SACC 2015中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2015
互联网+ 重塑IT架构

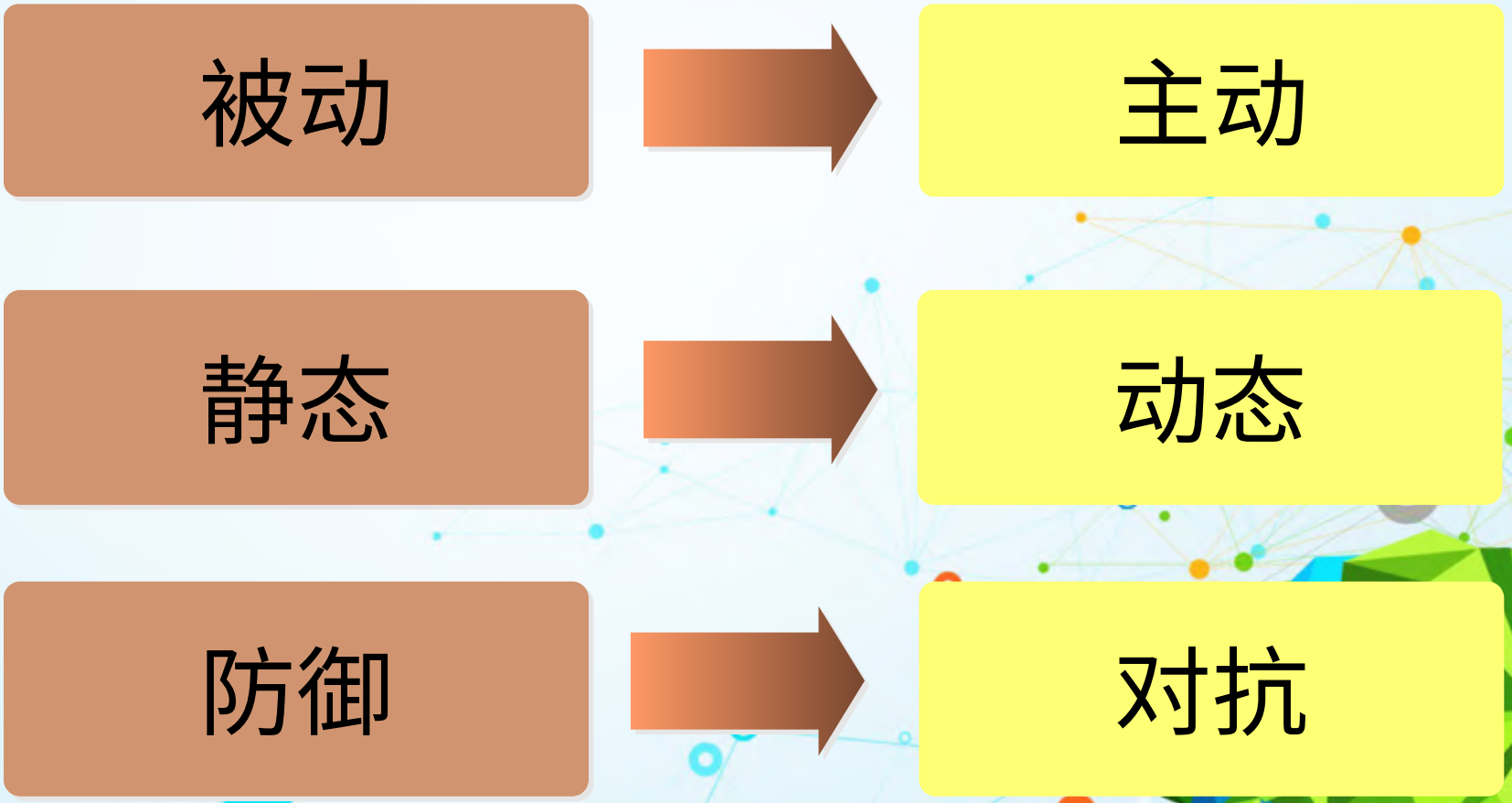
云时代下的安全实践

网康科技 周永刚


前所未见的
「地下」惊奇世界。
盗墓筆記
THE LOST TOMB


天脉之书
KING'S TREASURY

两种不同的防盗思维



战火纷飞的第五空间

索尼被黑事件

TARGET

Target 超过 4,000 万信用卡和借记卡帐户以及 7,000 万客户的信息被窃取

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

美国联邦人事 2150 万份信息被窃取

传统安全方法论： PPDR 模型

?

