碳泽 TANZE

碳泽千乘(SOAR)
安全运营编排自动化响应系统

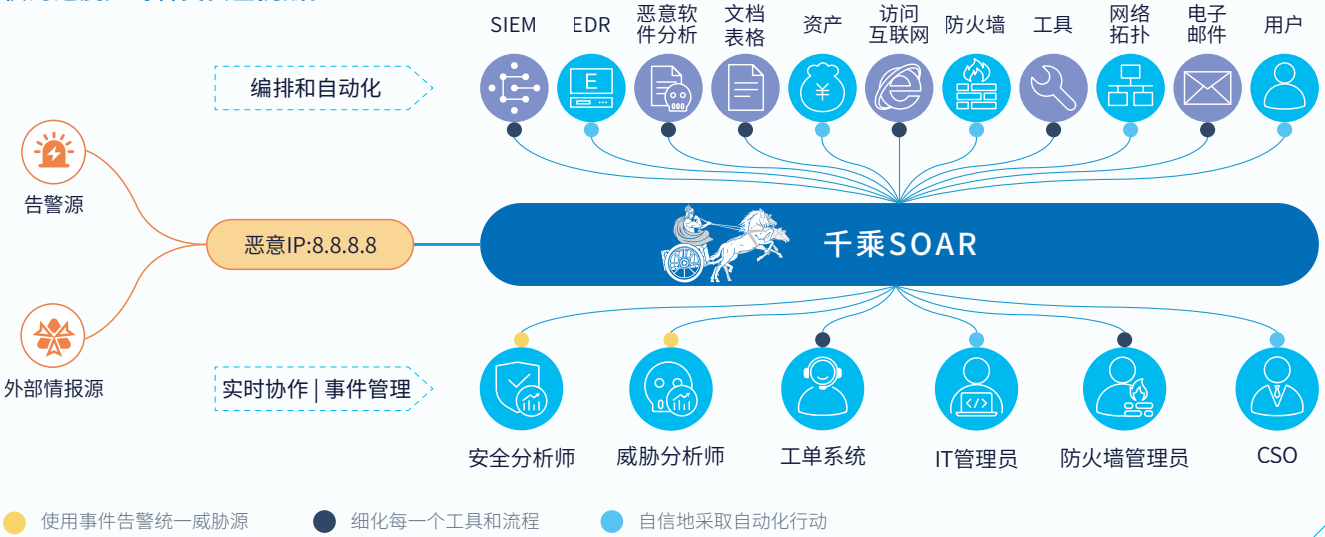
智能化工作流 | 插件社区 | 灵活短剧本 | 多种逻辑关系 | 状态监控 | 丰富的安全运营实践

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。面对纷繁复杂的安全态势，各类组织耗费了大量的人力物力以应对最新的安全威胁;与此同时，很多企业已经建立或正在建立完备的安全运营中心(SOC)。

在安全运营的过程中，也同样面临一些关键问题：

- 碎片化和离散式的信息安全解决方案，如何才能够协同工作?
- 怎么快速处理和跟踪来自SIEM/SOC/IPS的海量告警?
- 没有这足够的信息安全人才如何进行运营工作?
- 没有足够的安全预算如何建设运营中心?
- 如何形成自动化的安全运营体系?
- 如何构建安全运营工作流?
- 威胁情报如何快速响应?

千乘安全运营编排自动化响应系统是由碳泽信息研发的SOAR领域的综合解决方案，是唯一拥有安全数据湖来辅助安全运营的SOAR类产品，**能够帮助客户有效提高安全自动化水平及安全运营效率，帮助安全团队以较快的速度应对各类安全挑战。**



使用事件告警统一威胁源　细化每一个工具和流程　自信地采取自动化行动

01 产品功能特色

出色的工作流引擎

·安全流程编排自动化
·基于独立插件的编排体系
·灵活的插件语言(Python/Go)
·支持插件社区和流程社区
·支持在插件连接器列表中直接测试插件动作,以及优化插件编辑
·通过编排实现高性能的工作流运行
·灵活定义各类工作流逻辑
·支持多分支、分支合并、循环等多种逻辑
·人工决策和自动决策
·丰富的工作流调查和取证
·分布式部署的工作流引擎
·存储空间的横向扩展
·AI快捷指令配置

审计和告警

·工作流状态监控
·大屏展示和报告
·多用户、多权限
·搜索、调查和审计
·多种工作流报告模版
·基于角色的用户权限设定
·工作流、插件执行结果审计
·数据接收监控
·增加“离散分析”分析模型

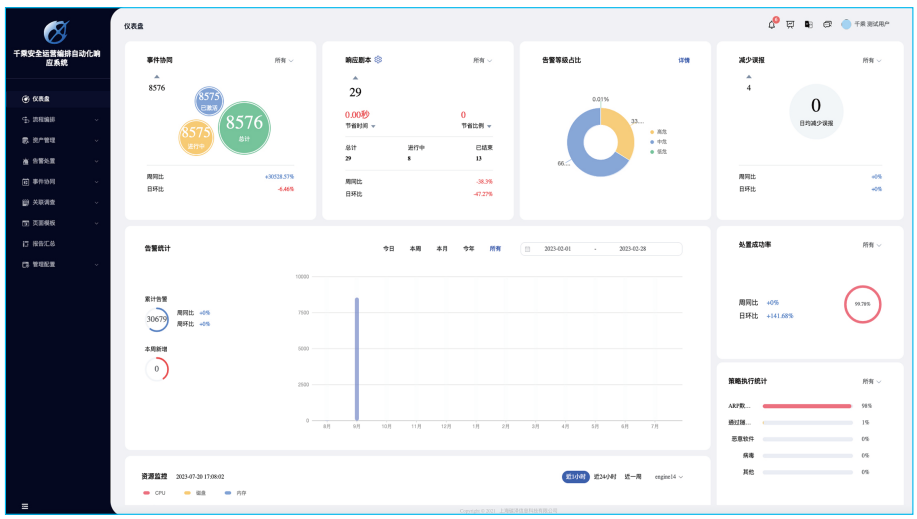
能力角色

·优秀的威胁情报落地者
·增加网络安全纵深
·更轻松的常态化检测
·应对比常规企业更多的供应链攻击
·快捷的异构云整合
·更优的安全策略(制度)的落地者
·容易协调的工控\物联网联动
·安全死角的清除者

安全运营实践

·告警信息快速响应
·威胁情报落地
·恶意邮件调查流程
·防火墙策略管理(一键封禁)
·数据安全工作流(分类分级等)
·漏洞管理工作流
·知识库覆盖发现、检测、响应、恢复等各个类型

02 状态展示



碳泽千乘安全运营编排自动化响应系统界面

支持国内在线大模型:

- 【文心一言(百度)】
- 【通义千问(阿里)】
- 【离线模型(CHARIOT_GPT_API)】

可在系统配置中选择大模型类型

03 工作流样例

上海碳泽信息科技有限公司
Shanghai Tanze Info Tech Co., Ltd
电话:400-1788-258
网址:www.tanze.net.cn
销售咨询:sales@tanze.net.cn
技术支持:support@tanze.net.cn