智能编排技术
如何加速
企业安全威胁响应

傅奎@雾帜智能

目录

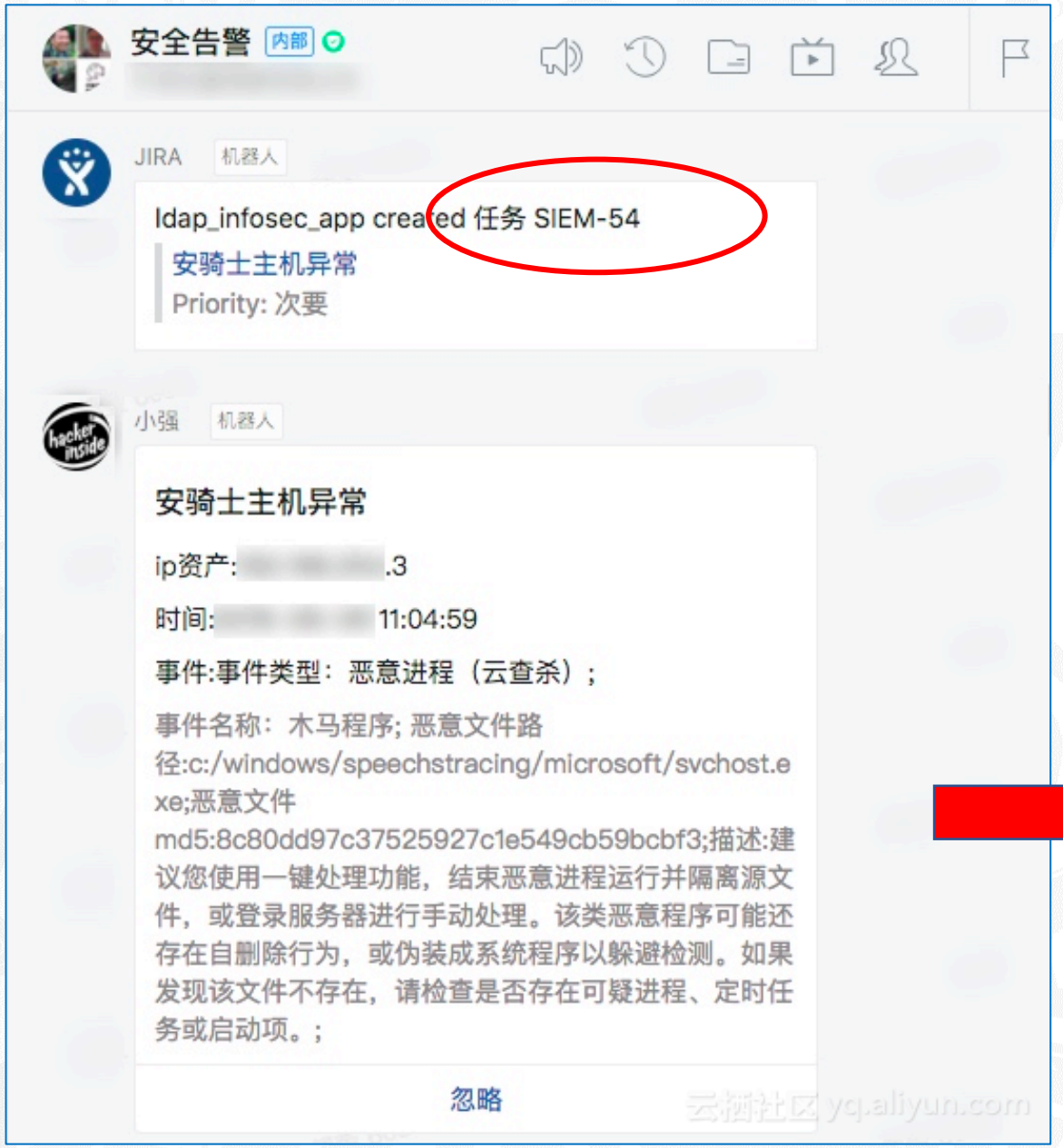
CONTENTS

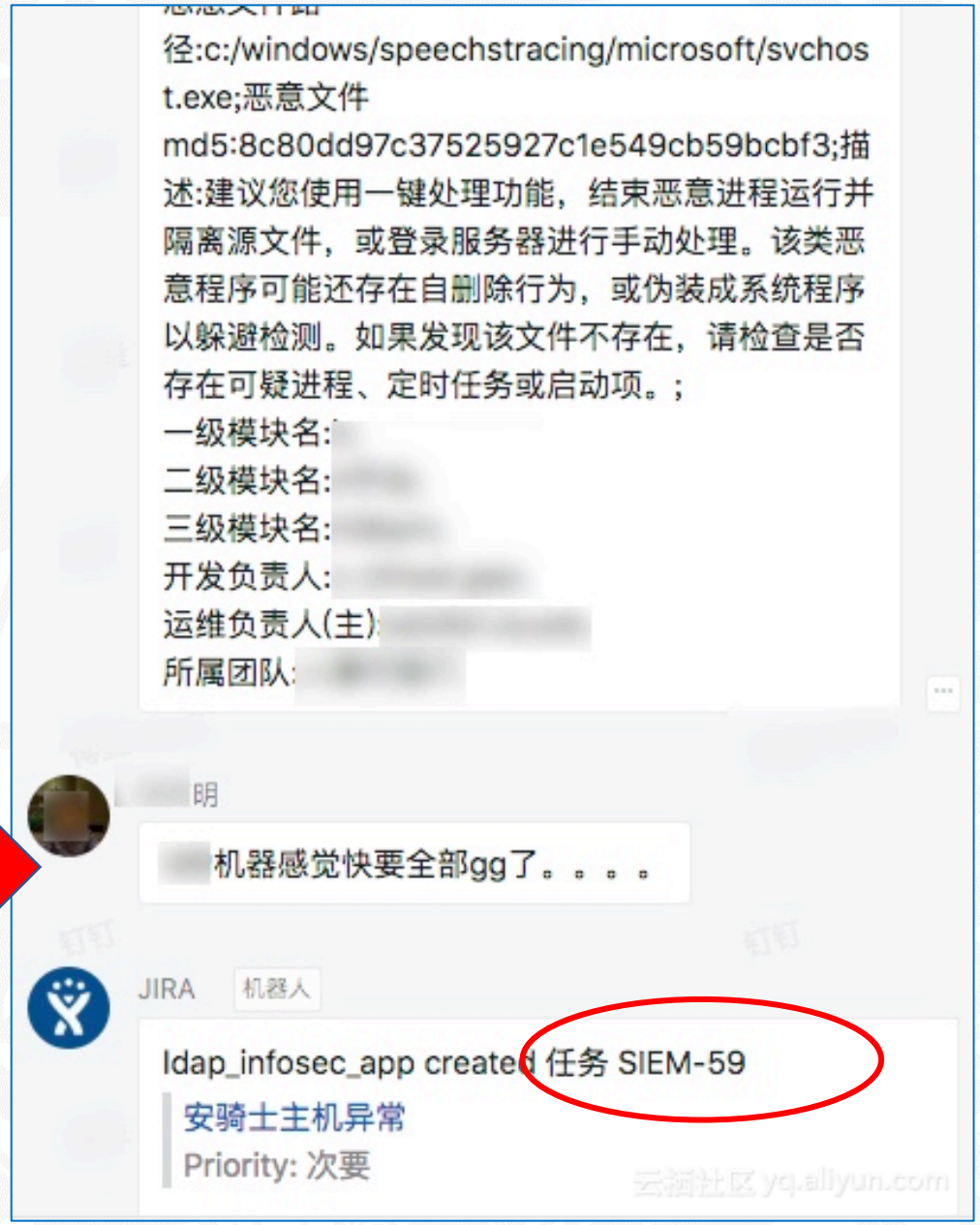
- 案例分享
- 现实困境
- 关于自动化
- 编排vs智能编排

安全事件运营真实案例分享

1

案例1: 一次云上病毒事件的应急响应





ROARTALK 嘶吼

启动内部应急响应流程——进入战斗准备

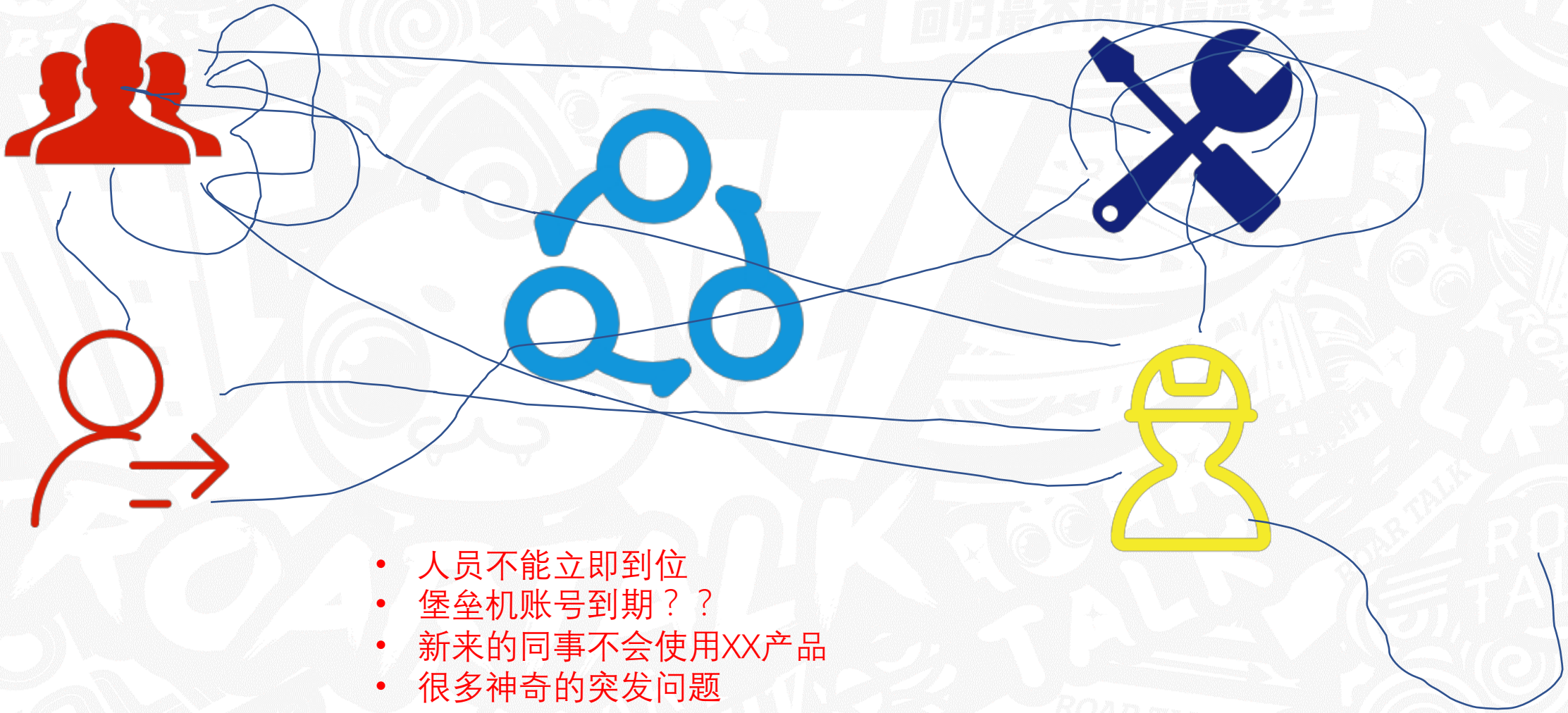
响应	调查	评估	隔离	复盘	跟进
• 启动流程	• 日志查看 • 情报整合	• 态势分析	• 安全组配置	• 攻击链还原	• 系统重置 • 漏洞修复 • 问题根因解决

