 13	00	
15	11 10.0.252.3		站点	80	只
16	12 10.0.252.4	*************************************	站点	80	<u>只</u> 只 只
17	13 10.0.252.5		站点	80	只
18 単个IP	14 10.0.252.6	1服务器	站点	80	Я
19	15 10.0.252.10		抽点	80	見

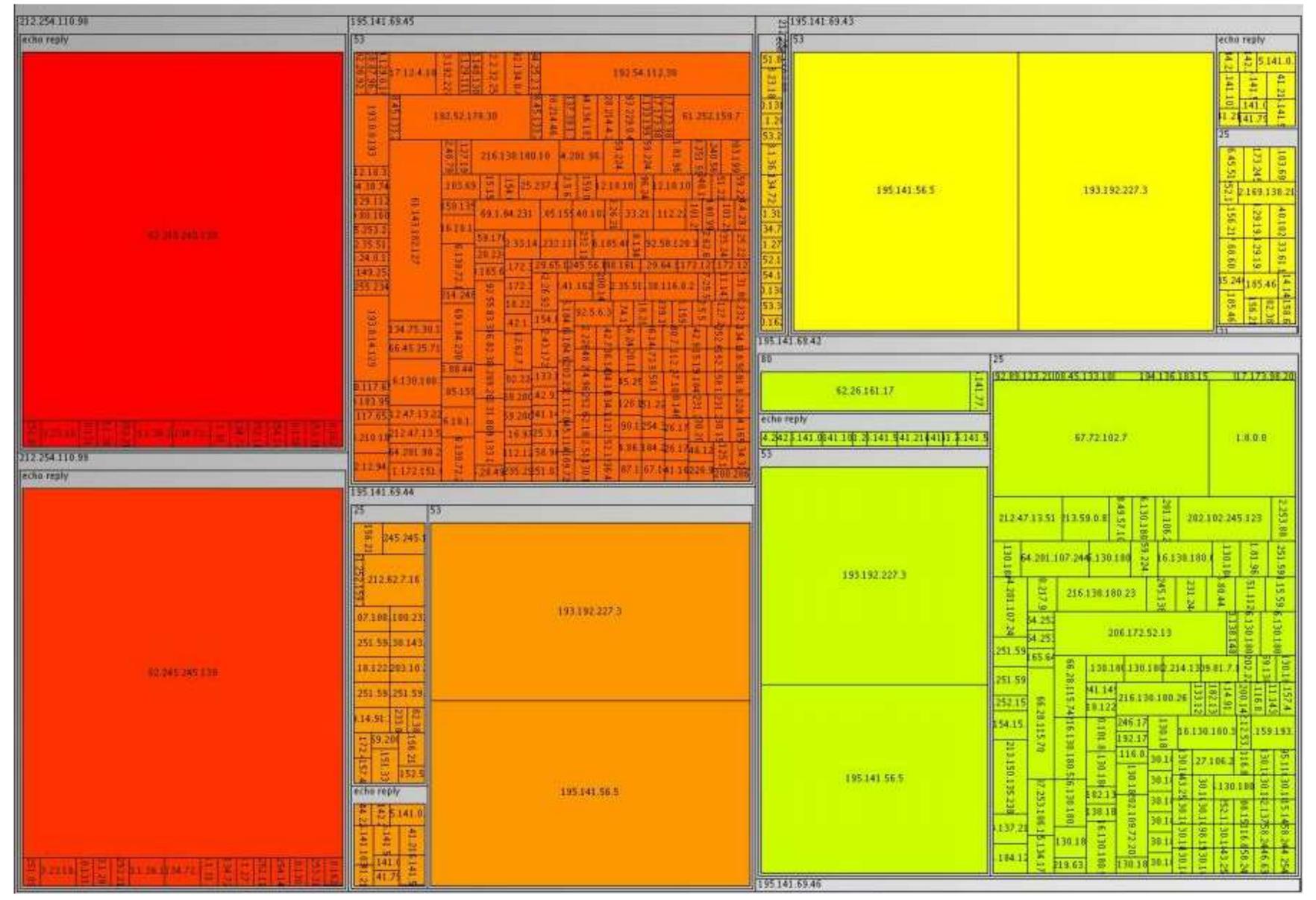
1		防火墙访问控制规则统计表							
2	IP类型	序号	IPv4地址	是否存 左	操作系统	用途	开启的服务	★访问限制	*备注
3	<b>(9)</b> 1	1	1.1.1.1	æ	Centos 6.0	web服务器	http:8080 https	只允许集团内网使用	
4	例2	/	2.2.2.0/24	是	1	xx部	/	只允许2. 2. 2. 86访问互联网	
5		1	10.0.2.1		windows	DHCP服务器		允许10.0.2.1到any目的端口53(tcp/udp)	
6		2	10.0.2.5		windows	杀毒补丁		禁止10.0.2.5访问10.24.0.0/14 允许10.0.2.5访问任意目的	進访问道
7		3	10.0.2.11		windows	OA泵统备份服务器		允许10.0.2.11访问任意目的	進访何進
8		4	10.0.2.234						
9		5	10.0.2.235			临时访问公网使用			
10		6	10.0.2.236						
10 11		7	10.0.5.200			信息情报系统服务器访问公网出口地址			
12		8	10.0.250.250						
13		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端口進访问道
14		10	10.0.252.2			站点	80		
15		11	10.0.252.3		隶属	站点	80	只允许80粥口访问	
16		12	10.0.252.4		表示 10.0.252.	站点	80	只允许80端口访问	
17	<b>*</b> *	13	10.0.252.5		1服务器	站点	80	只允许80端口访问	
18	単个IP	14	10.0.252.6		「月以づかるみ	站点	80	只允许806端口访问	
19		15	10.0.252.10		]	站点	80	只允许80粥口访问/只允许内网3389粥口访问、TELNET、FTP、开启22粥口	