信息系统蕴含的风险和威胁可以充分评估和认识?

信息系统永远存在未知的风险和威胁，无法发现?

是一种静态的、被动的、防御性的战略思维

战略思维需要转变

没有攻不破的系统

一万次里有一次成功了，攻击者就成功了。

一万次里有一次失败了，防御者就失败了。

从“防御”为主
向“防御＋检测”并重

知己知彼，百战不殆

态势感知和安全预警

新一代安全方法论： PDFP 模型

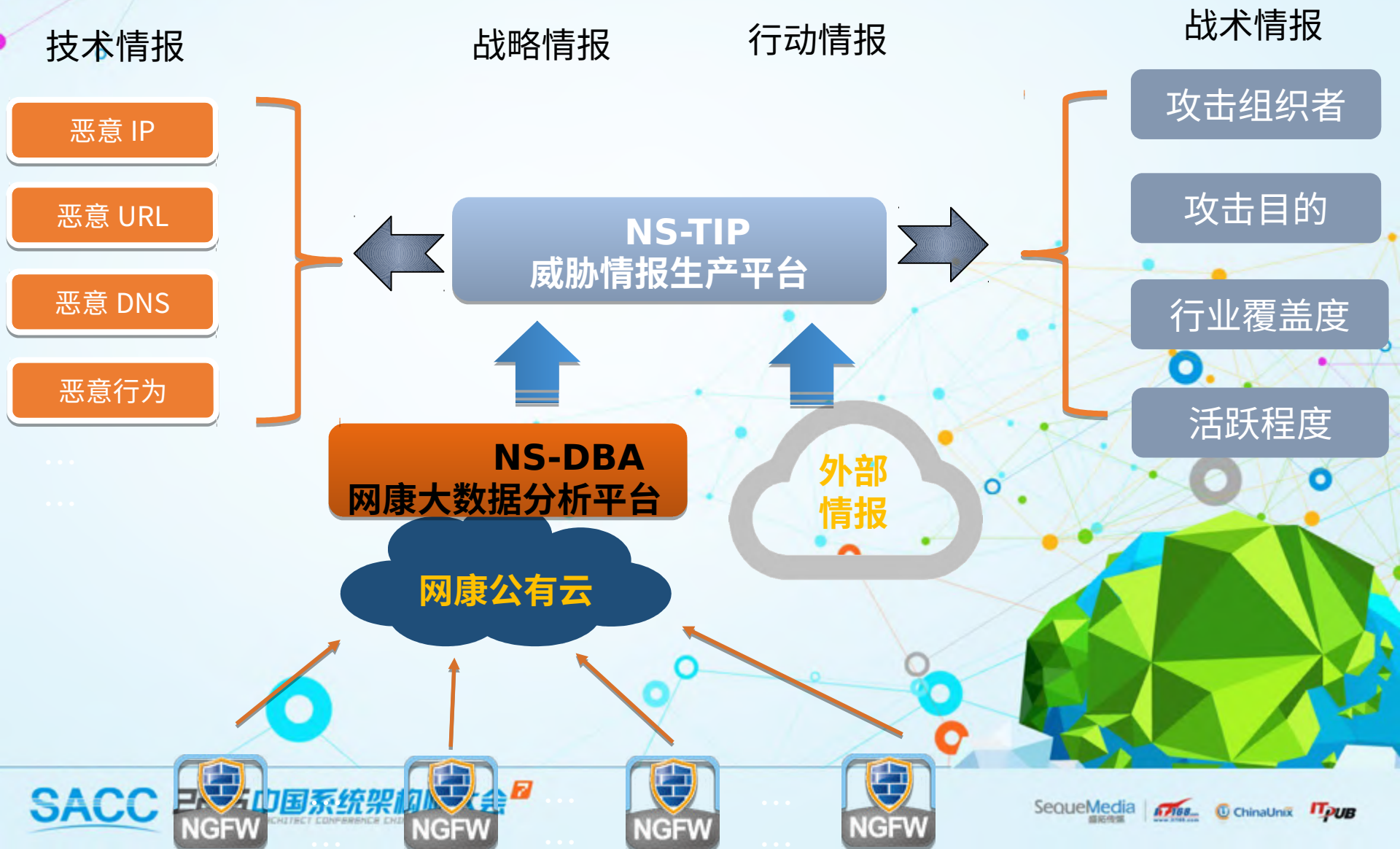
1. 未知威胁永远存在，系统已失陷
2. 借助威胁情报和大数据分析技术构建预测能力
3. 安全的起点从检测开始，通过安全情境和异常行为分析发现失陷点
4. 通过取证手段溯源攻击过程
5. 确定对抗措施，提升防御能力