嗯，这很理想～～ ☺

参考：https://yq.aliyun.com/articles/680783

ROARTALK 嘶吼

休假的赶紧给我上线！——最好还记得VPN密码(现实中)



- 人员不能立即到位
- 堡垒机账号到期？？
- 新来的同事不会使用XX产品
- 很多神奇的突发问题
- ……

参考VSRC： https://mp.weixin.qq.com/s/fVXr-mTx1Iob03vVzI7Bpw

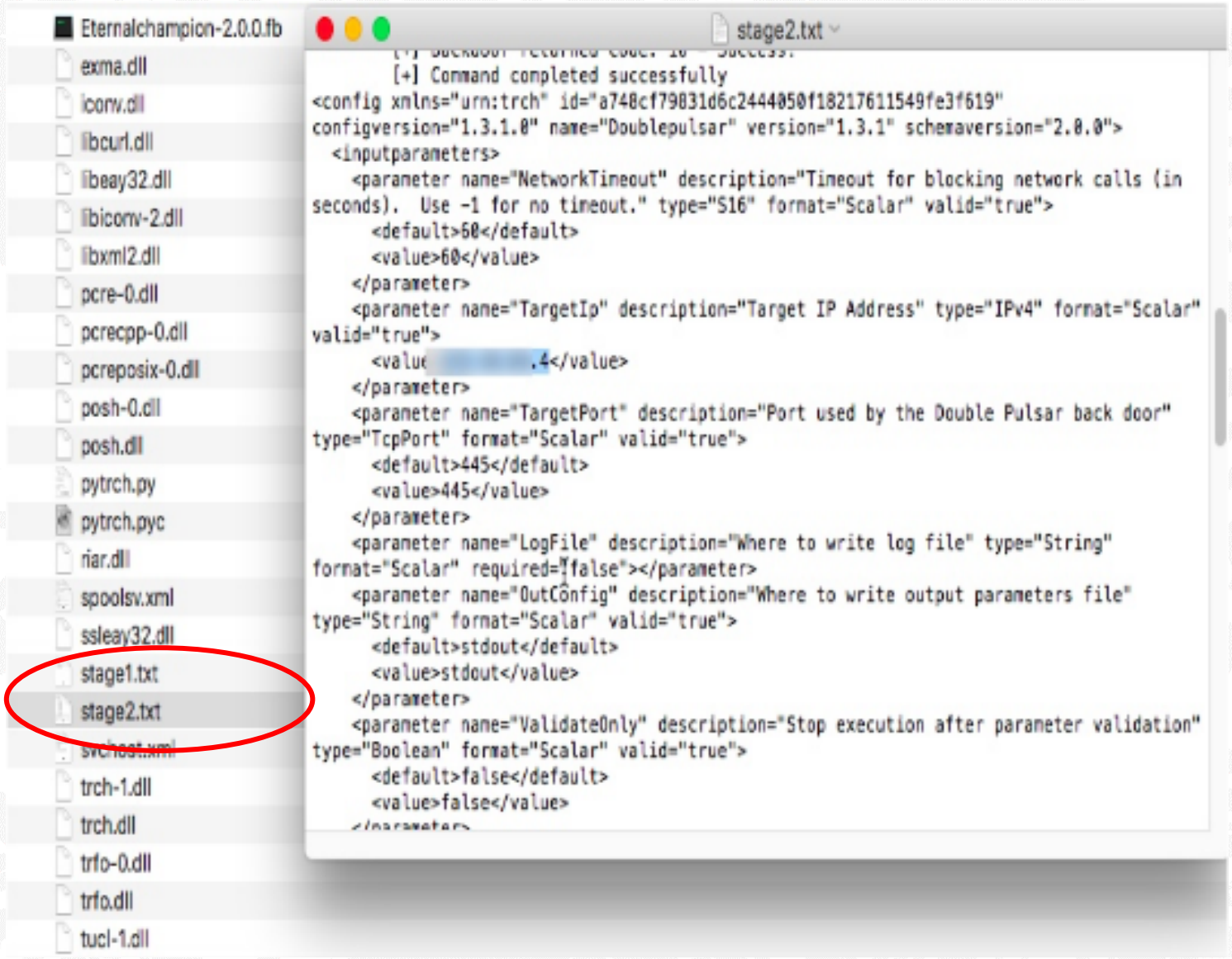
ROARTALK 嘶吼

云平台，多环境、多主机异常告警——查特征，看会话

参考VSRC： https://mp.weixin.qq.com/s/fVXr-mTx1Iob03vVzI7Bpw

ROARTALK 嘶吼
云栖社区 yq.aliyun.com

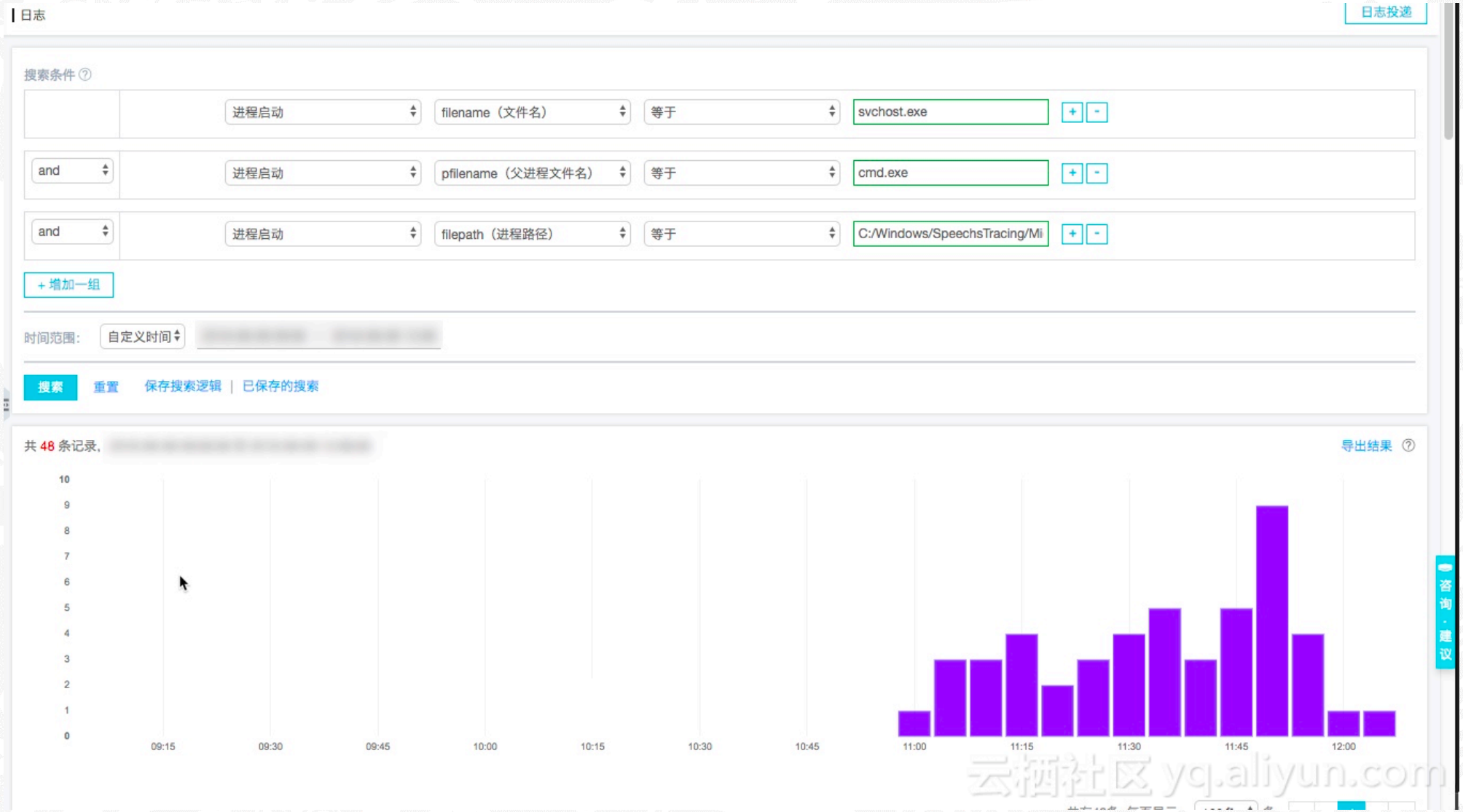
云平台，多环境、多主机异常告警——拉文件，找痕迹



参考VSRC： https://mp.weixin.qq.com/s/fVXr-mTx1Iob03vVzI7Bpw

ROARTALK 嘶吼

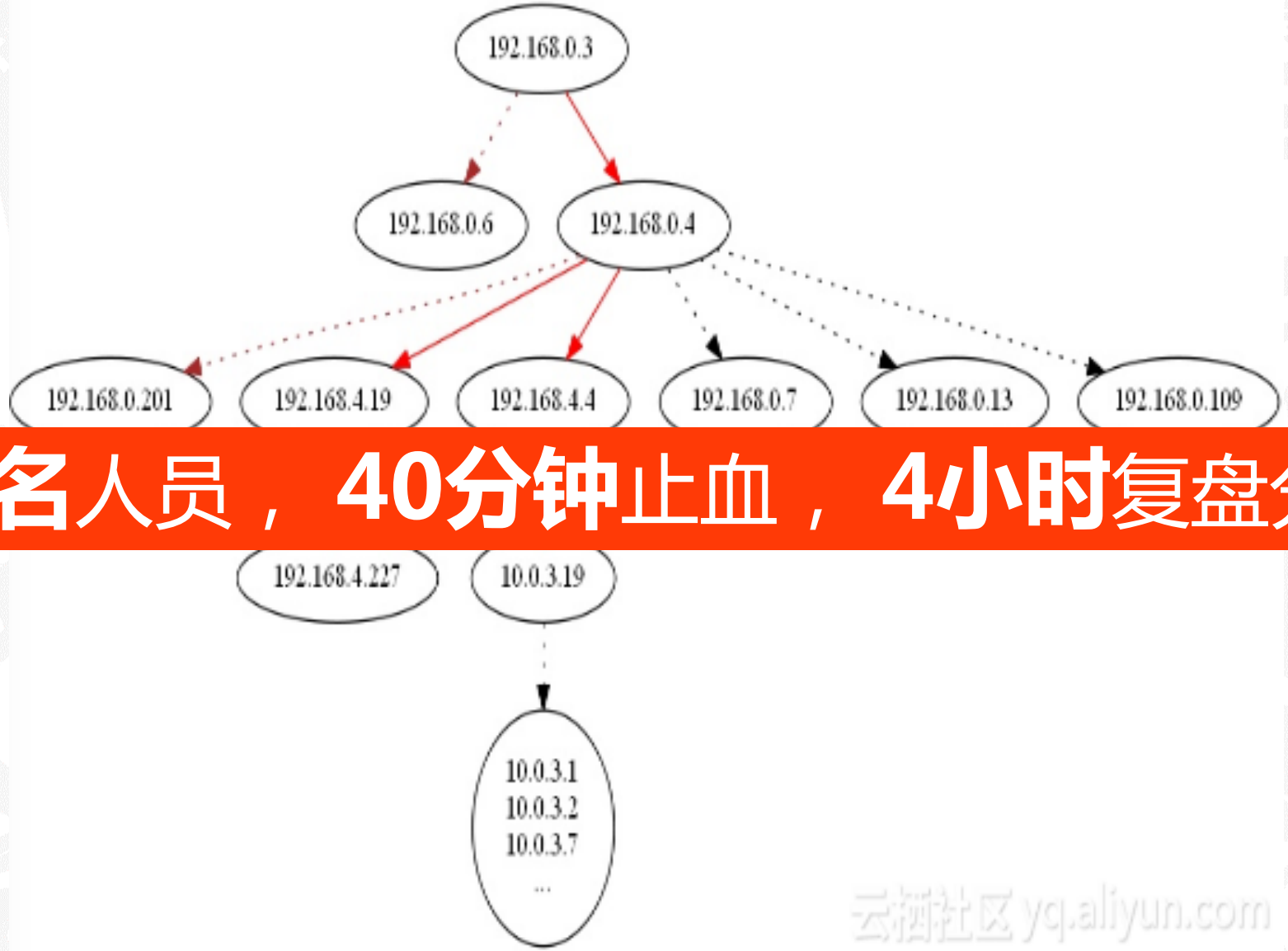
云平台，多环境、多主机异常告警——捞进程，找遗漏



参考VSRC： https://mp.weixin.qq.com/s/fVXr-mTx1lob03vVzI7Bpw

ROARTALK 嘶吼

云平台，多环境、多主机异常告警——输出攻击链



4名人员，40分钟止血，4小时复盘分析

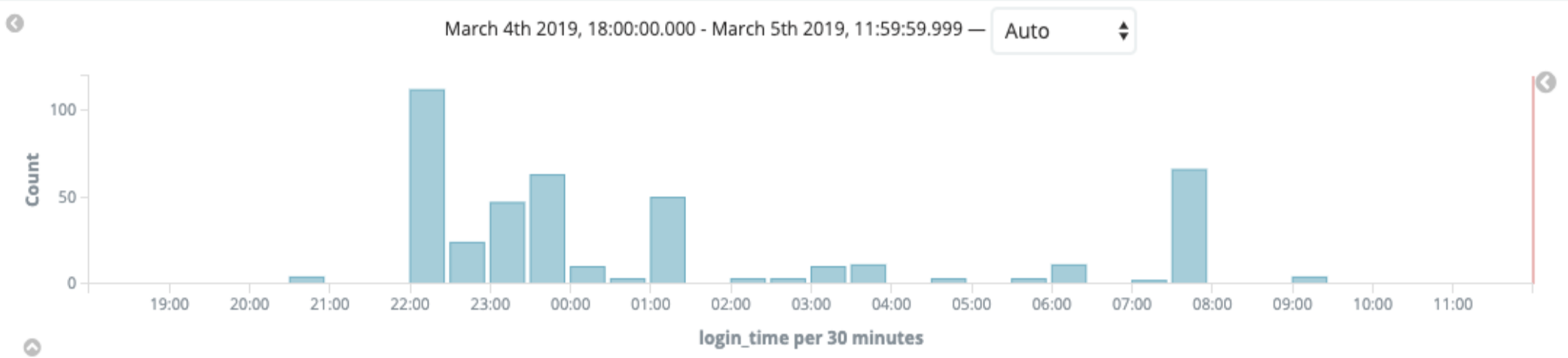
参考VSRC： https://mp.weixin.qq.com/s/fVXr-mTx1lob03vVzI7Bpw

