结合网络安全法的内网安全审计

神州网云CEO　　宋超

神州网云
SHENZHOU WANG YUN

网络安全法

网络安全法

《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，以制度建设掌握网络空间治理和规则制定方面的主动权，是维护国家网络空间安全发展的利器。

国家安全和发展

宣扬恐怖主义、极端主义、煽动颠覆国家政权、推翻社会主义制度，以及淫秽色情等违法信息，严重危害国家安全和社会公共利益。

信息基础设施安全

网络入侵、网络攻击等非法活动，严重威胁着电信、能源、交通、金融以及国防军事、行政管理等重要领域的基础设施的安全

个人信息

非法获取、泄漏甚至倒卖公民个人信息，侮辱诽谤他人、侵犯知识产权等违法活动在网络上时有发生。

内网安全审计主要通过以下几个过程实现，基于网络流量检测、注重可视化、设计几十个异常行为场景。其中异常行为检测主要有下面三个过程：

1、关键资产的识别和标识：

通过分析内部网络流量，采用机器学习的方式自动化的识别内网的安全资产

2、异常行为的发现：

大多数用户的日常行为是可预测的，每天的日常活动都差不多。恶意的内部人员在偷盗数据或搞破坏前一定有异常的行为

3、数据盗取的追踪：

使用机器学习方式主动发现单位大数据中非法获取的内部人员，及其针对业务数据的备份、窃取等行为通过网络来偷取数据，目前可以通过分析一个主机的流入和流出数据流通过关联分析，可以发现内部人员对重要数据窃取的整个行为视图。

