



2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# AiLPHA大数据 全方位保卫内网安全

主讲人：刘博





2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# 新时代内网安全挑战



**边界:** 清晰 → 模糊

**资产:** 单一 → 多元

**人员:** 简单 → 复杂



# 内网安全解决方案：平台产品现状

## 安全理念

SIEM – 安全信息与事件管理  
SOC – 安全运营中心  
NG-SIEM - 下一代SIEM  
NG-SOC - 下一代SOC  
USM - 统一安全管理平台  
UTM - 统一威胁管理平台  
UEBA - 用户行为分析

## 安全产品

IBM Qradar  
Splunk ES  
ArcSight ESM

.....



功能越来越多

产品越来越复杂

内网安全问题没有解决

应付合规的用不起来的产品

# 内网安全核心技术问题

数据源零散、形成孤岛；  
数据种类和格式庞大。

无法有效快速定位问题；  
无法快速响应和处置，形成闭环。



依赖局部静态规则；  
误报太多，安全价值丧失。

不能发现行为风险。  
无力应对高级威胁。



2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# “收集不全” - AiLPHA大数据全方位高保真收集





# “检测不准” - 当前检测方法误报过多

规则策略

<?php **eval**(\$\_POST[ 'a' ])?>

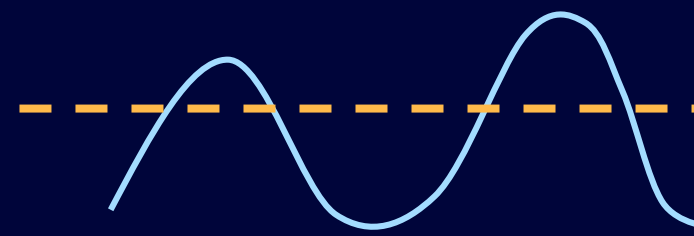
统计阈值

1分钟IP访问次数**>200**，异常访问

关联规则

首次登陆数据库 **5分钟之内** 拉取数据1百万条

基线分析

 **50%**  
本小时访问次数比昨天同期高50%







2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# “检测不准” - AiLPHA大数据改进模型

误报率↓400%

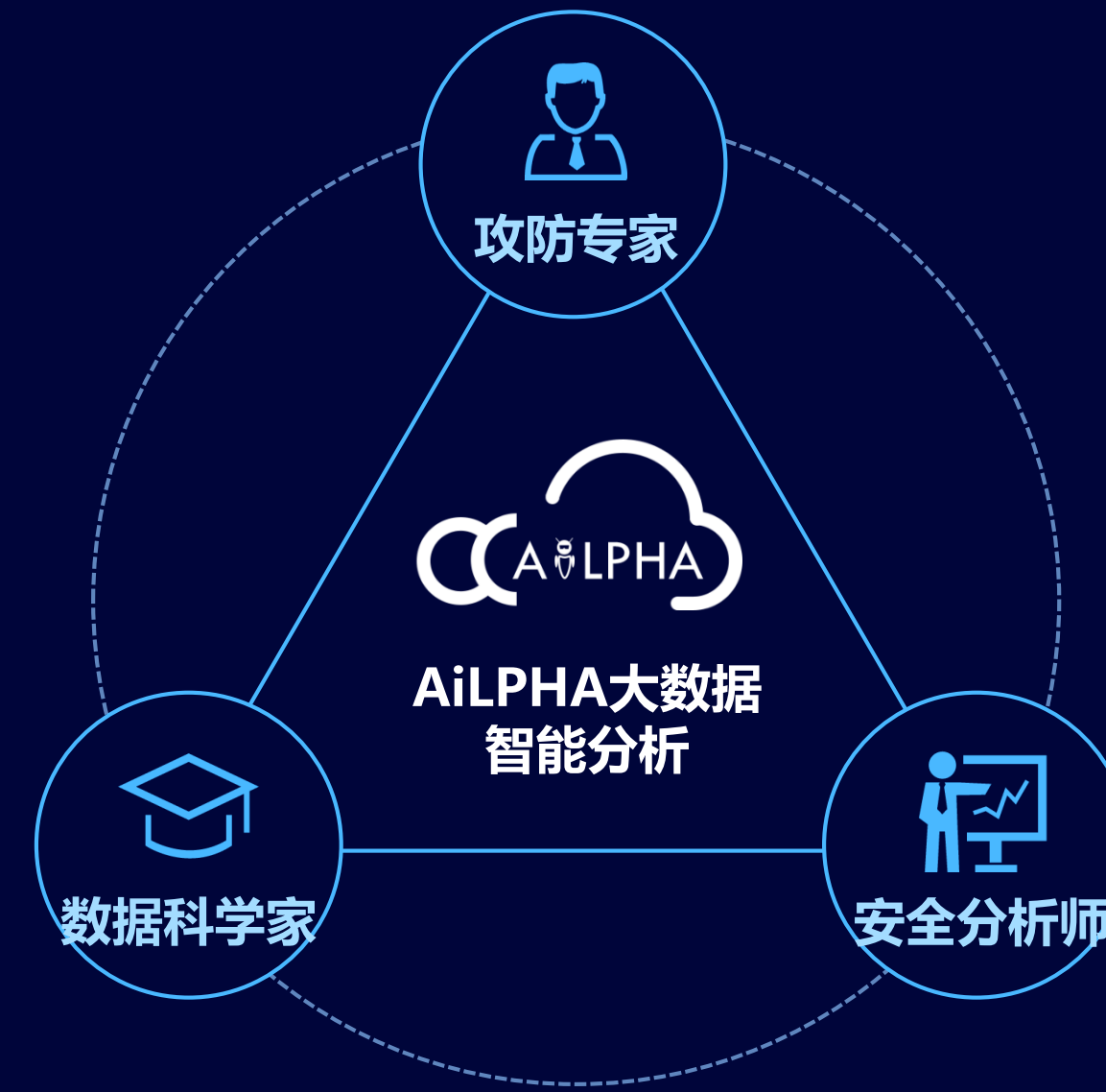
是否存在漏洞

漏洞是否利用成功

漏洞验证

请求返回包

系统应用日志



情报碰撞



200万	恶意IP	每天新增记录 2万
1.7亿	基础域名库	每天新增 400万
50万	僵尸网络	每天新增 100个
200万	恶意样本	每天新增 500个
500万	漏洞库	每天新增 3000个
58万	暗链站点	每天新增 500个