ROARTALK 嘶吼
云栖社区 yq.aliyun.com

案例2: 企业员工邮箱遭遇暴力破解

ROARTALK 嘶吼

多系统、跨部门，人工调查



Time	login_account	login_ip	geoip.region_name	login_type	login_result
March 5th 2019, 09:22:22.000	a[redacted].com	[redacted]9.220	Shanghai	客户端（IMAP）	失败
March 5th 2019, 09:22:16.000	a[redacted].com	[redacted]9.220	Shanghai	客户端（IMAP）	失败
March 5th 2019, 09:22:23.000	a[redacted].com	[redacted]9.220	Shanghai	客户端（IMAP）	失败
March 5th 2019, 07:58:25.000	a[redacted].com	[redacted]04.43	Shanghai	客户端（IMAP）	失败
March 5th 2019, 07:58:32.000	a[redacted].com	[redacted]04.43	Shanghai	客户端（IMAP）	失败
March 5th 2019, 07:55:59.000	a[redacted].com	[redacted]04.43	Shanghai	客户端（IMAP）	失败

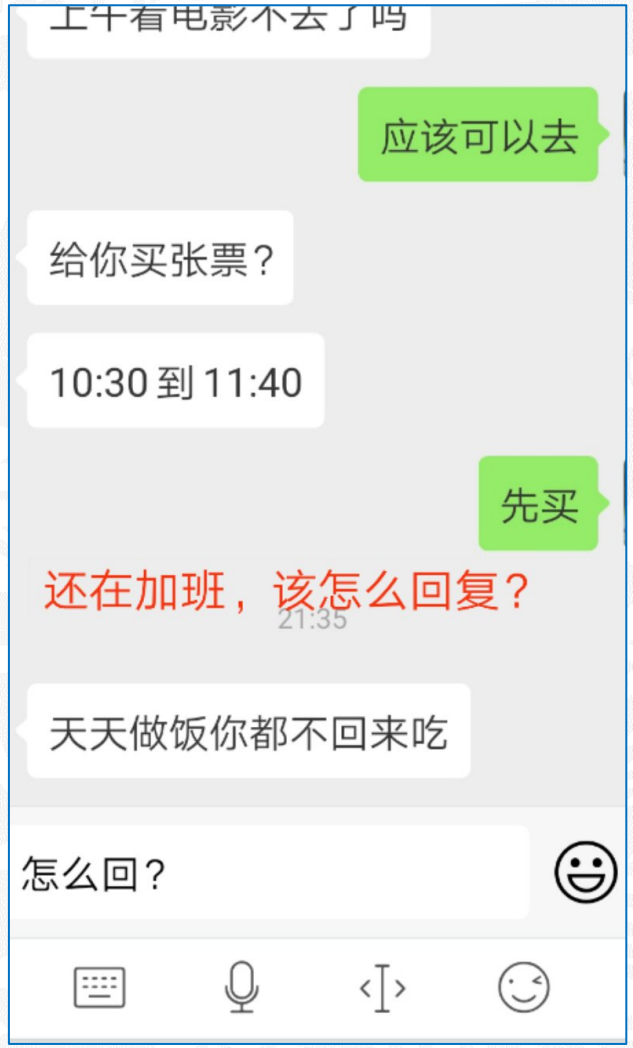
忙了一晚上，是个误报，坑！

ROARTALK 嘶吼

听听一线工程师发自内心的声音：

- 人工交互太多，费时费力
- 跨系统，跨平台，跨设备，操作技能要求高
- 即使有标准SOP，速度也无法保证
- 处置经验很难有效沉淀
- 类似事件频发且突发，太多不确定性