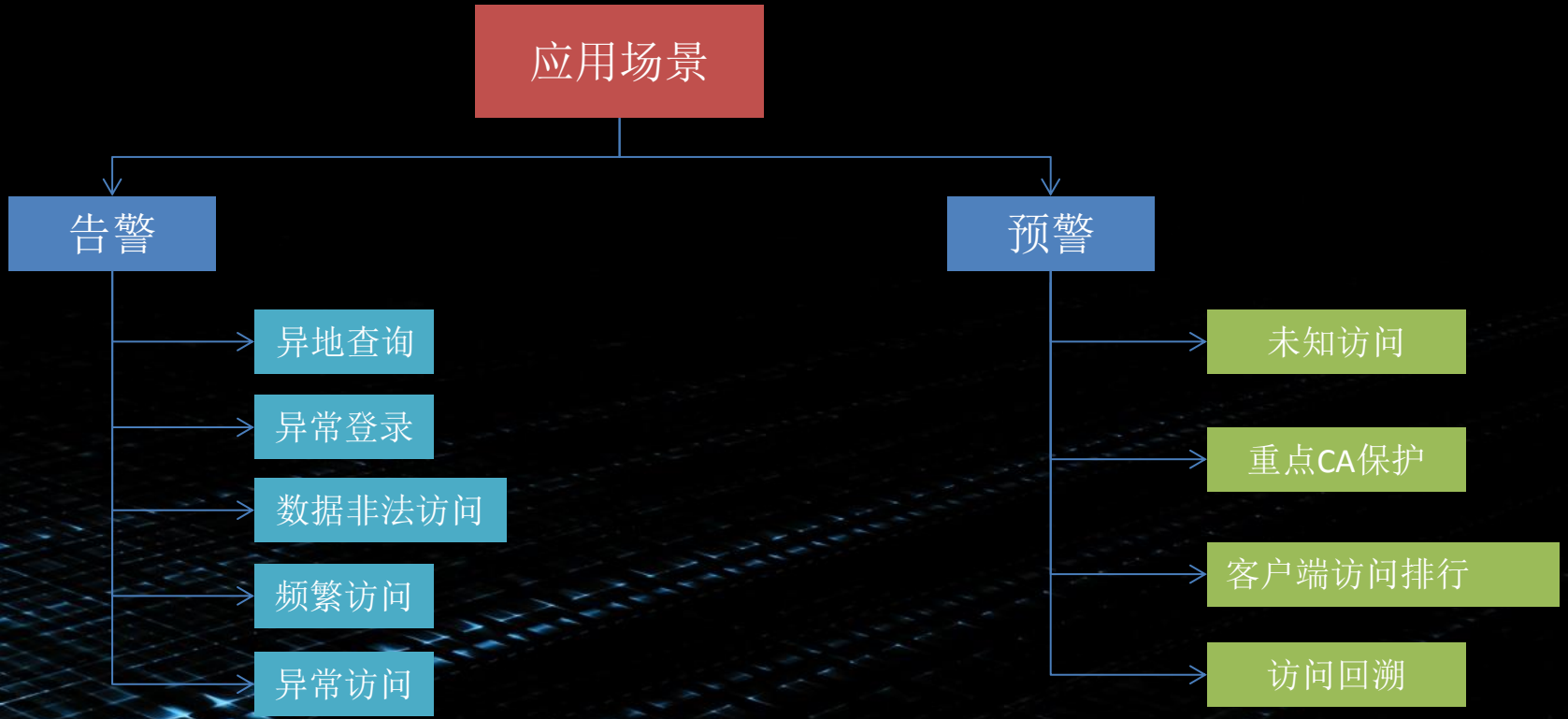
神州网云
SHENZHOU WANG YUN

02

场景框图

神州网云
SHENZHOU WANG YUN

1 场景框图

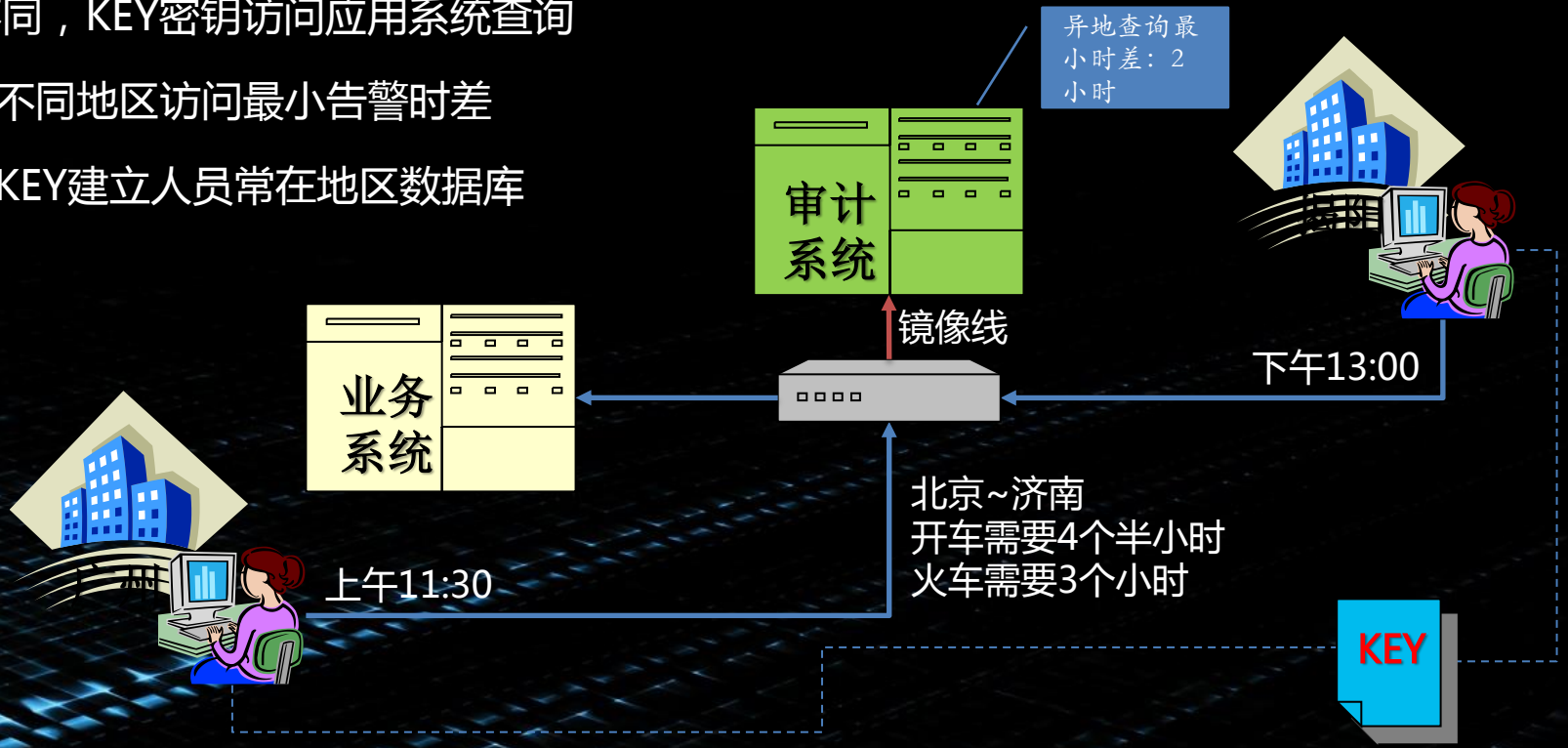


神州网云
SHENZHOU WANG YUN

