争分夺秒，加速应急响应

AI+SOAR

雾帜智能 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

虚拟作战室+AI机器人

解决人人、人机协同问题

SOAR安全编排自动化与响应

解决应急响应过度依赖人工的问题

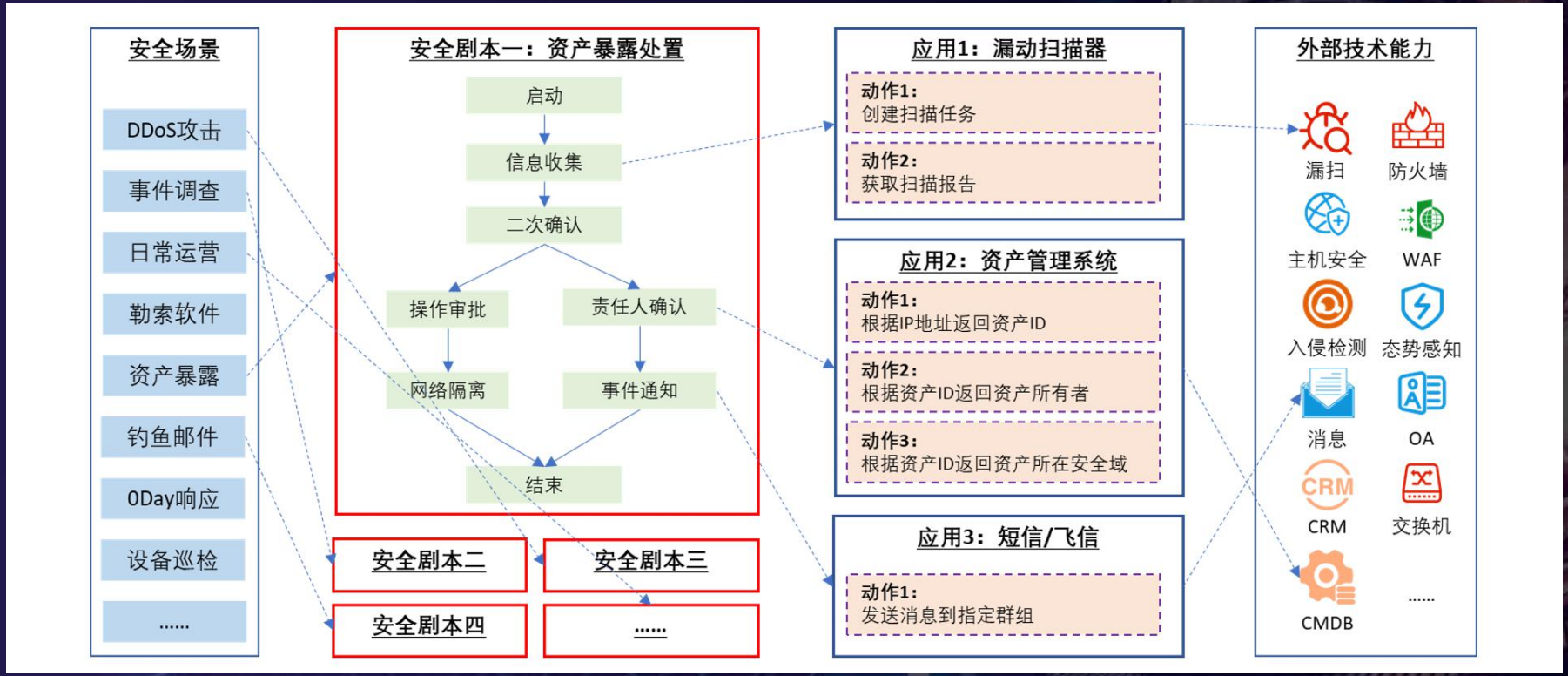
