



2022

畅享连世界

NTM典型使用场景一： 医院数据中心故障溯源

北京派网软件有限公司



目录

01

场景1：关键业务卡顿问题

02

场景2：安全异常问题分析

03

场景3：数据溯源排查



01

关键业务系统卡顿问题

问题1：当各位下班在家刷短视频的时候，是否出现过短视频卡住不动的情况呢？





场景一：关键业务系统卡顿问题

问题1：当各位下班在家刷短视频的时候，是否出现过短视频卡住不动的情况呢？

- 1、是
- 2、否





场景一：关键业务系统卡顿问题

问题2：当各位在家中正刷着短视频，突然发现视频卡了，屏幕上开始出现转圈圈，大家会想到是哪里的问题呢？





场景一：关键业务系统卡顿问题

问题2：当你在家中正刷着短视频，突然发现视频卡了，屏幕上开始出现转圈圈，大家会想到是哪里的问题呢？

- 1、手机的问题，重启一下
- 2、家里无线的问题，把WIFI重启一下
- 3、运营商的问题，打电话投诉他们
- 4、内容提供商的问题（短视频公司），打电话投诉他们



问题3：刚刚大家判断的依据是什么？





场景一：分析业务系统卡顿问题

问题3：刚刚大家判断的依据是什么？

- 1、凭经验感觉，猜的
- 2、进行过明确的测试，得出数据后判断的
- 3、有专业的测试工具，可以进行快速、客观地展现
- 4、蒙一个





场景一：分析业务系统卡顿问题

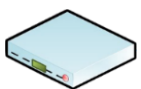
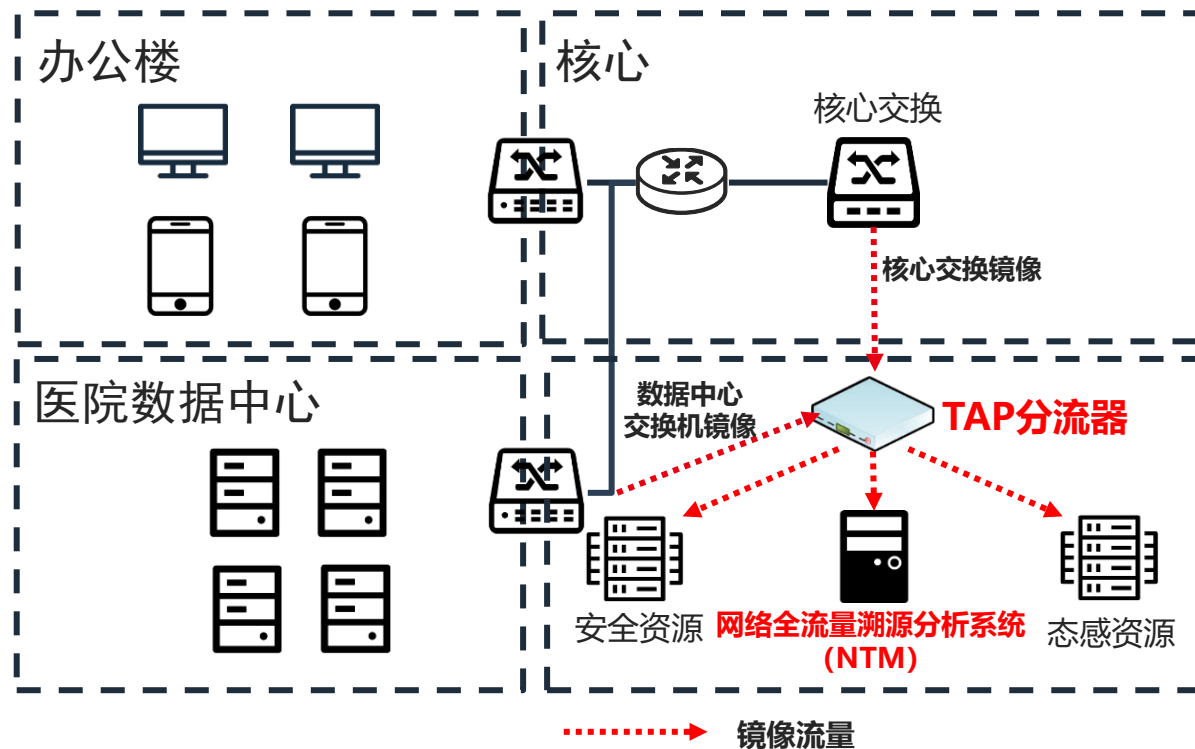
当医院的关键业务系统出现卡顿，比如：PACE、HIS、LIS等等，我们怎么办？