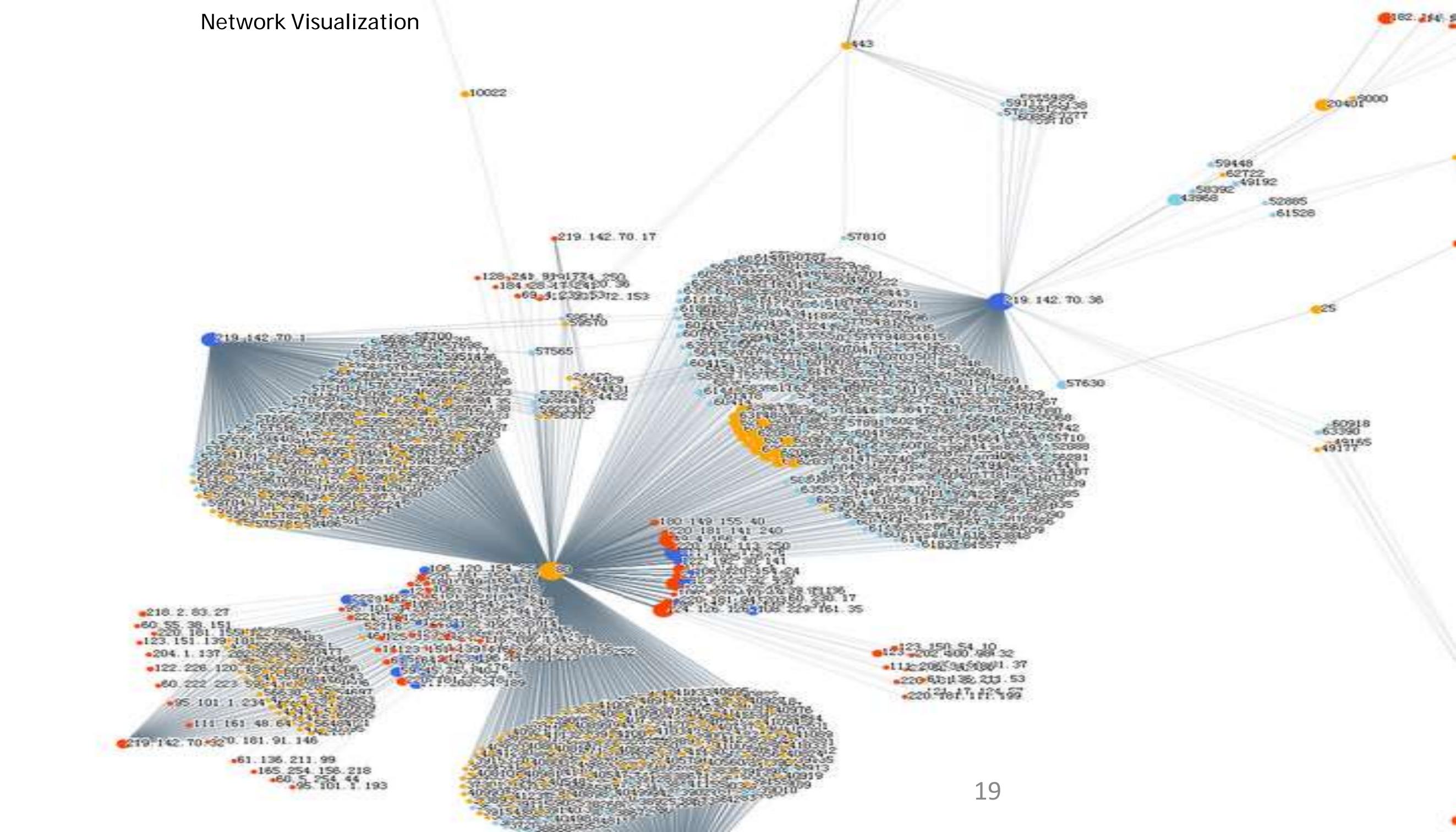


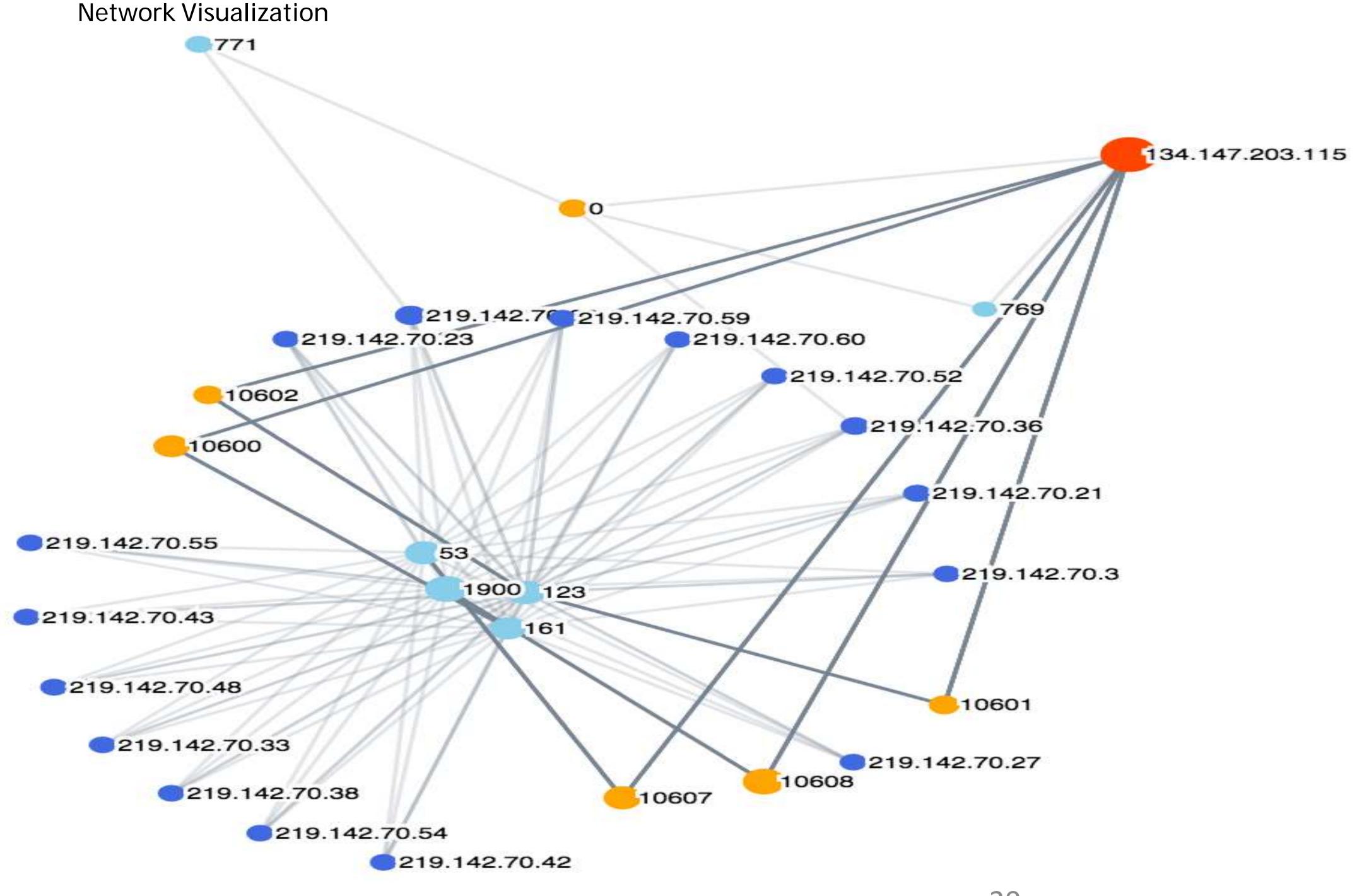
缩放比例 X 10%