加速安全响应

Security Orchestration Automation & Response

HoneyGuide：连接中枢和调度指挥中心

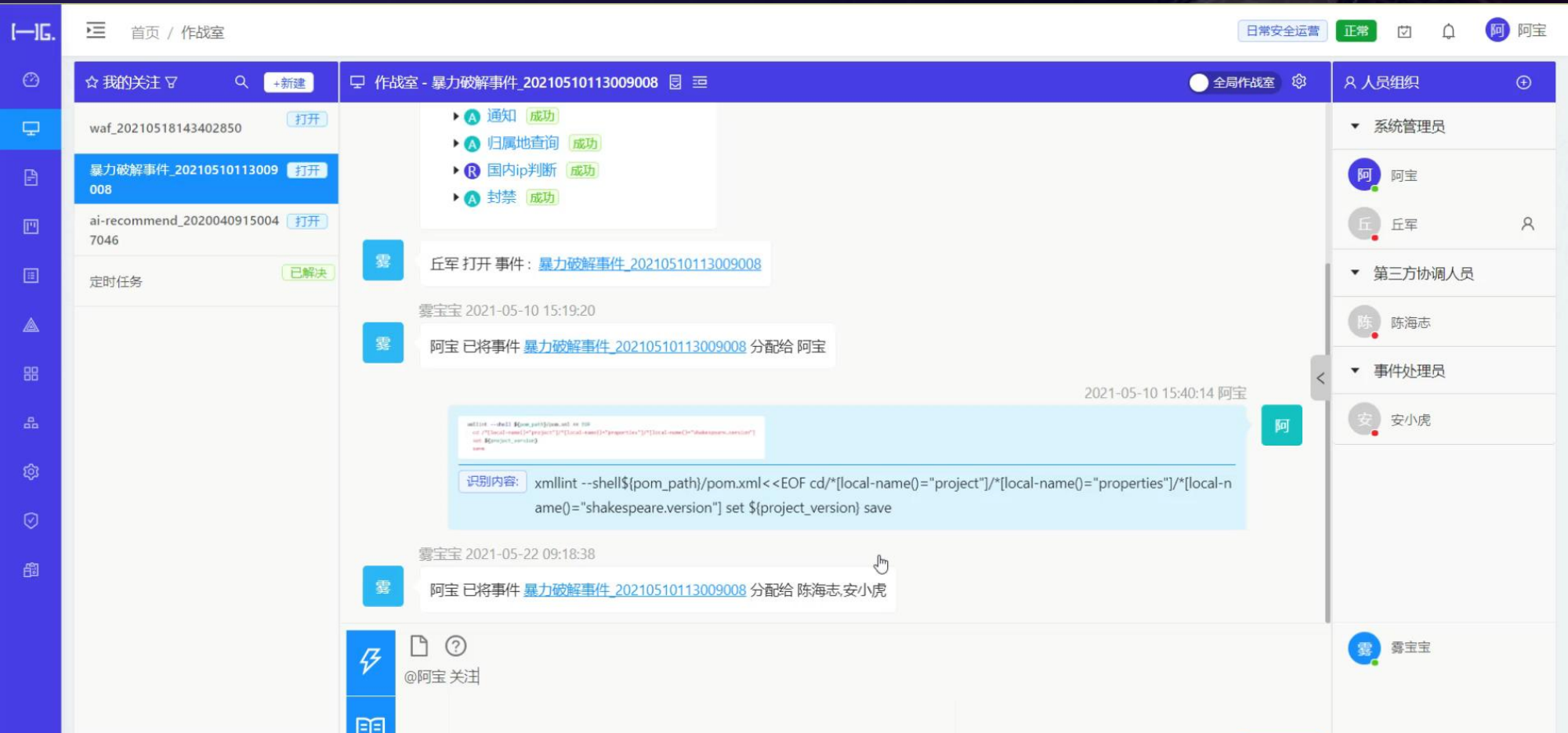
全面加速多人、多系统、多界面切换的事件响应

一图看懂SOAR原理：“ 安全套路自动化”