严重影响从业人员的生活幸福指数……

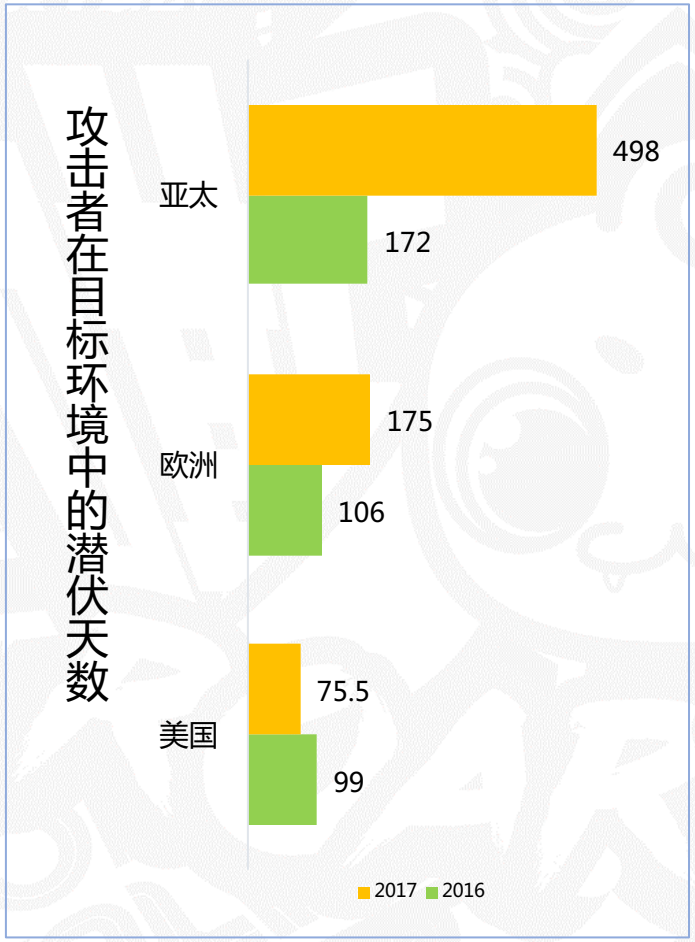


ROARTALK 嘶吼

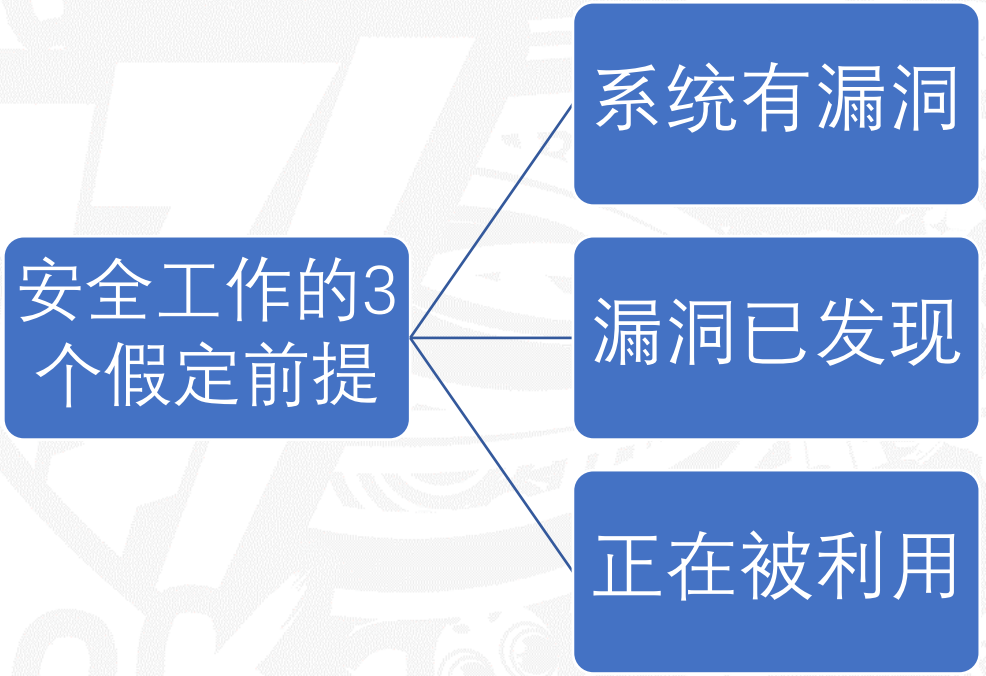
安全运营的现实困境

2

时间是企业安全威胁响应的最大敌人（1）——威胁检测

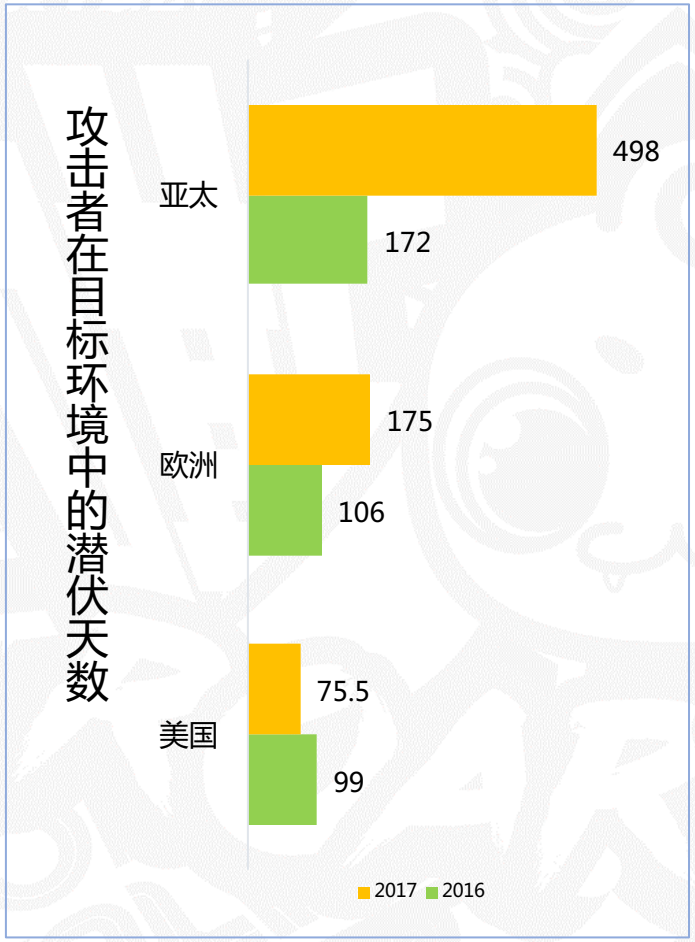


*数据来源：《Mtrends-2018(fireeye)》

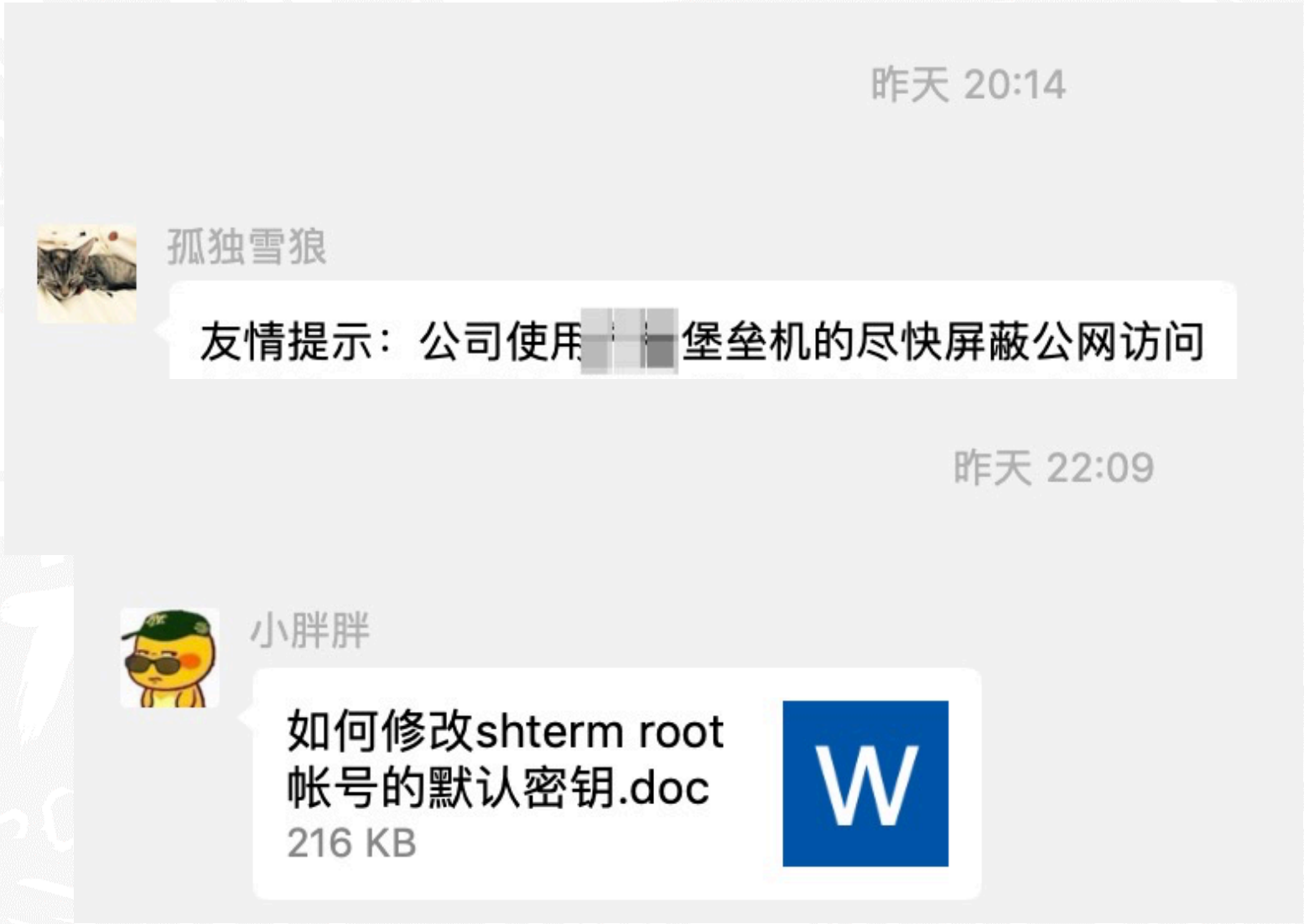


ROARTALK 嘶吼

时间是企业安全威胁响应的最大敌人（1）——威胁检测



*数据来源：《Mtrends-2018(fireeye)》



ROARTALK 嘶吼