是一种动态的、主动的、对抗性的战略思维

异常行为分析

“风过留痕，雁过留声”，行为终究无法隐藏

威胁情报生产


技术情报
战略情报
行动情报
战术情报
恶意 IP
恶意 URL
恶意 DNS
恶意行为
NS-TIP
威胁情报生产平台
攻击组织者
攻击目的
行业覆盖度
活跃程度
NS-DBA
网康大数据分析平台
外部
情报
网康公有云
NGFW
NGFW
NGFW
NGFW

网康基于云技术的安全实践

慧眼云
WiseEye

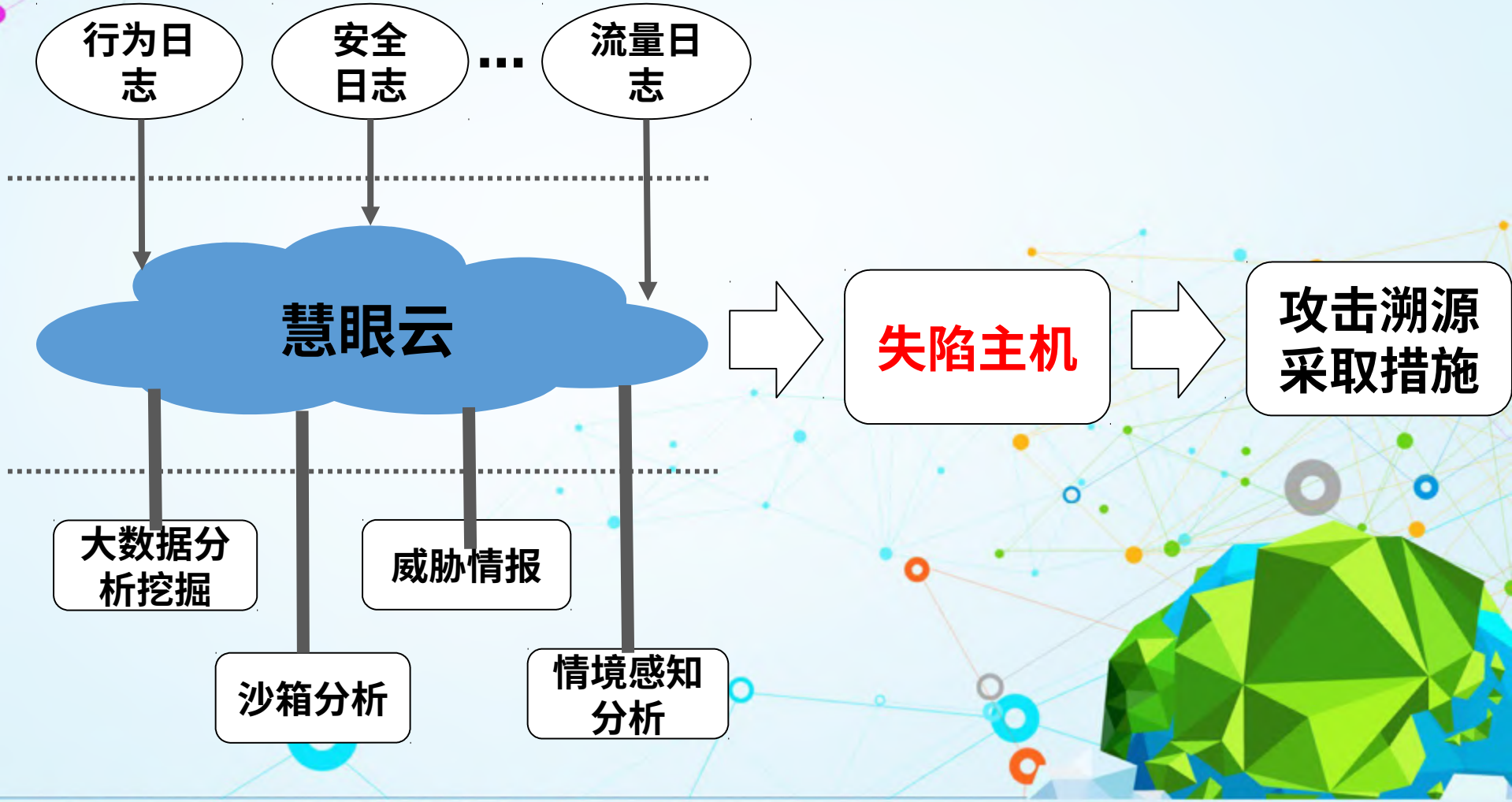
下一代网络威胁感知系统

针对高级威胁，

利用威胁情报和异常行为分析技术，

失陷主机检测与取证方案

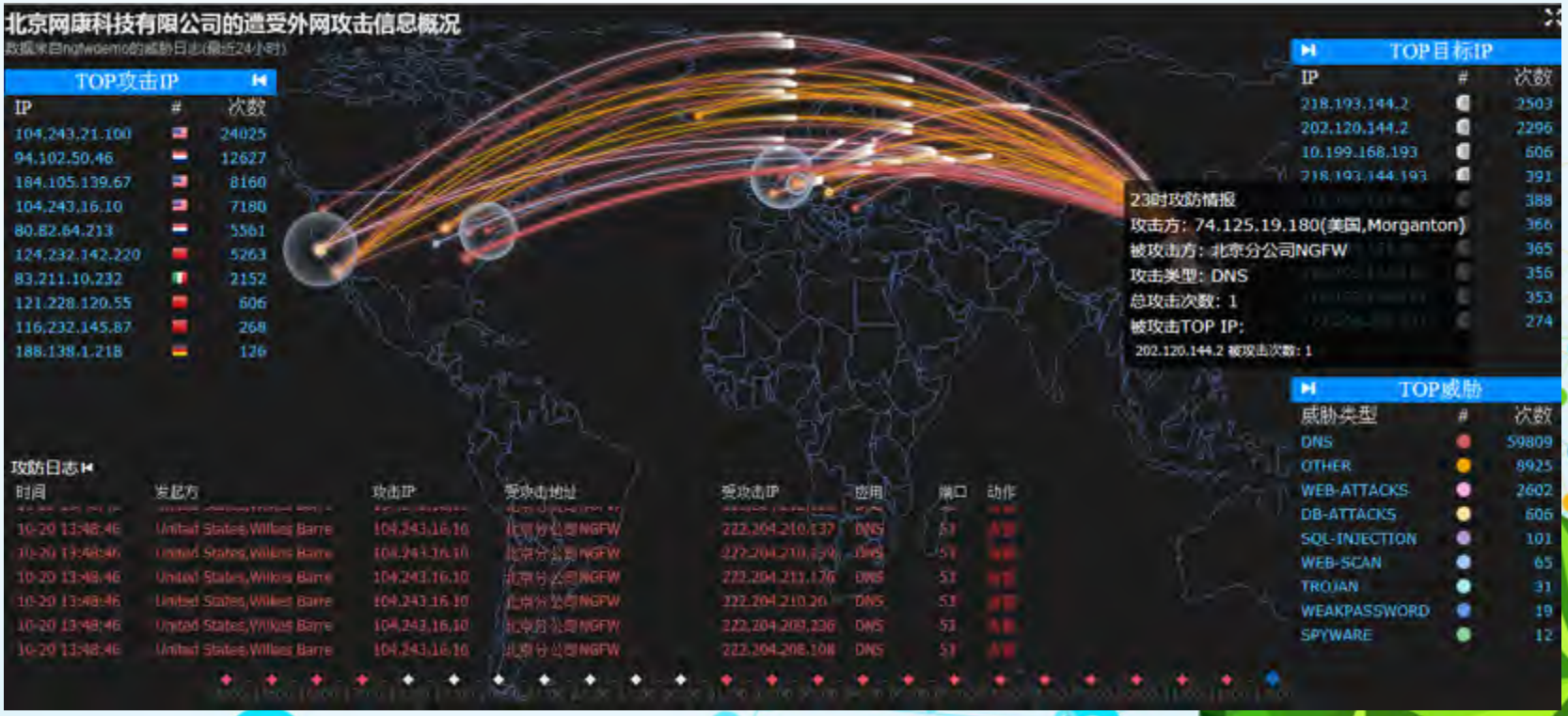
慧眼云组成



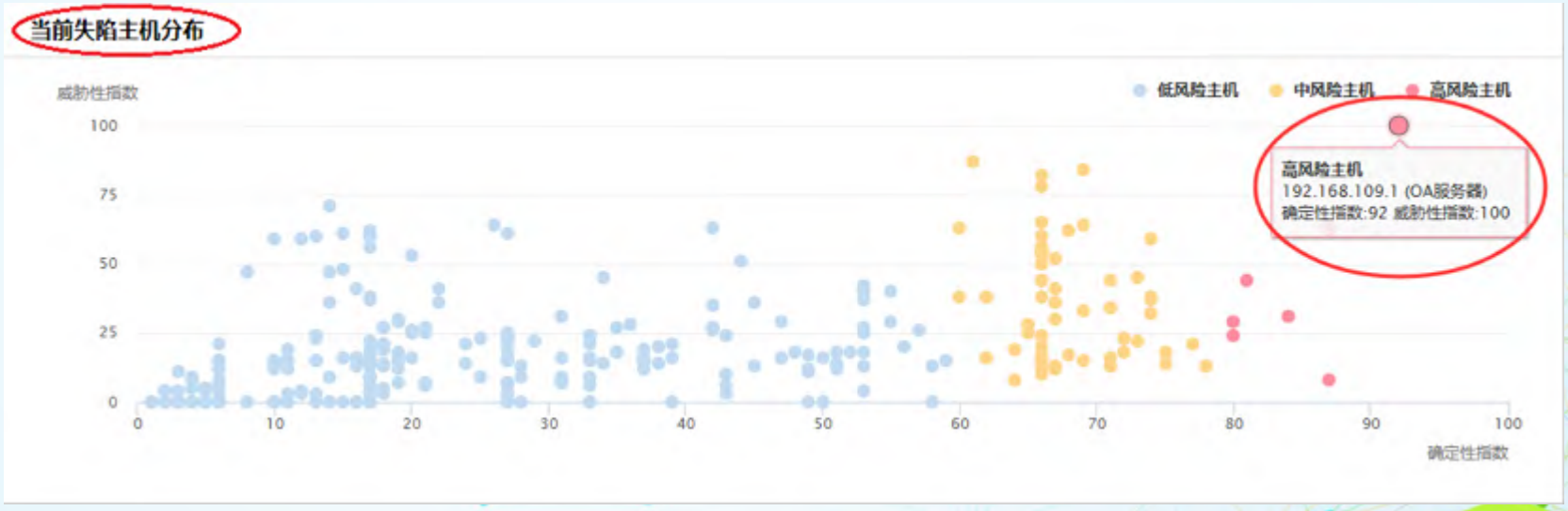
威胁情报地图


24小时攻防情报
TOP攻击国家
IP数 # 国家
34080 中国
3955 美国
1067 西萨摩亚
848 加拿大
450 德国
203 巴西
195 冰岛
112 朝鲜
85 新加坡
82 中国台湾省
TOP目标国家
IP数 # 国家
39463 中国
943 美国
754 新加坡
194 巴西
40 德国
0时攻防情报