- 1、如何定责？
- 2、如何快速定责？
- 3、如何有理有据地快速定责？





场景一：分析业务系统卡顿问题



探针/TAP

Panabit探针或TAP分流器，采集数据中心交换机镜像，并将镜像分流给NTM和其他安全产品



NTM

NTM网络全流量溯源系统，对数据中心网络进行可视化分析，主要针对异常安全数据的分析，并对关键业务数据进行原始数据包留存，以便溯源

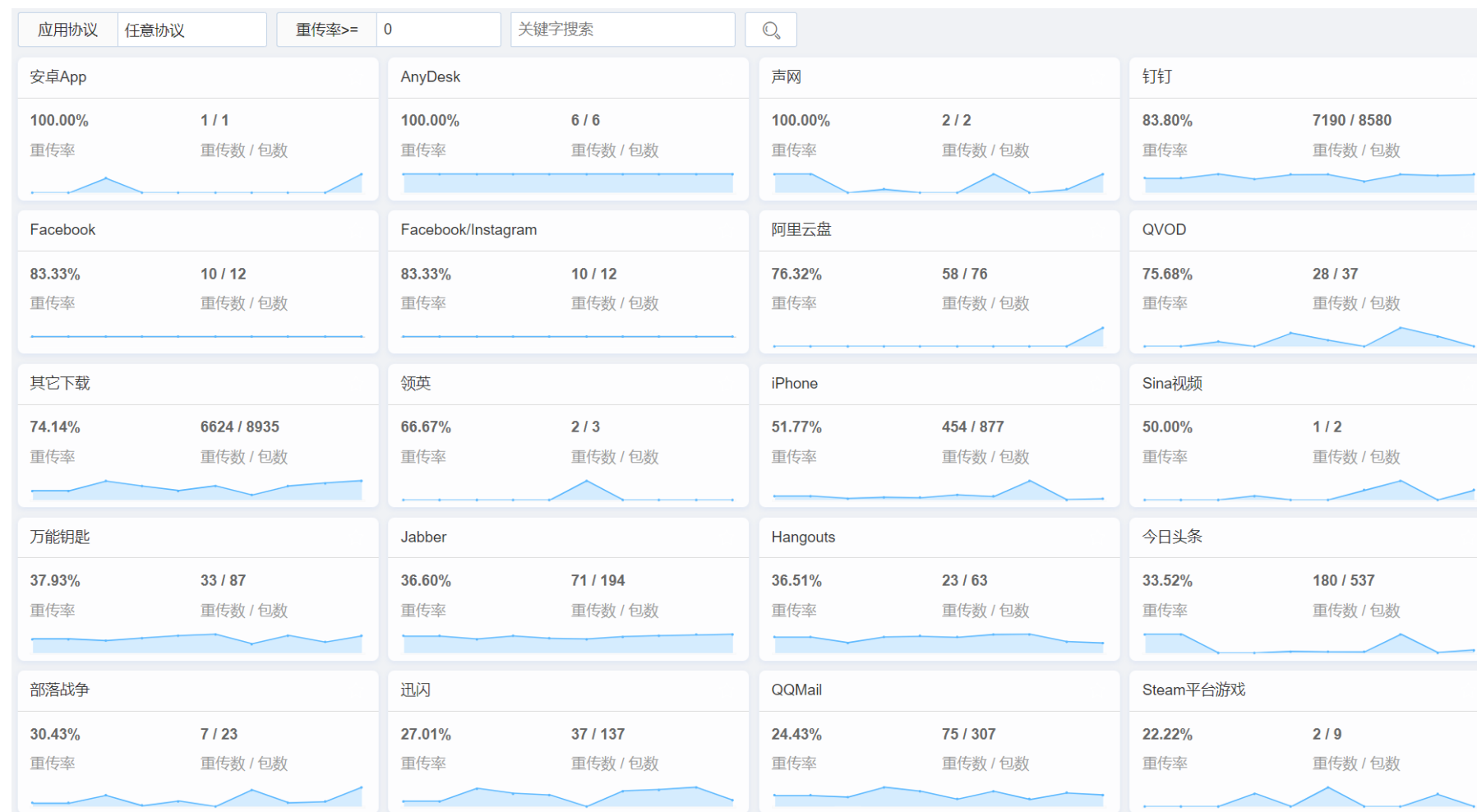
实时监控业务时延

及时发现网络波动

重点关注TOP访问

大幅提升运维效率

主机分析											
自动刷新	10秒	排序方式	连接数	主机组	所有组	关键字搜索			+添加	导入	导出
PACS				LIS				EMR			
8906	10721	19	71.62 ms	7720	11992	13	71.00 ms	3263	14802	25	88.99 ms
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延
54.87M	4.28M	79.19G	10.43G	60.62M	23.11M	75.93G	13.11G	83.48M	20.00M	132.83G	79.63G
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量
HIS				RIS				挂号			
2717	1739	39	76.65 ms	827	2405	100	0.00 ms	5	0	0	13.87 ms
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延
8.67M	1.11M	83.01G	15.36G	0	1.16M	0	4.53G	0	0	19.54M	2.65M
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量
CIS				手麻				PEIS			
1	14	3	49.74 ms	0	0	0	0.00 ms	0	0	0	0.00 ms
连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延	连接数	PPS	失败率	平均时延
10.06K	17.45K	104.64M	37.23M	0	0	0	0	0	0	0	0
流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量	流入速率	流出速率	流入流量	流出流量
<div><div><</div><div>1</div><div>2</div><div>></div><div>到第</div><div>1</div><div>页</div><div>确定</div><div>总共 12</div><div>9 条/页</div><div>></div></div>											



协议重传:

指TCP连接建立后, 由于通讯超时或者TCP序列不对产生的重传包。

常规使用:


如果某类应用的重传率非常高, 用户体验感肯定不好。

时延监测快速定责



目标地理位置	传输协议	应用协议	客户时延 ⓘ	服务时延 ⓘ	应用时延 ⓘ	流量(前10秒) ⓘ	请求域名	状态	操作
天津 联通	TCP	手	11.04	4.55	0.45	403/562	d...		数据包
河南南阳 联通	TCP	手	3.25	19.14	39.67	1498/27681			数据包
北京 BGP	TCP	手	5.4	3.26	4.08	823/3113	6		数据包
河北唐山 联通	TCP	手	12.02	11.56	20.35	1127/18548	n...		数据包
天津 联通	TCP	手	11.85	4.13	5.61	431/13791			数据包
内蒙古 联通	TCP	手	2.16	16.66	16.96	3544/5475			数据包
天津 联通	TCP	手	7.95	7.83	0.42	344/554	v...		数据包
北京 联通	TCP	手	7.79	2.61	16.82	431/7484			数据包
北京 联通	TCP	手	8.65	3.62	14.73	407/8187			数据包
天津 联通	TCP	手	15.89	8.41	10.96	1509/25370	om		数据包
天津 联通	TCP	手	20.08	6.98	11.59	1042/47070	om		数据包
北京 联通	TCP	手	27.01	5.3	0	0/0		失败	数据包
河北唐山 联通	TCP	手	5.16	15.2	20.18	1131/27290	n...		数据包
天津 联通	TCP	手	11.81	5	6.29	487/8804	/...		数据包
河北唐山 联通	TCP	手	5.34	14.77	23.19	1123/13834	n...		数据包
天津 联通	TCP	手	10.55	5.33	6.72	401/1381	200		数据包
天津 联通	TCP	手	5.99	4.47	5.6	413/4224	200		数据包
天津 联通	TCP	手	4.38	5.89	6.87	399/4628	200		数据包
天津 联通	TCP	手	9.85	5.87	0.46	403/562	d...		数据包

 监测网络时延情况

 60s 1分钟快速排障

 完整记录事件日志



事件全数据记录留存



原始数据

源IP

x.x.x.x

源端口

80 / 8000-8080

目标IP

x.x.x.x

目标端口

80 / 8000-8080

传输协议

任意

应用协议

HIS系统

源IP ISP

任意

目标IP ISP

任意

源IP区域

任意

目标IP区域

任意

请求域名

客户时延>=

0

服务时延>=

0

应用时延>=

ms

时间范围

2021-07-06 09:56:57 - 2021-07-06 10:56:57

🔍

序号	请求时间	源IP	目标IP	目标地理位置	传输协议	应用协议	客户时延	服务时延	应用时延	流量(前10秒)	请求域名	操作
1	2021-07-06/10:11:54	192.168.8.100:51316	192.168.2.251:3911		TCP	HIS系统	0.1	0.12	1.77	1892/11646	192.168.2.251 200	数据包
2	2021-07-06/10:11:54	192.168.8.100:51315	192.168.2.251:80		TCP	HIS系统	0.1	0.12	29.75	1764/5480	192.168.2.251 200	数据包
3	2021-07-06/10:13:46	192.168.10.177:50143	192.168.2.251:80		TCP	HIS系统	18.88	0.13	31.33	1062/48874	192.168.2.251 200	数据包
4	2021-07-06/10:15:53	192.168.10.102:50509	192.168.2.251:3910		TCP	HIS系统	3.34	0.15	0.84	12272/30430	192.168.2.251 200	数据包
5	2021-07-06/10:15:54	192.168.10.156:10886	192.168.2.251:3910		TCP	HIS系统	6.28	0.14	0.86	6786/8538	192.168.2.251 200	数据包
6	2021-07-06/10:16:16	192.168.10.102:50528	192.168.2.251:53048		TCP	HIS系统	2.3	0.12	1.03	2266/2816	192.168.2.251 200	数据包
7	2021-07-06/10:16:16	192.168.10.156:10932	192.168.2.251:53048		TCP	HIS系统	1.09	0.12	0.78	2266/2816	192.168.2.251 200	数据包
8	2021-07-06/10:16:16	192.168.10.156:10933	192.168.2.251:53048		TCP	HIS系统	2.34	0.11	1.06	2266/2816	192.168.2.251 200	数据包
9	2021-07-06/10:16:16	192.168.10.156:10931	192.168.2.251:53048		TCP	HIS系统	1.66	0.13	1.18	2266/2816	192.168.2.251 200	数据包
10	2021-07-06/10:16:17	192.168.10.102:50529	192.168.2.251:53048		TCP	HIS系统	2	0.11	0.96	2266/2816	192.168.2.251 200	数据包
11	2021-07-06/10:16:17	192.168.10.102:50530	192.168.2.251:53048		TCP	HIS系统	2.3	0.12	0.96	2266/2816	192.168.2.251 200	数据包
12	2021-07-06/10:16:17	192.168.10.156:10935	192.168.2.251:53048		TCP	HIS系统	1.64	0.12	0.75	2266/2816	192.168.2.251 200	数据包
13	2021-07-06/10:16:17	192.168.10.156:10934	192.168.2.251:53048		TCP	HIS系统	5.9	0.12	0.75	2266/2816	192.168.2.251 200	数据包
14	2021-07-06/10:16:17	192.168.10.102:50531	192.168.2.251:53048		TCP	HIS系统	2.56	0.12	0.7	2266/2816	192.168.2.251 200	数据包
15	2021-07-06/10:16:18	192.168.10.102:50532	192.168.2.251:53048		TCP	HIS系统	2.4	0.12	0.69	2266/2816	192.168.2.251 200	数据包

