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

Autohome

论坛、电商、车金融、后市场

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


M880
ProxCard® II


又有“大鱼”上钩啦！

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

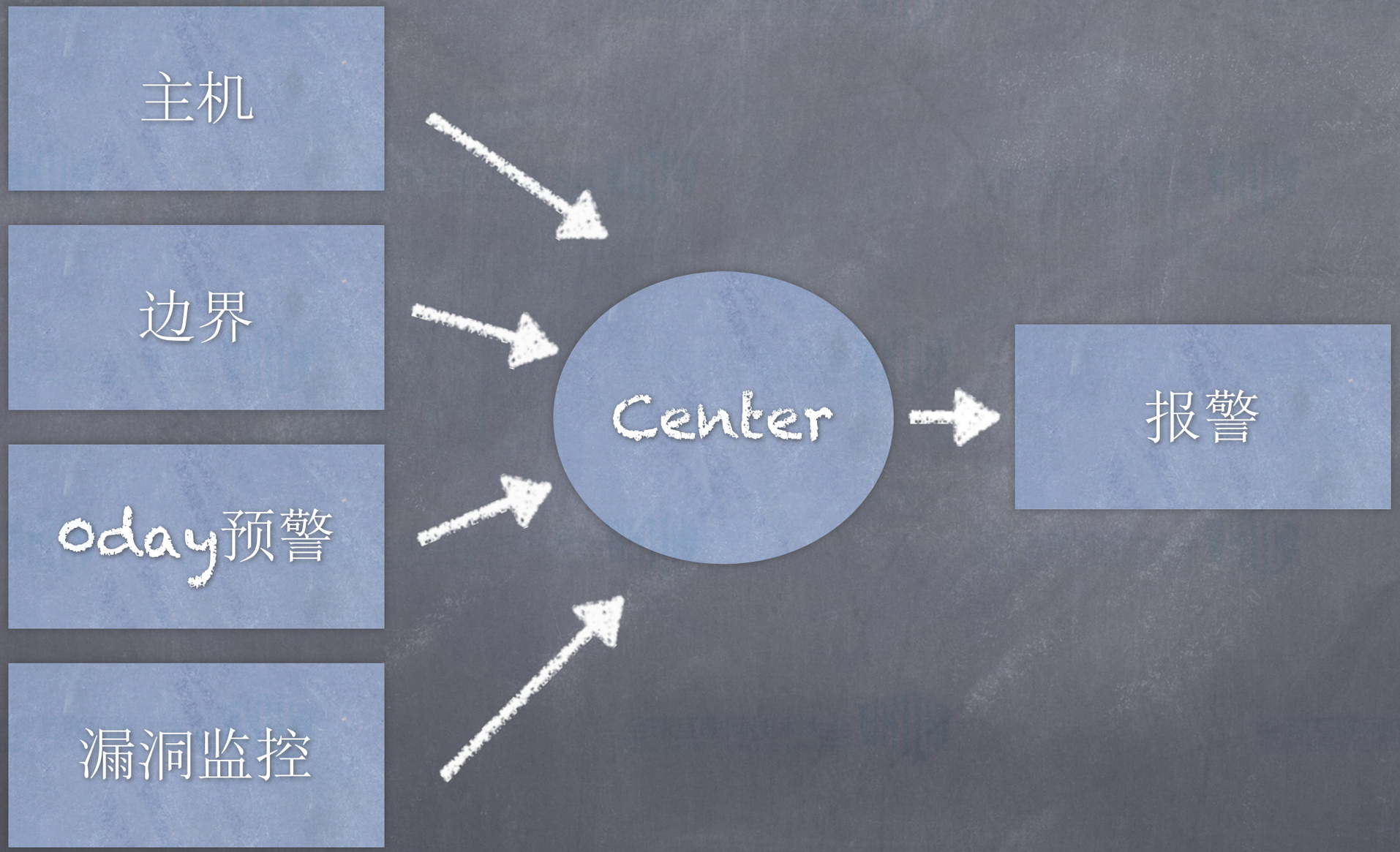
甲方安全

- 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

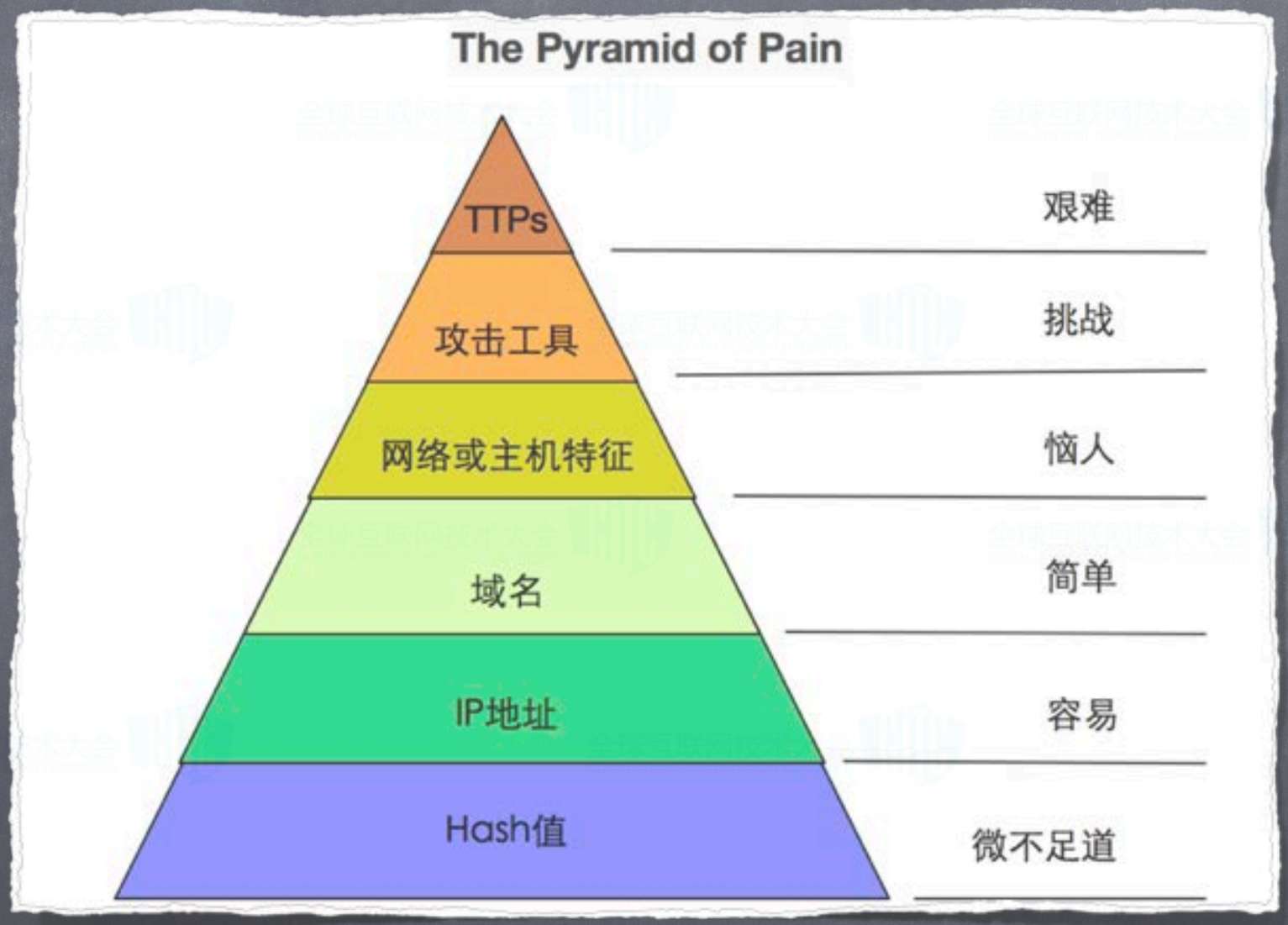


情报联动