时间是企业安全威胁响应的最大敌人（2）——威胁响应

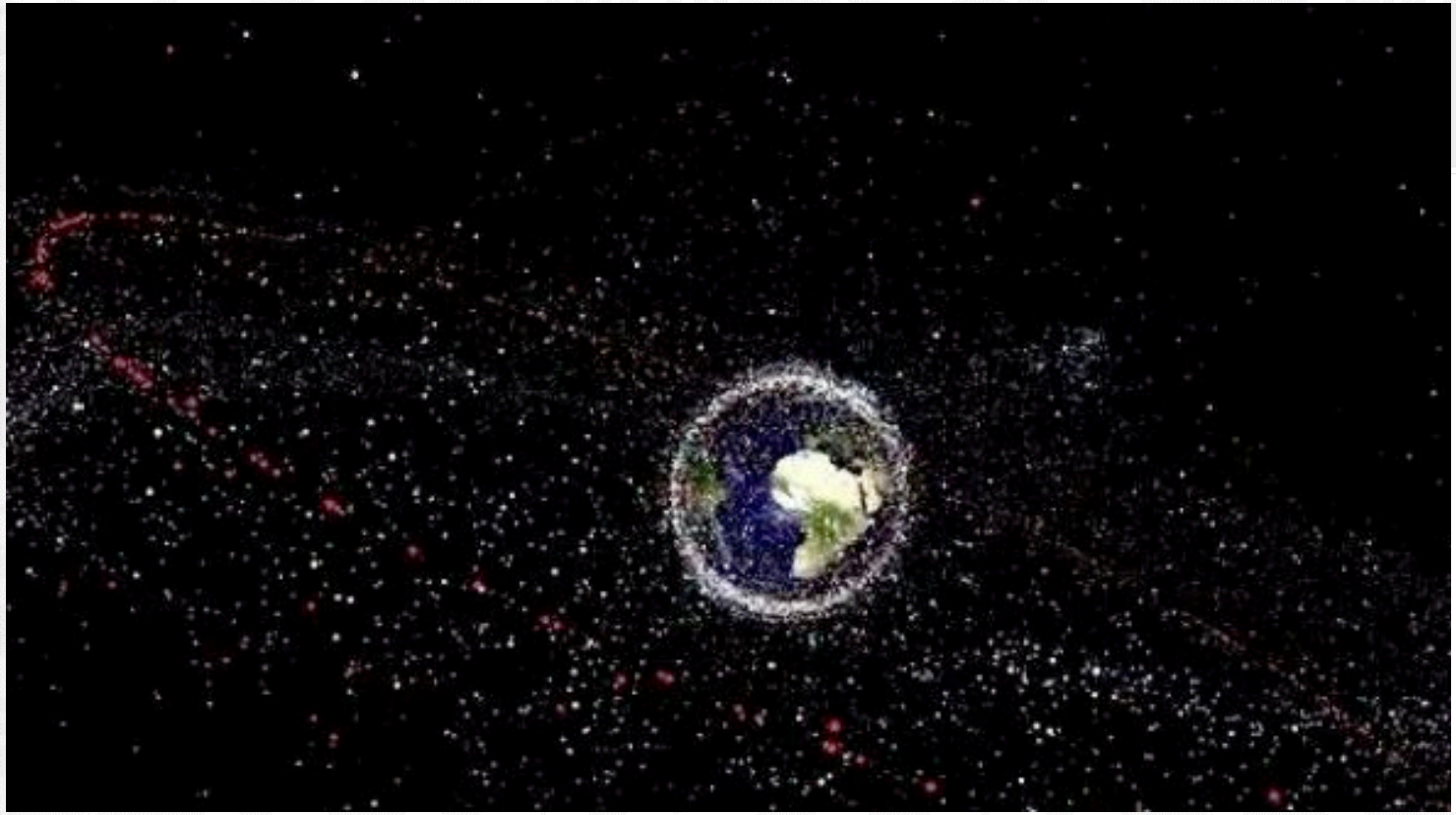
SOC

中型企业每月收到超过15000条安全告警

告警淹没和告警忽略是常有的事……

ROARTALK 嘶吼

安全事件运营的最后一公里……



覆盖到宇宙的态势感知，也解决不了当前威胁响应的缓慢

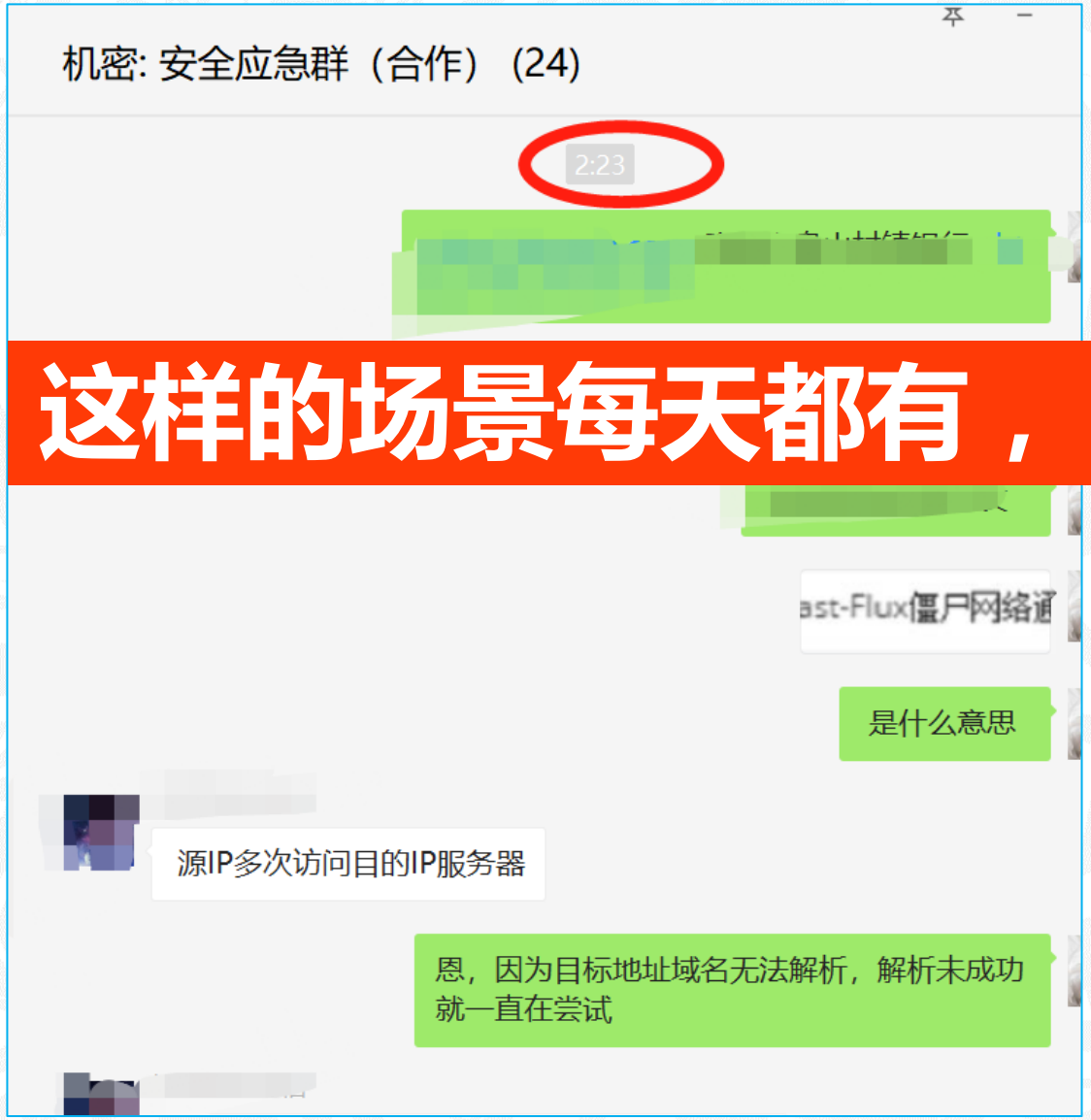
加速威胁响应是未来安全运营的趋势

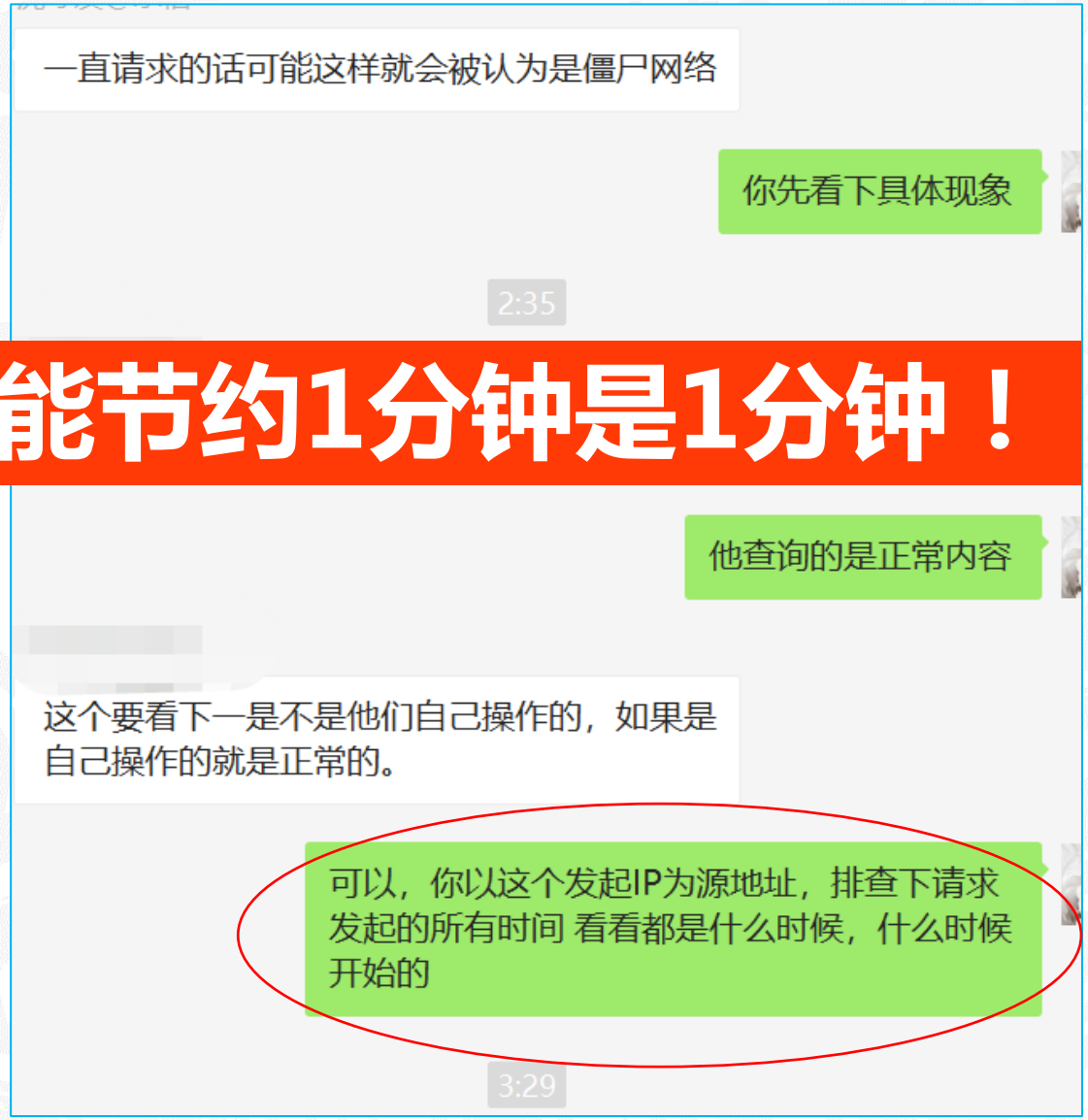
ROARTALK 嘶吼

自动化是不错的开始

3

防守方HW真实工作场景

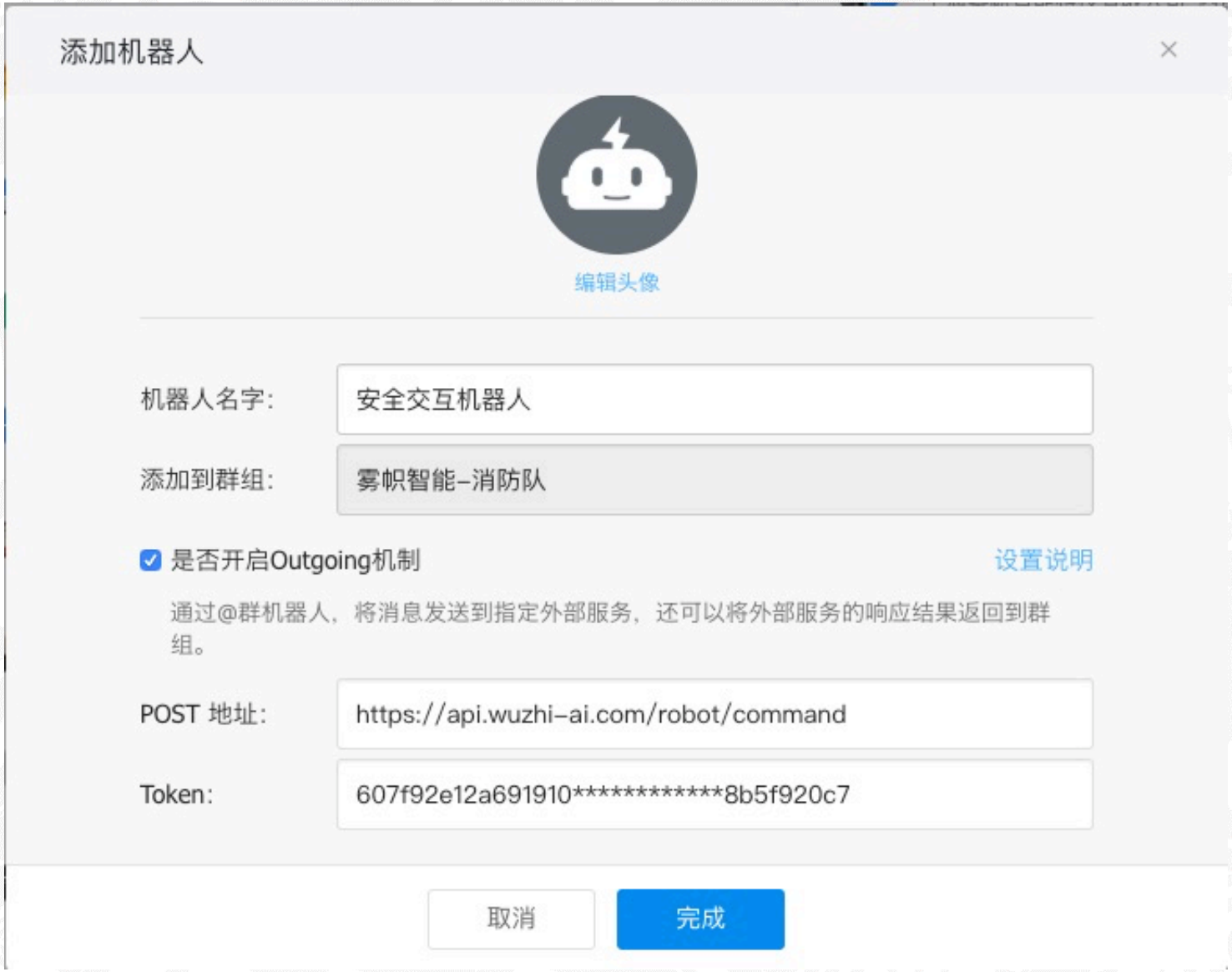




