

电商与威胁情报

—纪舒瀚(HS)

我是谁

- 姓名：纪舒瀚
- id：H5
- 汽车之家安全负责人，自0到1
- 阿里巴巴，淘宝安全，双11、双12

Autokhome

论坛、电商、车金融、后市场

11.11
疯狂购车节
拒绝猫腻 买车来汽车之家

截至11月11日24:00

订单总量
134225
辆

交易总额
196.92
亿元

客单价
14.67
万元

大纲

- 企业安全的理解
- 电商的威胁
- 感知风险，情报价值
- 安全着陆

企业面临的问题

- 安全现状是什么？
- 如何体现安全团队价值？
- 如何量化价值？
- 没有安全漏洞，就是真的没有风险么？

企业内部

- 管理机制：人VS(人or机器)
- 标准化流程
- 技术力量
- 安全与业务的对抗
- 最终交付的安全状态

提升安全感知能力

电商风险





危机四伏

- 信息泄露、诈骗
- 恶意交易
- 薅羊毛
- 入侵，脱裤，黑产

内部一样惊险

- 业务裸奔
- 人 意识淡薄
- 外包情况严重
- 频繁变更

对手，知己知彼

情报

- 小道消息？
- **src**
- 众测、扫描器
- 可视化监控

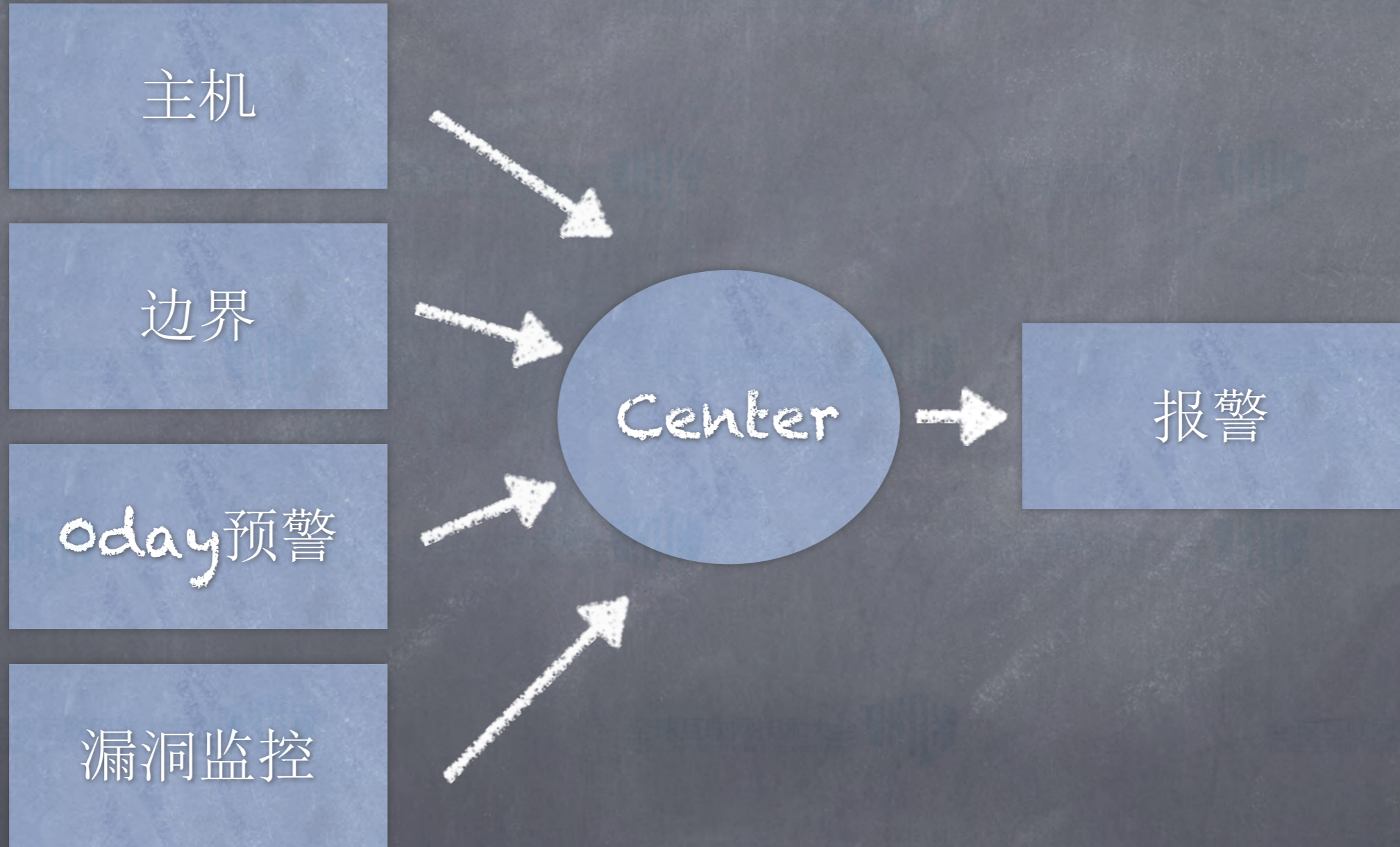
甲方安全

- 防火墙
- WAF
- IDS/IPS
- SOC
- ...

