安世加

Face the challenge,Embrace the best practice

EISS-2021

企业信息安全峰会

上海站 2021.11.19

Security Operations Center

企业自建SOC安全运营的探索实践

合合信息 廖超豪

安全运营-落实企业安全管理和治理目标

安全设备

安全漏洞

信息资产

安全需求

数据合规

知识库

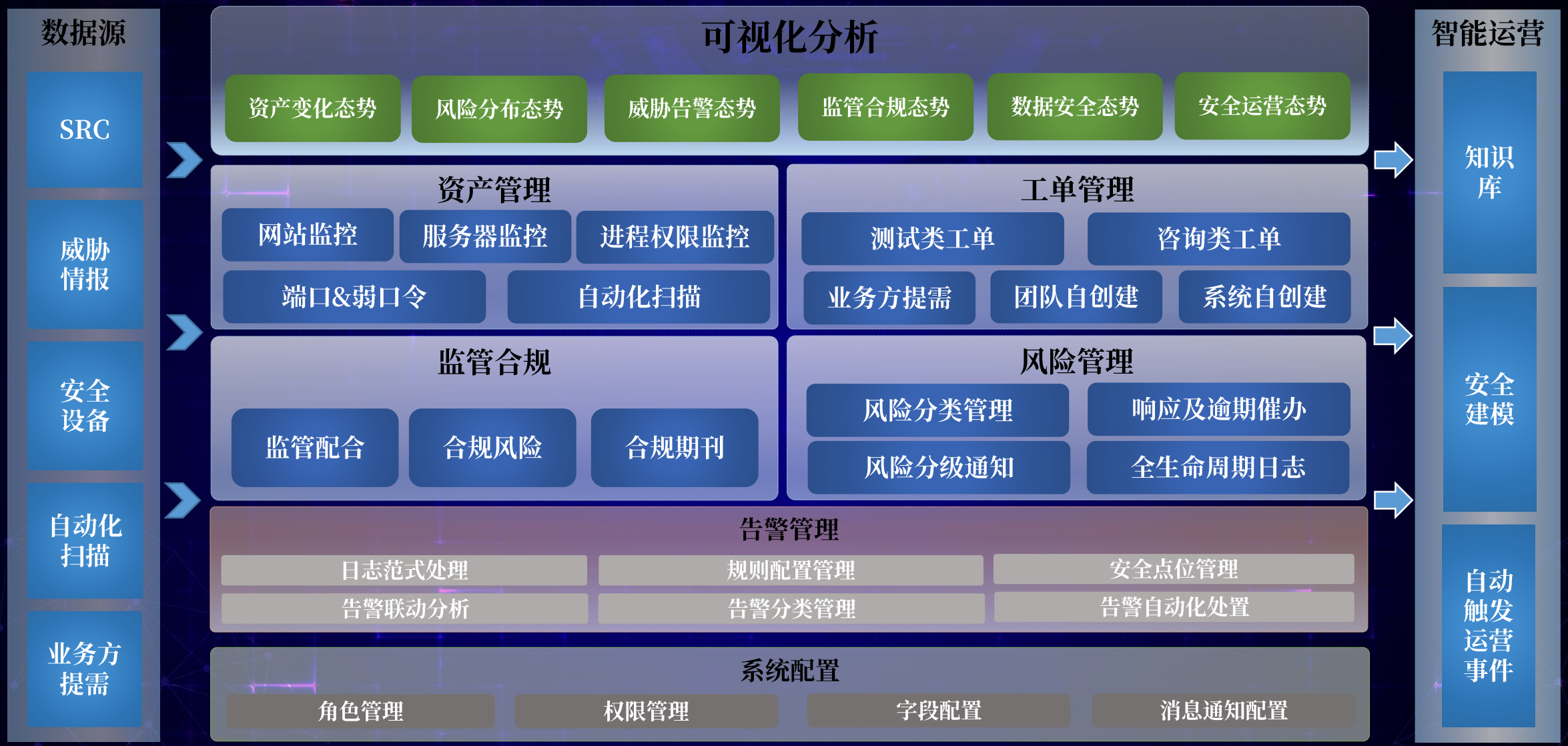
应急响应

安全运营 ≠ 安全运维

随着企业安全建设进入一定阶段的时候，安全运营就显得尤为重要，安全运营常被认为是落实企业安全管理和治理目标的重要途径，那么安全运营到底都需要运营些什么呢?