162.158.56.197 > 221.226.63.198
美国,San Francisco > 中国,Nanjing
攻击类型:XSS
TOP攻击类型
IP数 # 威胁类型
14289 WEB-ATTACKS
7295 TROJAN
4324 OTHER
3794 DB-ATTACKS
1995 SQL-INJECTION
1977 SPYWARE
1475 WEB-SCAN
1357 XSS
1137 DNS
905 POP
攻防日志
时间 发起方 攻击IP 受攻击地址 次数 应用 端口
10-19 00:01:31 China,Nanjing 218.94.92.10 China,Beijing 10 IMAP4 143
10-19 00:01:35 China,Beijing 220.181.112.244 China,Beijing 13 Web浏览 80
10-19 00:01:39 Hungary 94.125.182.255 China,Beijing 14 未识别 6660
10-19 00:01:43 United States,Chesterfield 165.193.78.187 China,Zhengzhou 12 Web浏览 80

安全态势感知


北京网康科技有限公司的遭受外网攻击信息概况
TOP攻击IP
IP # 次数
104.243.21.100 24025
94.102.50.46 12627
184.105.139.67 8160
104.243.16.10 7180
80.82.64.213 5561
124.232.142.220 5263
83.211.10.232 2152
121.228.120.55 606
116.232.145.87 268
188.138.1.218 126
TOP目标IP
IP # 次数
218.193.144.2 2503
202.120.144.2 2296
10.199.168.193 606
218.193.144.193 391
388
366
365
356
353
274
23时攻防情报
攻击方: 74.125.19.180(美国,Morganton)
被攻击方: 北京分公司NGFW
攻击类型: DNS
总攻击次数: 1
被攻击TOP IP:
202.120.144.2 被攻击次数: 1
TOP威胁
威胁类型 # 次数
DNS 59809
OTHER 8925
WEB-ATTACKS 2602
DB-ATTACKS 606
SQL-INJECTION 101
WEB-SCAN 65
TROJAN 31
WEAKPASSWORD 19
SPYWARE 12
攻防日志
时间 发起方 攻击IP 受攻击地址 受攻击IP 应用 端口 动作