<

1

>

到第

1

页

确定

总共 58



完整记录重要数据



出现问题有据可查



从此告别无谓背锅

硬声硬气

关键业务
监控

1分钟快
速排障

所有事件
全记录

不再背锅



02

安全异常分析



场景二：安全异常分析

问题1： 你曾经是否想象过自己是一个不太冷的杀手？





场景二：安全异常分析

问题1：你曾经是否想象过自己是一个不太冷的杀手？

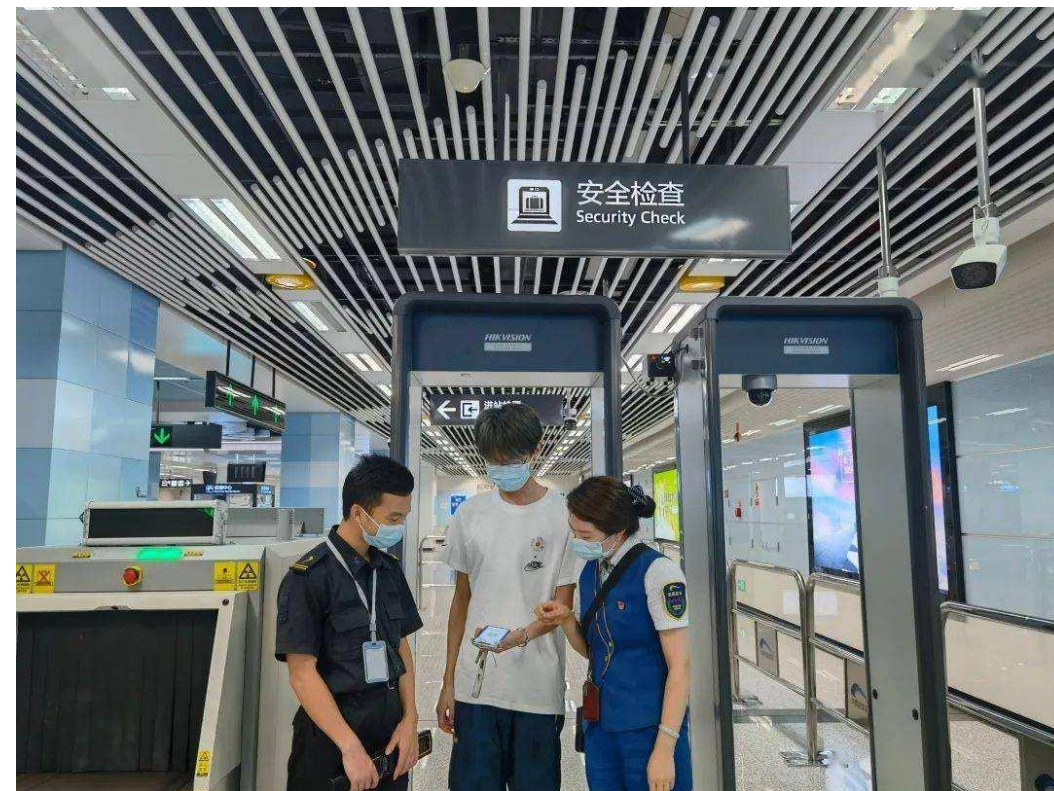
- 1、是
- 2、否





场景二：安全异常分析

问题2：假如你是一个杀手，想要在地铁上解决目标，请问，你将采用何种方式动手？

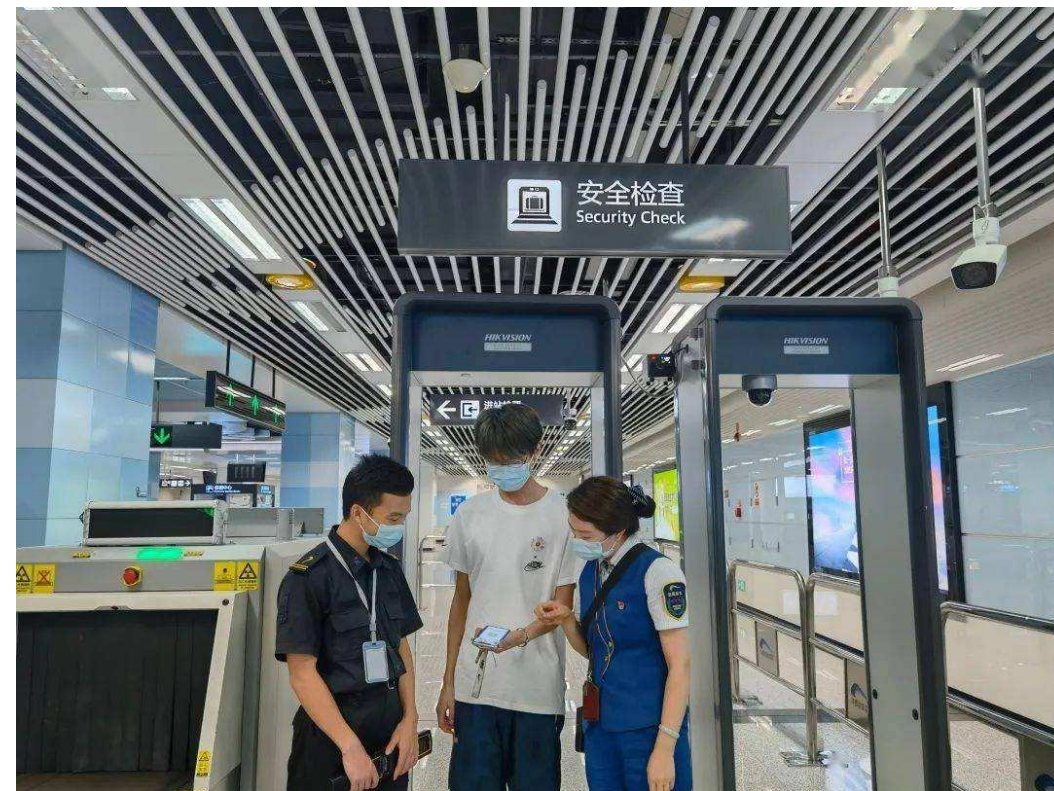




场景二：安全异常分析

问题2：假如你是一个杀手，想要在地铁上解决目标，请问，你将采用何种方式动手？