- 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

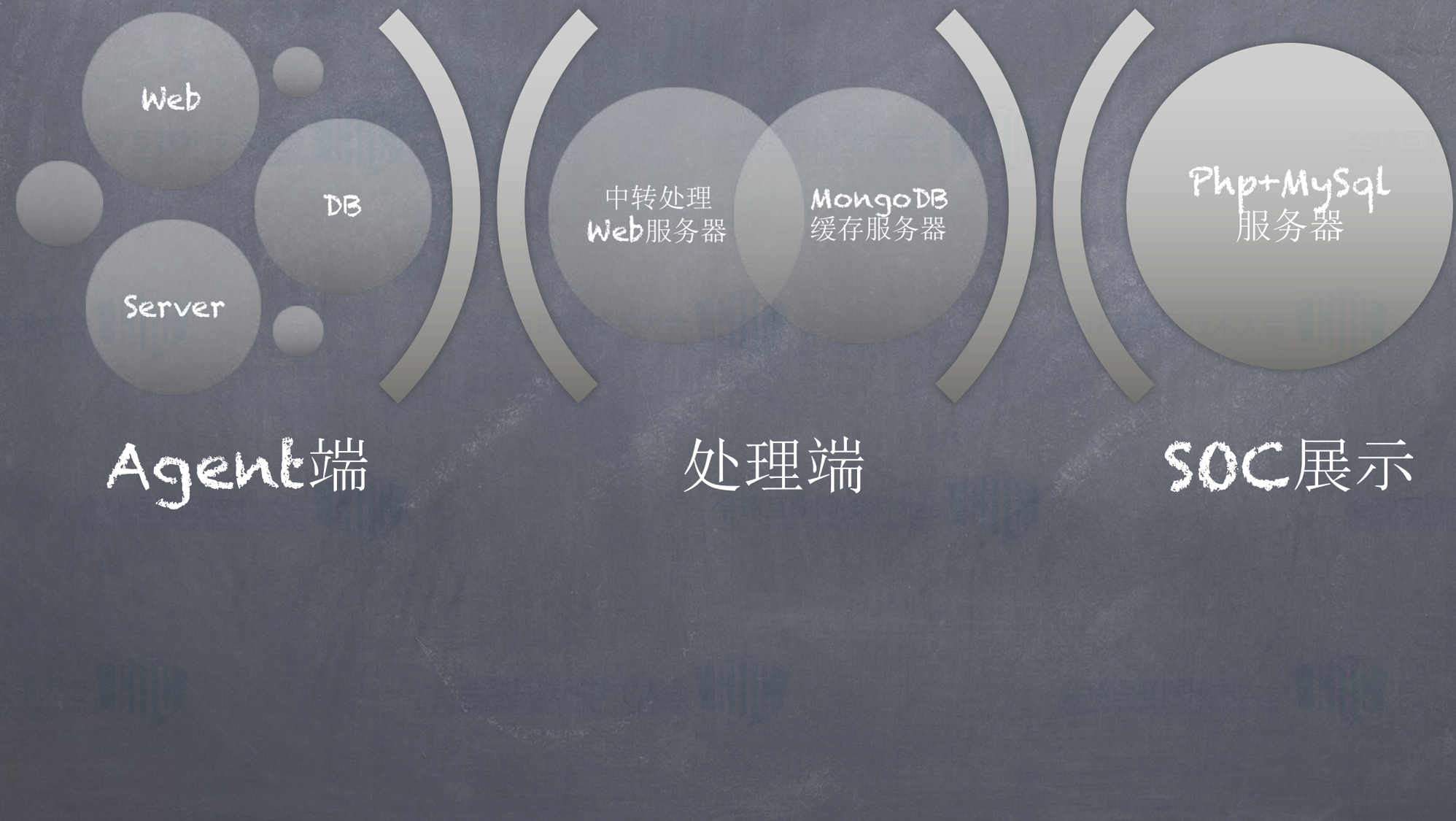

The Pyramid of Pain
TTPs
攻击工具
网络或主机特征
域名
IP地址
Hash值
艰难
挑战
恼人
简单
容易
微不足道

安全着陆

- 防御->监控->响应
- 花样式布点
- 报警->止损(自动化)

