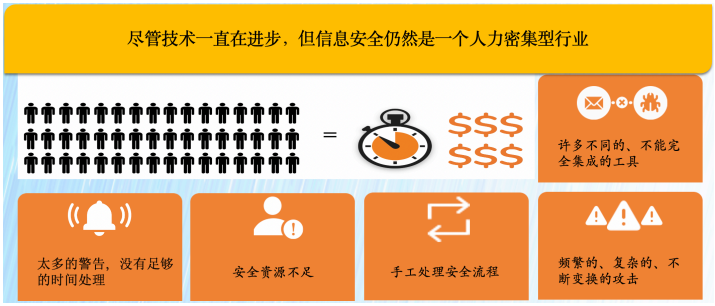
千乘安全自动化（SOAR）平台

自动化工作流、插件社区、全流程、多种逻辑关系、状态展示、安全最佳实践

安全编排、自动化和响应（Security Orchestration, Automation and Response）是信息安全领域近几年提出来的新概念，Gartner预计越来越多的企业会进行SOAR平台建设。很多企业已经建立或正在建立完备的安全运营中心（SOC），为什么又要提出SOAR的概念呢？主要是因为在SOC的运营过程中，面临以下一些关键问题：

- 安全情报、SOC告警、海量日志，您是如何完成响应的？
- 安全工具种类众多，如何完成配置和响应？
- 安全资源不足、人手不足、预算不足、离职率高？
- 具有经验的安全分析师浪费大量时间在无关紧要的事件分析上。
- 业务高峰、关键人离职、疫情期间在家办公，安全响应怎么办？

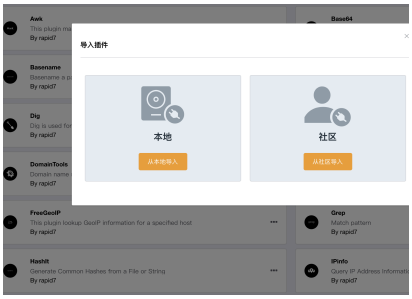


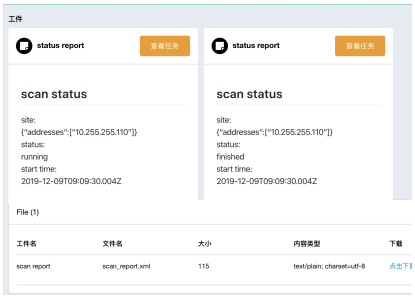
- 信息安全事件处理不可追溯？
- 信息安全事件响应的经验、流程如何传递？

千乘SOAR平台是由上海碳泽信息科技有限公司研发的安全编排自动化响应平台，提高企业的安全自动化水平及SOC运营效率，帮助安全团队以最快的速度对时间密集型安全事件实现自动化/半自动化（需要人工决策）流程。

基于业务优先级

- 基于要保护的核心资产
- 响应高风险威胁
- 整合内部信息安全资源
- 对接SIEM等多种数据源





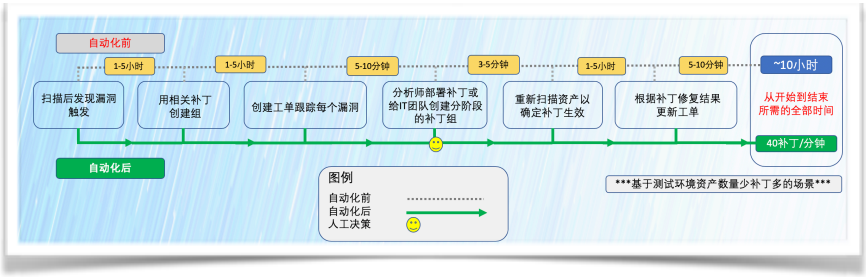
自动化工作流

- 信息安全事件自动处理流程
- 模块化处理，对接无限资源
- 支持超过300家厂商的工具
- 支持自定义对接插件和社区
- 采用核心引擎+插件的结构，避免性能问题
- 工作流自定义、重复调用
- 支持人工处理台，人机结合
- 提供详细的工作流取证功能
- 支持循环、决策、调查等多种工作逻辑

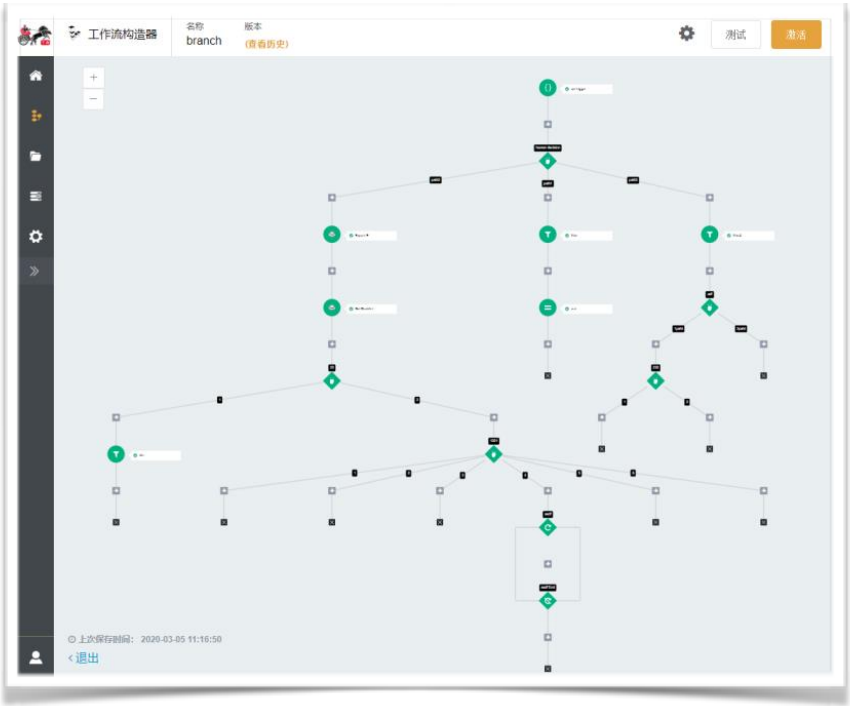
SOAR可视化

- 完善的工作流状态呈现
- 一目了然的工作流结果展现
- 多用户协同工作
- 数据快速取证和搜索

工作流最佳实践



杰出的工作流性能和协调能力



最佳实践工作流

- 结合常见场景的最佳实践
- 威胁情报处理工作流
- 垃圾邮件响应工作流
- 防火墙策略调整工作流
- 数据分析工作流
- 漏洞发现和修补工作流
- 恶意软件调查工作流等