甲方安全

- 边界
- 业务应用
- 主机
- 数据

防御监控



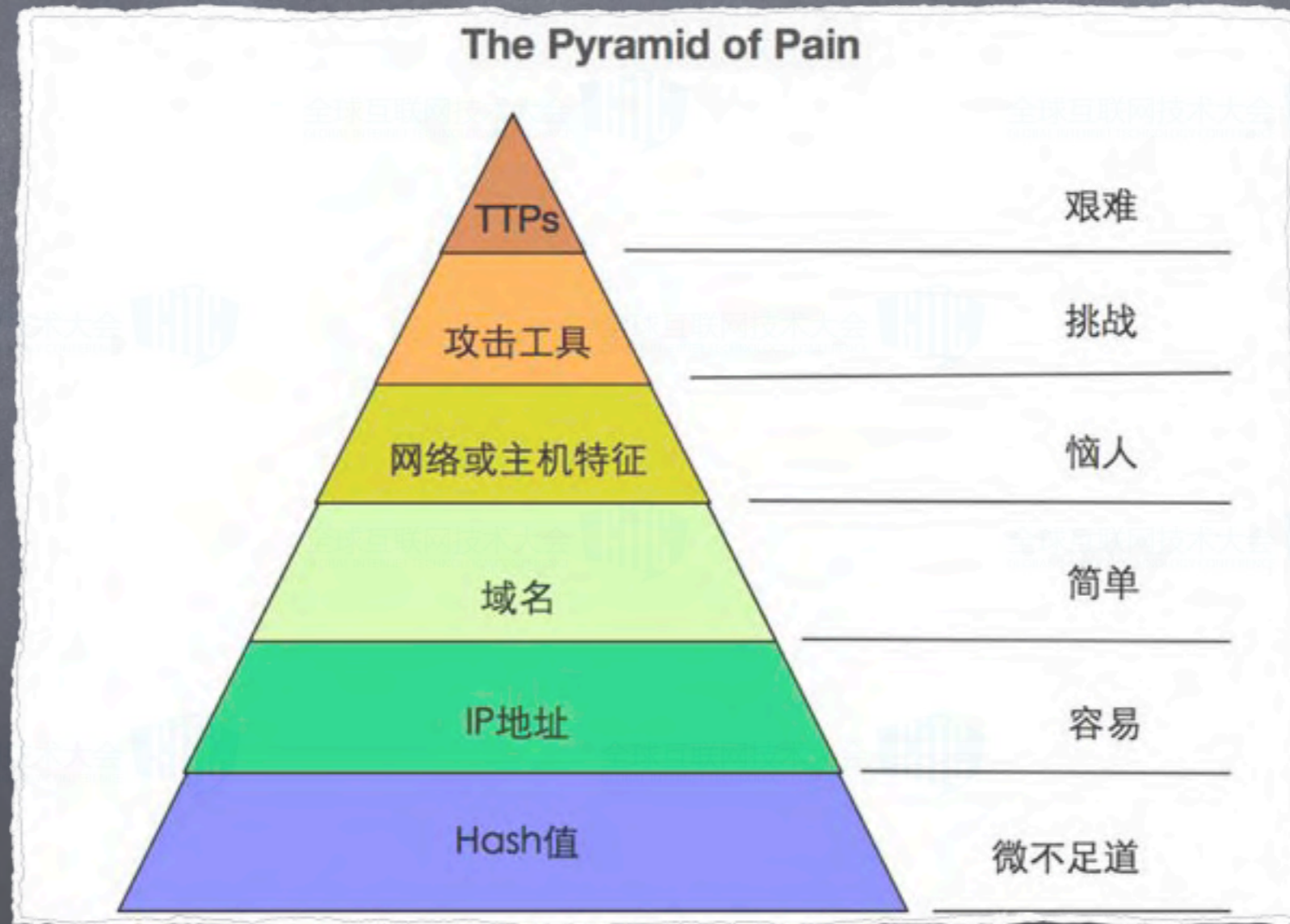
情报联动

- 防御多样化
- 监控可视化
- 响应自动化



止损及时

威胁情报金字塔



安全着陆

- 防御→监控→响应
- 花样式布点
- 报警→止损(自动化)