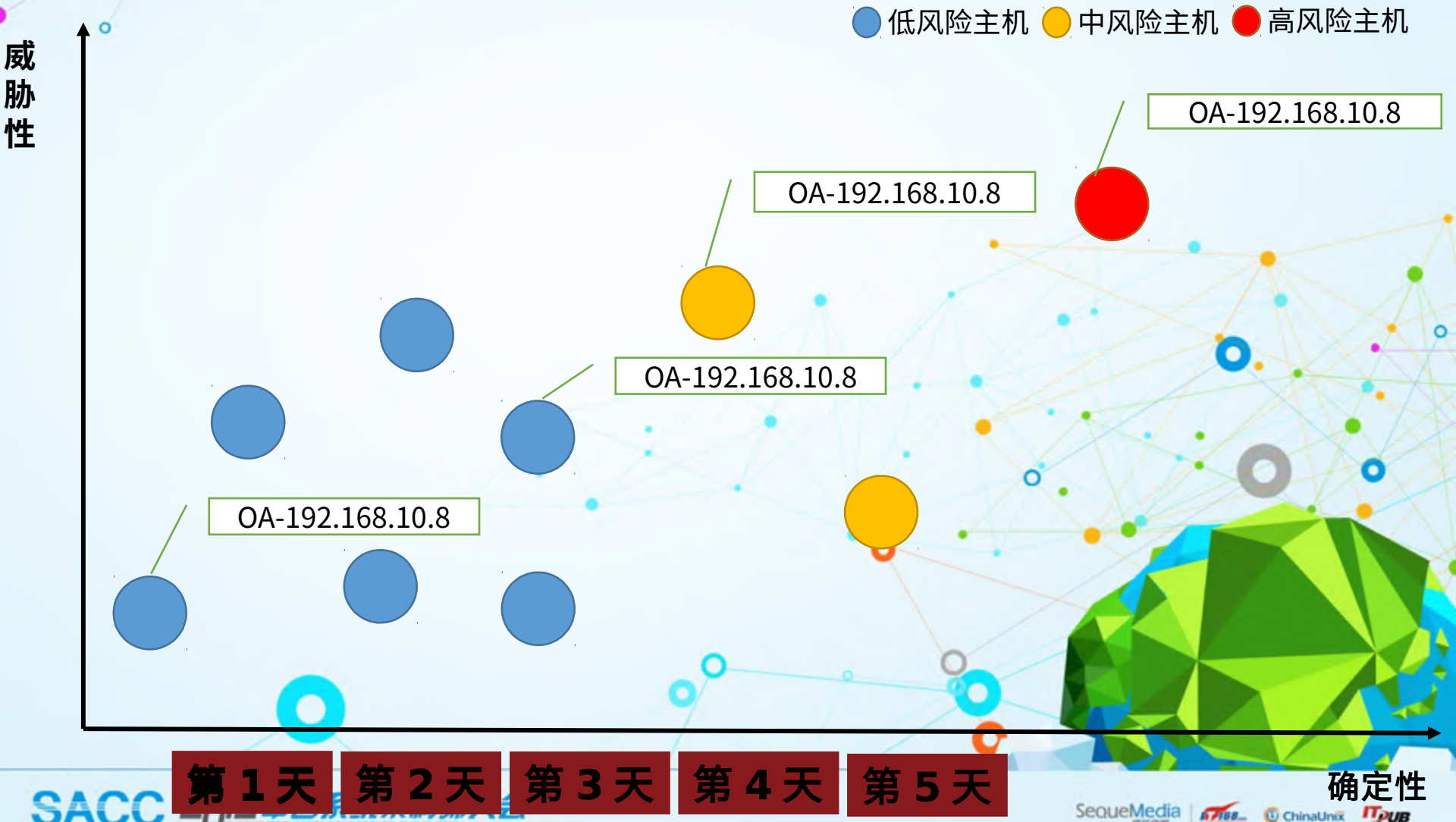
失陷主机检测

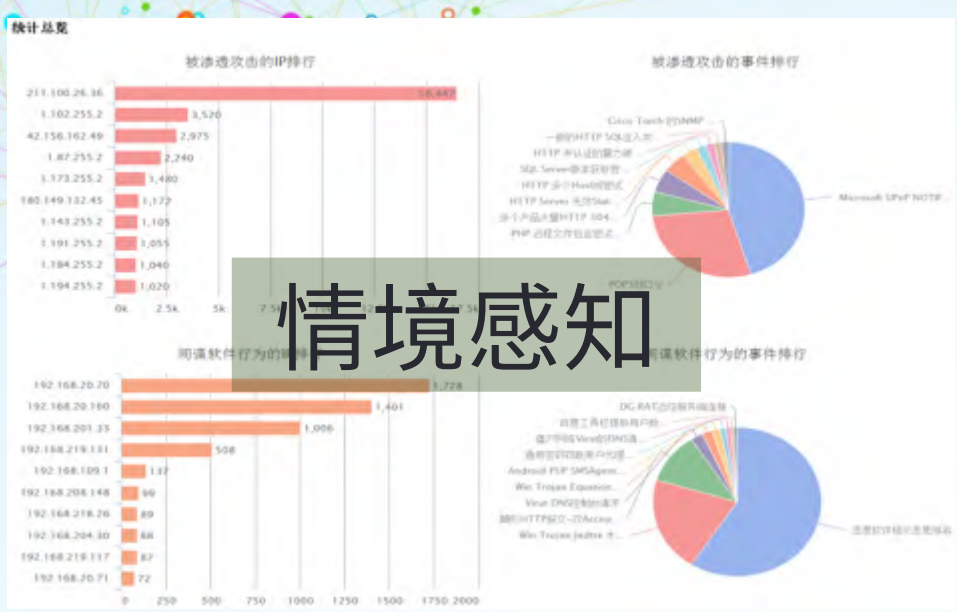

当前失陷主机分布
威胁性指数
低风险主机
中风险主机
高风险主机
100
75
50
25
0
0
10
20
30
40
50
60
70
80
90
100
确定性指数
高风险主机
192.168.109.1 (OA服务器)
确定性指数:92 威胁性指数:100