误报率↓400%

误报率↓200%

深入调研用户环境拓扑和业务背景，不断试验策略,提高准确率及召回率

智能模型

攻击链分析



误报率↓100%



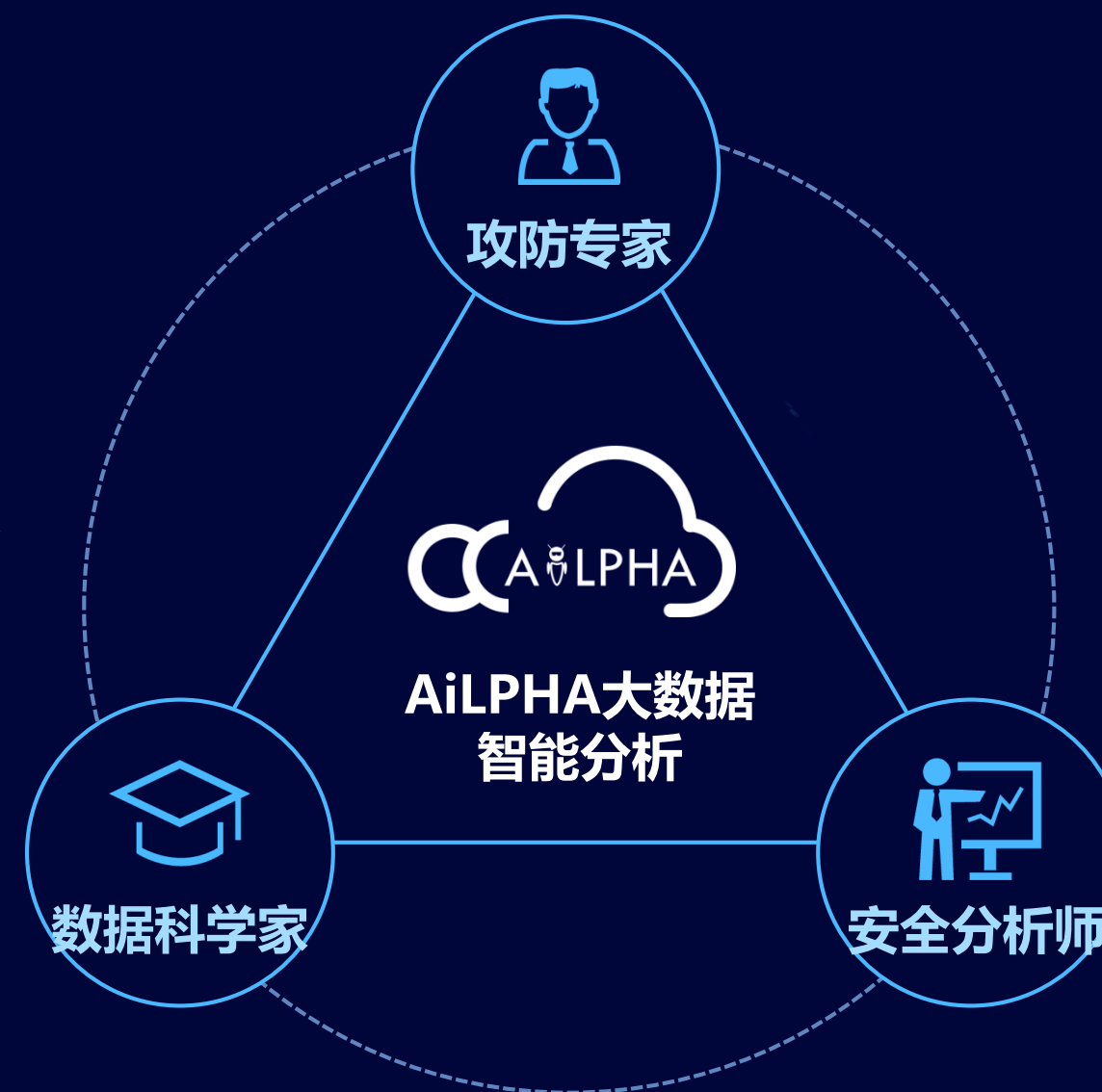
2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# 检测不准” - AiLPHA大数据自适应学习