### 防火墙数据体现的业务规律



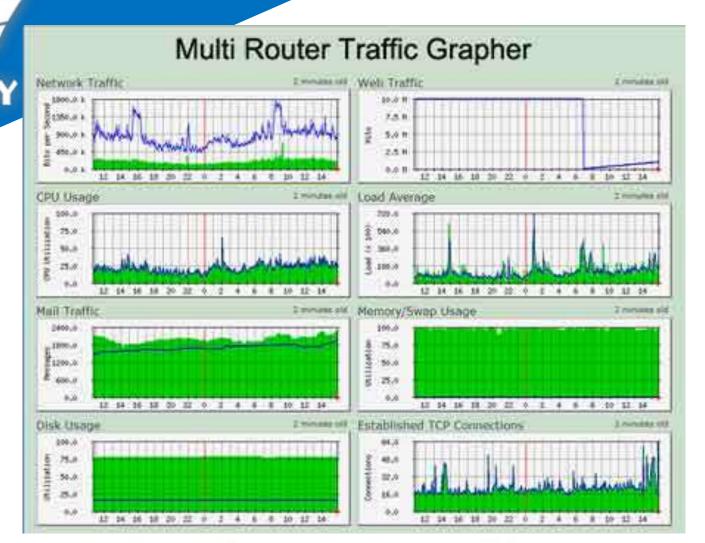


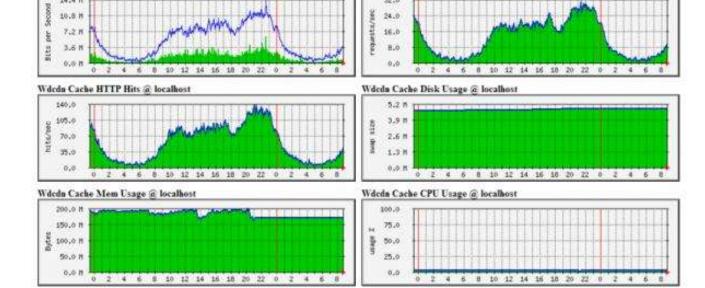