举个栗子

基本框架



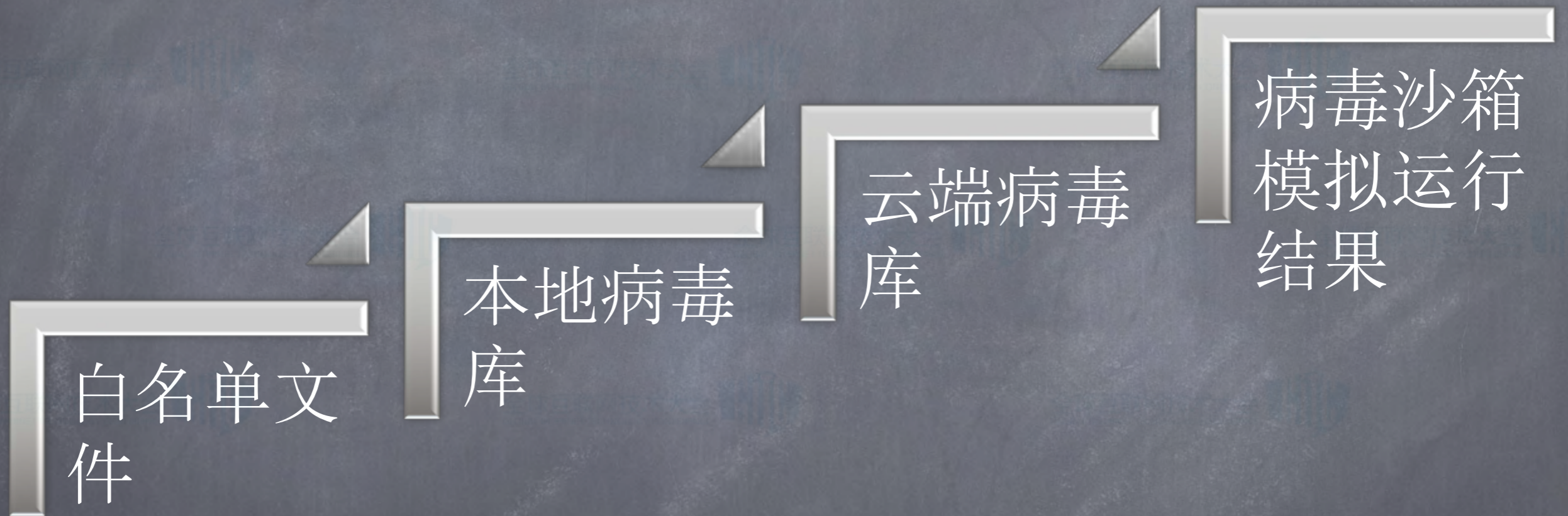
Agent



中转服务器构成



中转处理结果升级



处理效率

Agent
端

15分钟增量
扫描

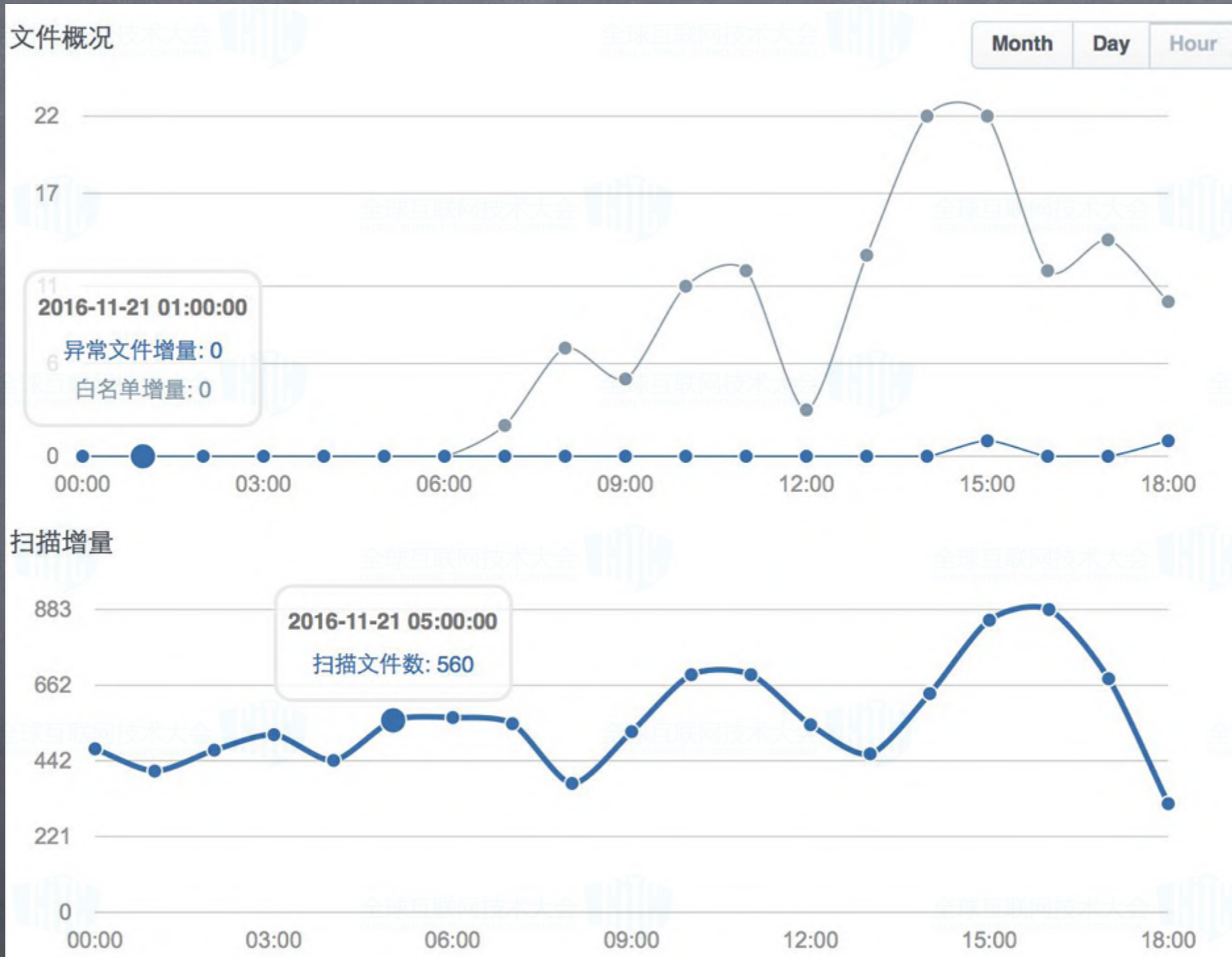
30天全盘扫
描

中转

实时检测
Agent提交
的数据

60天本地病
毒库更新

扫描动态图



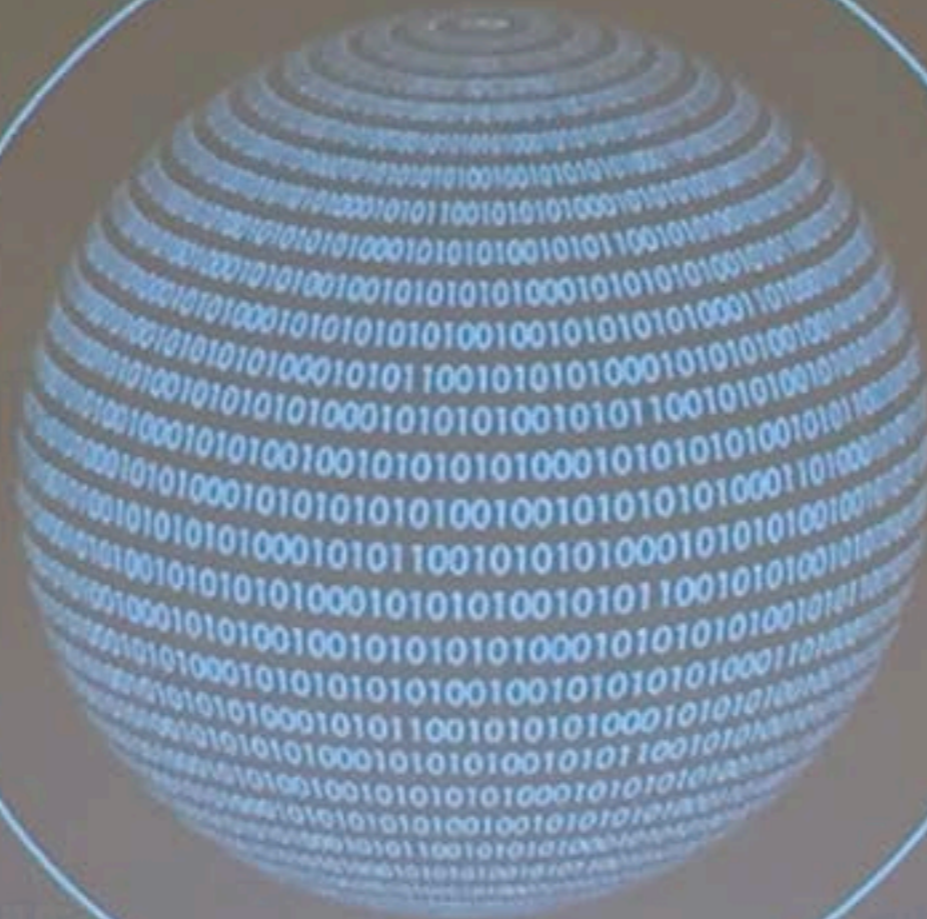
检测报告:

序号	杀毒引擎	结果	update	version
1	Avast	safe	2011-10-24	2011-10-24
2	Avira	safe	2011-10-24	2011-10-24
3	Avast	safe	2011-10-24	2011-10-24
4	Avast	safe	2011-10-24	1.0.0