告警场景

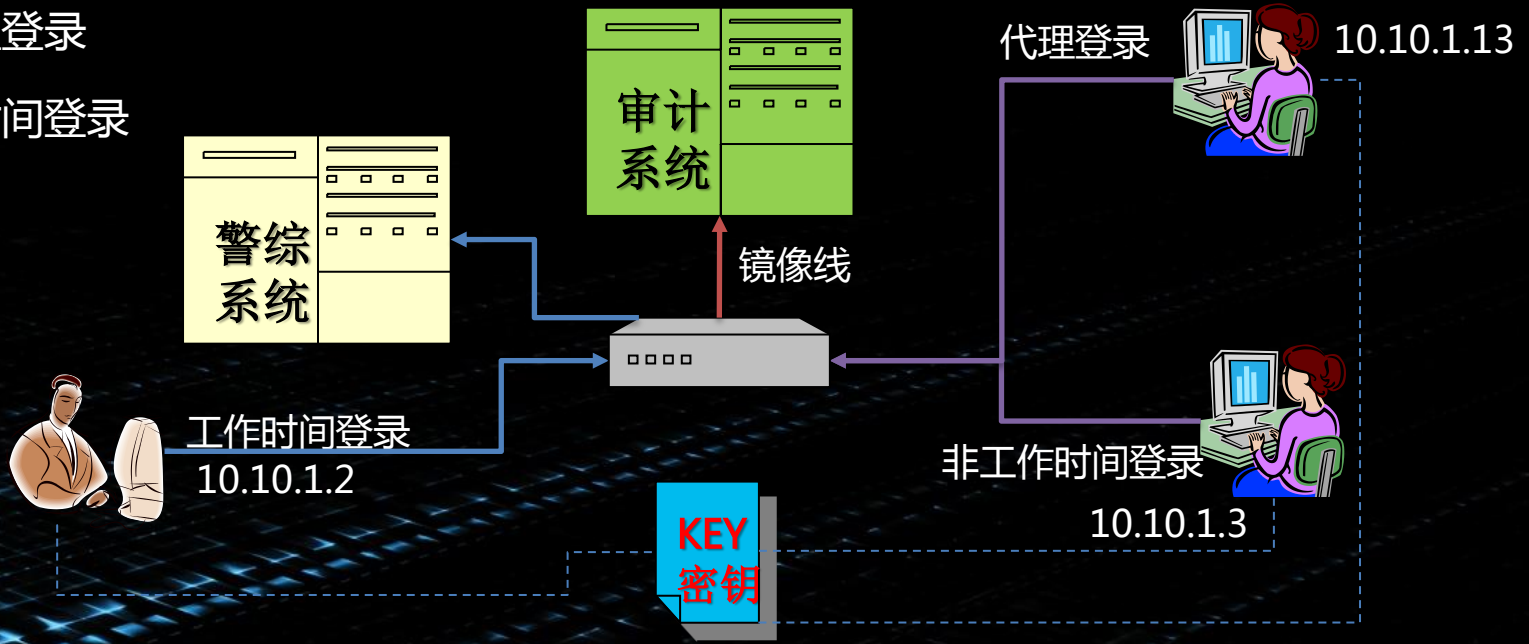
2.1告警—异地查询

- IP不同，KEY密钥访问应用系统查询
- 设置不同地区访问最小告警时差
- 跟据KEY建立人员常在地区数据库



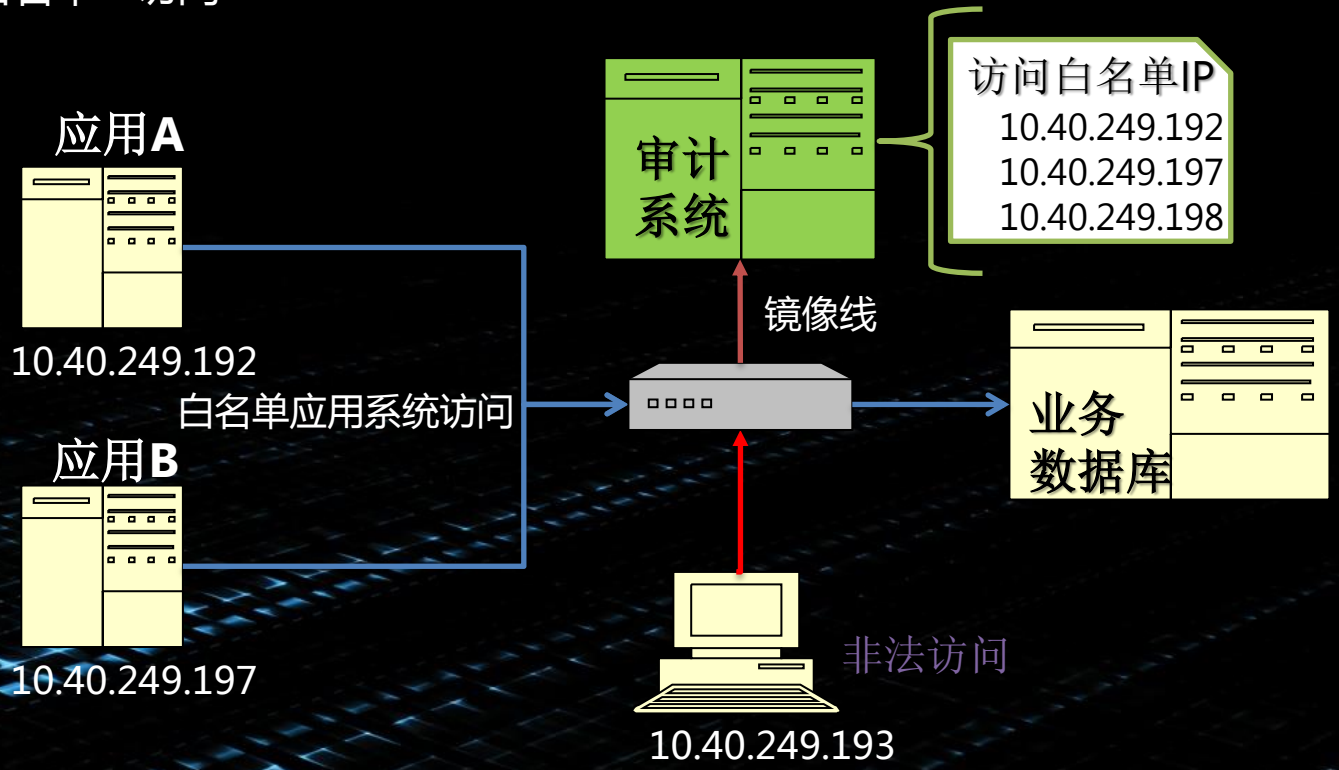
