KNOWNSEC
知 道 创 宇

大数据与新一代的信息安全

知道创宇　彭 戈

议程

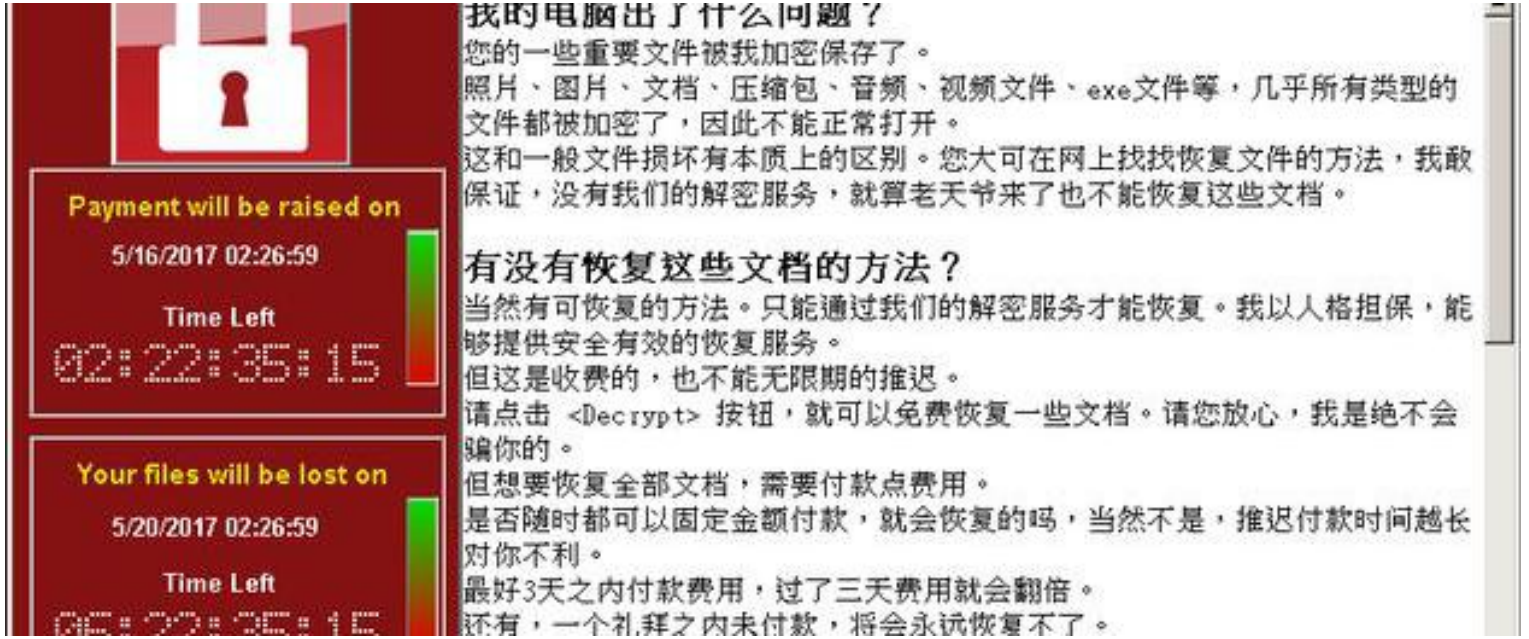
- 数据感知风险
- 大数据分析与应用

知道

新一代的信息安全！

没有一个人或组织可以独善其身，整个网络空间整个社会息息相关！

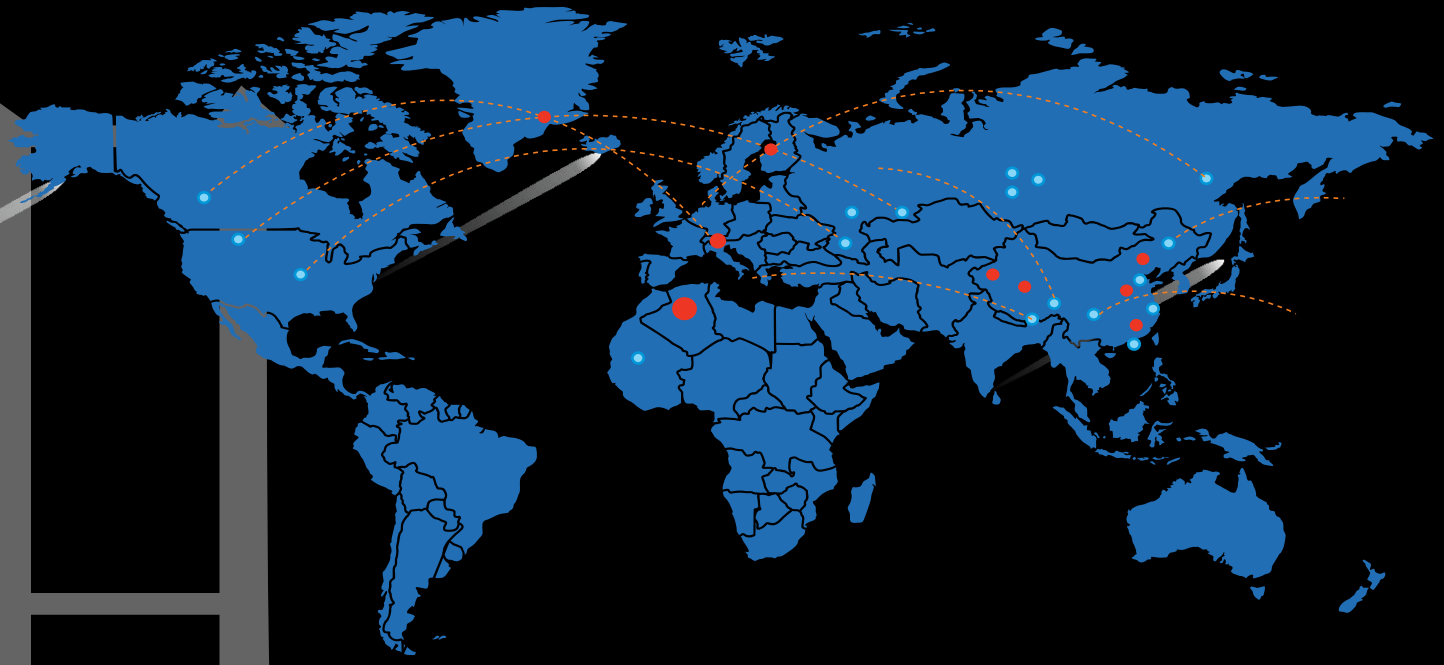

CCTV 13
新闻


Payment will be raised on
5/16/2017 02:26:59
Time Left
02:22:35:15
Your files will be lost on
5/20/2017 02:26:59
Time Left
我的电脑出了什么问题？
您的一些重要文件被我加密保存了。
照片、图片、文档、压缩包、音频、视频文件、exe文件等，几乎所有类型的文件都被加密了，因此不能正常打开。
这和一般文件损坏有本质上的区别。您大可在网上找找恢复文件的方法，我敢保证，没有我们的解密服务，就算老天爷来了也不能恢复这些文档。
有没有恢复这些文档的方法？
当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以人格担保，能够提供安全有效的恢复服务。
但这是收费的，也不能无限期的推迟。
请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，我是绝不会骗你的。
但想要恢复全部文档，需要付款点费用。
是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟付款时间越长对你不利。
最好3天之内付款费用，过了三天费用就会翻倍。