人机共智



告警



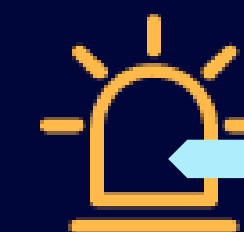
误报预测

剔除误报的告警



持续强化  
机器学习

带标签的告警



安全分析人员打标签



针对数值型告警  
误报率

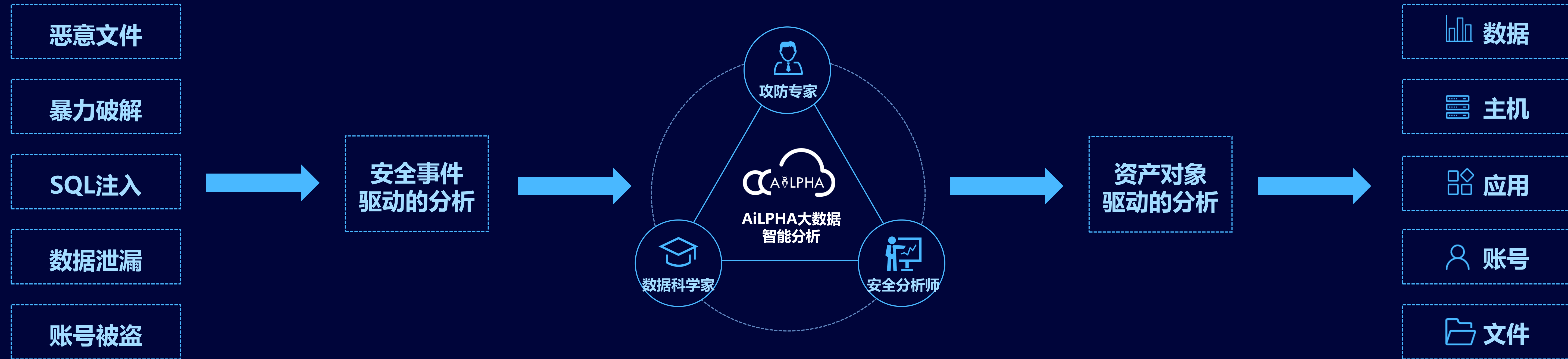


300%

