BIG

安全数据分析

ALIBABA
聂万泉(来往)

SERAPH NIE

安全
游戏
心学
小说

N

- 做了很多年的镖师
- 13YEAR

- 梦想有一家游戏公司
- 5YEAR

BIG DATA

只是矿山，不是宝藏！

D

5.5T的HTTP DATA.

15T的LOG DATA.

20T的 NETWORK DATA

云

离线

5K SERVER COMPUTING

云计算让大数据计算不再复杂

HADOOP

阿里云-飞天

OTHER

数据元结构化存储

做好安全分析，需要一些能与安全挂上钩的元数据

元

H HTTP DATA
TIME | RQUEST DATA |SRC DATA

五 五元组
TIME | SRC DATA |DST DATA

D DNS DATA
TIME | REQUEST DATA |DOMAIN DATA

L LOG DATA
TIME | APP DATA | ACTION DATA

X 元素
那些不稳定的家伙

我们的数据里充满复杂的不稳定的元素，他们会干扰我们的分析和判断

V

C

爬虫

冒充的还是真实的，让IP说话

M

自动任务的机器人

机器人总是有条理的在工作

P

自己人

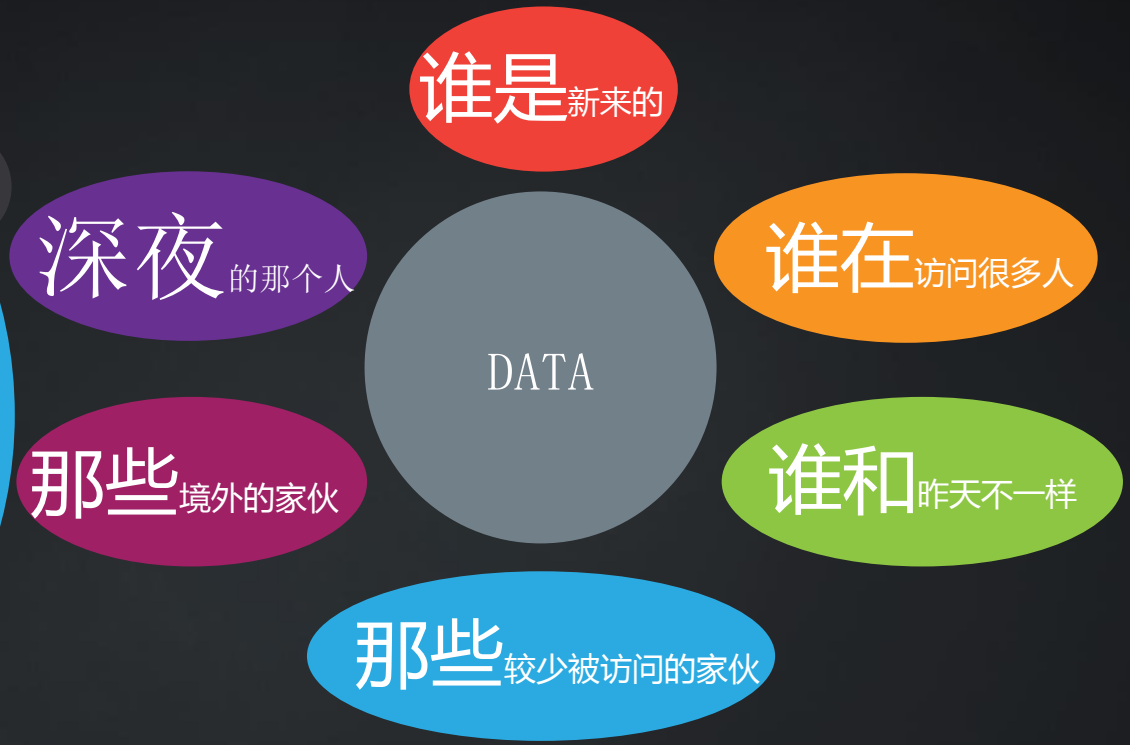
自家人不识自家人，打个标记更好认

魔镜

说

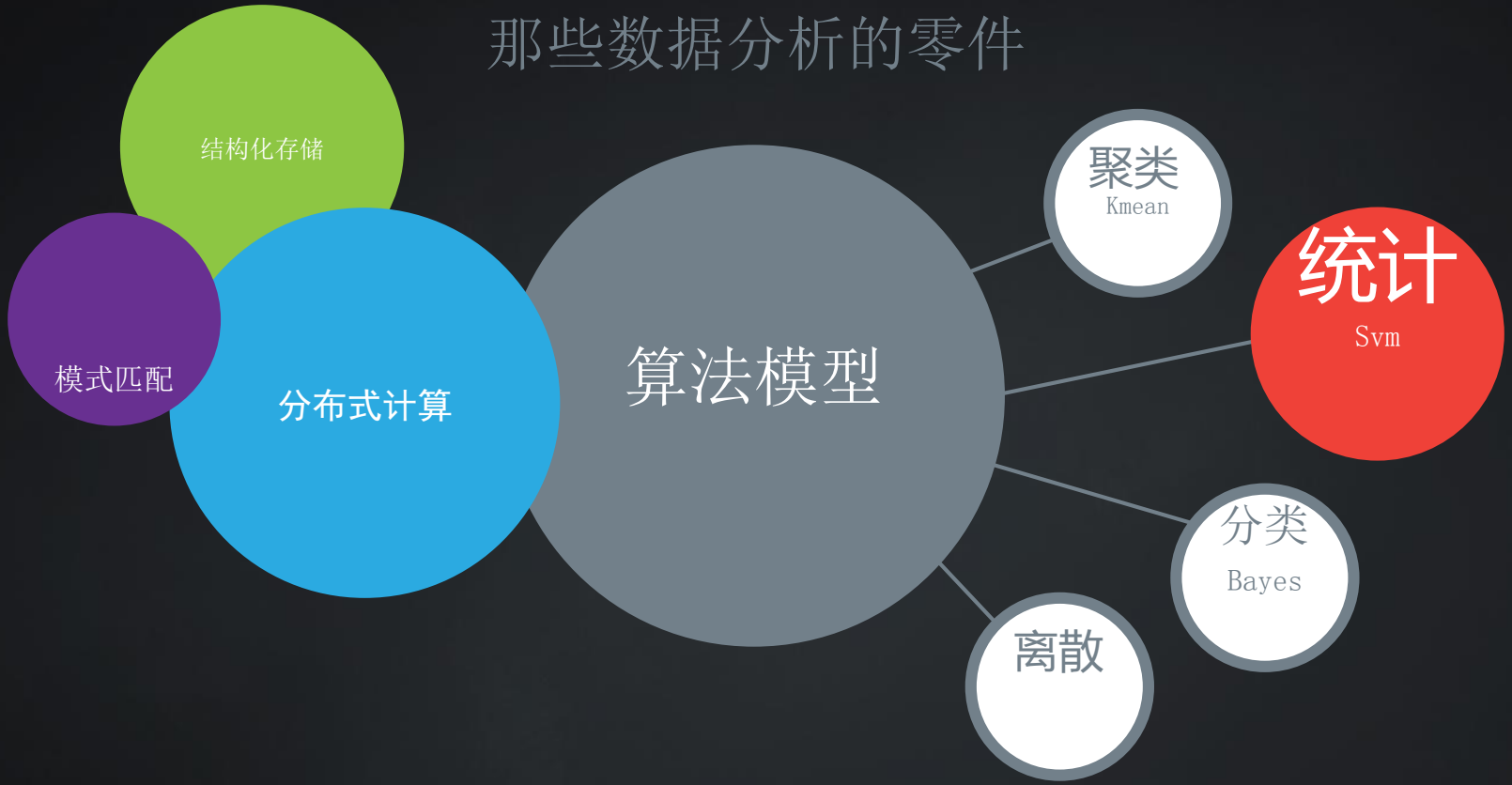
尝试让这些数据告诉我们点什么