2.2告警—异常登陆

- 不同IP、同KEY密钥
- 使用代理登录
- 非工作时间登录



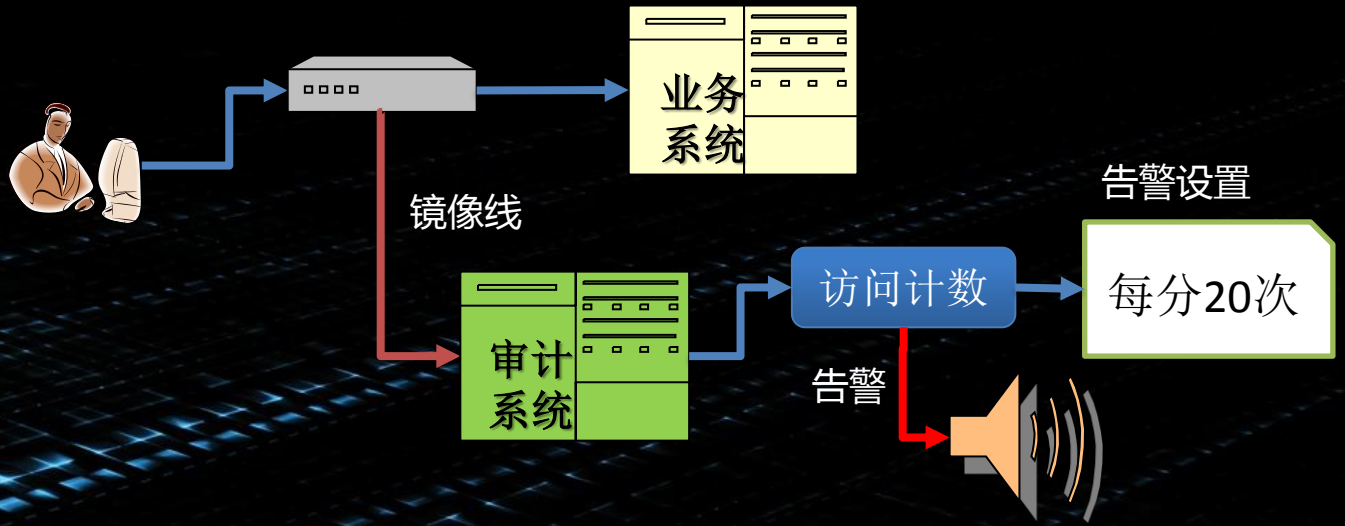
2.3告警—数据非法访问

- 非数据库白名单IP访问



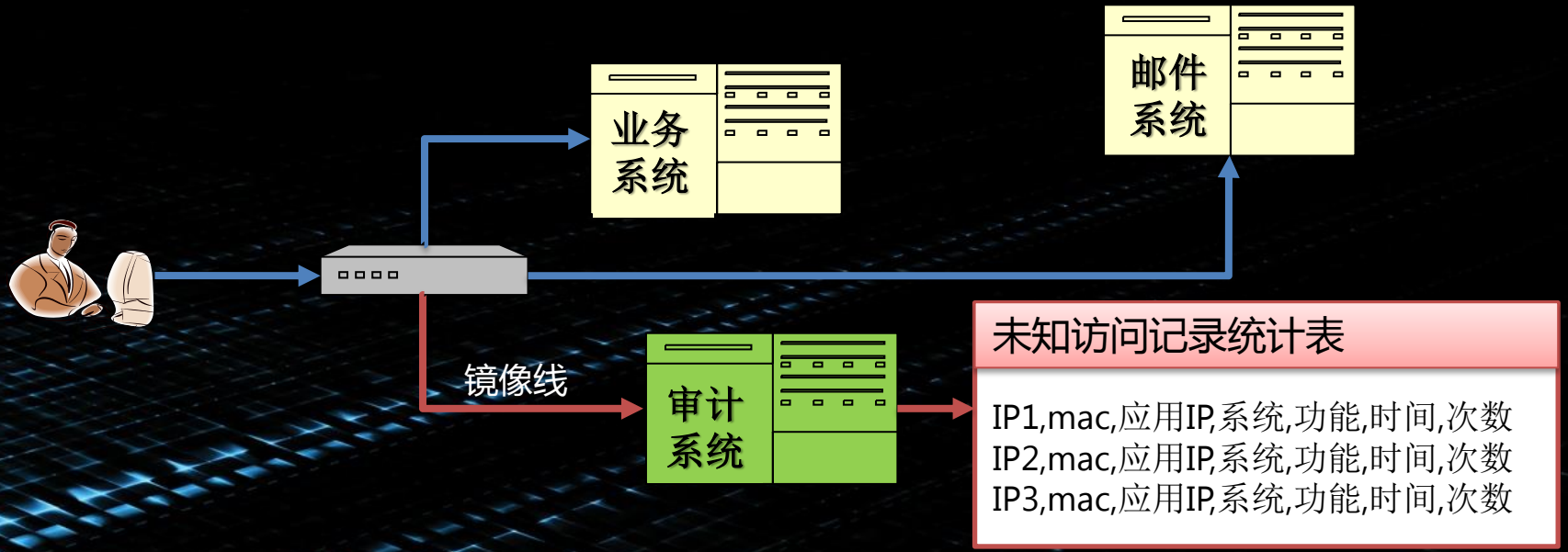
2.4告警—频繁访问