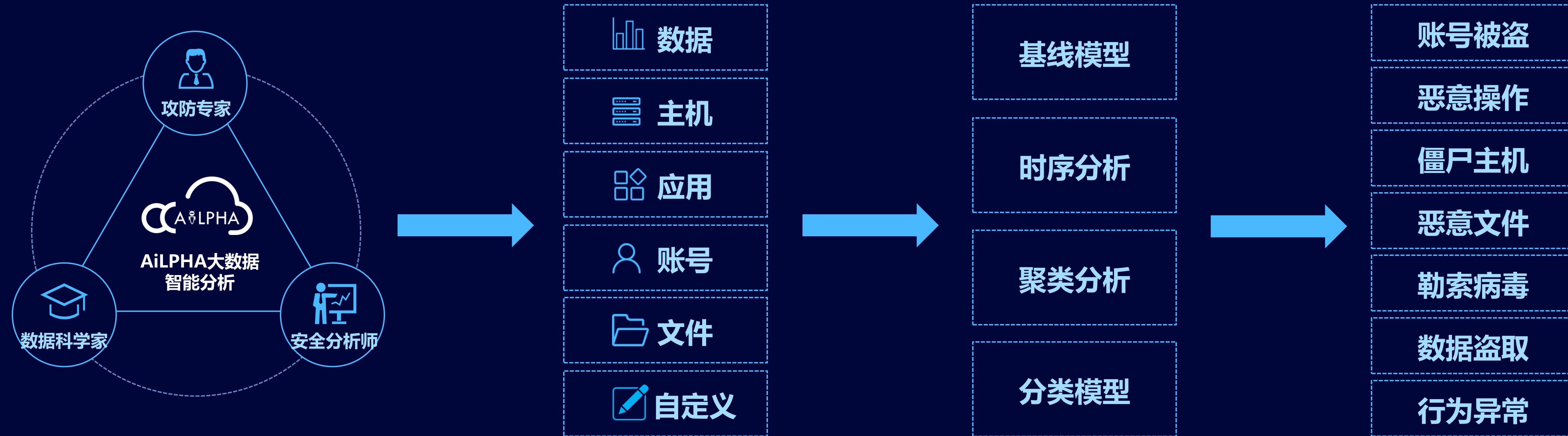
国内首家



# “模型不灵” - AiLPHA大数据改进分析视角



# “模型不灵” - AiLPHA大数据资产智能模型

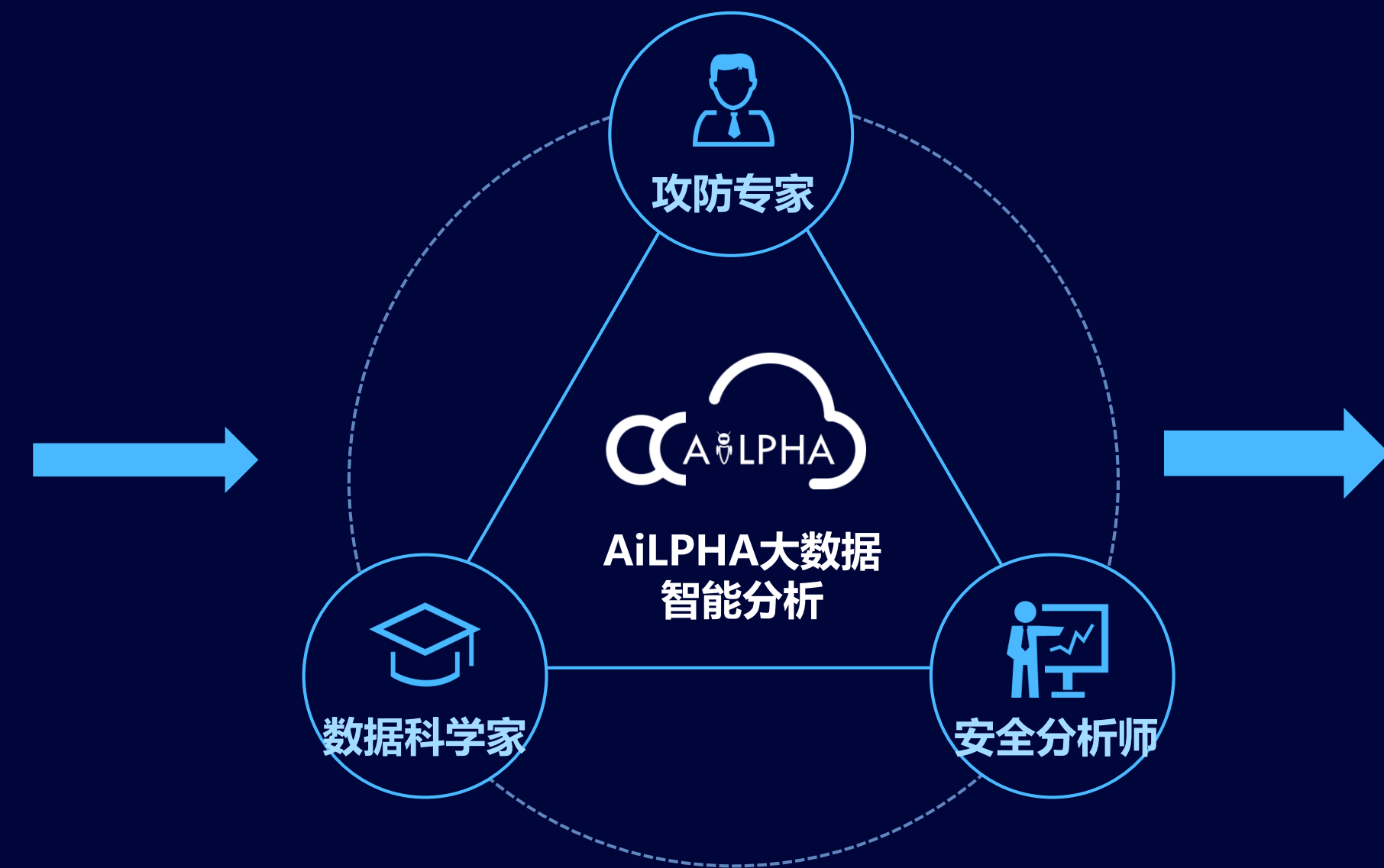
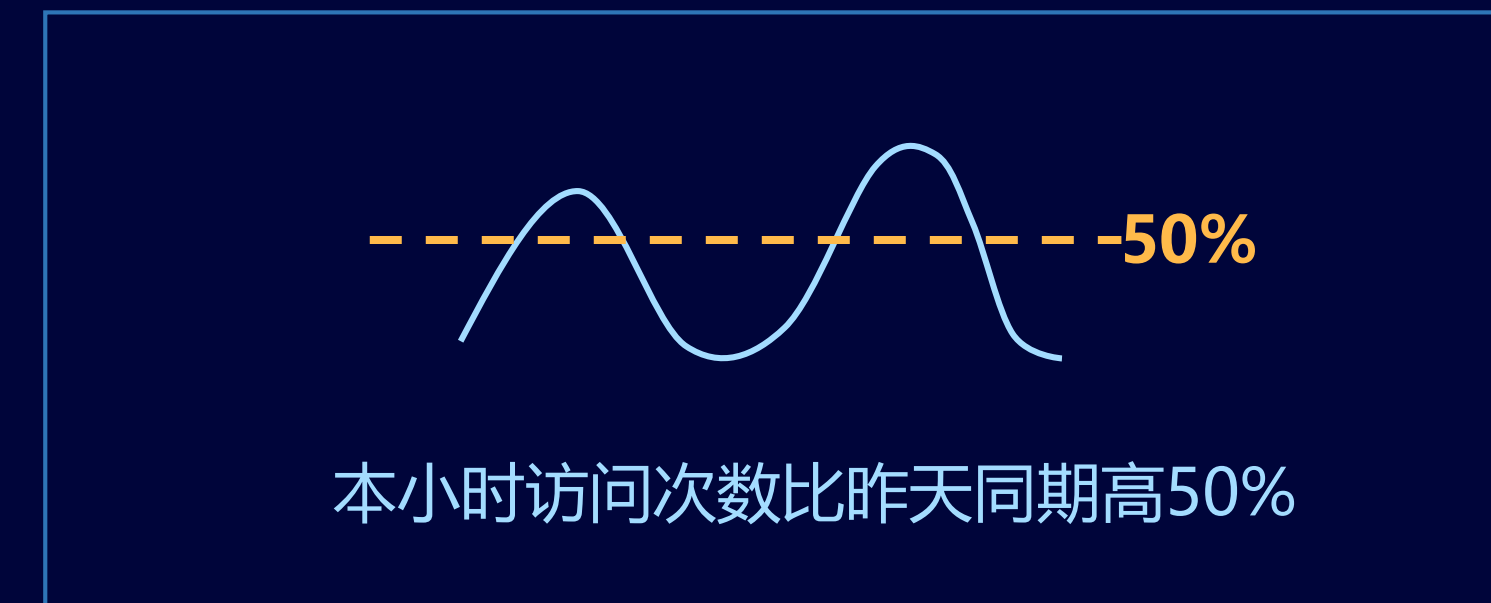