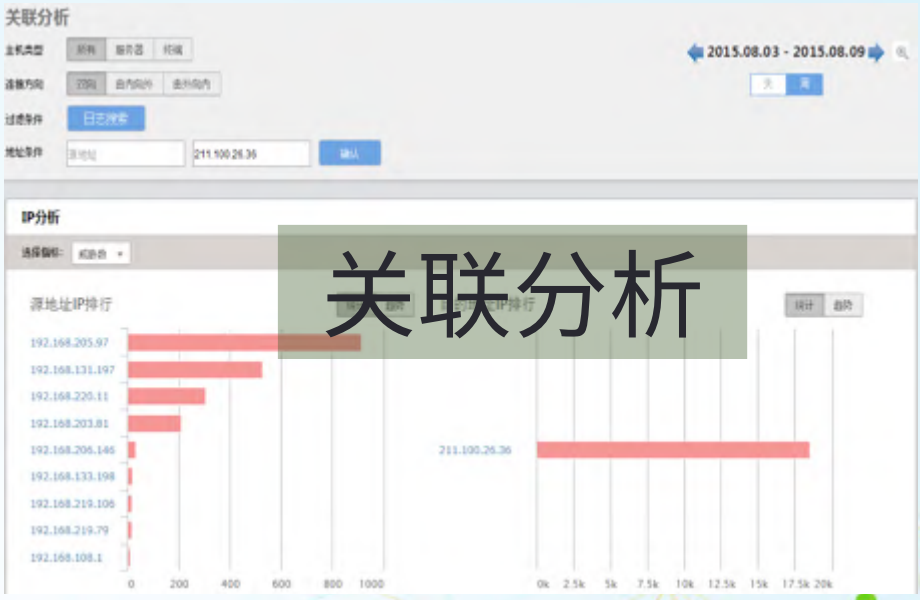
失陷主机回溯


主机基本信息
主机IP 192.168.109.1
确定性和威胁性
确定性指数
威胁性指数
主机威胁活动详情
威胁活动时间分布(最近7天)
详细数据
分类 威胁活动名称 首次发生时间 最近发生时间 次数 确定性指数 威胁性指数 查看详情
遭受入侵 访问恶意网站 2015-07-31 12:44:50 2015-07-31 14:05:04 3 4 10 查看详情
事件详情
活动基本信息
活动名称 木马通信
相关主机IP 192.168.109.1
活动与确定性关系 主机感染的概率较高
活动与威胁性关系 对安全和资产威胁较大
活动解析 木马通信是木马激活后攻击者与主机之间的通信。攻击者可以通过木马软件在受感染主机上所设置的后门登录受感染主机。
活动时间分布
1.5
1
0.5
0
15:30
16:00
16:30
17:00
17:30
2015-07-29 17:06
次数: 1

失陷主机状态迁移图


低风险主机
中风险主机
高风险主机
威胁性
OA-192.168.10.8
OA-192.168.10.8
OA-192.168.10.8
OA-192.168.10.8
第1天
第2天
第3天
第4天
第5天
确定性


统计总览
被渗透攻击的IP排行
被渗透攻击的事件排行
情境感知


关联分析
2015.08.03 - 2015.08.09
IP分析
源地址IP排行
关联分析


all
Android AND 微信
最近12小时
总事件:2,480 (2014-10-23 04:50:00 —— 2014-10-23 16:51:38)
日志搜索


安全报告

未来安全在云端

不管技术演进如何，

网络安全最终是人与人的对抗。

对抗需要强有力的资源和数据支撑。

云和大数据，是提升未来安全能力的必经之路。

THANKS

SequeMedia 盛拓传媒 | IT168 www.it168.com | ChinaUnix.net | ITPUB