这样的场景每天都有，能节约1分钟是1分钟！

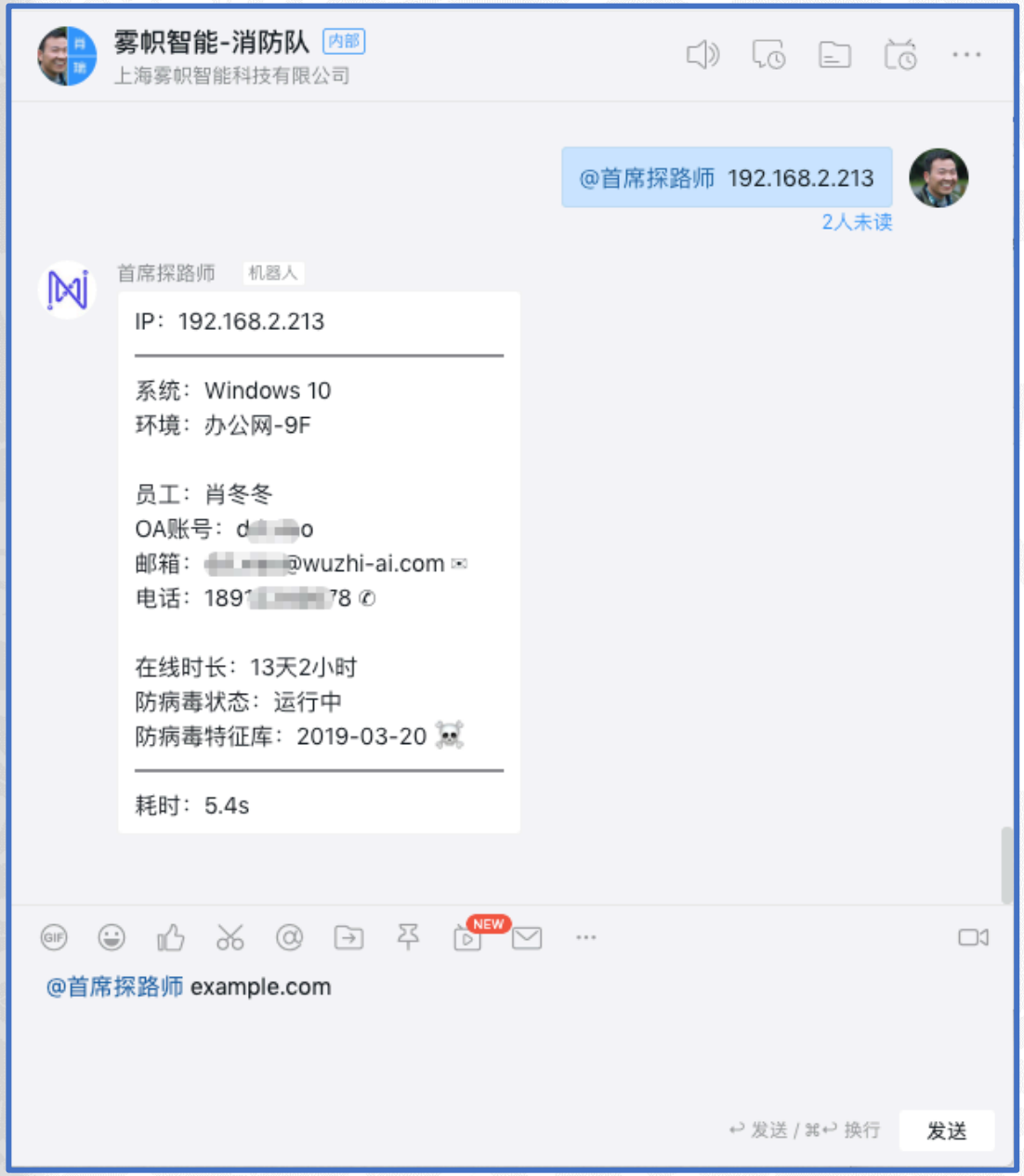
ROARTALK 嘶吼

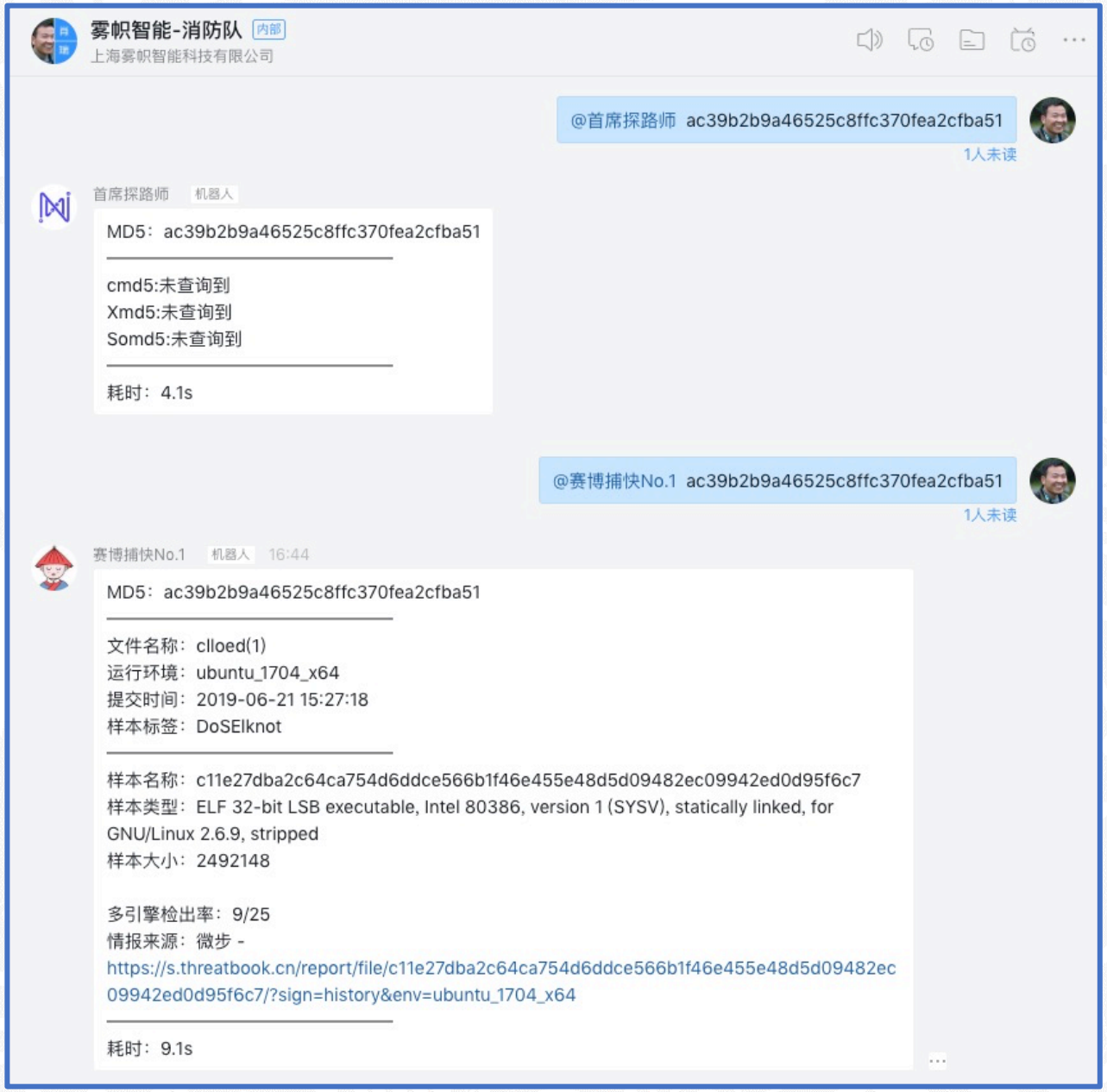
自动化从办公群聊开始——钉钉机器人～outgoing



ROARTALK 嘶吼

减少安全工程师手工工作量——钉钉机器人交互





ROARTALK 嘶吼

减少安全工程师手工工作量——企业微信应用

这些都还不够，还需要解放更多的手工操作

ROARTALK 嘶吼

智能编排如何加速威胁响应

4

构建自适应网络安全，自动化只是开始……

“我们寻求革命化的网络安全，在网络防御中借助通用自动化和交互式操作的方式，最终超越网络攻击的速度和规模。”