# “模型不灵” - AiLPHA大数据账号画像异常分析

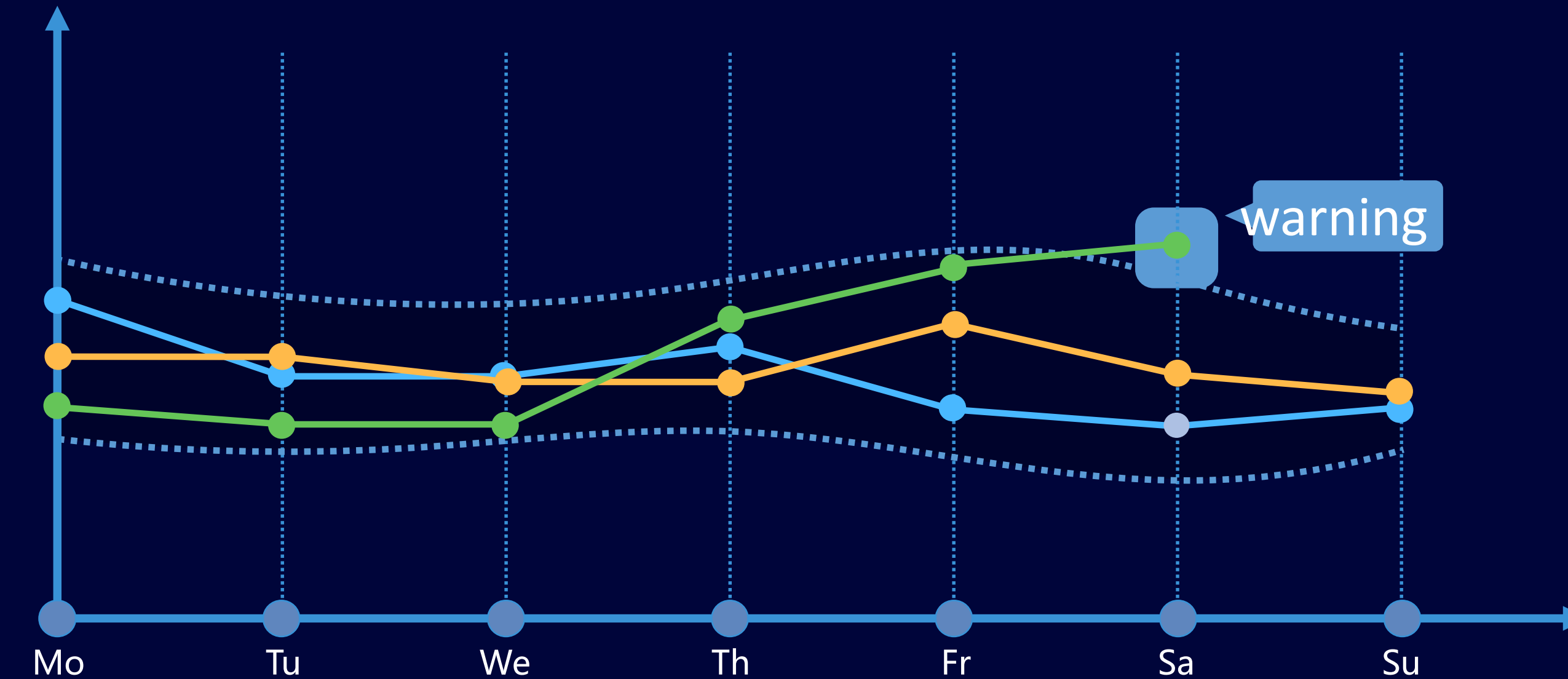




# “模型不灵” - AiLPHA大数据时序基线异常分析



上上周  
上周  
本周



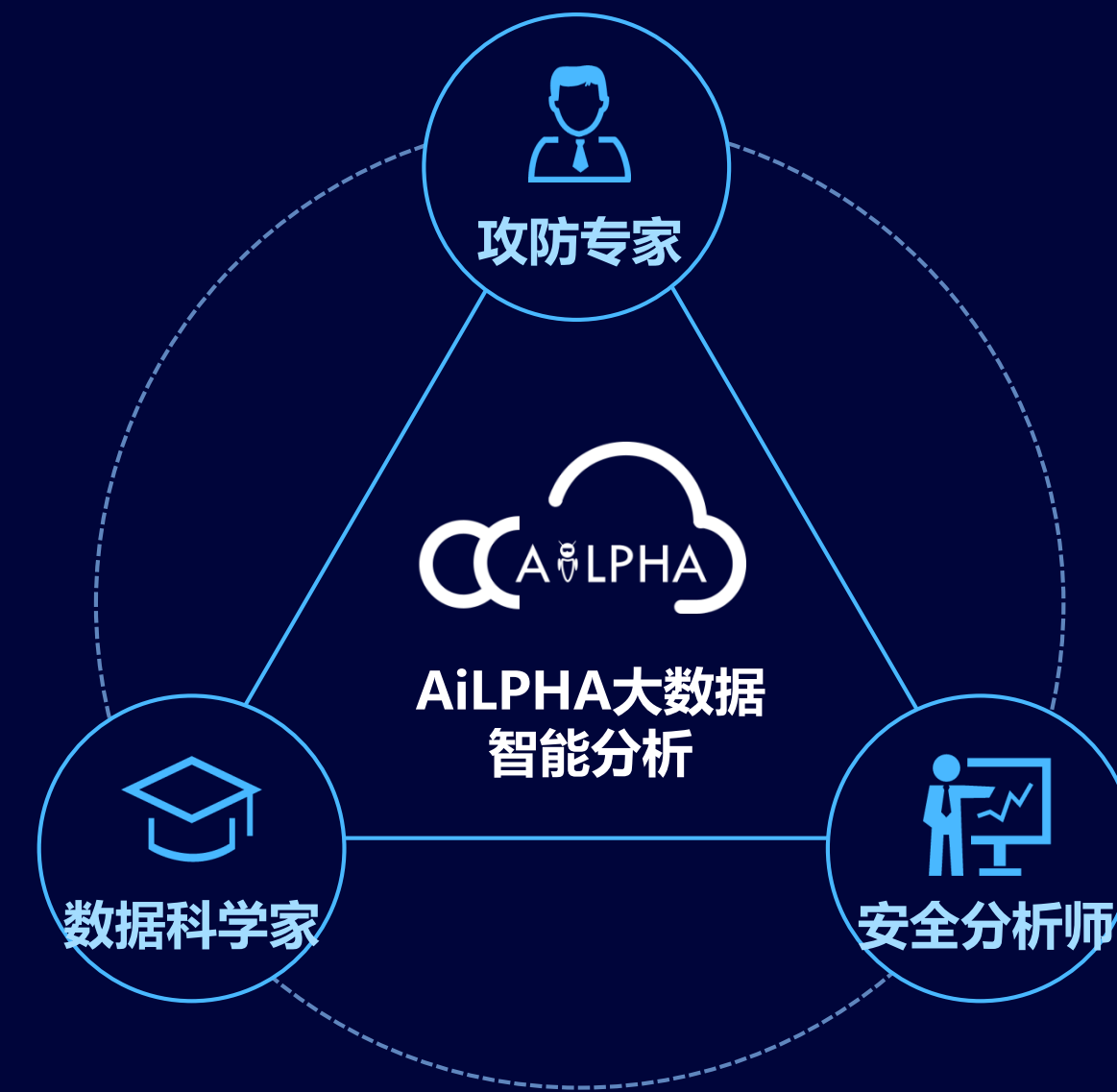
发现未知异常行为

即将发表的文章

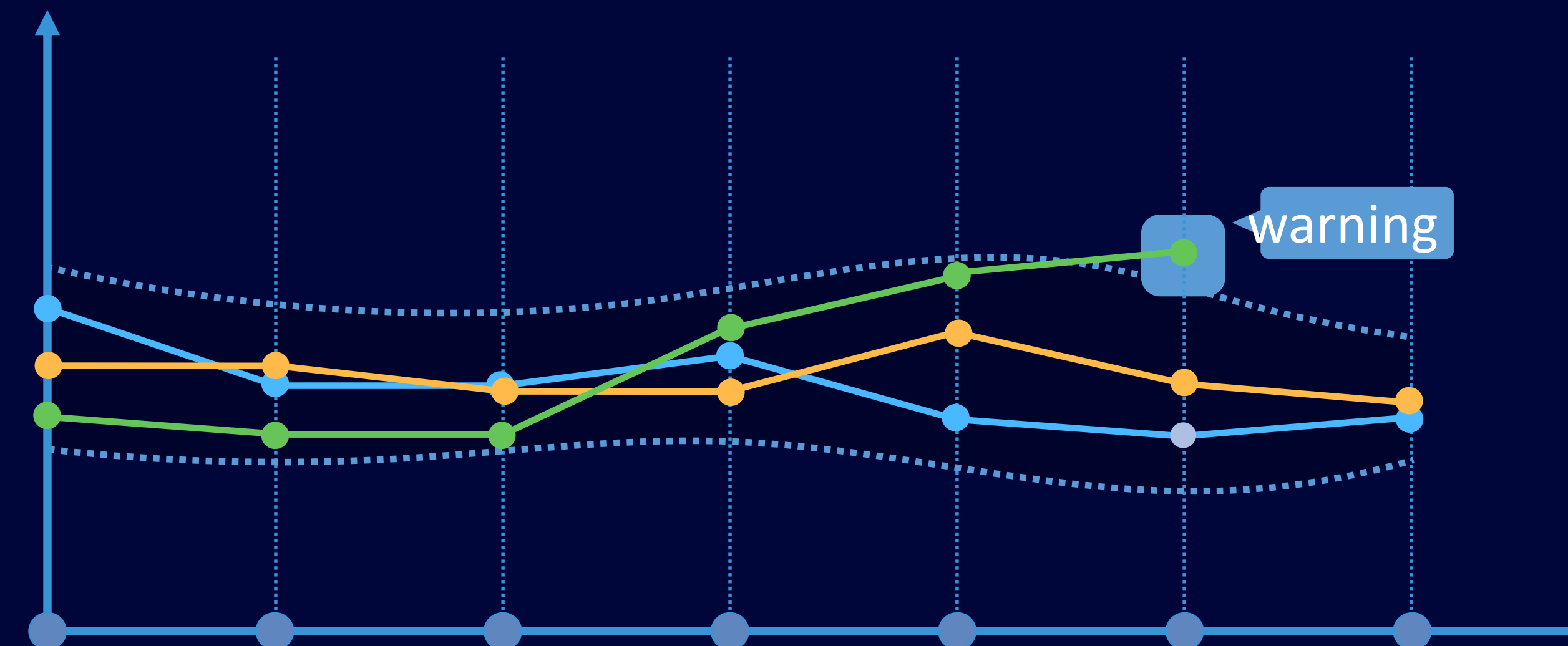


2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# “模型不灵” - AiLPHA大数据自定义对象异常分析