安世加

SOC-落地安全运营的靠谱工具



安世加

建设思路-分阶段交叉同步建设

平台化建设

安全点位联动

智能化运营

高扩展和可持续性建设

安世加

平台化建设-工单&资产&风险全生命周期管理

INTSIG安全运营中心

安世加

风险管理-让系统替人跟进风险

- 风险超时未接受，系统催办

- 风险逾期未修复，系统催办

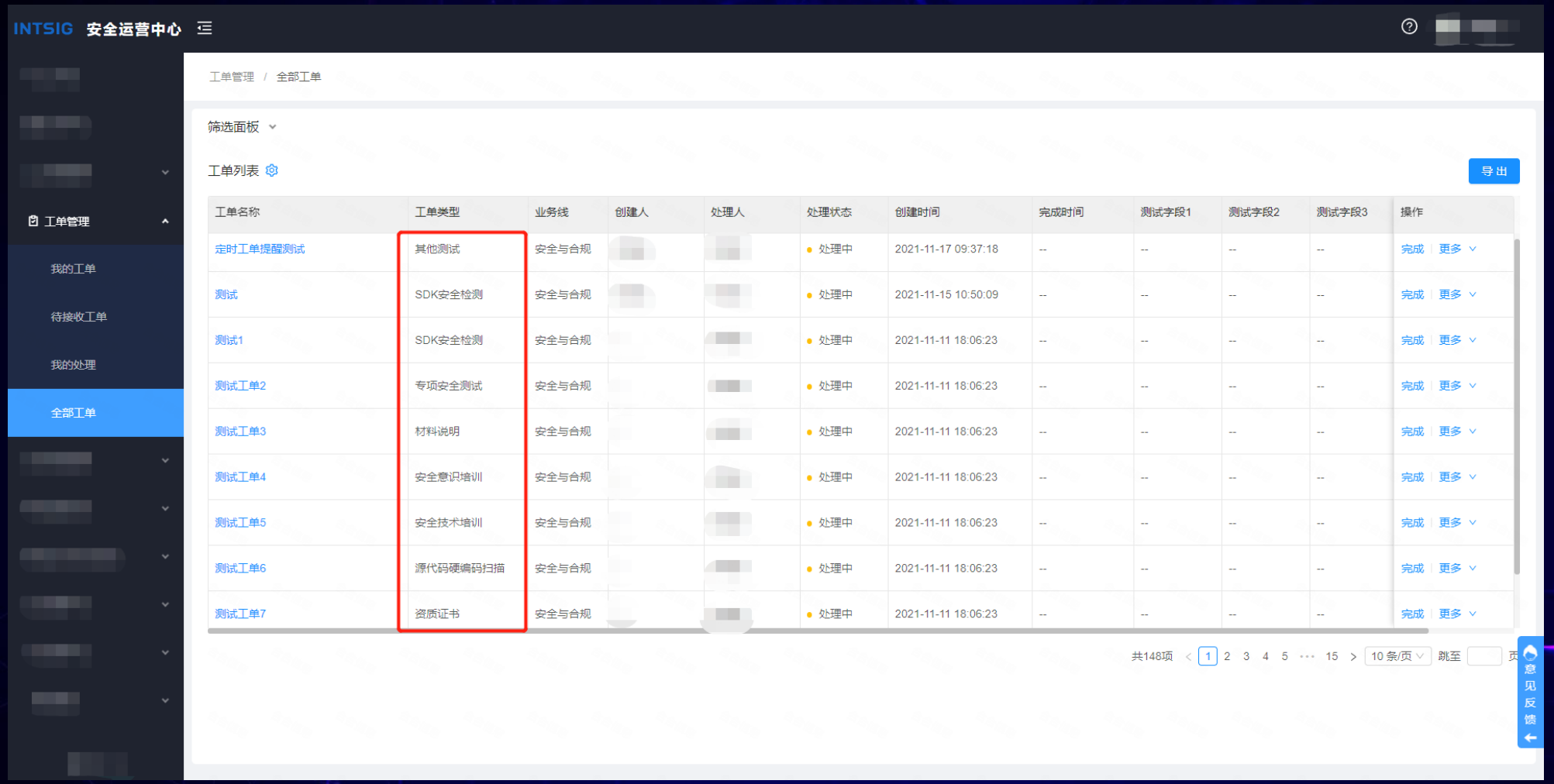
- 风险逾期未复测，系统催办

高危及以上风险关键节点系统自动抄送业务部门负责人

所有风险逾期未修复，系统自动抄送业务部门负责人

安世加

安全工单-通过安全服务提升企业安全性