和数据的对话是一个有意思的过程

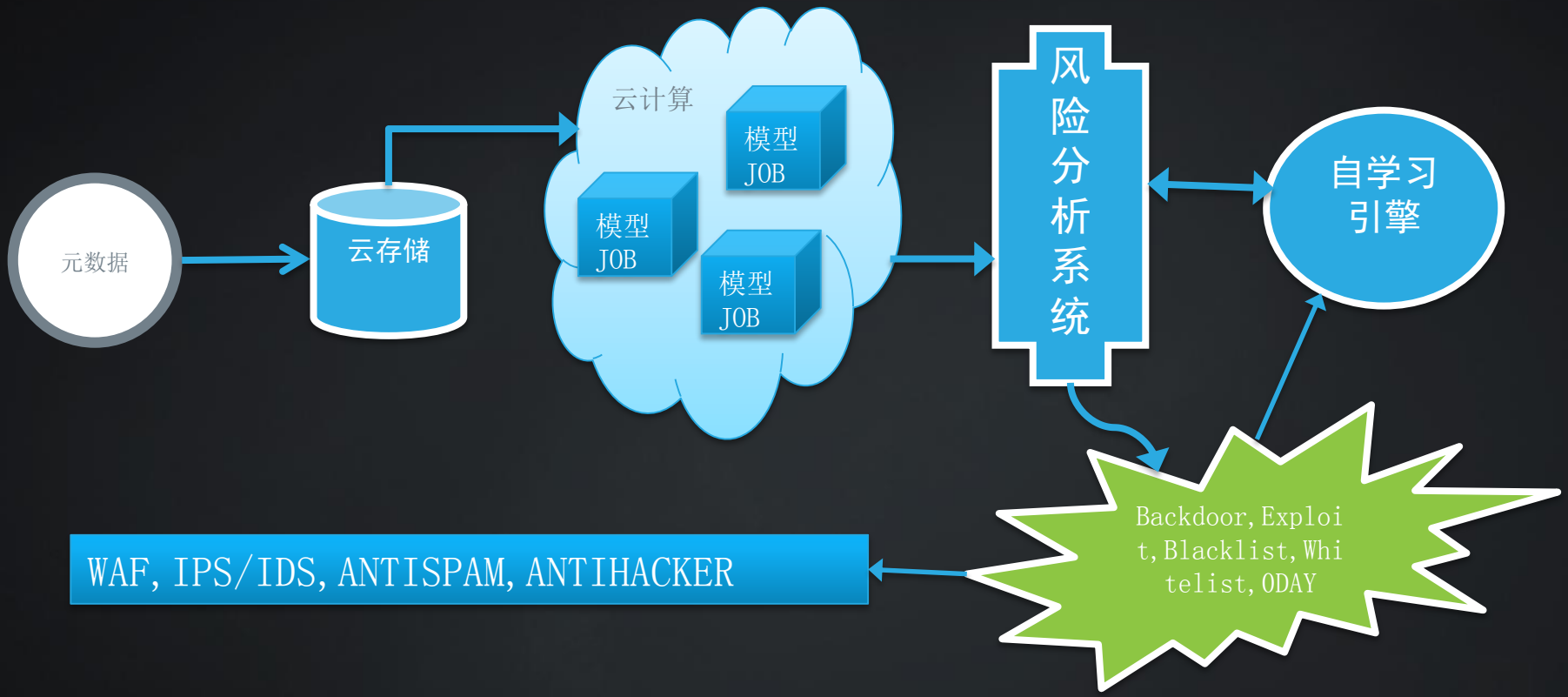


不简单的工程

那些数据分析的零件



大数据安全分析系统架构



VI

区别

大数据对**安全分析**区别传统安全产品**对抗**输出方式，更多从数据关系中检出安全风险。

传统安全产品

用规则检测攻击和风险，依赖规则的持续完善和改进。

大数据安全分析

从数据行为和关系中检测风险，并能产生举一反三的学习能力，无需人工干预并持续完善检测能力。

价值

应用场景

入侵检测

调查取证

签名收集

趋势预警

产品改进

风险评估

THANK YOU

FOR WATCHING

See you soon!