



争分夺秒，加速应急响应

AI+SOAR

雾帆智能 CTO 傅奎

# 一、背景介绍

# 时间是最大的敌人



# 与攻击者赛跑抢的是时间



告警淹没，处置缓慢



操作靠手，沟通靠吼



新手不会，老手不够

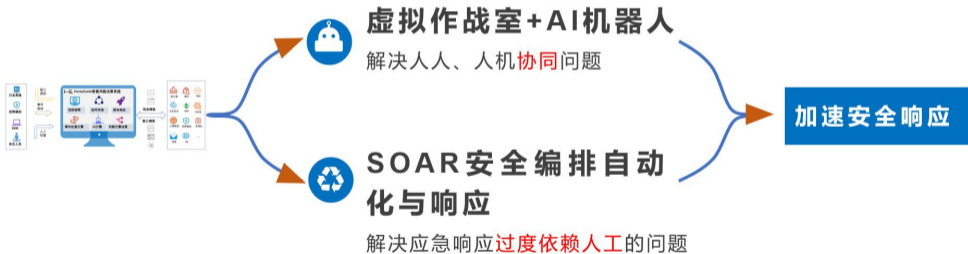


情绪不稳，记忆出错

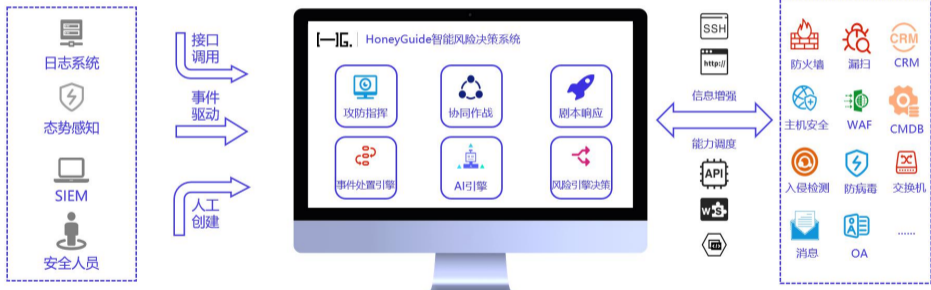
自动化、智能化的网络武器作战平台

高成本、低效率的人工响应团队

# HoneyGuide: 虚拟作战室+AI+SOAR

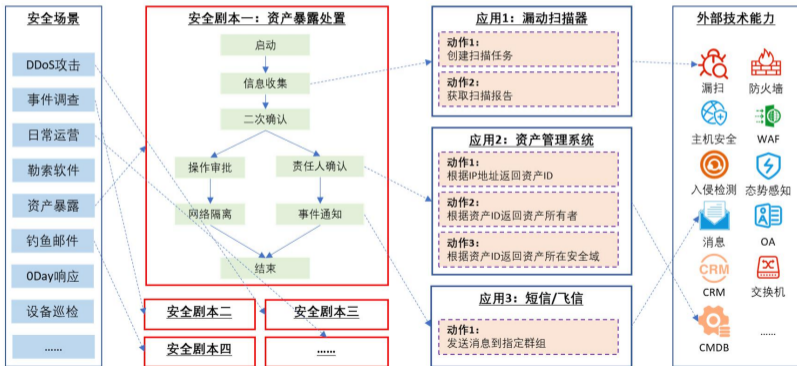


# HoneyGuide: 连接中枢和调度指挥中心



全面加速多人、多系统、多界面切换的事件响应

# 一图看懂SOAR原理：“安全套路自动化”



## 二、产品概览





# 支持自然语言交互的机器人和作战室

首页 / 作战室

日常安全运营 正常

阿宝

我的关注

作战室 - 暴力破解事件\_20210510113009008

全局作战室

人员组织

- 系统管理员
  - 阿宝
  - 丘军
- 第三方协调人员
  - 陈海志
- 事件处理员
  - 安小虎

雾宝宝 2021-05-10 15:19:20

阿宝 2021-05-10 15:40:14

```
xmlint --shell${pom_path}/pom.xml <<EOF cd/*[local-name]="project"/*[local-name]="properties"/*[local-name]="shakespeare.version" set ${project_version} save
```

雾宝宝 2021-05-22 09:18:38

@阿宝 关注

# 可视化无代码拖拽式剧本编排

1-16

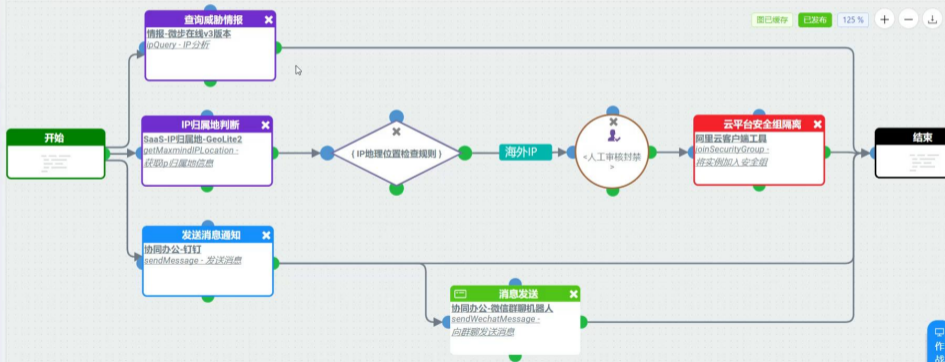
首页 / 安全剧本 / 剧本编排

日常安全运营 正常 消息 通知 阿 阿宝

剧本名: 暴力破解处置剧本\_云上 \* 描述: 暴力破解处置剧本\_云上 类型: 普通 场景: HW安全保障 标签: demo

发布

图已缓存 已发布 125% + - 下载



作战室

# 300+安全产品（国产为主）调度，降低使用成本





# 雾帆智能SOAR：支持云、容器、软硬件、国产化

- **部署**：硬件、软件和容器化
- **云环境**：阿里云、腾讯云、华为云、UCloud、AWS等
- **高可用**：多引擎、跨网络、分布式
- **操作系统**：CentOS、Redhat、Ubuntu、中标麒麟、Debian
- **适配硬件**：X86、ARM CPU、鲲鹏架构处理器

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/185201044020011320>