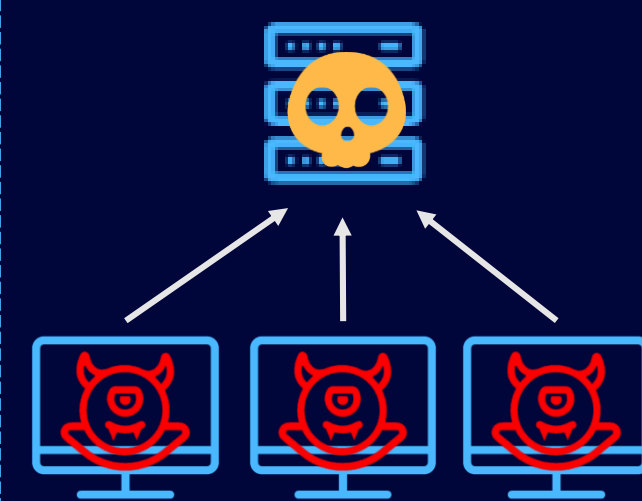
上上周  
上周  
本周



国内首家

# “处置不解” - AiLPHA大数据资产网络分析

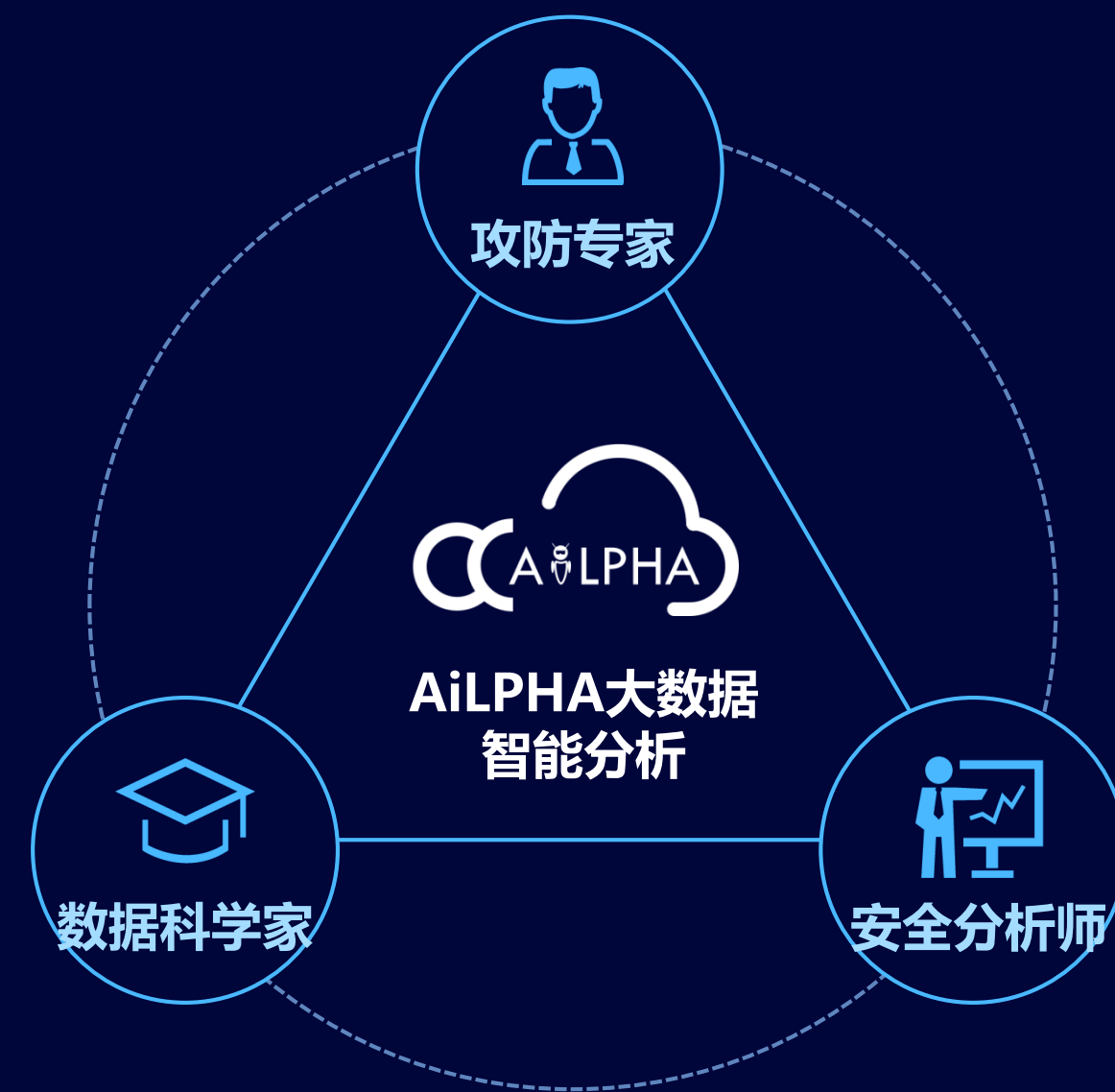
## 僵尸主机



## 病毒是怎么传播进来的?

## 哪些主机被感染了?

## 病毒的危害是什么?



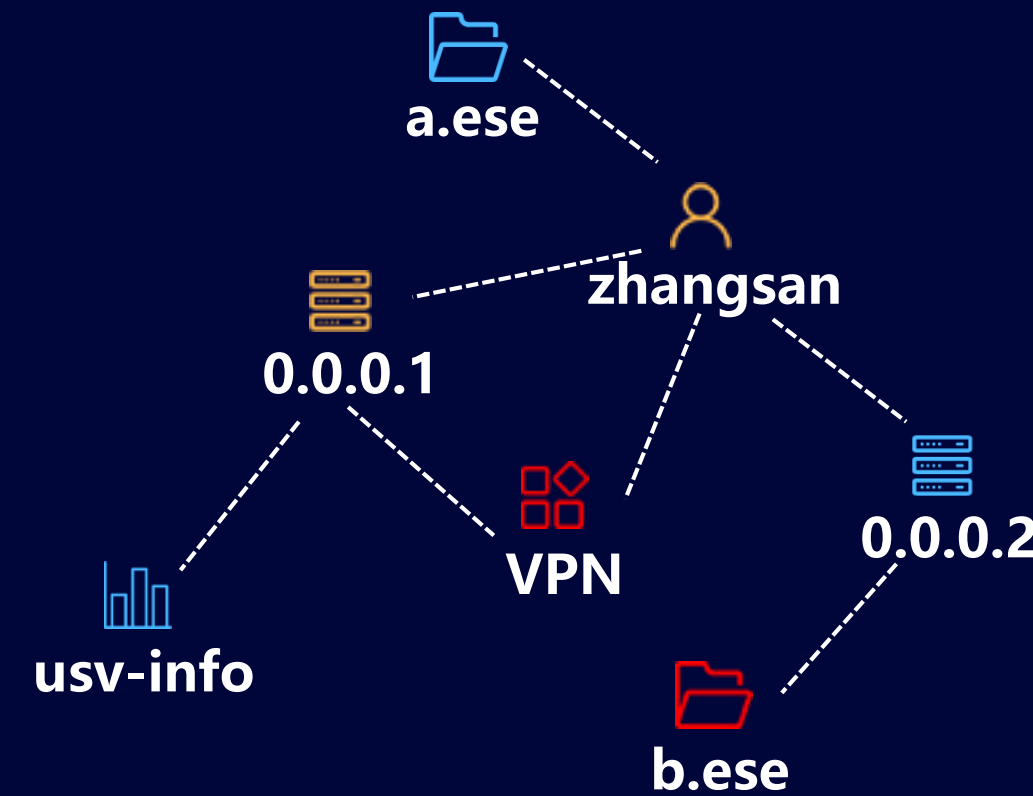
## 资产网络分析

## 智能联动

## 知识库

数据  
主机  
应用  
账号  
文件

异常  
可疑  
正常



首页 / 用户页 / 详情页 / 最近行为操作的时间表

姓名: 张三 告警总数: 65 风险指数: 95  
所在部门: 研发部门 最后登录时间: 2017-06-07 22:32:20  
职位: 研发经理 告警事件: 异常操作

最近一次操作时间为: 2017-06-07 22:32:20

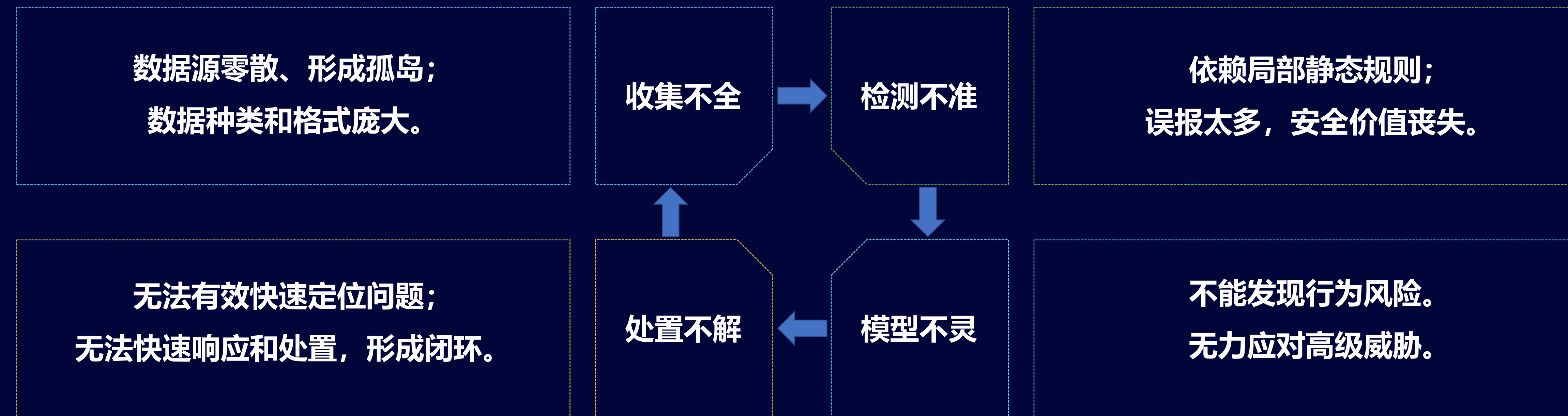
时间	事件	异常操作	异常次数	操作
2017-06-07 08:50:08	访问网站: www.banqia.com.cn	异常操作	访问次数: 5次	编辑 更多
最后访问时间: 2017-06-07 08:32:06 事件: 异常访问 风险指数: 85				
2017-06-07 09:50:32	4次异常访问	异常地点异常	异常地点: 北京	编辑 更多
2017-06-07 10:35:08	GitHub提交事件	正常	提交次数: 5次	编辑 删除
2017-06-07 11:25:08	GitHub提交事件	正常	提交次数: 3次	编辑 更多
2017-06-07 11:38:28	GitHub提交事件	正常	提交次数: 1次	编辑 更多
2017-06-08 03:20:12	2次异常访问	异常登录时间	异常登录时间: 2017-06-08 03:20:12	编辑 更多
2017-06-08 09:38:28	GitHub提交事件	正常	提交次数: 1次	编辑 更多
2017-06-08 11:18:15	GitHub提交事件	正常	提交次数: 1次	编辑 更多