参考：https://www.iacdautomate.org/

ROARTALK 嘶吼

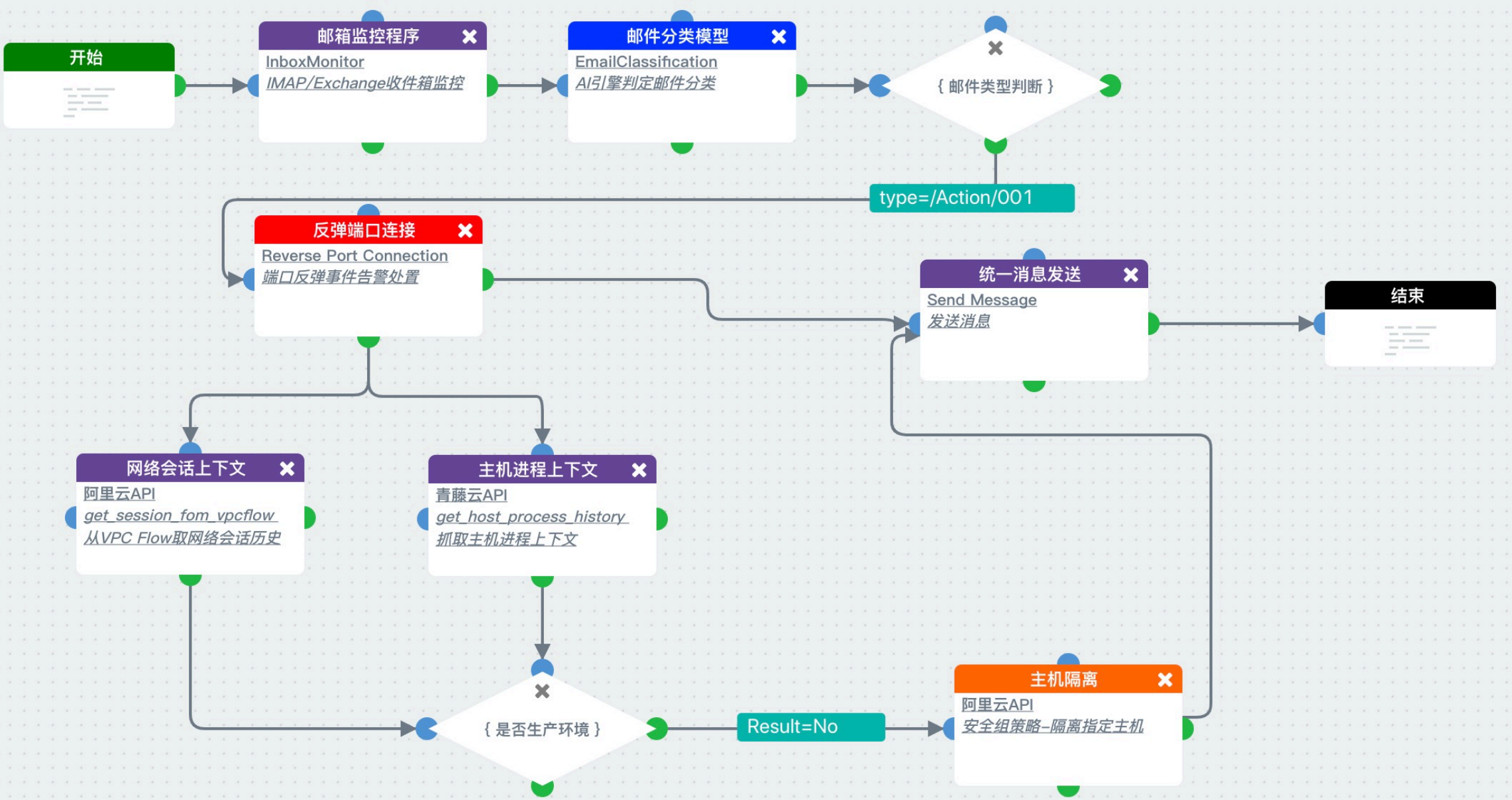
SOAR（安全编排、自动化和响应）是IACD的实现形式

简单地说：安全事件来了，让机器按照你编排的计划去干活

- 像剧本一样开展安全运营工作
- 提高并衡量 SIEM/SOC团队的生产力
- 让SOP执行更加标准化
- 机器没有情绪，总能稳定发挥☺

ROARTALK 嘶吼

安全编排——机器人托管工作邮件



ROARTALK 嘶吼

智能编排又是什么？

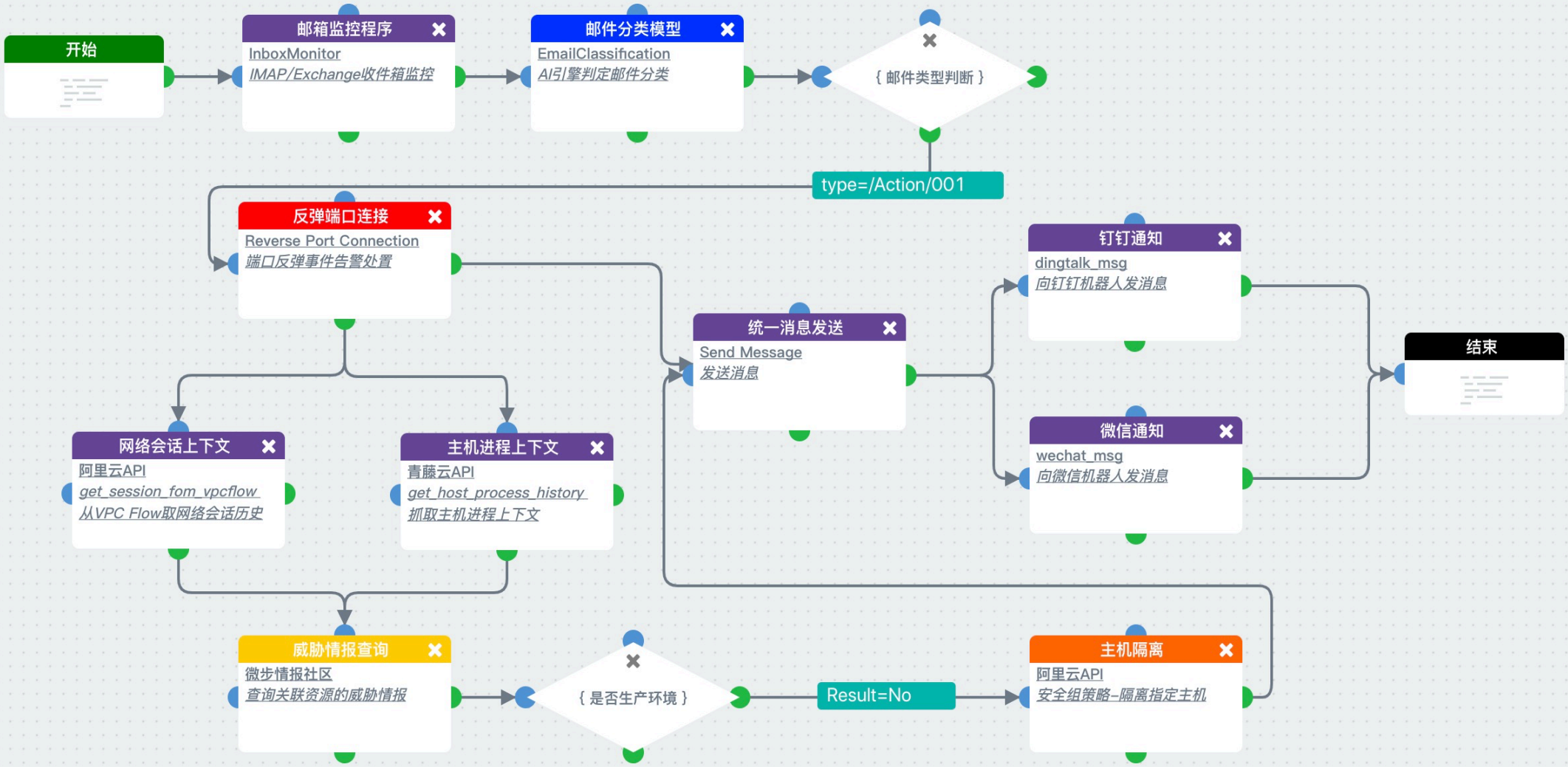
简单地说：将人工智能与安全编排结合，实现人机协同，助力安全运营

- 实现对复杂攻击的引导式响应
- 人机系统相互迭代优化
- 未来让“无人值守”的安全运营中心变得可能

ROARTALK 嘶吼

安全剧本描述： 机器人托管邮件

保 存

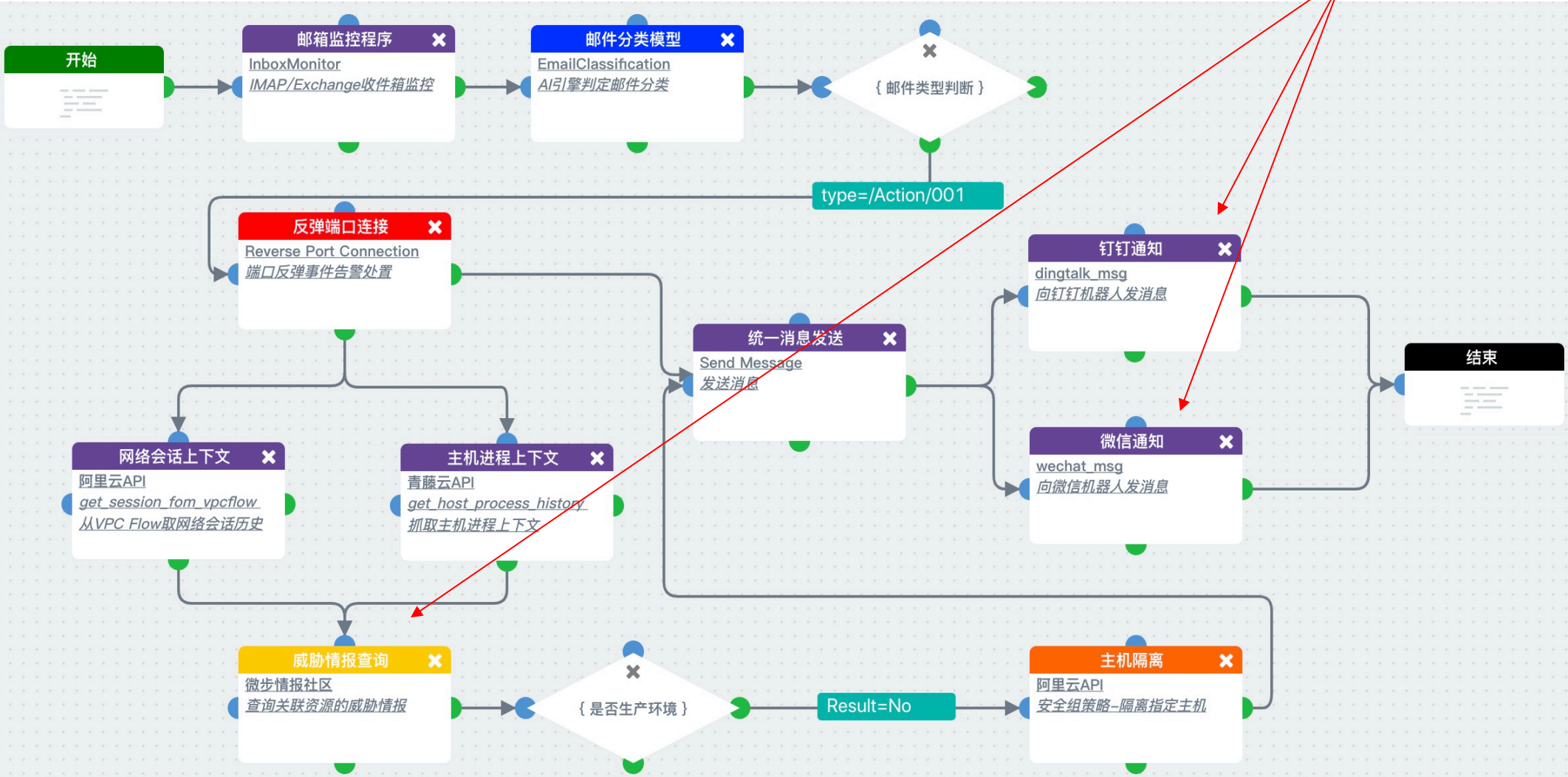