- 预防数据被爬取泄密做告警设置
- 设定单个客户端IP时间段内访问系统最大告警数值
- 超过这个界限告警



3.1预警—未知访问

- 统计所有未知IP地区的日访问量
- 统计内容：客户端IP、MAC、服务端IP、系统、功能、次数

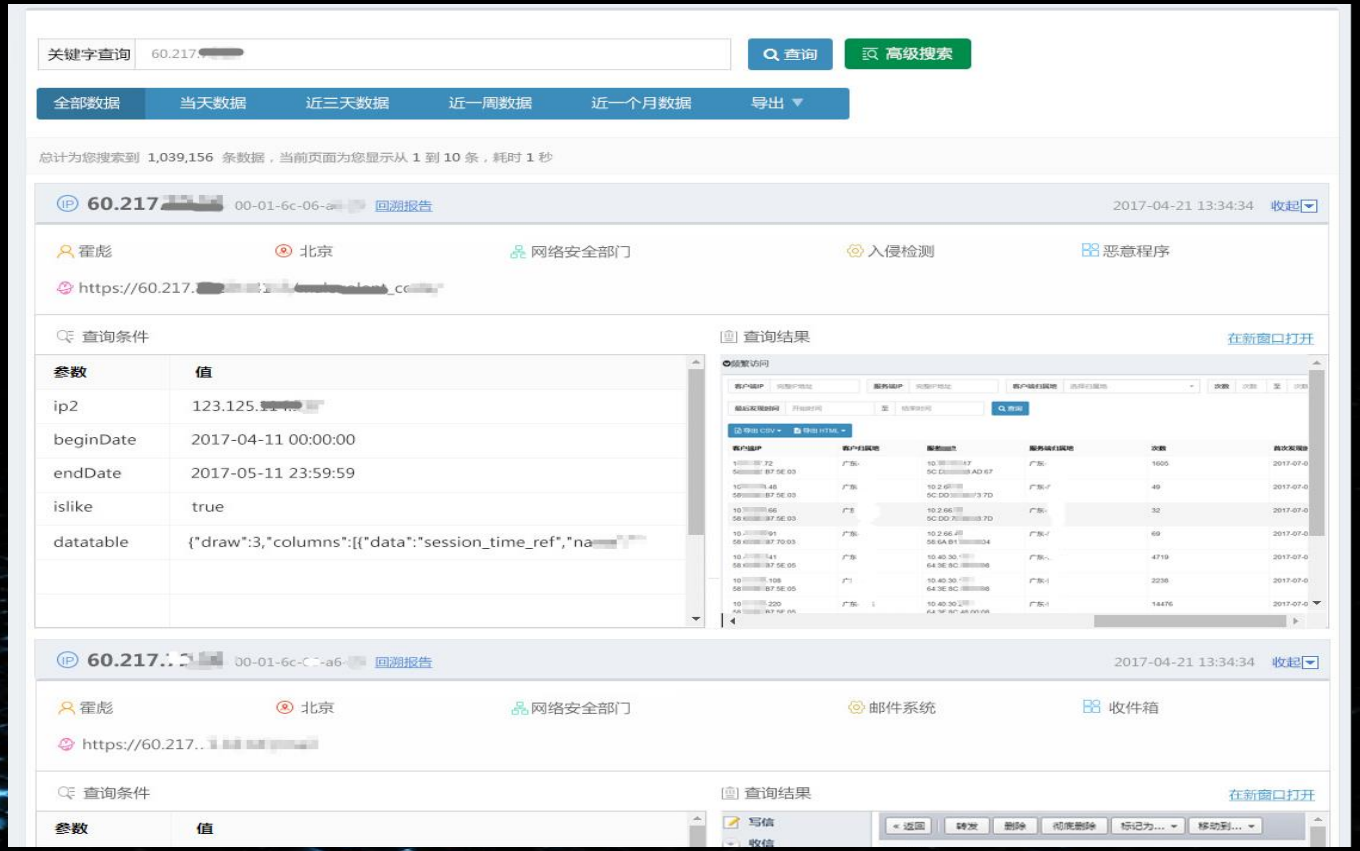


神州网云