#### Network Visualization



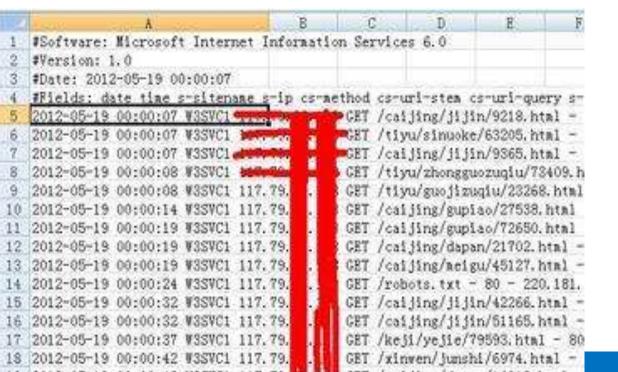


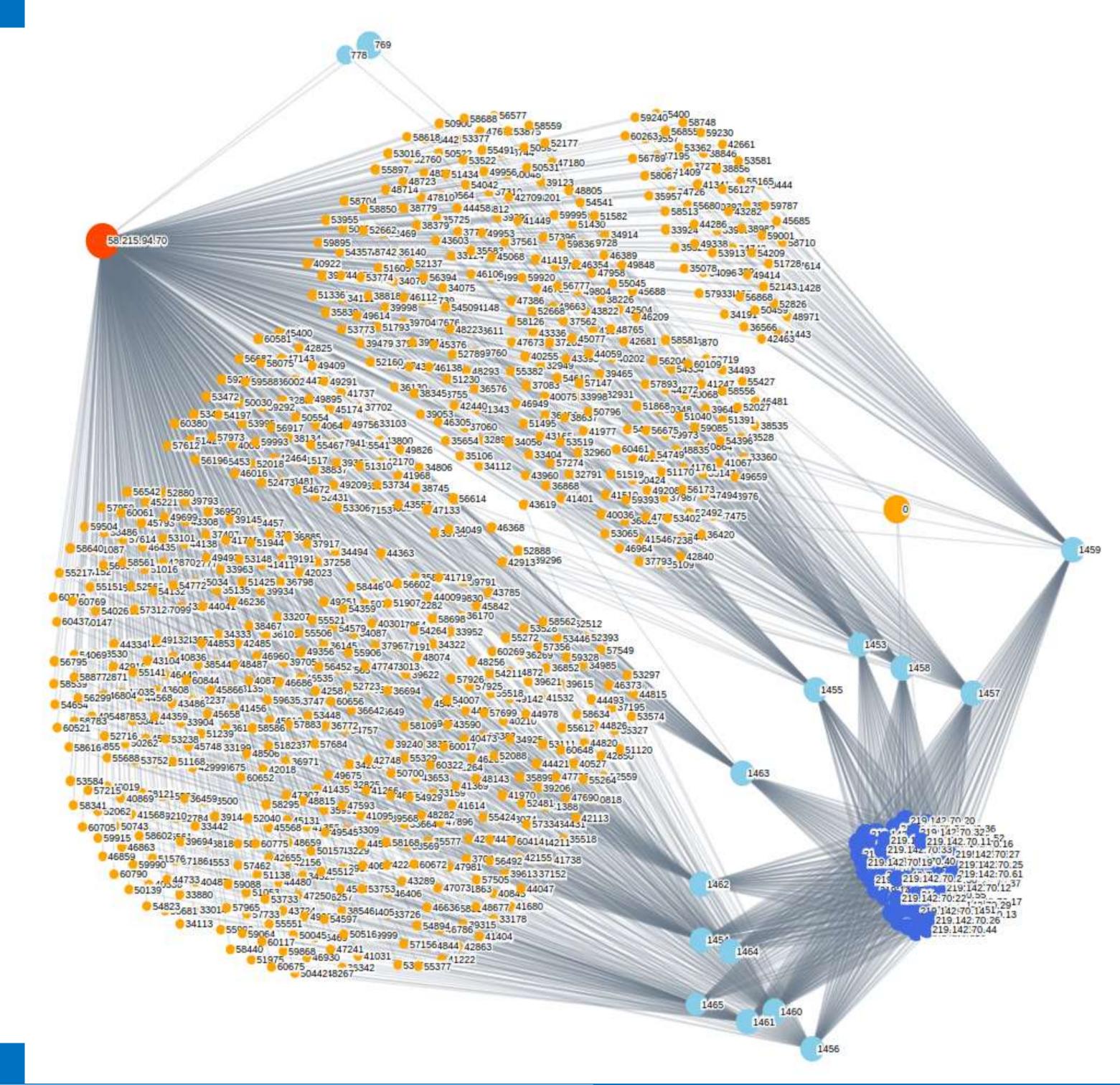




Wdcda Cache Server Requests @ localhost