网络安全蝴蝶效应

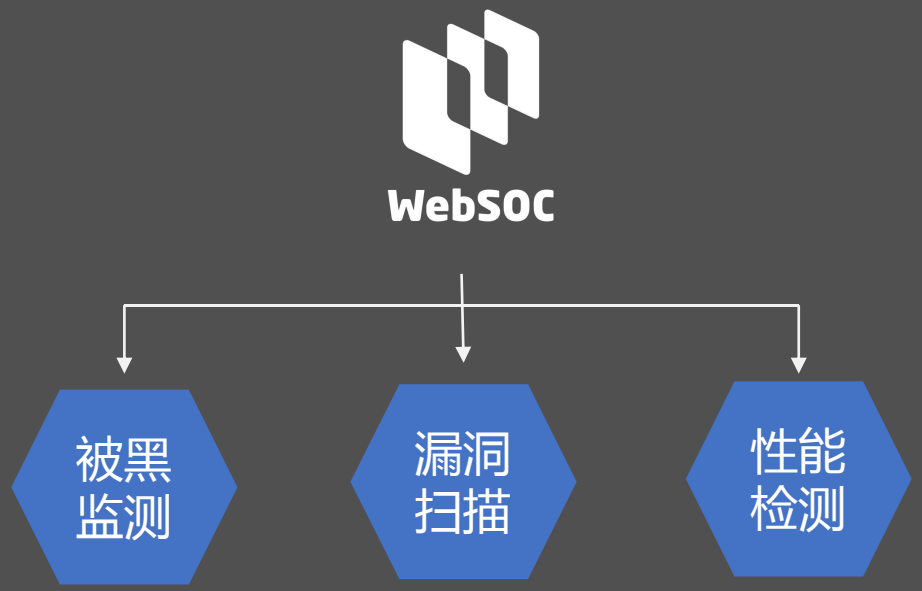
数据感知风险

知



知

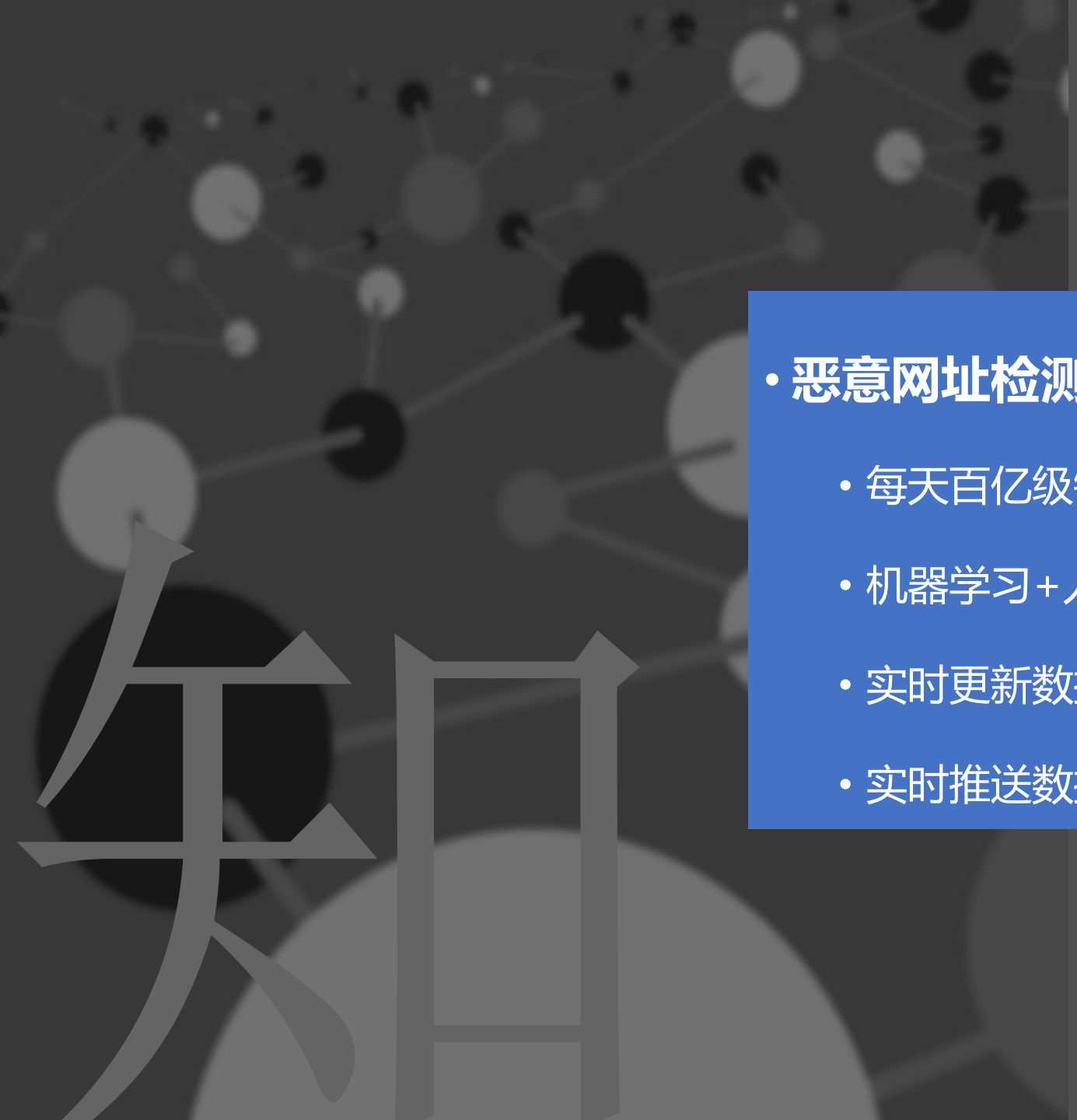
- **ZoomEye网络空间雷达（资产）**
  - 具备全球范围资源探测能力
  - 全面覆盖全球42亿IPV4地址空间
  - 准确识别40000+常见组件指纹
  - 7-10天遍历全部IPV4地址空间
  - 精准探测24h以内
  - 覆盖路由器、摄像头、物联网、工控等所有联网系统