SHENZHOU WANG YUN

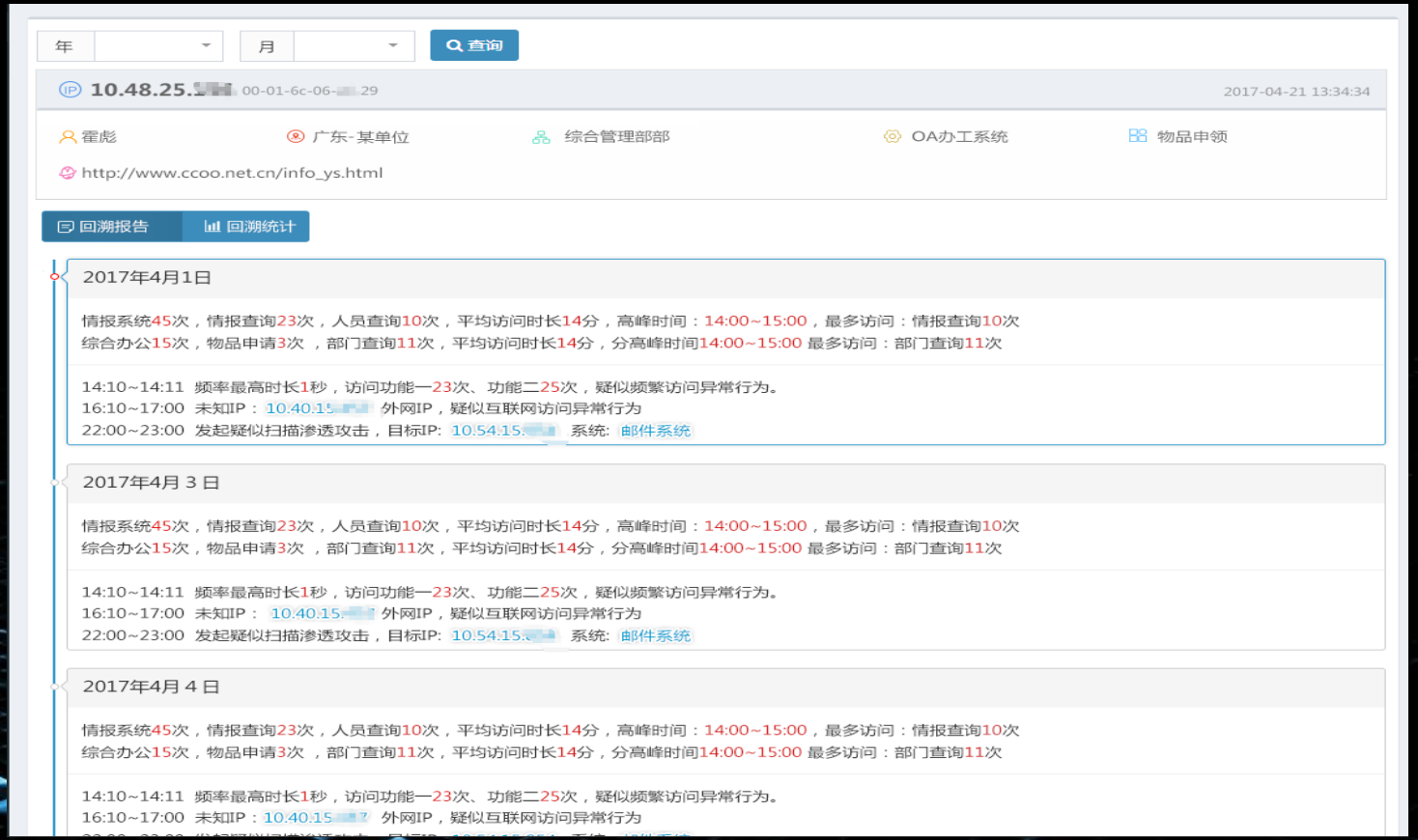
04

访问回溯

4.1 访问回溯查询


关键字查询
查询
高级搜索
全部数据
当天数据
近三天数据
近一周数据
近一个月数据
导出
总计为您搜索到 1,039,156 条数据，当前页面为您显示从 1 到 10 条，耗时 1 秒
回溯报告
2017-04-21 13:34:34
收起
霍彪
北京
网络安全部门
入侵检测
恶意程序
查询条件
查询结果
在新窗口打开
参数
值
ip2
beginDate
2017-04-11 00:00:00
endDate
2017-05-11 23:59:59
islike
true
datatable
邮件系统
收件箱