- 1、手枪
- 2、炸弹
- 3、铁锤
- 4、刀





场景二：安全异常分析

问题3：你曾经是否想象过自己是一个隐姓埋名，潜伏于网络之后，“杀人夺旗”于无形的黑客？





场景二：安全异常分析

问题3：你曾经是否想象过自己是一个隐姓埋名，潜伏于网络之后，“杀人夺旗”于无形的黑客？

- 1、是
- 2、否





场景二：安全异常分析

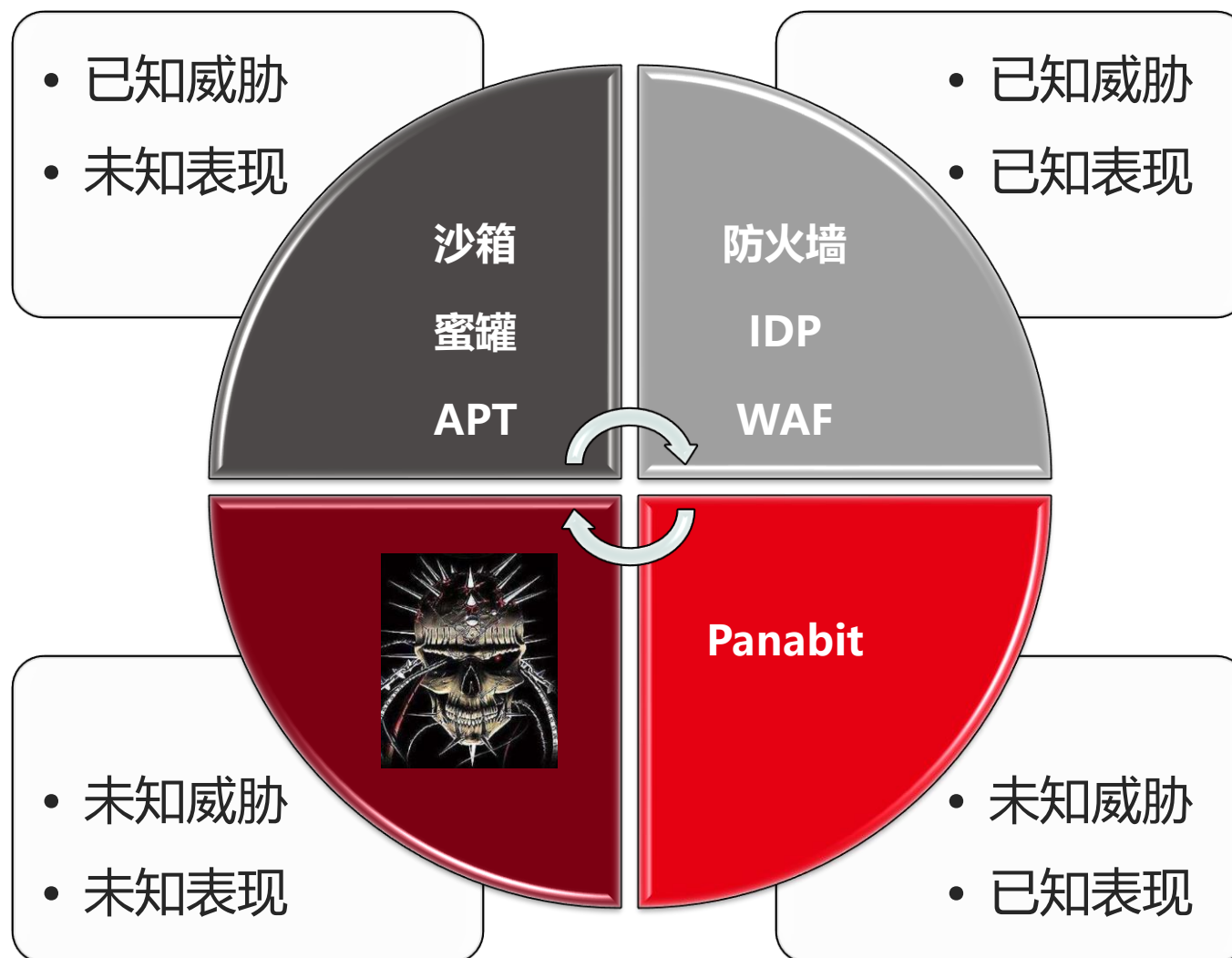
问题4：假如你是一位黑客，想要攻陷派网的数据中心，得到本人的帅照，你将？

- 1、套用网络中已有的病毒，进行入侵，窃取
- 2、自己开发新的病毒，进行入侵，窃取
- 3、加本人微信，直接要
- 4、加销售微信，迂回要



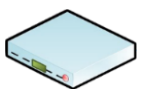
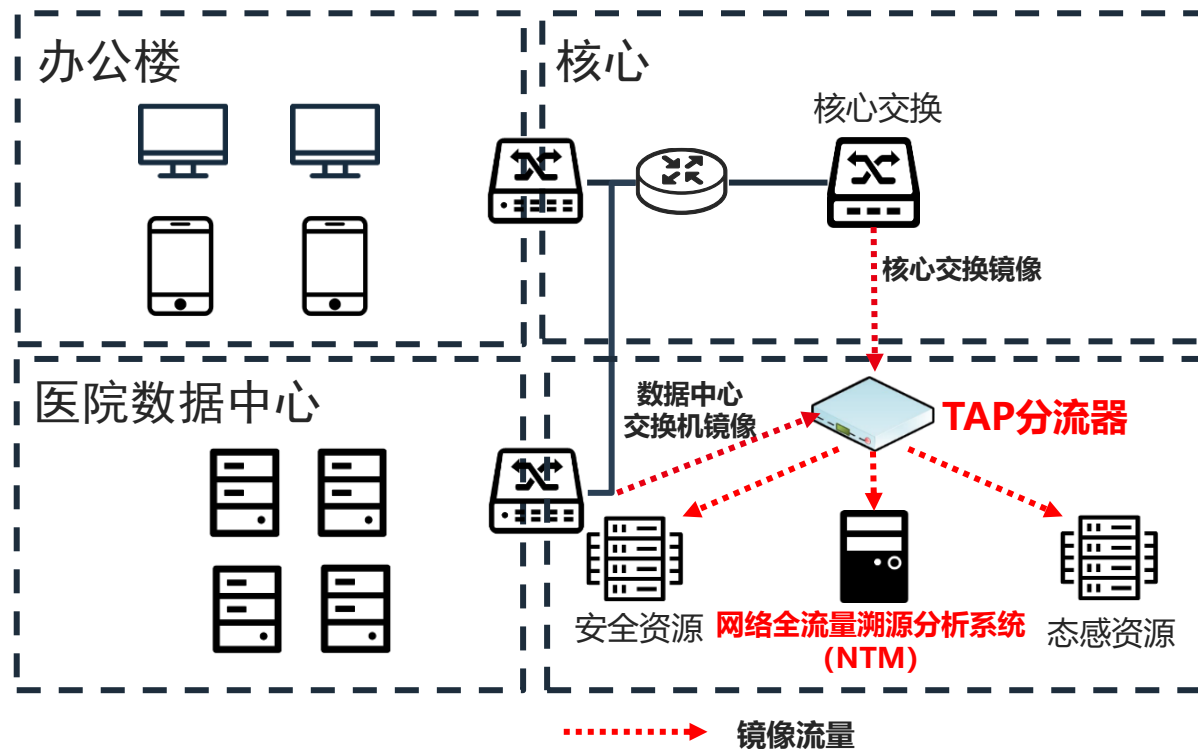