- **Websoc网站监测引擎（风险）**
  - 支持万个站点的并行扫描和监控
  - 支持7x24小时实时监控，不放过一个被黑站点
  - 大数据集中可视化展示，智能分析，及时高效
  - 内置漏洞验证POC，可在平台内对高危漏洞直接验证

- **创宇盾云防护（威胁）**
  - 90万网站防护
  - 过去6年多来，33万不同黑客针对防护网站发起过攻击
    - 黑客设备指纹、常用跳板、社交信息、常用工具
  - 过过去6年多来，发起攻击的IP地址
    - 攻击IP的频率、时间、水平

知



- **恶意网址检测引擎（恶意服务）**
  - 每天百亿级链接检测
  - 机器学习+人工验证
  - 实时更新数据库
  - 实时推送数据接口

C&C通讯

木马

- **云图高级威胁监测（恶意行为）**
  - 依托腾讯安全云库与知道创宇大数据威胁情报
  - 百G级骨干网络检测能力
  - 大数据集中可视化展示，智能分析
  - 独有基因图谱监测技术

病毒

僵尸

云图

流量中捕获恶意行为

创宇盾

针对应用服务的攻击

ZoomEYE

全网设备指纹监测

Websoc

Web服务安全监测

恶意URL库

恶意服务监测

哈勃

恶意程序样本监测