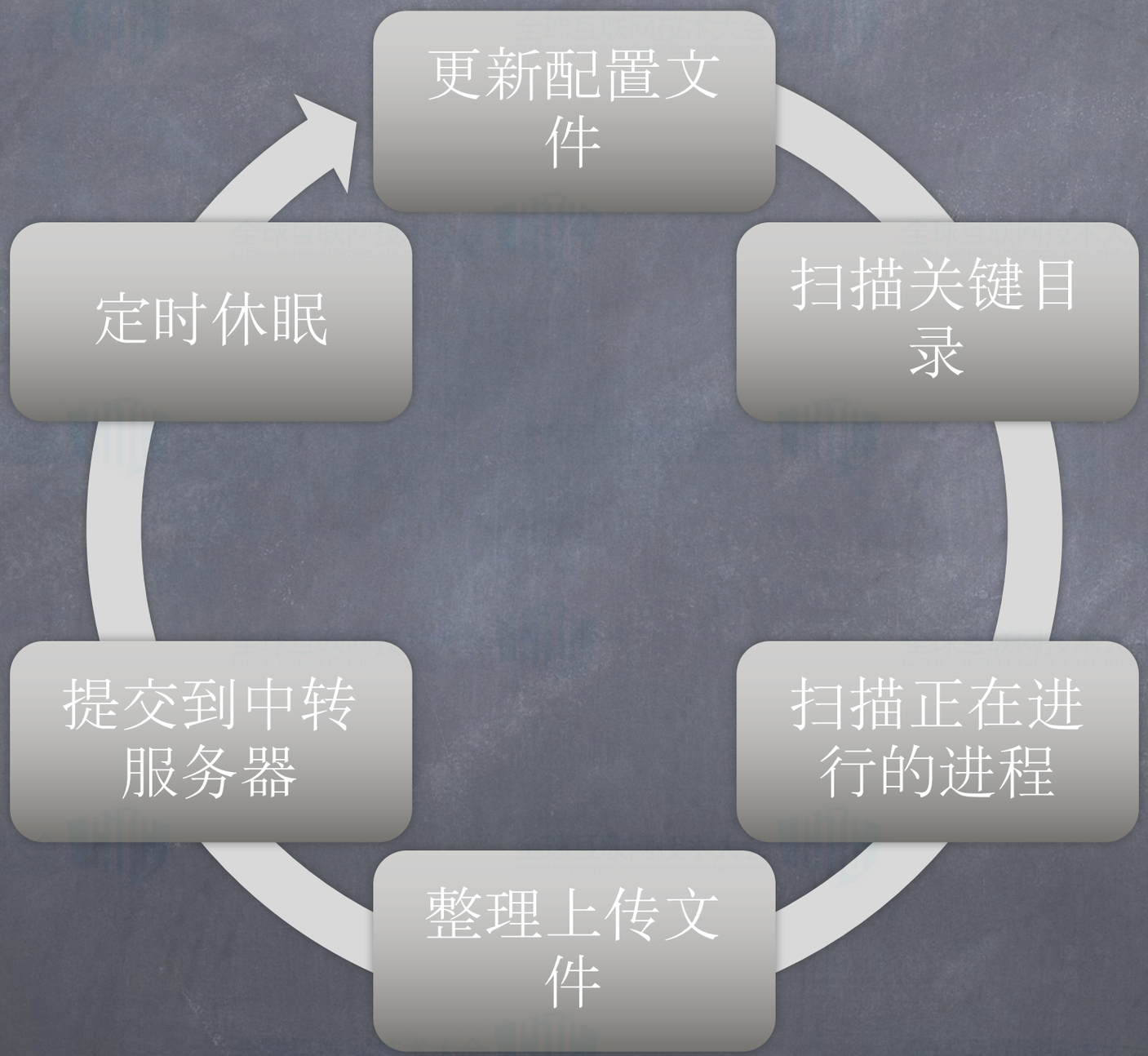
举个栗子

基本框架



Agent端　　处理端　　SOC展示

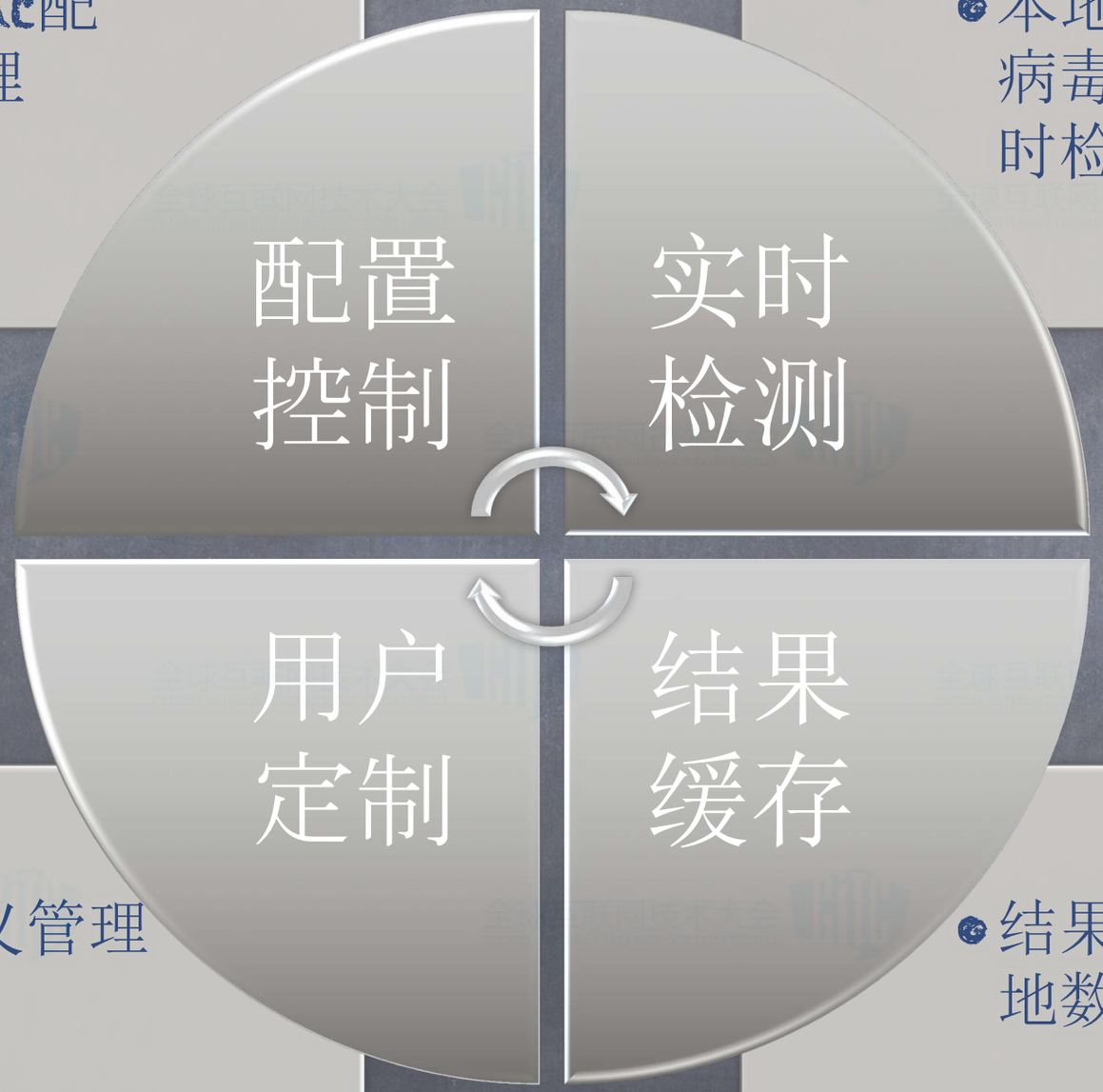
Agent



中转服务器构成

- Agent配置管理

- 本地+云端病毒库 实时检测



- 自定义管理