场景二：安全异常分析





场景二：安全异常分析



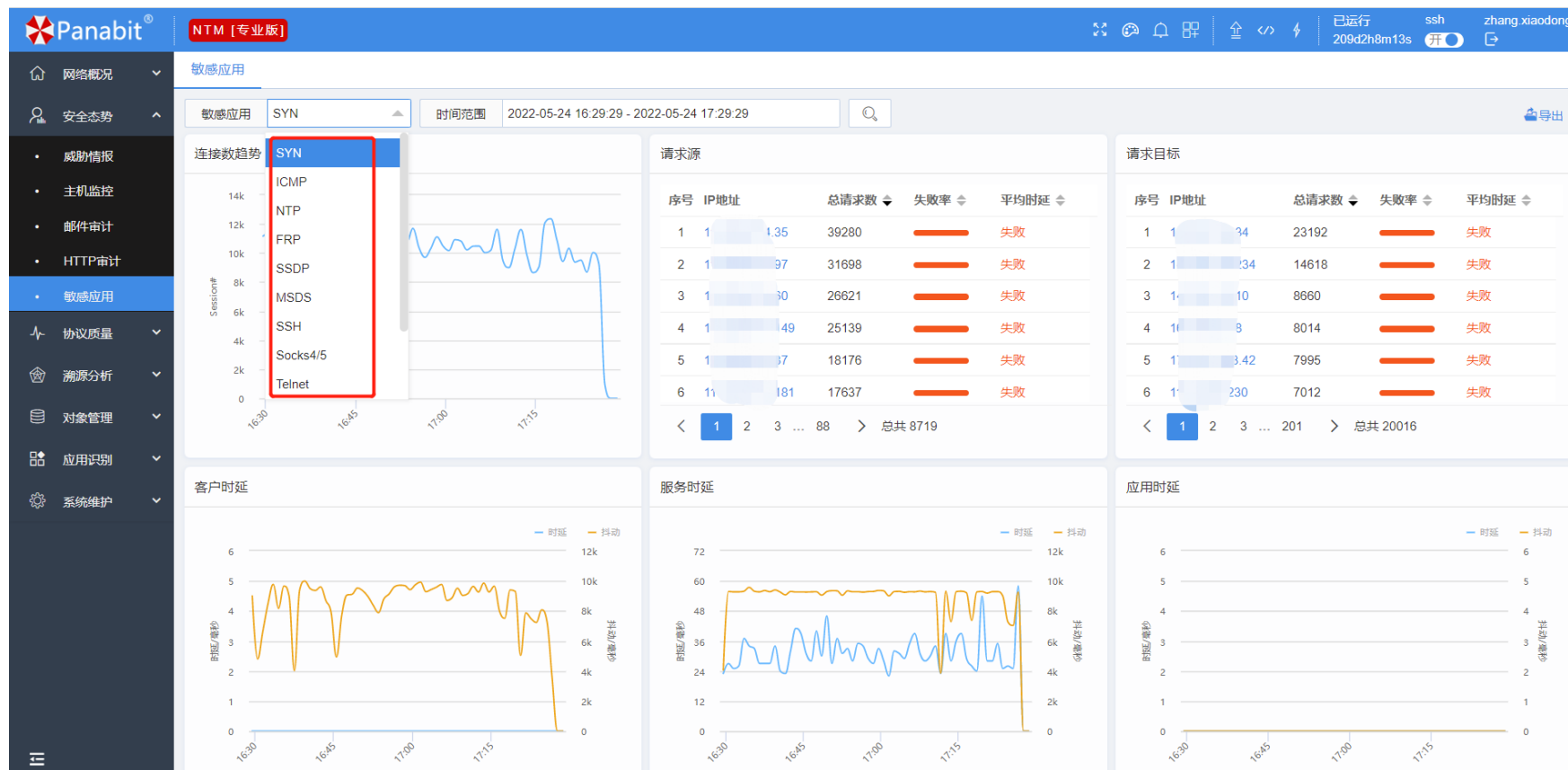
探针/TAP

Panabit探针或TAP分流器，采集数据中心交换机镜像，并将镜像分流给NTM和其他安全产品



NTM

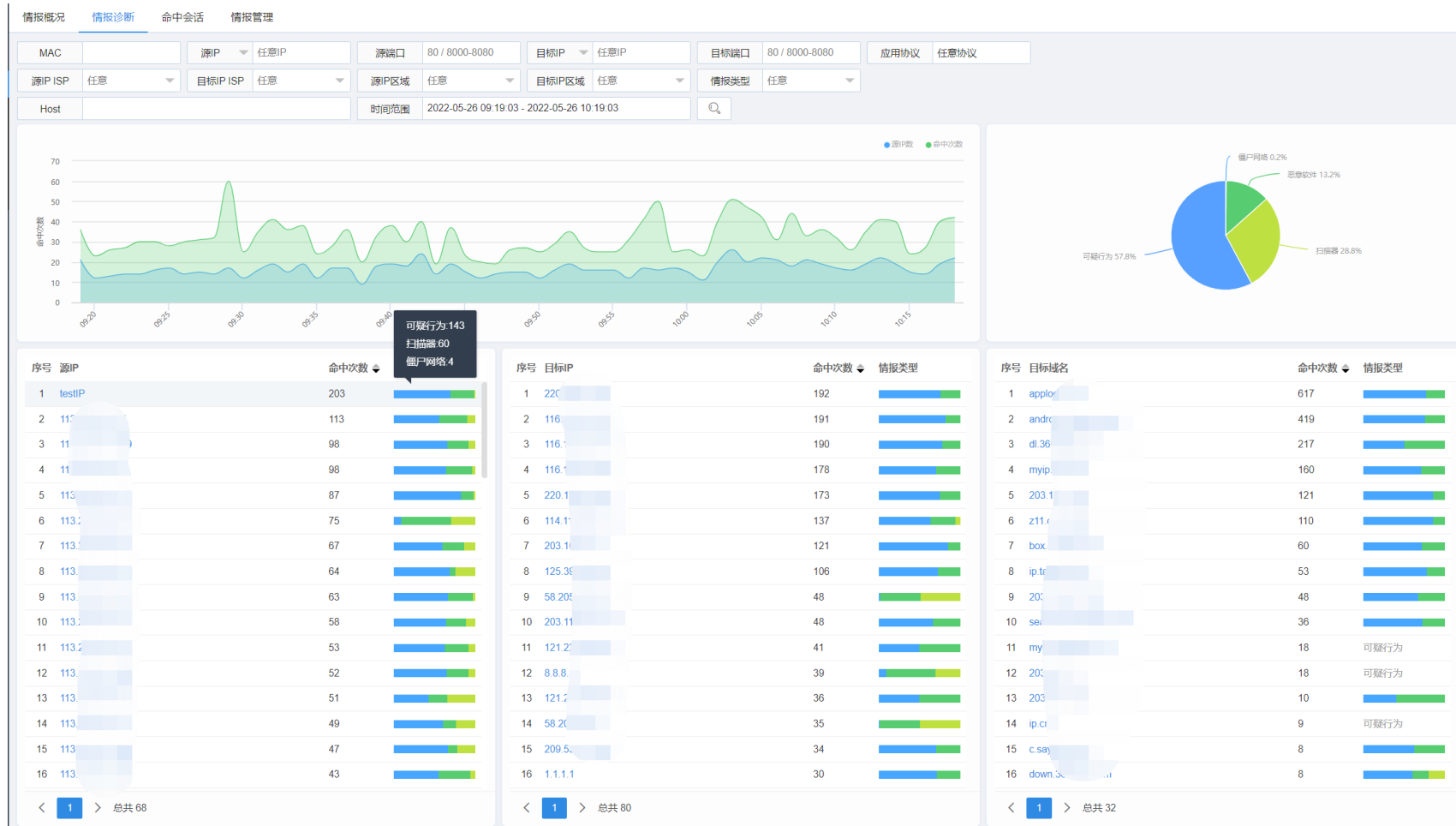
NTM网络全流量溯源系统，对数据中心网络进行可视化分析，主要针对异常安全数据的分析，并对关键业务数据进行原始数据包留存，以便溯源



安全敏感应用智能展现

内网安全异常快速发现

威胁情报命中会话展示

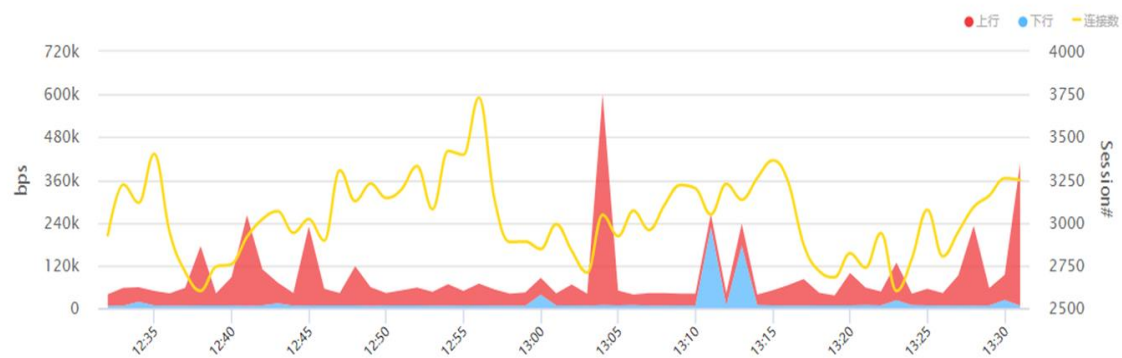


威胁情报命中情况展示

威胁情报命中关系展示

威胁情报命中会话展示

异常行为诊断



序号	源IP	总请求数	上行	下行
1	192.168.1.210	24643	2.49M	0
2	192.168.1.211	16534	1.57M	0
3	10.3.55.19	14395	0	128
4	10.3.17.49	13055	0	0
5	10.3.190.81	5097	341.12K	1.37M
6	10.3.210.83	4005	0	320

序号	目标IP	总请求数	上行	下行
1	10.123.192.156	13055	0	0
2	198.41.0.4	12986	1.36M	6.69K
3	199.7.83.42	12983	1.35M	12.57K
4	8.8.8.8	10380	1.61M	73.29K
5	223.5.5.5	10074	1.59M	0
6	10.3.9.44	6833	84.34K	165.09K

异常应用协议

序号	应用协议	总请求数	上行	下行
1	SYN_ACK	94705	0	0
2	内网IP伪装	71723	25.38M	3.65M
3	无连接TCP	11922	8.06M	904.69K
4	异常域名访问	3441	271.48K	669.31K
5	未知80端口	2161	348.96K	1.38M

< 1 > 总共 5

序号	目标域名	总请求数	上行	下行
1	s	600	39.00K	84.00K
2	x	380	25.55K	53.80K
3	td1	327	21.91K	46.43K
4	异常域名访问	152	12.52K	27.05K
5	www.afdvr.com	130	74.84K	0
6	ATD	120	8.04K	17.04K