ROARTALK 嘶吼

安全剧本描述： 机器人托管邮件

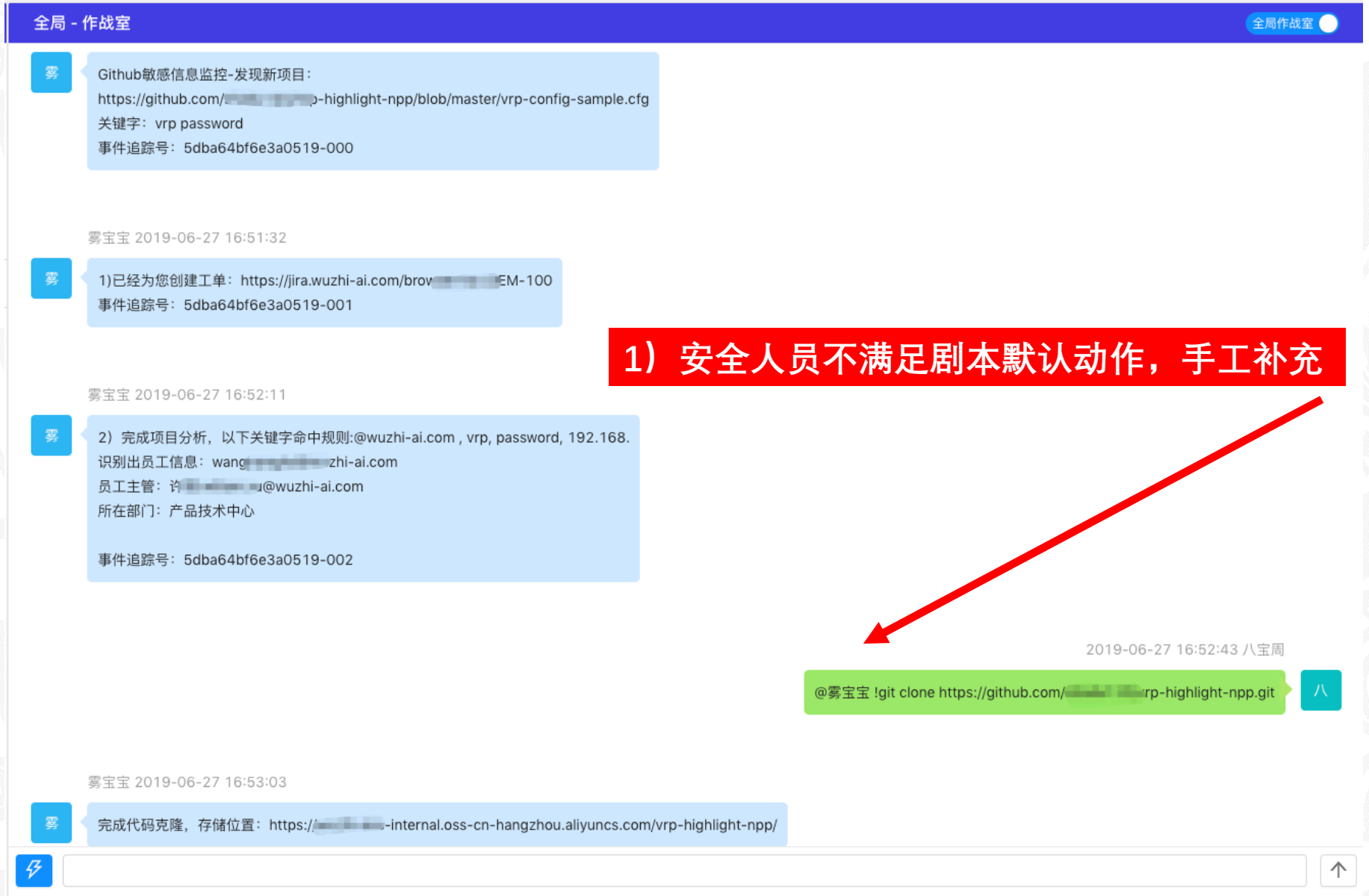
AI智能编排向用户推荐操作指令

保存



ROARTALK 嘶吼

安全编排案例——Github敏感信息泄露

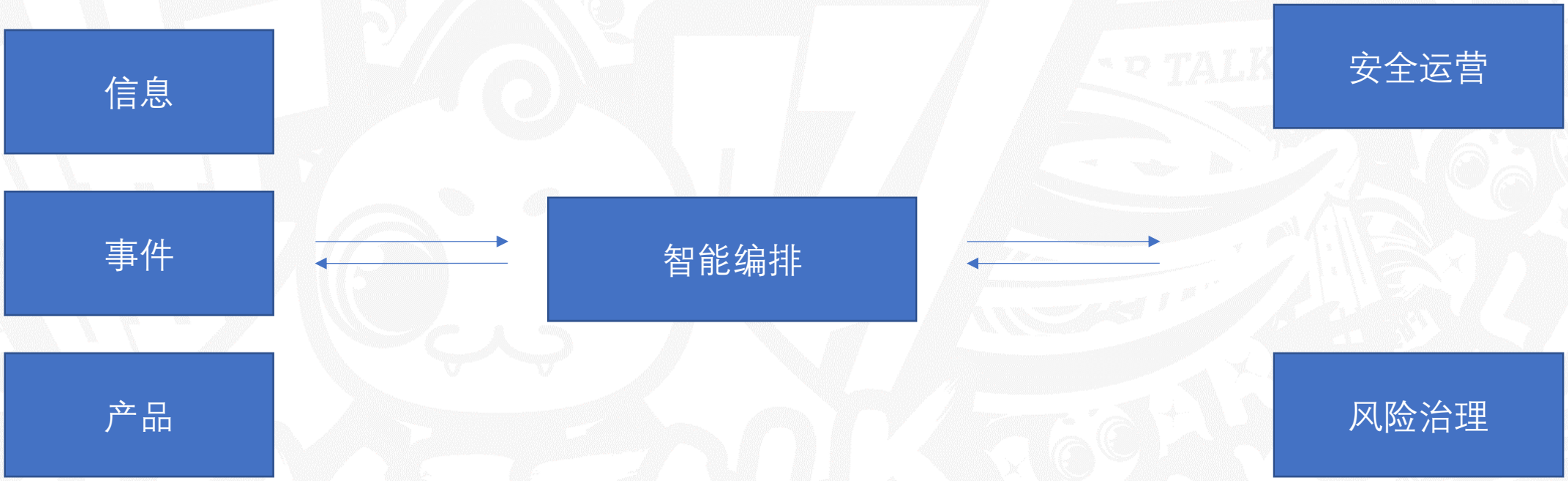


ROARTALK 嘶吼

智能编排案例——Github敏感信息泄露（操作行为学习）

ROARTALK 嘶吼

智能编排加速安全威胁响应



ROARTALK 嘶吼

期待智能编排的未来：

更快	更好用	更开放	更智能
• 减少人脑CPU的切换 • 减少系统交互时间 • 智能补齐上下文	• 主动推荐响应动作 • 沉淀安全剧本（套路） • 沉淀安全案例（知识） • 数字化并动态评估安全能力	• 开放交互接口 • 允许自定义动作 • 适配企业产品 • 兼容主流协作平台	• 智能风险决策 • 场景自适应 • 自然语言交互

每一天，请给我留一杯咖啡的时间……

ROARTALK 嘶吼

THANKS!

嘶吼
ROARTALK