## 数据规律观

多维度的数据应用,发现规律



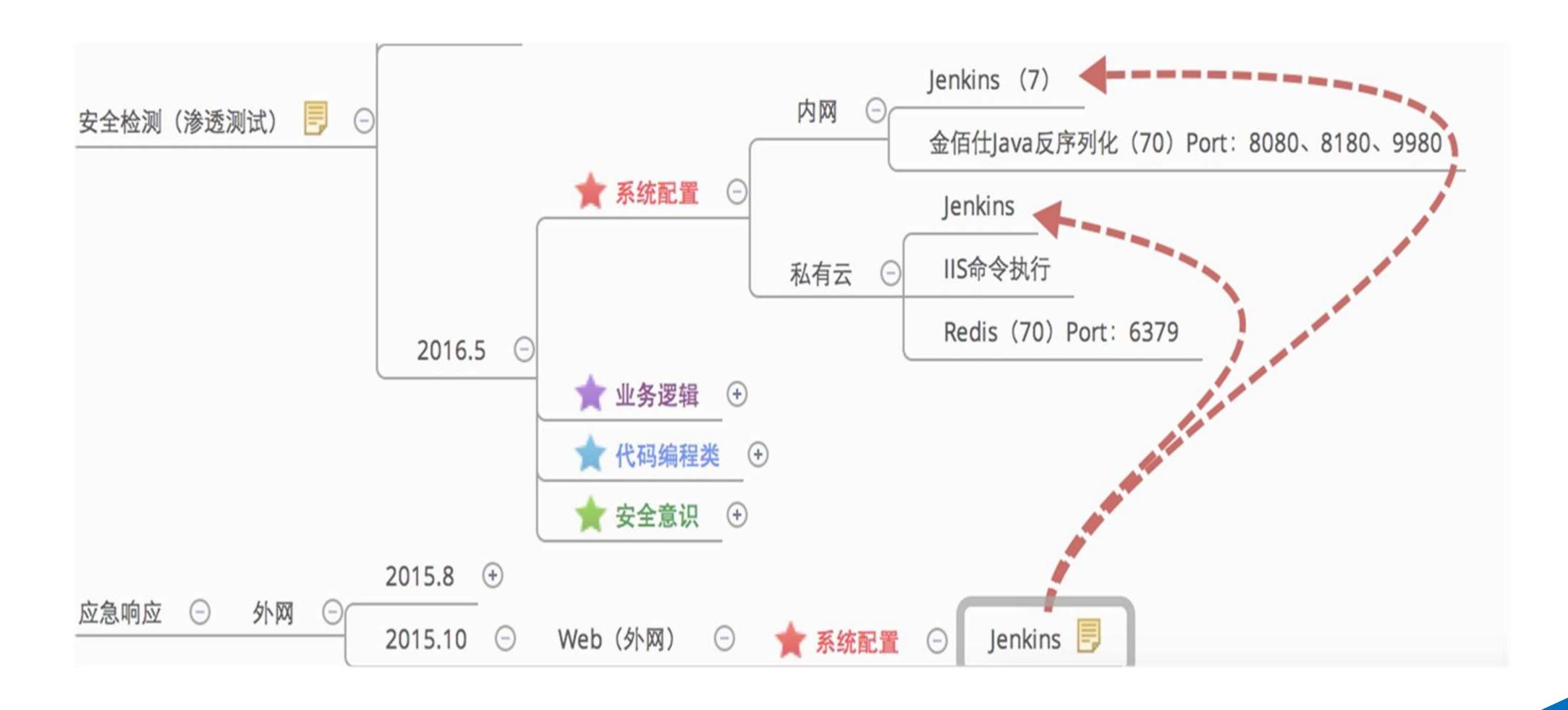
安全数据在企 业落地的价值 三足:

"责任"