< 1 2 3 > 总共 62

⊕ 常见安全协议重点展示

❓ 未知威胁安全隐患定位

≡ 医疗数据泄露及时发现

🔗 终端恶意访问实时掌握

报文播放

播放选项

本地上传

播放网卡: em1

Panabit NTM [专业版]

网络概况

协议质量

溯源分析

会话时延

会话流量

报文播放

IP画像

域名画像

敏感应用

对象管理

应用识别

系统维护

源IP: 任意IP

源端口: 80 / 8000-8080

目标IP: 任意IP

目标端口: 80 / 8000-8080

传输协议: 任意

应用协议: WWW

源IP ISP: 任意

目标IP ISP: 任意

源IP区域: 任意

目标IP区域: 任意

请求域名:

客户时延>= ms

服务时延>= ms

应用时延>= ms

时间范围: 2022-04-22 11:08:38 - 2022-04-22 12:08:38

连接类型: 所有

批量播放

报文播放

播放选项

播放网卡: igb1

播放次数: 1 次

播放速度: 1/8x 1/4x 1/2x 原速 2x 4x 8x 最高

开始

播放信息

文件大小: -

报文数量: -

已发送: -

播放耗时: -

已播放次数: -

单次播放进度: -

1 2 3 4 5 ... 4259 到第 1 页 确定 总共 425840

威胁情报

挖矿分析
木马分析
暗网访问
...

IDS

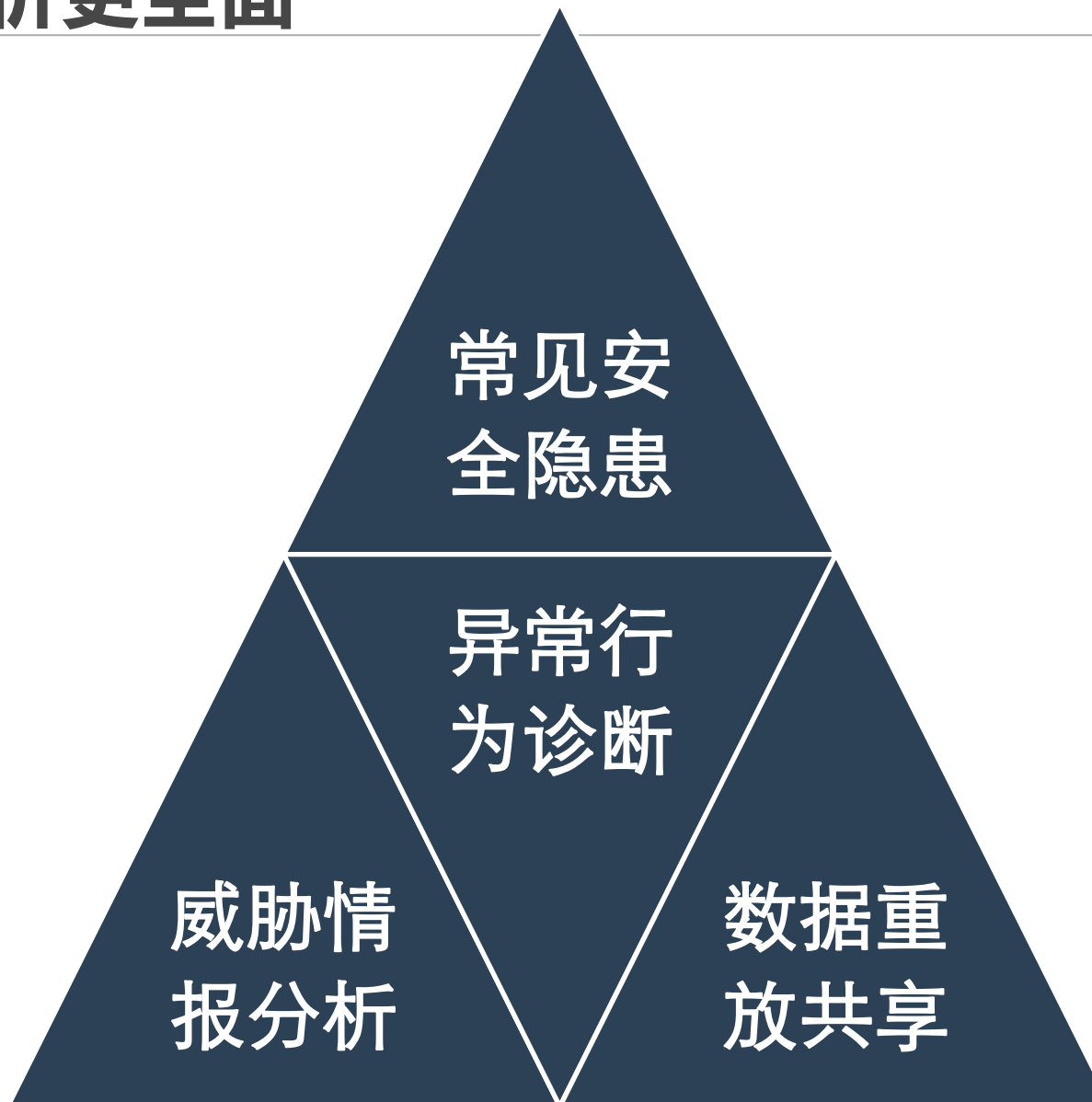
已知病毒
木马审计
...

沙箱

未知行为病毒
木马分析系统
...

...

...





03

数据溯源排查



场景三：数据溯源排查

问题1：假如你是一位警察，有人向您报警说：“昨晚下班后，公司价值5个小目标的卫生纸丢了”，你会进行下列哪些排查？





场景三：数据溯源排查

问题1：假如你是一位警察，有人向您报警说：“昨晚下班后，公司价值5个小目标的卫生纸丢了”，你会进行下列哪些排查？

- 1、封锁现场，对现场进行取证
- 2、查看公司及周围的监控系统，调取当时的录像
- 3、走访物业，询问当时的情况
- 4、走访周围群众，寻找是否有目击者





场景三：数据溯源排查

问题1：假如你是一位警察，有人向您报警说：“昨晚下班后，公司价值5个小目标的卫生纸丢了”，你会进行下列哪些排查？

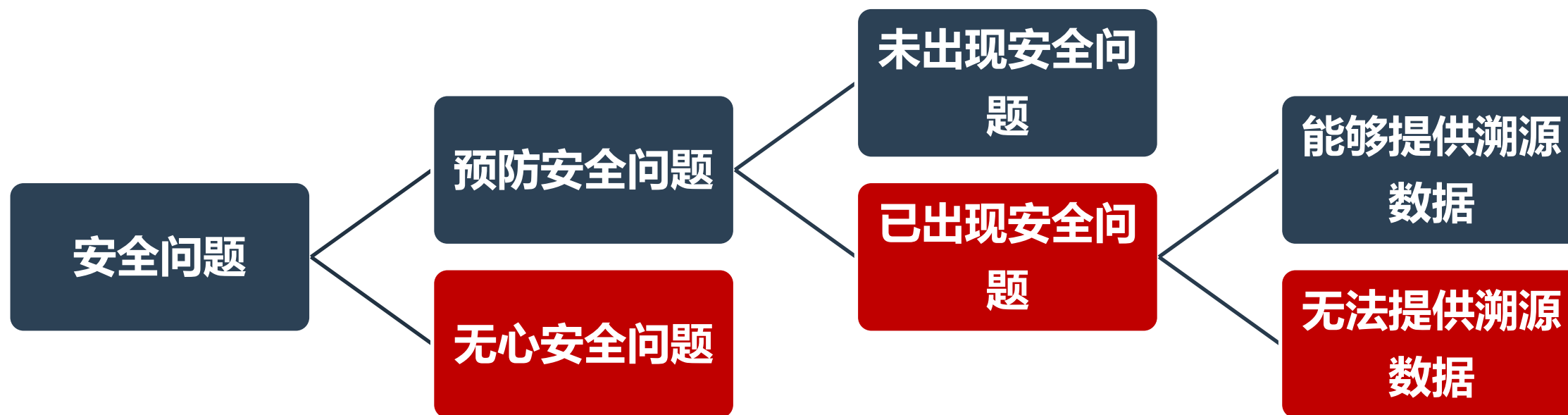
- 1、封锁现场，对现场进行取证
- 2、查看公司及周围的监控系统，调取当时的录像
- 3、走访物业，询问当时的情况
- 4、走访周围群众，寻找是否有目击者