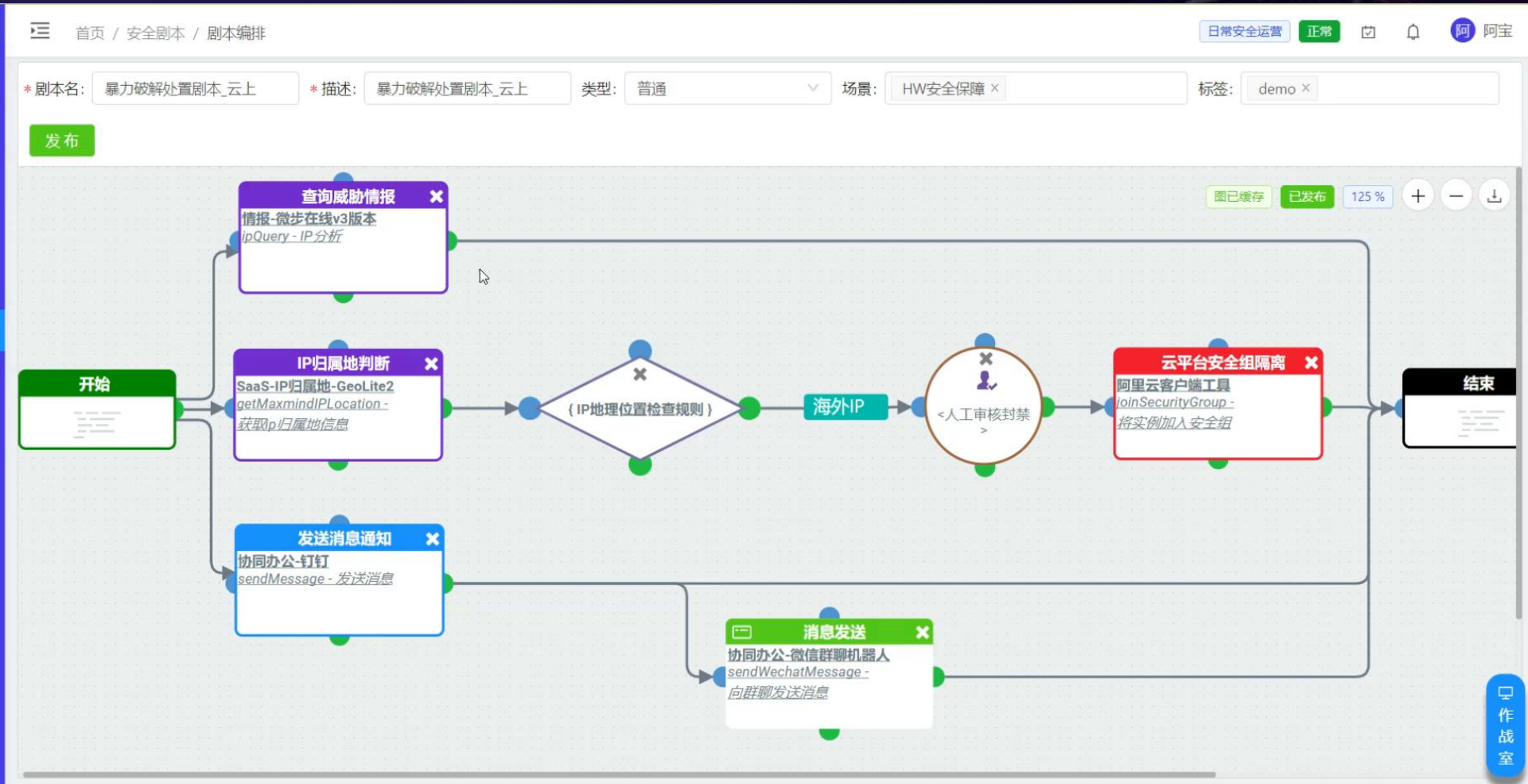


二、产品概览

支持自然语言交互的机器人和作战室



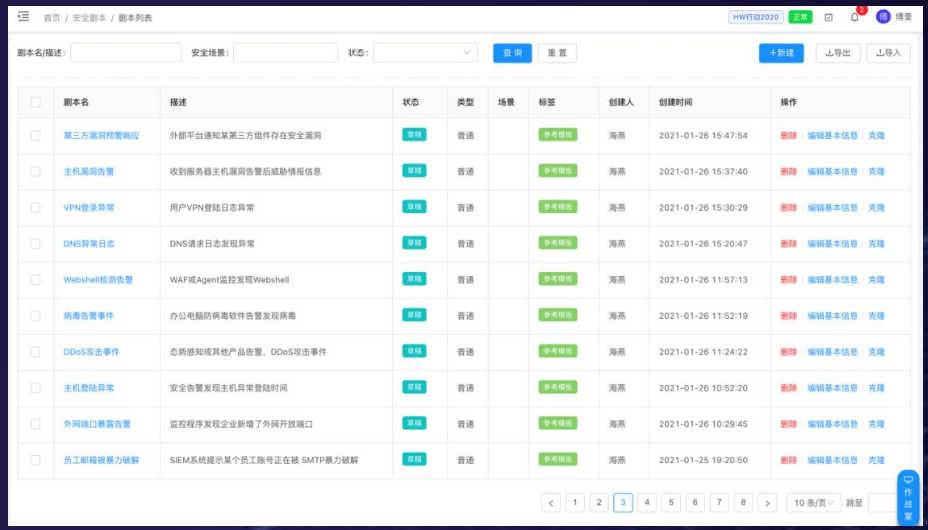
可视化无代码拖拽式剧本编排



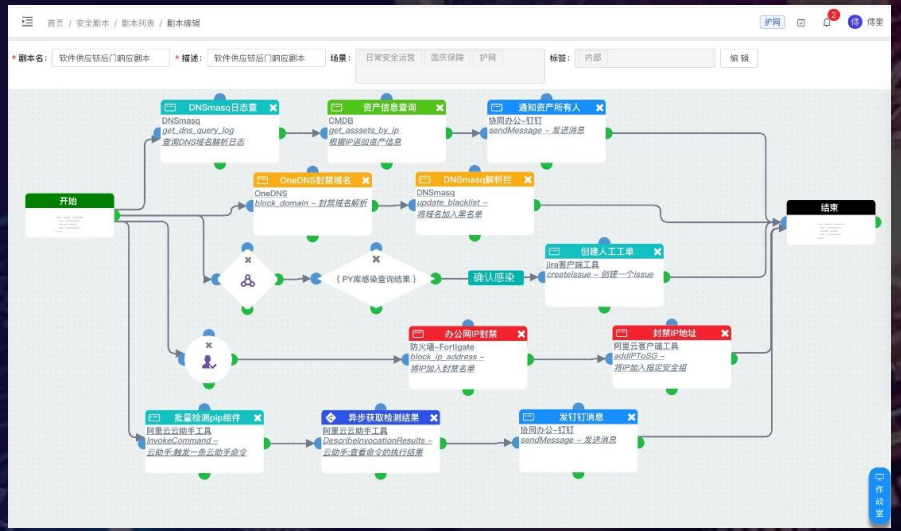
300+安全产品（国产为主）调度，降低使用成本

丰富的安全场景处置剧本 降低落地难度

内置50+适配场景的通用剧本模板



支持客户自主拖拽创建剧本



雾帜智能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