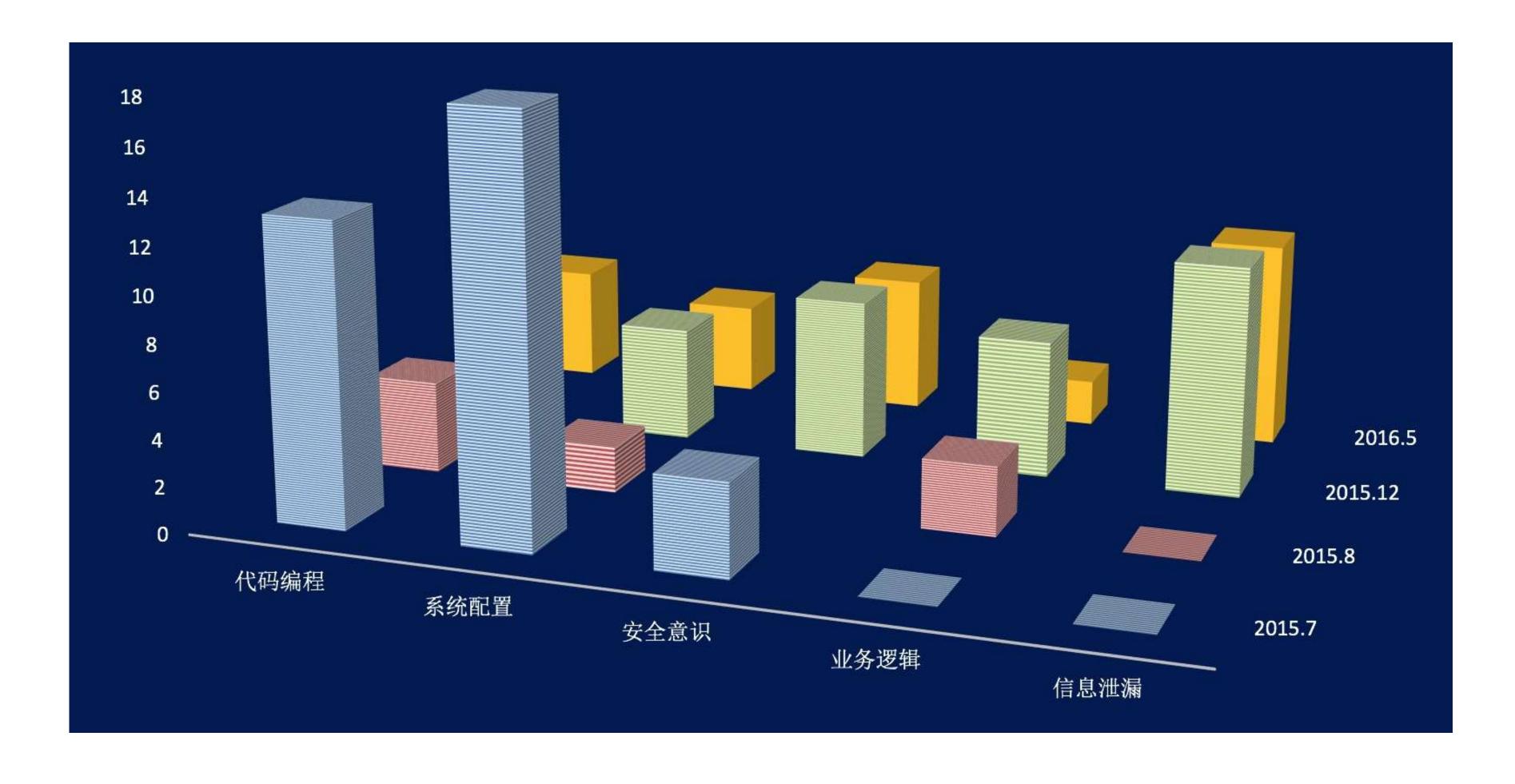
### 时间发现的"责任"







## 数据规律,指引价值







## 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



-N161

RMC 136a1

Hødge 301

-NGC 2070

BSDL 2463-

-KMK 87

€ TLD1

NGC 2060

<- NGC 2044

13370166271 拨信:Guolance

N158

Hodge 308

SN1987-

Honeycomb Nebula

KMK 78-



# 朗朗野門

THANK YOU FOR YOUR ATTENTION