# AiLPHA Lambda大数据技术架构



# 内网安全核心技术问题





2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

# 技术+人才

管理和解决信息安全问题离不开安全人才。

-Steve Martuno, Cisco CISO

-ISO 27001, ISMS(信息安全管理系统)

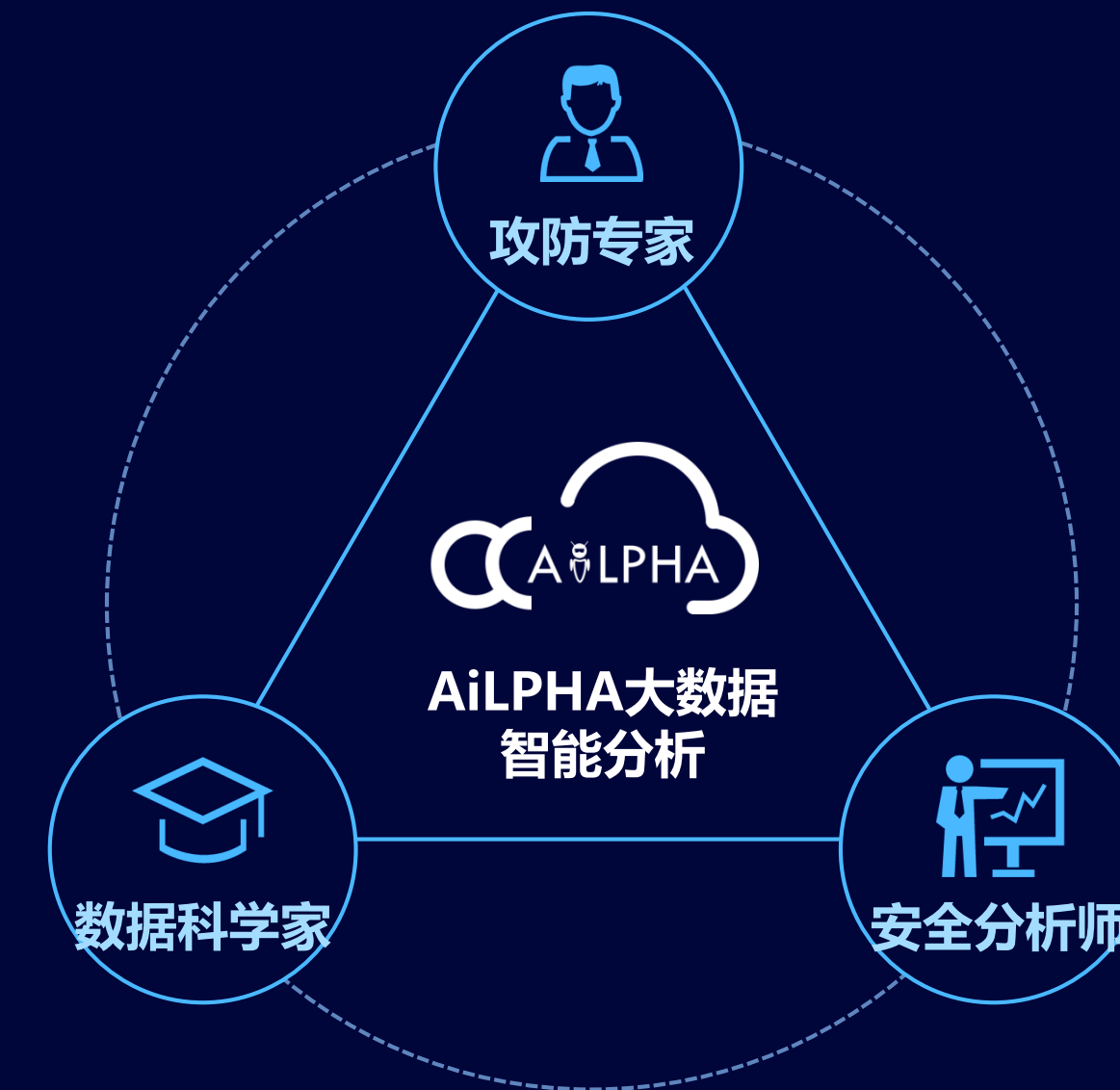
安全人才

国测CISP培训

大数据安全

云安全

安全服务



最佳内网解决方案

月  
周  
日  
小时  
分钟

20X

↓  
误报降低  
500%

MTTD平均检测时间  
MTTR平均响应时间

能效  
能效  
还是能效





# 为您提供全方位、省心的内网安全防护





2018 西湖论剑·网络安全大会  
West Lake Cybersecurity Conference

THANKS  
谢谢大家