平台共支持安全测试、合规评估、安全调研等50+种工单类型供业务方选择

安世加

安全工单-通过安全服务提升企业安全性

安世加

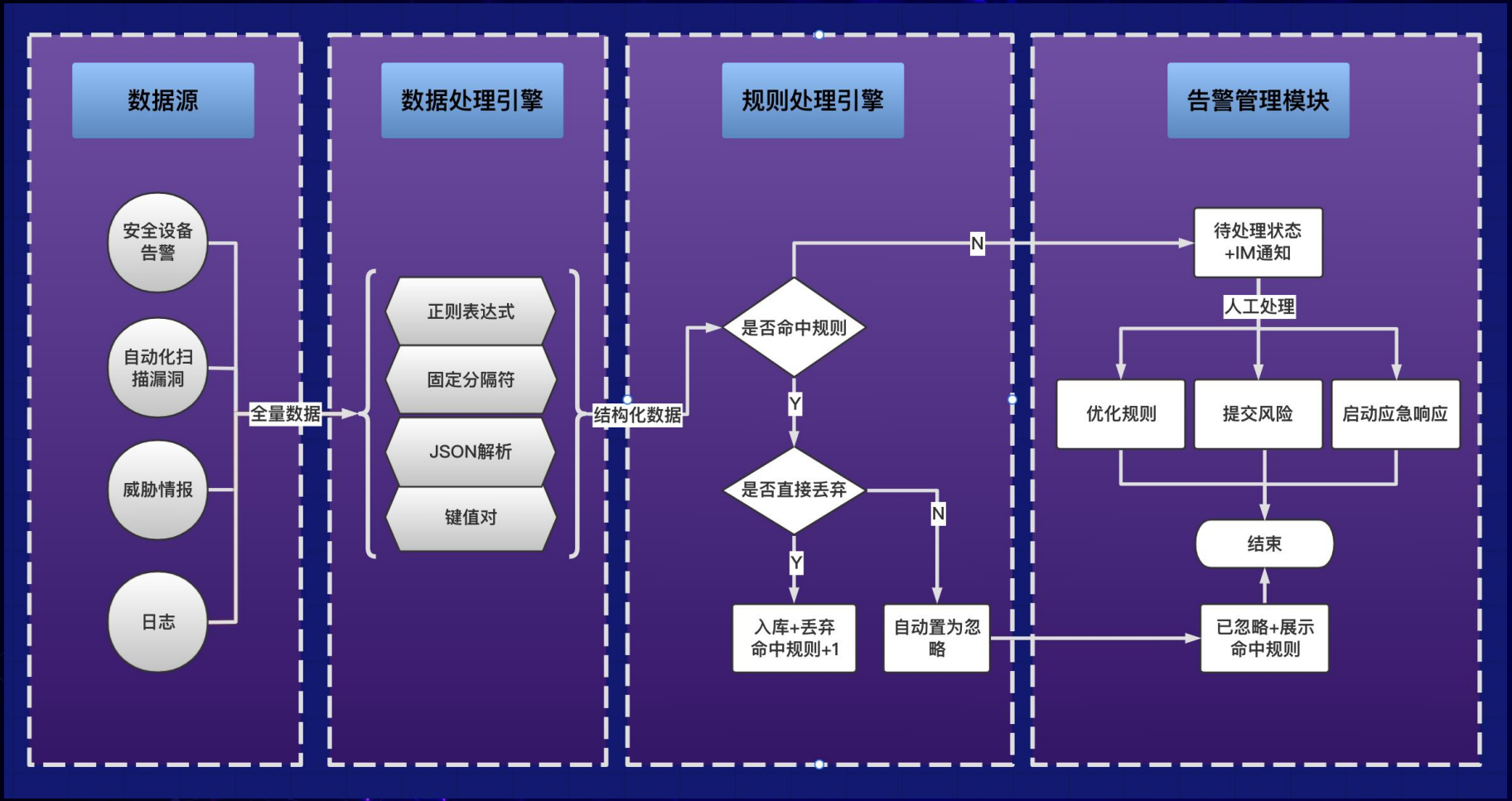
安全工单-提升用户体验

安世加

安全工单-增加应用场景

安世加

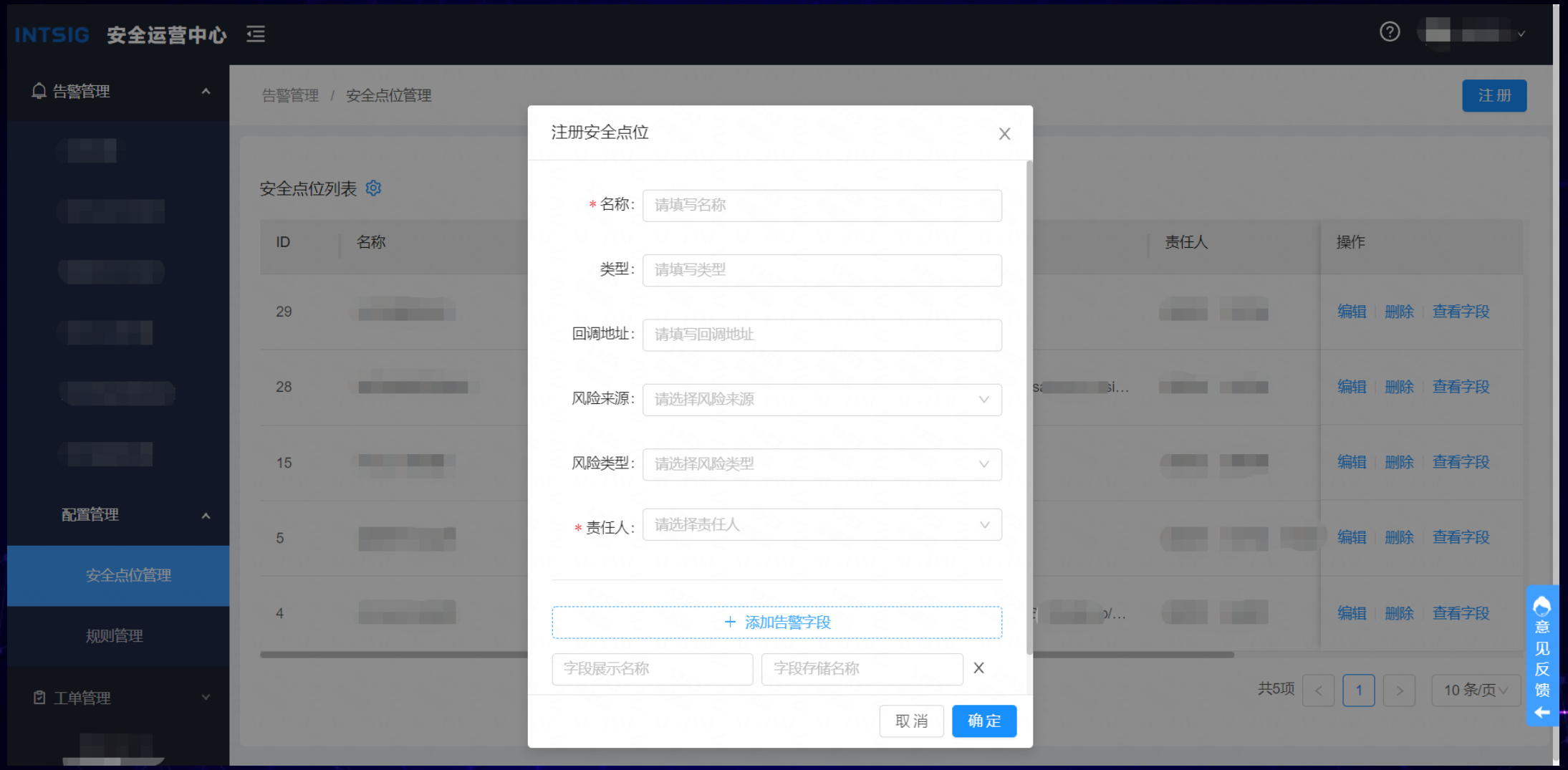