黑客库

定义33万黑客的指纹

IP信誉机制

定义10多亿来访IP指纹

法人库

提供服务对应的法人，如ICP备案库。关联信息库，如工商，税务、法院等相关信息

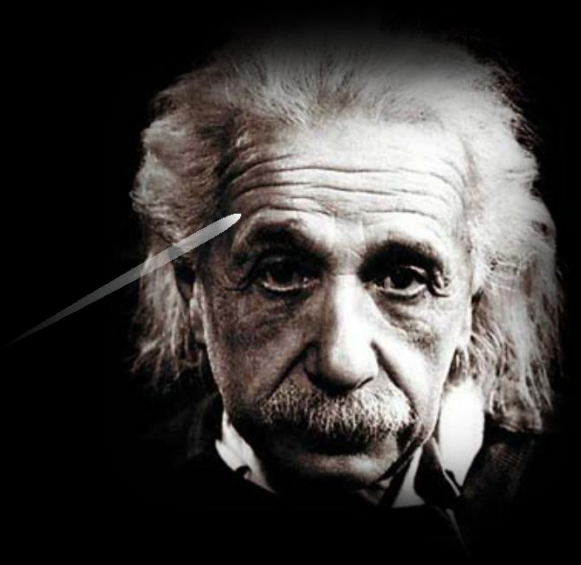
使用者库

终端设备的使用者，关联的个人信息，如社交账号，社保信息，不动产信息、车辆、保险、消费记录、通讯记录，GPS轨迹等

灰黑产

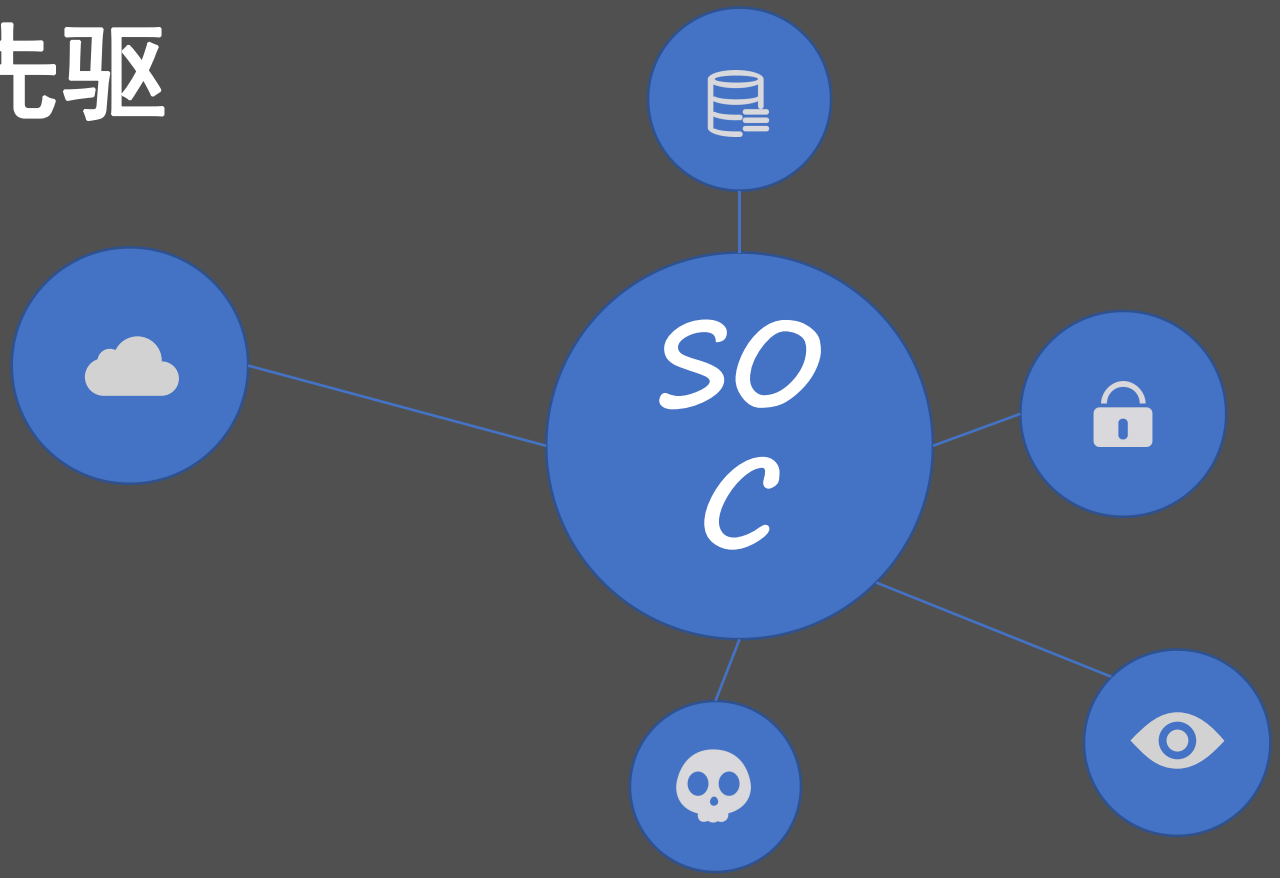
大数据分析与应用

道



安全大数据应用先驱

- 全日志采集