还原案件真实情况

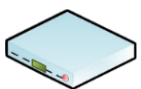
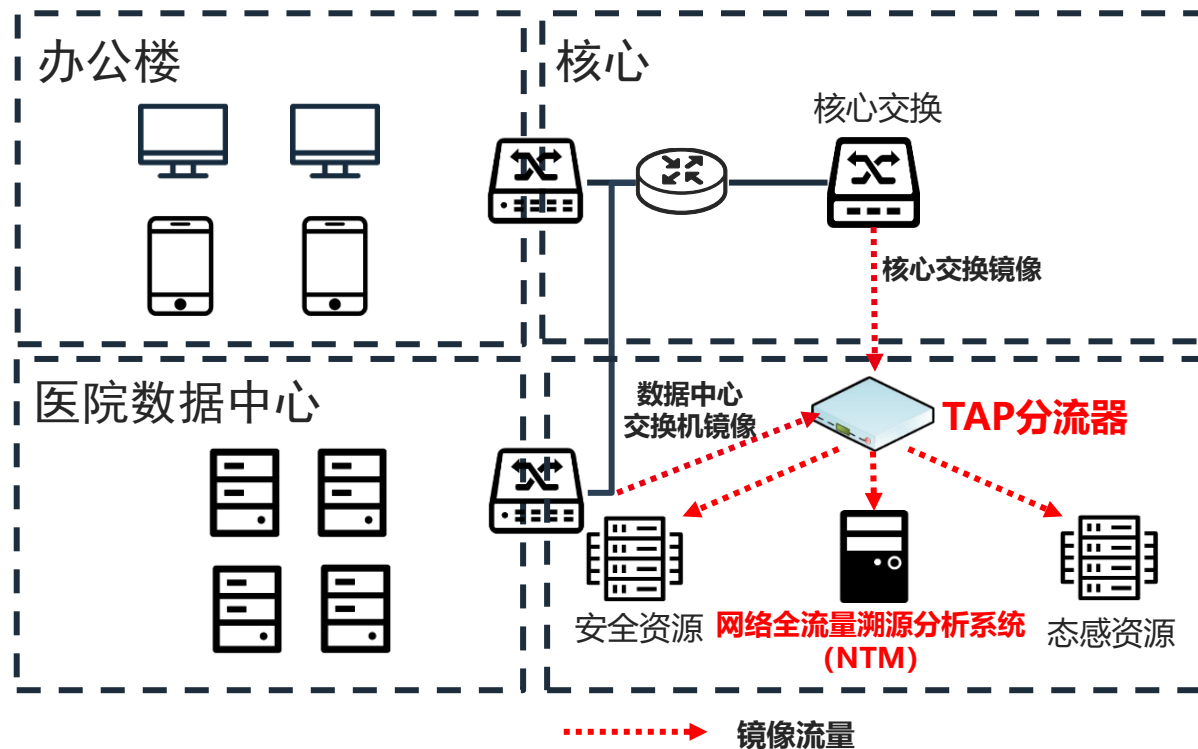


场景三：数据溯源排查





场景三：数据溯源排查



探针/TAP

Panabit探针或TAP分流器，采集数据中心交换机镜像，并将镜像分流给NTM和其他安全产品



NTM

NTM网络全流量溯源系统，对数据中心网络进行可视化分析，主要针对异常安全数据的分析，并对关键业务数据进行原始数据包留存，以便溯源

重要系统原始数据留存



原始数据

源IP

x.x.x.x

源端口

80 / 8000-8080

目标IP

x.x.x.x

目标端口

80 / 8000-8080

传输协议

任意

应用协议

HIS系统

源IP ISP

任意

目标IP ISP

任意

源IP区域

任意

目标IP区域

任意

请求域名

客户时延>=

0

服务时延>=

0

应用时延>=

ms

时间范围

2021-07-06 09:56:57 - 2021-07-06 10:56:57

Q

序号	请求时间	源IP	目标IP	目标地理位置	传输协议	应用协议	客户时延	服务时延	应用时延	流量(前10秒)	请求域名	操作
1	2021-07-06/10:11:54	192.168.8.100:51316	192.168.2.251:3911		TCP	HIS系统	0.1	0.12	1.77	1892/11646	192.168.2.251 200	数据包
2	2021-07-06/10:11:54	192.168.8.100:51315	192.168.2.251:80		TCP	HIS系统	0.1	0.12	29.75	1764/5480	192.168.2.251 200	数据包
3	2021-07-06/10:13:46	192.168.10.177:50143	192.168.2.251:80		TCP	HIS系统	18.88	0.13	31.33	1062/48874	192.168.2.251 200	数据包
4	2021-07-06/10:15:53	192.168.10.102:50509	192.168.2.251:3910		TCP	HIS系统	3.34	0.15	0.84	12272/30430	192.168.2.251 200	数据包
5	2021-07-06/10:15:54	192.168.10.156:10886	192.168.2.251:3910		TCP	HIS系统	6.28	0.14	0.86	6786/8538	192.168.2.251 200	数据包
6	2021-07-06/10:16:16	192.168.10.102:50528	192.168.2.251:53048		TCP	HIS系统	2.3	0.12	1.03	2266/2816	192.168.2.251 200	数据包
7	2021-07-06/10:16:16	192.168.10.156:10932	192.168.2.251:53048		TCP	HIS系统	1.09	0.12	0.78	2266/2816	192.168.2.251 200	数据包
8	2021-07-06/10:16:16	192.168.10.156:10933	192.168.2.251:53048		TCP	HIS系统	2.34	0.11	1.06	2266/2816	192.168.2.251 200	数据包
9	2021-07-06/10:16:16	192.168.10.156:10931	192.168.2.251:53048		TCP	HIS系统	1.66	0.13	1.18	2266/2816	192.168.2.251 200	数据包
10	2021-07-06/10:16:17	192.168.10.102:50529	192.168.2.251:53048		TCP	HIS系统	2	0.11	0.96	2266/2816	192.168.2.251 200	数据包
11	2021-07-06/10:16:17	192.168.10.102:50530	192.168.2.251:53048		TCP	HIS系统	2.3	0.12	0.96	2266/2816	192.168.2.251 200	数据包
12	2021-07-06/10:16:17	192.168.10.156:10935	192.168.2.251:53048		TCP	HIS系统	1.64	0.12	0.75	2266/2816	192.168.2.251 200	数据包
13	2021-07-06/10:16:17	192.168.10.156:10934	192.168.2.251:53048		TCP	HIS系统	5.9	0.12	0.75	2266/2816	192.168.2.251 200	数据包
14	2021-07-06/10:16:17	192.168.10.102:50531	192.168.2.251:53048		TCP	HIS系统	2.56	0.12	0.7	2266/2816	192.168.2.251 200	数据包
15	2021-07-06/10:16:18	192.168.10.102:50532	192.168.2.251:53048		TCP	HIS系统	2.4	0.12	0.69	2266/2816	192.168.2.251 200	数据包

<

1

>

到第

1

页

确定

总共 58



完整留存重要数据

报文解析 报文交互 元数据 报文播放 应用层

连接时间	2022-04-12 10:40:04 - 2022-04-12 10:40:04	协议	TCP
源MAC	00:50:00:00:00:00:99:e9	目标MAC	88:df:c6:00:00:00:2a:01
源IP:端口	10.3.9.162:25292	目标IP:端口	10.3.9.100:80
源	Packets: 26 Bytes: 3160 Databytes: 1324	目	Packets: 30 Bytes: 32306 Databytes: 30190
TCP Flags	SYN: 4, SYN_ACK: 0, ACK: 52, FIN: 0, PSH: 0, RST: 0, URG: 0		
Status code	200	Method	GET
Host	www.163.com	Cookie	
Referer		X-forward	2001:da8:2::2b61:d9f7
User-Agent		URL	/images/ztrrg.png HTTP/1.0

交互过程

Source	Destination
88 df 9e 39 2a 01 00 50 56 80 99 e9 81 00 0f a9 08 00 45 00 00 3c f7 8f 40 00 40 06 f0 20 0a 03 09 a2 0a 03 35 64 62 cc 00 50 c8 ee 7f 52 00 00 00 00 a0 02 39 08 de 36 00 00 02 04 05 b4 04 02 08 0a a9 78 88 dd 00 00 00 00 01 03 03 09	Num: 1. 2022/04/12 10:40:04 78 bytes ...9*..PV..... ..E.....@..5db..P...R.. ...9..6..... ...X.....