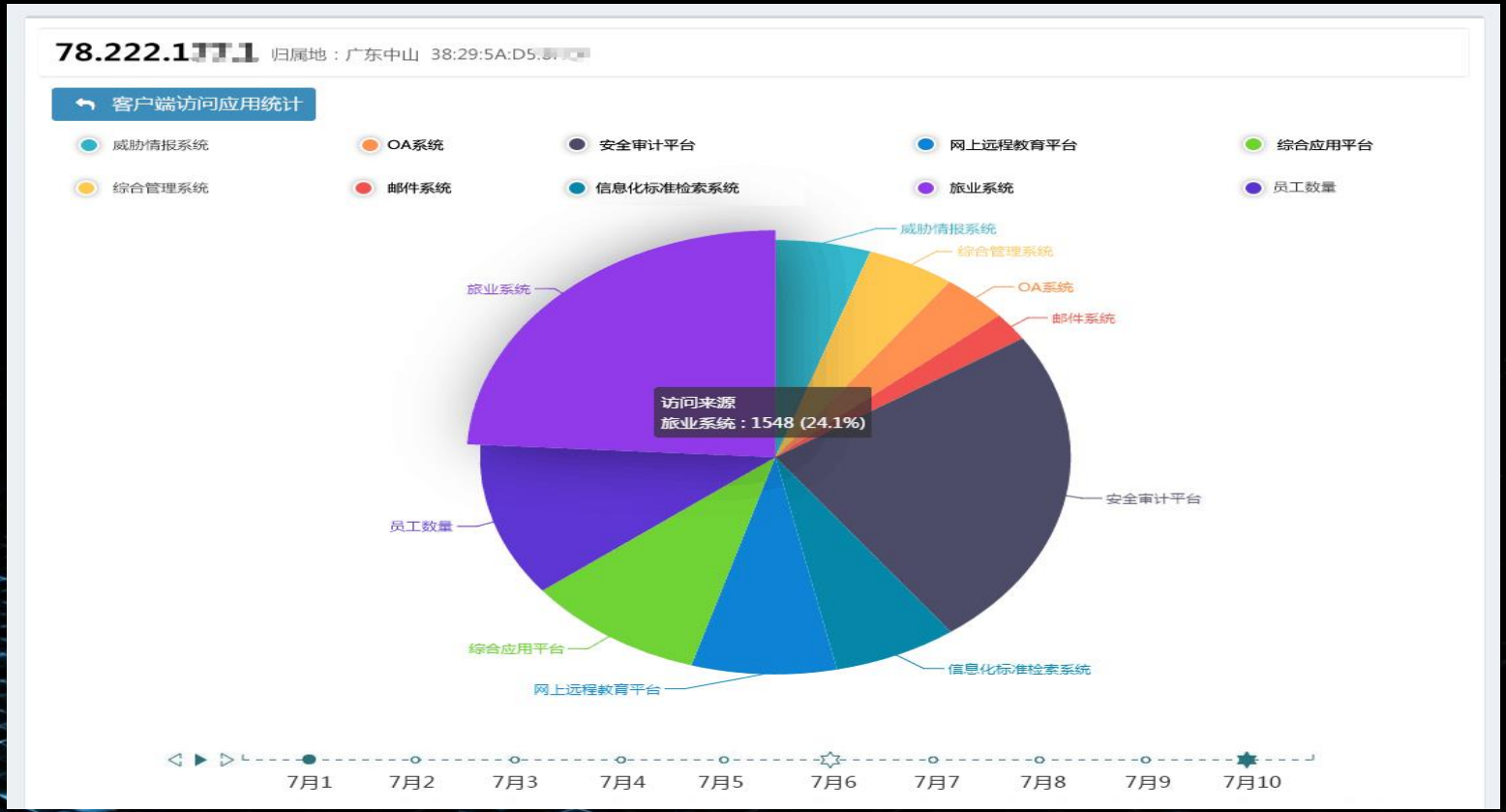
4.2 回溯报告


年
月
查询
10.48.25.
00-01-6c-06-
29
2017-04-21 13:34:34
霍彪
广东-某单位
综合管理部部
OA办工系统
物品申领
http://www.ccoo.net.cn/info_ys.html
回溯报告
回溯统计
2017年4月1日
情报系统45次，情报查询23次，人员查询10次，平均访问时长14分，高峰时间：14:00~15:00，最多访问：情报查询10次
综合办公15次，物品申请3次 ，部门查询11次，平均访问时长14分，分高峰时间14:00~15:00 最多访问：部门查询11次
14:10~14:11 频率最高时长1秒，访问功能一23次、功能二25次，疑似频繁访问异常行为。
16:10~17:00 未知IP： 10.40.15 外网IP，疑似互联网访问异常行为
22:00~23:00 发起疑似扫描渗透攻击，目标IP: 10.54.15 系统: 邮件系统
2017年4月 3 日
情报系统45次，情报查询23次，人员查询10次，平均访问时长14分，高峰时间：14:00~15:00，最多访问：情报查询10次
综合办公15次，物品申请3次 ，部门查询11次，平均访问时长14分，分高峰时间14:00~15:00 最多访问：部门查询11次
14:10~14:11 频率最高时长1秒，访问功能一23次、功能二25次，疑似频繁访问异常行为。
16:10~17:00 未知IP： 10.40.15 外网IP，疑似互联网访问异常行为
22:00~23:00 发起疑似扫描渗透攻击，目标IP: 10.54.15 系统: 邮件系统
2017年4月 4 日
情报系统45次，情报查询23次，人员查询10次，平均访问时长14分，高峰时间：14:00~15:00，最多访问：情报查询10次
综合办公15次，物品申请3次 ，部门查询11次，平均访问时长14分，分高峰时间14:00~15:00 最多访问：部门查询11次
14:10~14:11 频率最高时长1秒，访问功能一23次、功能二25次，疑似频繁访问异常行为。
16:10~17:00 未知IP： 10.40.15 外网IP，疑似互联网访问异常行为

4.3 回溯统计


年
月
查询
10.48.23 00-01-6c-06-a6-29
2017-04-21 13:34:34
霍彪
广东- 某单位
综合管理部部
OA办工系统
物品申领
http://www.ccoo.net .html
回溯报告
回溯统计
邮件系统
OA办工系统
员工数量
4月7
4月6
4月5
4月4
4月3
4月2
4月1
320
210
310
330
230
330
390
90
290
334
1
134
234
301
101
191
302
132
182
320
120
220
0
200
400
600
800
1000

4.3 回溯统计


78.222.1
归属地：广东中山 38:29:5A:D5:
客户端访问应用统计
威胁情报系统
OA系统
安全审计平台
网上远程教育平台
综合应用平台
综合管理系统
邮件系统
信息化标准检索系统
旅业系统
员工数量
访问来源
旅业系统：1548 (24.1%)
7月1
7月2
7月3
7月4
7月5
7月6
7月7
7月8
7月9
7月10

神州网云
SHENZHOU WANG YUN

谢谢大家

神州网云（北京）信息技术有限公司
地址：北京市海淀区紫竹院路98号化大科技园326室
电话：010—62670617
邮箱：consen@secsky.net
网址：www.secsky.net