- 时间轴窗口
- 事件关联归并



创宇盾

大数据应用于WEB防御

专属防御
防御能力
99.99%

安全
评级
云

防御
联动

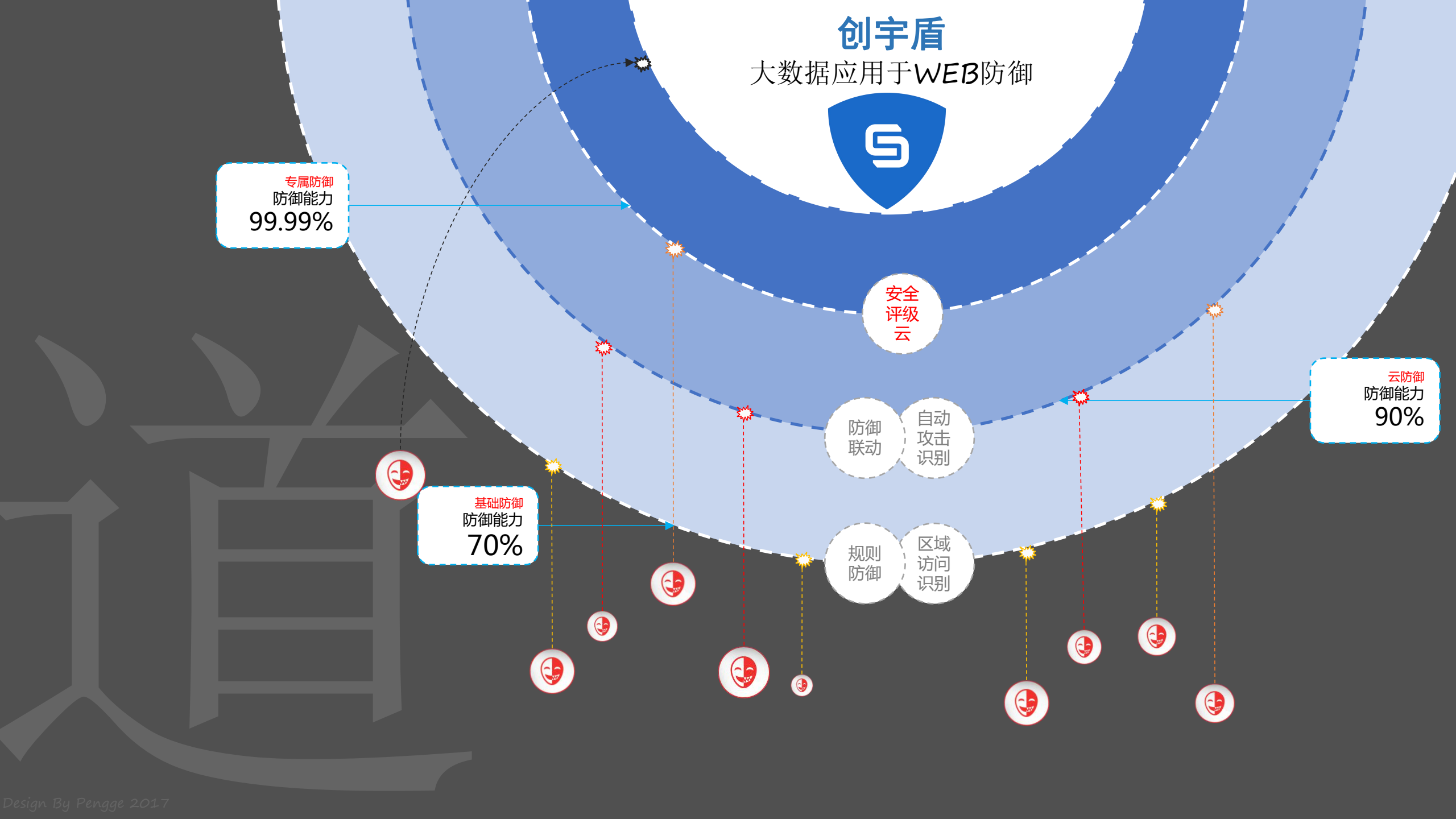
自动
攻击
识别

云防御
防御能力
90%

基础防御
防御能力
70%

规则
防御

区域
访问
识别

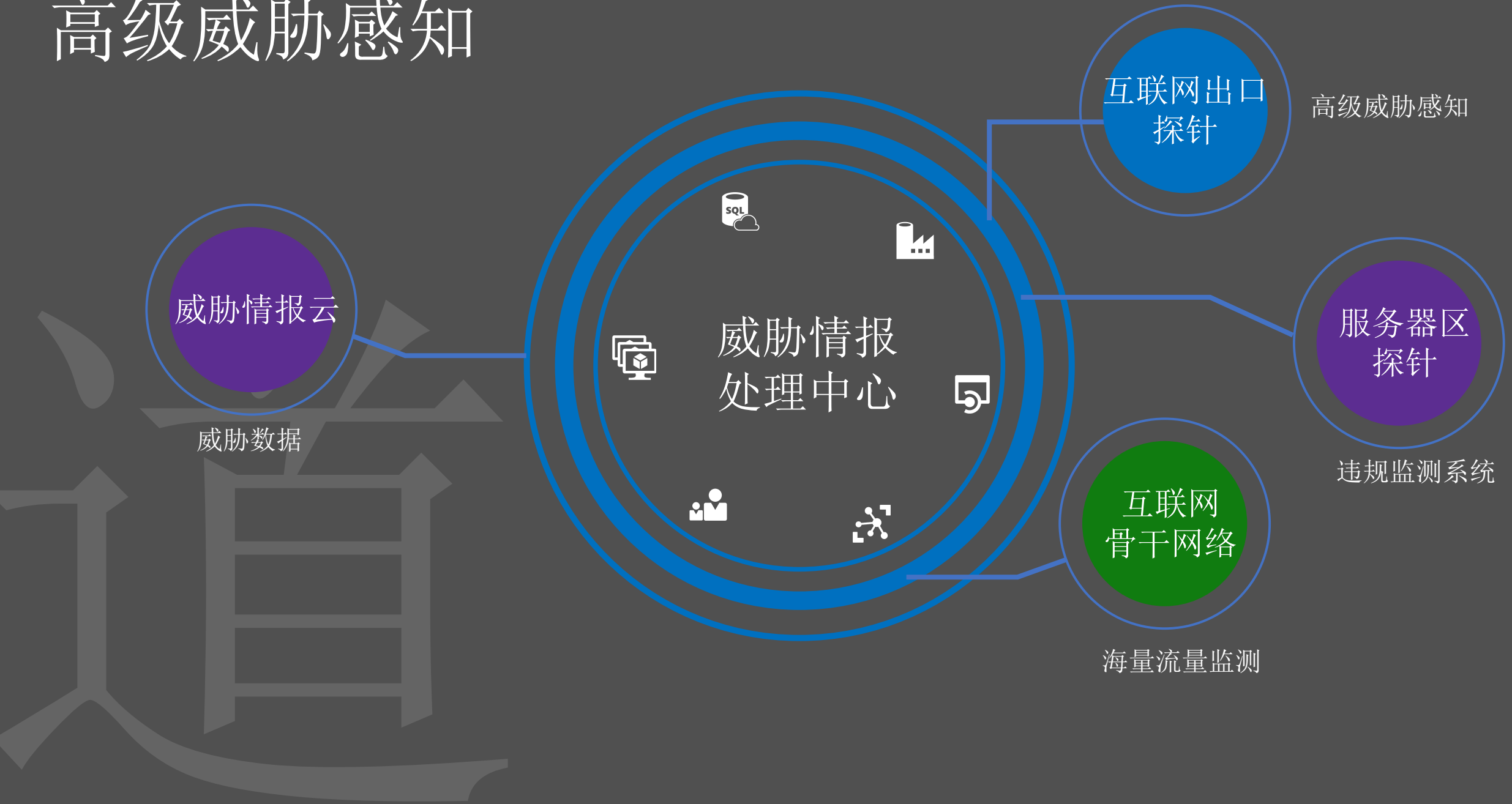


应用案例　江门市直单位网站群60+　整体云防御

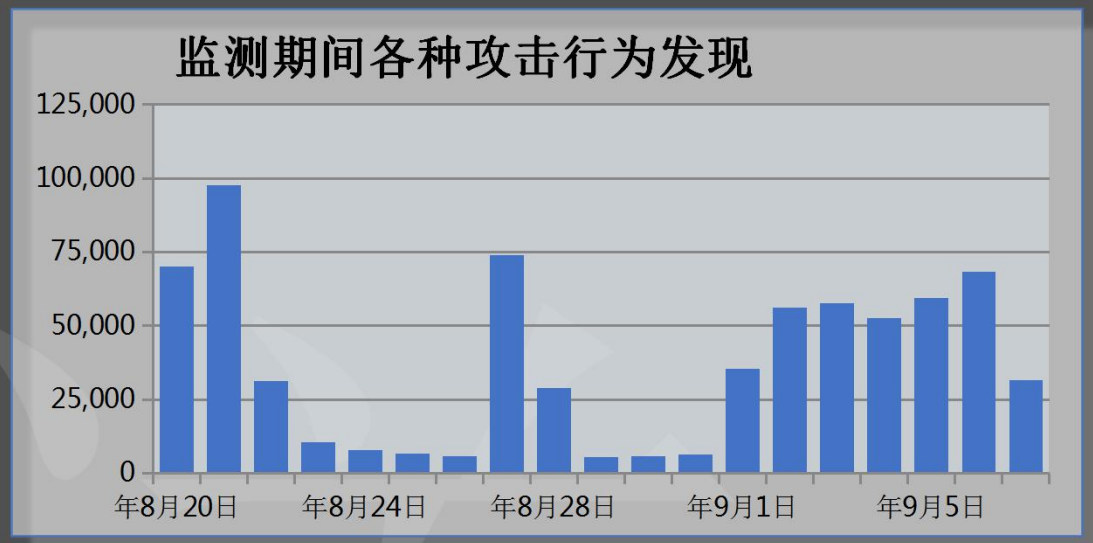