原始数据包随时查看



The screenshot displays the Panabit NTM (Professional Edition) web interface. The main menu on the left includes options like '网络概况' (Network Overview), '协议质量' (Protocol Quality), '溯源分析' (Source Analysis), '数据抓包' (Data Capture), '质量诊断' (Quality Diagnosis), '流量诊断' (Traffic Diagnosis), '会话时延' (Session Delay), '会话流量' (Session Traffic), '报文播放' (Packet Playback), 'IP画像' (IP Profile), '域名画像' (Domain Profile), '敏感应用' (Sensitive Applications), '对象管理' (Object Management), '应用识别' (Application Identification), and '系统维护' (System Maintenance). The '会话时延' (Session Delay) section is active, showing a list of sessions with columns for '源IP' (Source IP), '源端口' (Source Port), '目标IP' (Destination IP), '目标端口' (Destination Port), '传输协议' (Transport Protocol), '应用协议' (Application Protocol), '客户时延' (Client Delay), '服务时延' (Service Delay), '应用时延' (Application Delay), '时间范围' (Time Range), '连接类型' (Connection Type), and '状态' (Status). A red box highlights the '报文播放' (Packet Playback) button in the top right corner of the session list.

A modal window titled '报文播放' (Packet Playback) is open, showing the '播放选项' (Playback Options) and '播放信息' (Playback Information) sections. The '播放选项' section includes a '播放网卡' (Playback Network Card) dropdown set to 'igb1', a '播放次数' (Playback Count) input set to '1', and a '播放速度' (Playback Speed) slider set to '原速' (Original Speed). A '开始' (Start) button is visible. The '播放信息' section displays details about the playback process, including '文件大小' (File Size), '报文数量' (Packet Count), '已发送' (Sent), '播放耗时' (Playback Time), '已播放次数' (Already Played Count), and '单次播放进度' (Single Playback Progress).

In the background, the '会话时延' (Session Delay) table is visible, showing a list of sessions with columns for '源IP', '源端口', '目标IP', '目标端口', '传输协议', '应用协议', '客户时延', '服务时延', '应用时延', '时间范围', '连接类型', and '状态'. A red arrow points from the '报文播放' button in the top right corner of the session list to the '开始' (Start) button in the '报文播放' modal window.

The bottom of the interface shows a pagination bar with '1' selected, indicating the first page of results. The total number of items is 425840.



批量播放

文件还原



报文解析 报文交互 应用协议: WWW 报文下载 内容下载

http

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	0.24	209	TCP	78	36302 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1462282903 TSecr=0 WS=128
2	0.018677	209	24	TCP	78	80 → 36302 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1456 SACK_PERM=1 TSval=3731791363 TSecr=1462282903 WS=6
3	0.018947	24	209	TCP	70	36302 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1462282922 TSecr=3731791363
4	0.019015	24	209	HTTP	310	GET /w...
5	0.038333	209	24	TCP	70	80 → 36302 [ACK] Seq=1 Ack=241 Win=15552 Len=0 TSval=3731791368 TSecr=1462282922
6	0.039200	209	24	HTTP	287	HTTP/1.1 200 OK

源IP 任意IP 源端口 80 / 8000-8080 目标IP 任意IP 目标端口 80 / 8000-8080 传输协议 任意 应用协议 任意协议

源IP ISP 任意 目标IP ISP 任意 源IP区域 任意 目标IP区域 任意 请求域名

客户时延>= ms 服务时延>= ms 应用时延>= ms 时间范围 2022-03-18 12:38:21 - 2022-03-18 13:38:21 连接类型 所有

请求时间	源IP	目标IP	目标地理位置	传输协议	应用协议	客户时延	服务时延	应用时延	流量(前10秒)	请求域名	状态	操作	
2022-03-18/12:38:21		4500	3103	北京 联通	UDP	未知应用	0	0	0	0/279	-	失败	数据包
2022-03-18/12:38:22		0:51251	27:8081	天津 BGP	TCP	火影使者	27.22	7.16	7.54	836/161	-		数据包
2022-03-18/12:38:22		87:57949	22:53	北京 教育网	UDP	DNS	0	0	0	202/0	lb	0.10... 失败	数据包
2022-03-18/12:38:22		87:61316	22:53	北京 教育网	UDP	DNS	0	0	0	174/0	187	ad... 失败	数据包
2022-03-18/12:38:22		122:57557	000	广东深圳 电信	UDP	未知应用	0	0	45.15	724/636	-		数据包
2022-03-18/12:38:22		156:24099	4:53	114DNS.COM	UDP	DNS	0	0	91.05	96/541	eg t...		数据包
2022-03-18/12:38:22		156:12767	4:53	114DNS.COM	UDP	DNS	0	0	1.68	82/482	ga	i.c...	数据包
2022-03-18/12:38:22		156:47072	1:8080	广东深圳 BGP	TCP	企业微信	18.89	43.25	49.5	447/352	-		数据包
2022-03-18/12:38:23		165:138	255:138		UDP	NETBIOS	0	0	0	486/0	-	失败	数据包
2022-03-18/12:38:23		52:47088	114:53	114DNS.COM	UDP	DNS	0	0	69.4	237/1429	r		数据包
2022-03-18/12:38:23		128:61445	3:443	北京 电信	TCP	百度搜索	16.79	3.73	0	0/0	-	失败	数据包
2022-03-18/12:38:23		5:50251	38:11520		TCP	迅捷2003	1.06	0.24	3.34	9312/4538	-		数据包
2022-03-18/12:38:23		160:45494	9:22		TCP	SSH	1767.39	0.06	456.45	1669/2979	-		数据包
2022-03-18/12:38:23		24:36302	209:80	山东青岛 BGP	TCP	WWW	0.27	18.67	20.18	310/287	1	200	数据包

< 1 2 3 4 5 ... 733 > 到第 1 页 确定 总共 73280



真实还原数据文件



数据重放回溯重演

真实还原数据文件

原始数据包随时查看

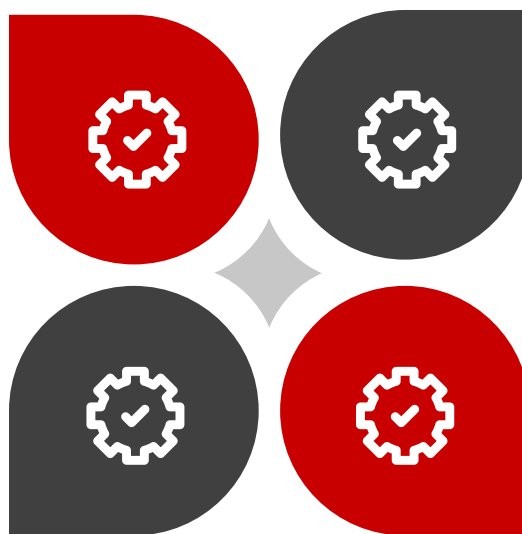
完整记录重要数据

关键业务访问监控

对业务系统访问情况实时监控，重点关注TOP访问，随时掌握关键业务服务状态。

安全异常分析

基于网络异常行为，对安全隐患流量快速发现，并进行内网隐患点（扫描、攻击、勒索等）快速定位。



业务卡顿快速排障

监测网络时延情况，1分钟快速排障，记录原始事件日志，以备后续排查。

数据溯源排查

对关键性、敏感性数据进行原始数据包留存，用于数据分析、溯源排查、文件还原。



Panabit服务号



Panabit订阅号



Panabit视频号



2022

畅享连世界

THANK YOU