- 结果缓存本地数据库

中转处理结果升级

白名单文件

本地病毒库

云端病毒库

病毒沙箱模拟运行结果

处理效率

Agent端

15分钟增量扫描

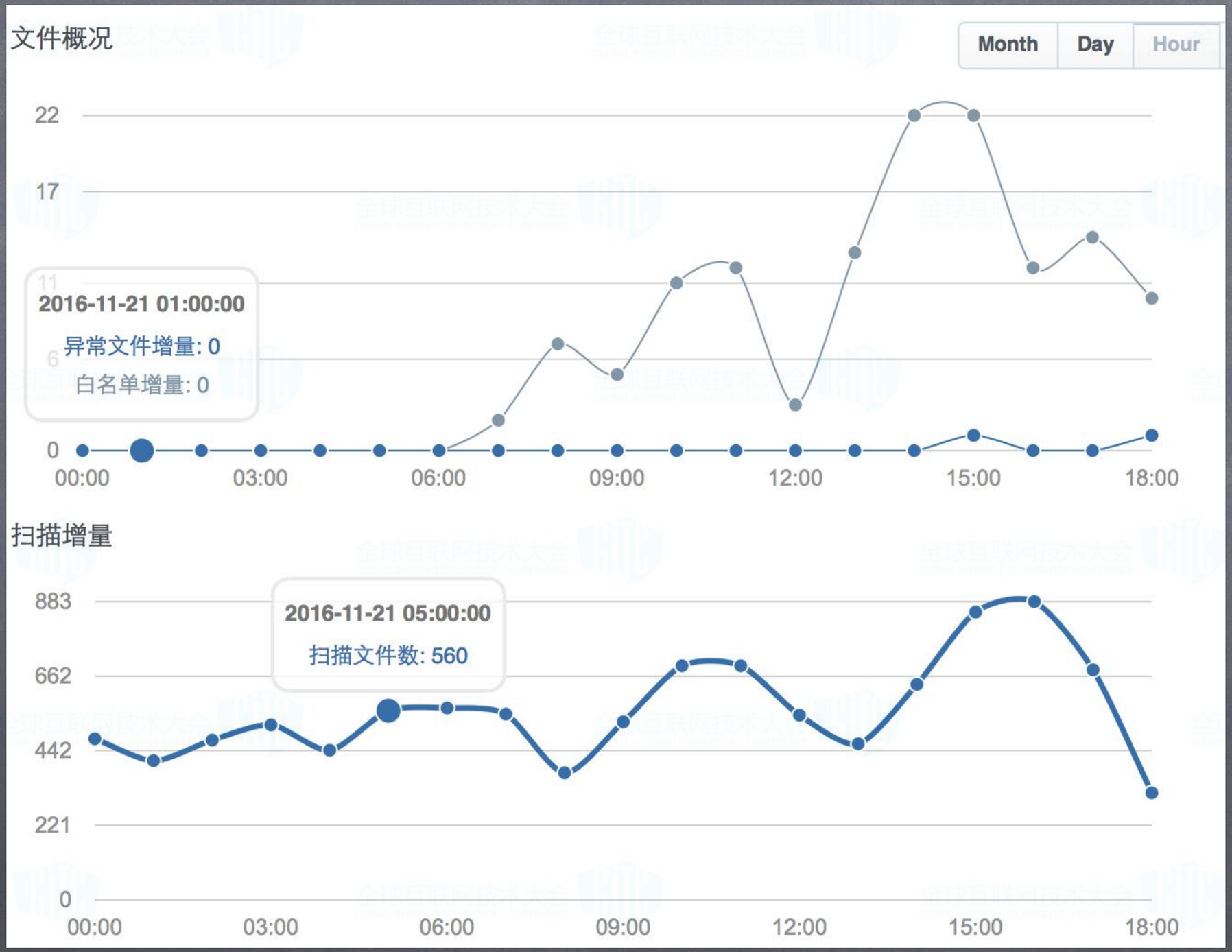
30天全盘扫描

中转

实时检测Agent提交的数据

60天本地病毒库更新

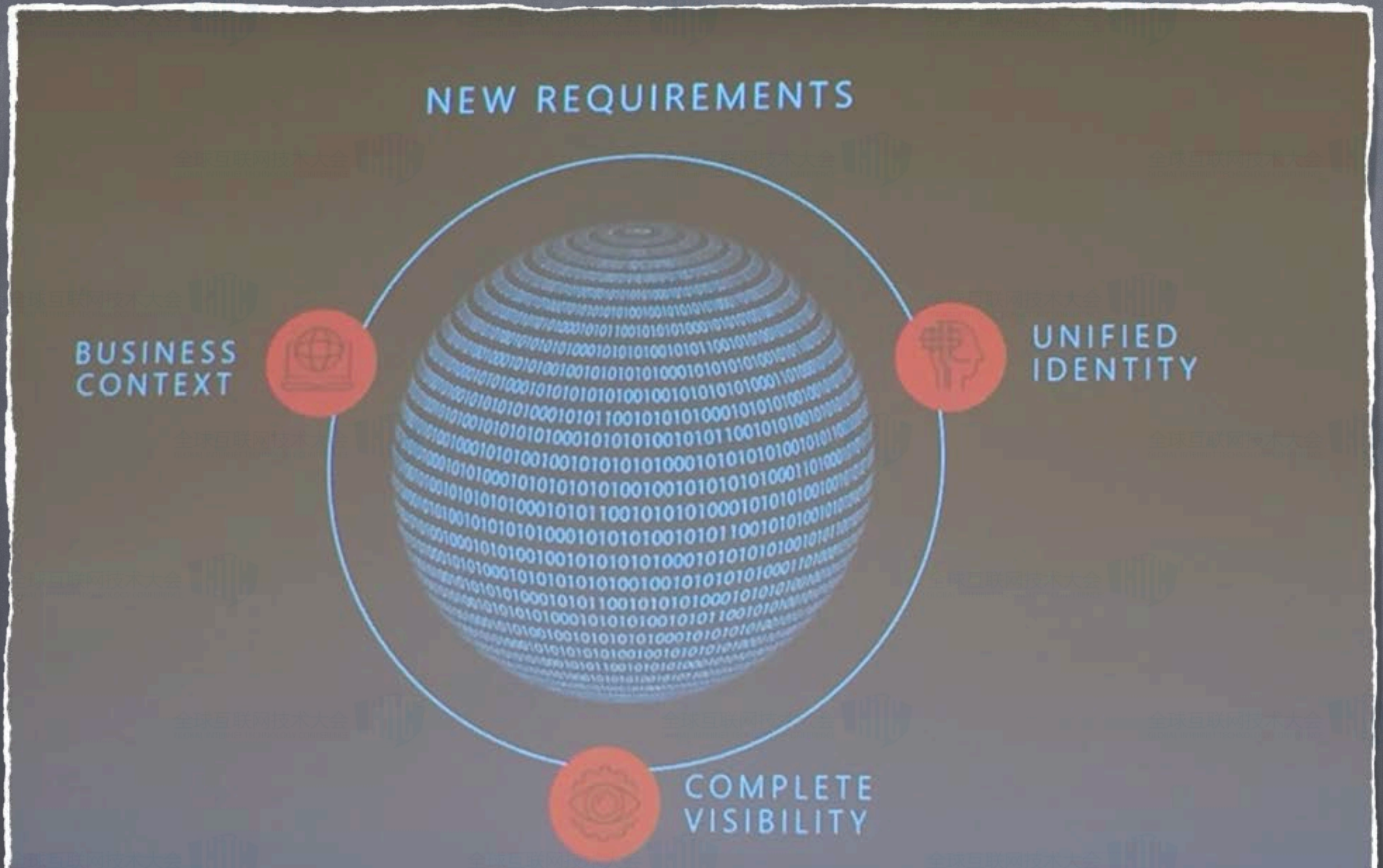
扫描动态图


文件概况
Month
Day
Hour
22
17
11
6
0
2016-11-21 01:00:00
异常文件增量: 0
白名单增量: 0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
扫描增量
883
662
442
221
0
2016-11-21 05:00:00
扫描文件数: 560
00:00
03:00
06:00
09:00
12:00
15:00
18:00

检测报告:

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

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