- 上线近一年

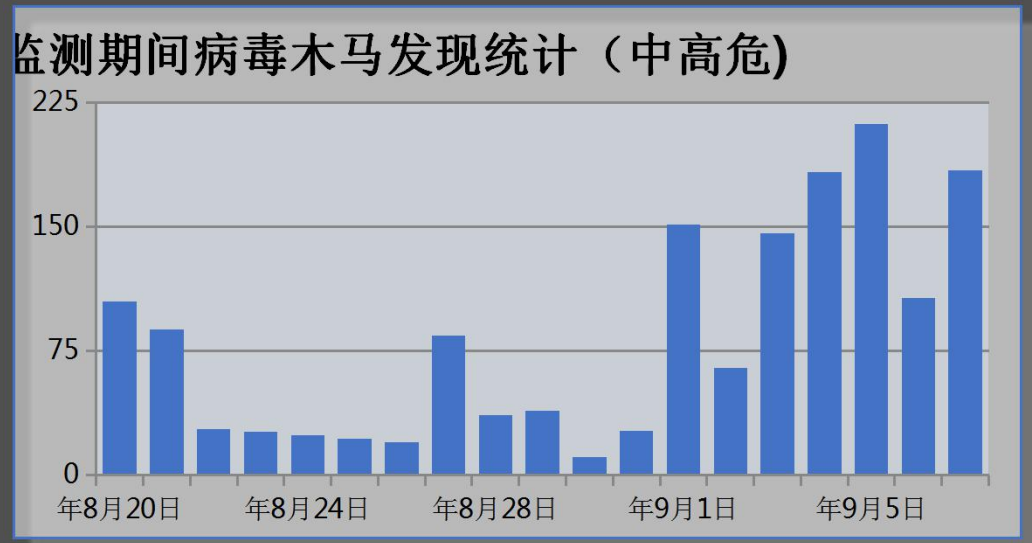
- 被篡改　零
- 被通报　零

高级威胁感知



应用案例 G20期间安全保障





- 平均每天6万次左右攻击行为
- 发现众多被控主机，大量连接外网恶意IP地址或DGA恶意域名
- 发现漏洞攻击成功、DDoS攻击、各种扫描、SQL注入攻击

- 共计发现中高危病毒木马1600次
- 病毒木马种类：种类繁多，有外连恶意IP、下载程序、盗取私密信息、发送数据、横向渗透，到直接控制设备或僵尸网络等等。
- 特种木马采用组合攻击方式