5	Avast	TR/Taranis.2676	2011-10-24	2011-10-24
6	Avast	safe	2011-10-24	2011-10-24
7	Avast	Trojan-Downloader(004e02c41)	2011-10-24	2011-10-24
8	Avast	safe	2011-10-24	2011-10-24
9	Avast	safe	2011-10-24	2011-10-24
10	Avast	safe	2011-10-24	2011-10-24
11	Avast	safe	2011-10-24	2011-10-24
12	Avast	Trojan horse Downloader.Generic14.ANYP	2011-10-24	2011-10-24
13	Avast	safe	2011-10-24	2011-10-24
14	Avast	safe	2011-10-24	2011-10-24
15	Avast	Gen:Variant.Symmi.63060	2011-10-24	2011-10-24
16	Avast	safe	2011-10-24	2011-10-24
17	Avast	QVM07.1.Malware.Gen	2011-10-24	2011-10-24
18	Avast	a variant of Win32/TrojanDownloader.Agent.CEN trojan	2011-10-24	2011-10-24
19	Avast	safe	2011-10-24	2011-10-24

回归业务

NEW REQUIREMENTS

BUSINESS
CONTEXT



UNIFIED
IDENTITY



COMPLETE
VISIBILITY

我们的交付

威胁的先扬后抑，寻找对抗的平衡点

谢谢