安全点位联动-注册制&数据范式处理



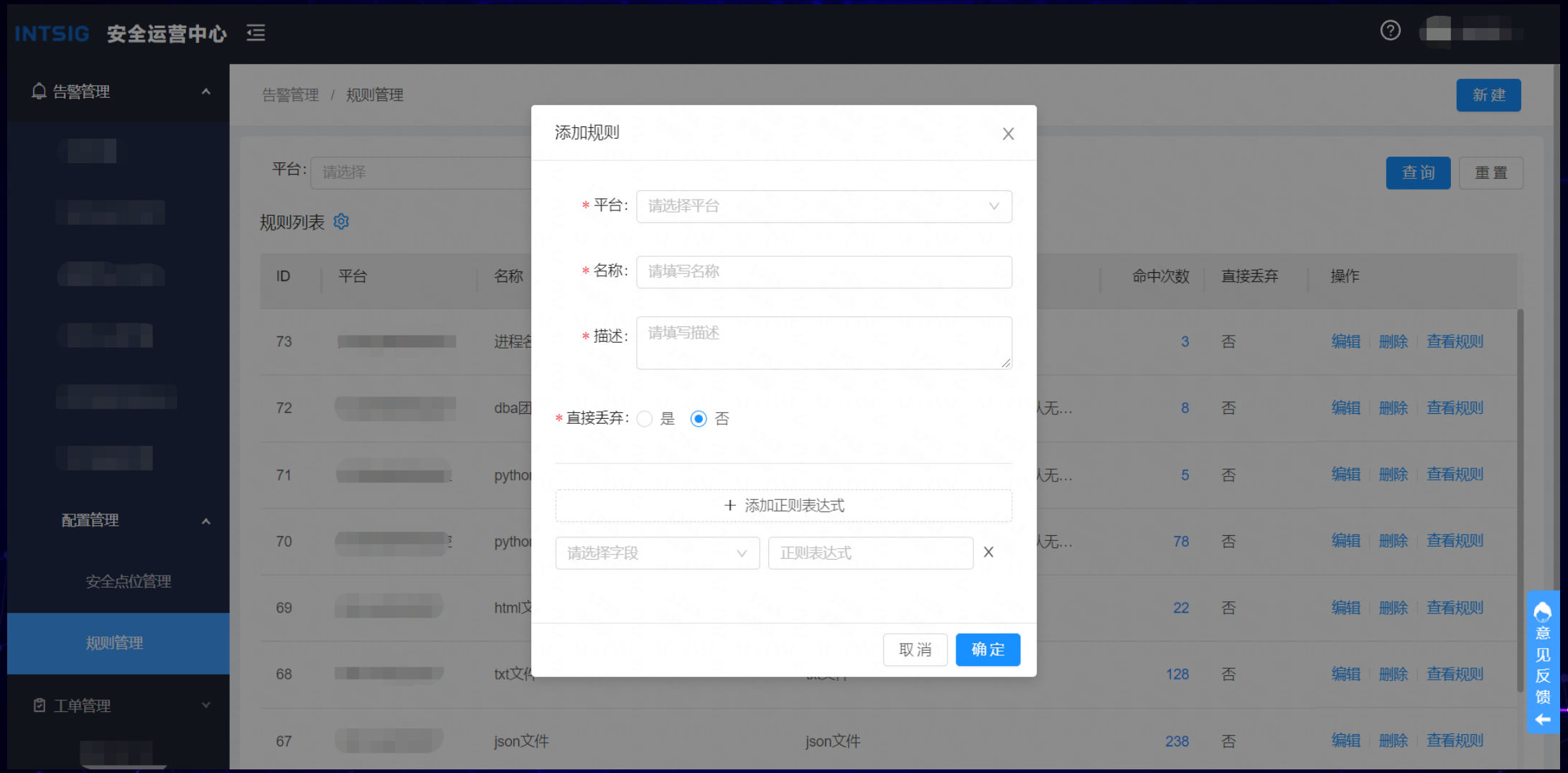
- 插件式注册接入，保证用户端充分灵活
- 全量数据范式处理，保证安全点位高扩展性
- 告警分类匹配半自动处理，避免海量告警淹没
- 全量信息入库，保证真实告警不丢失

安世加

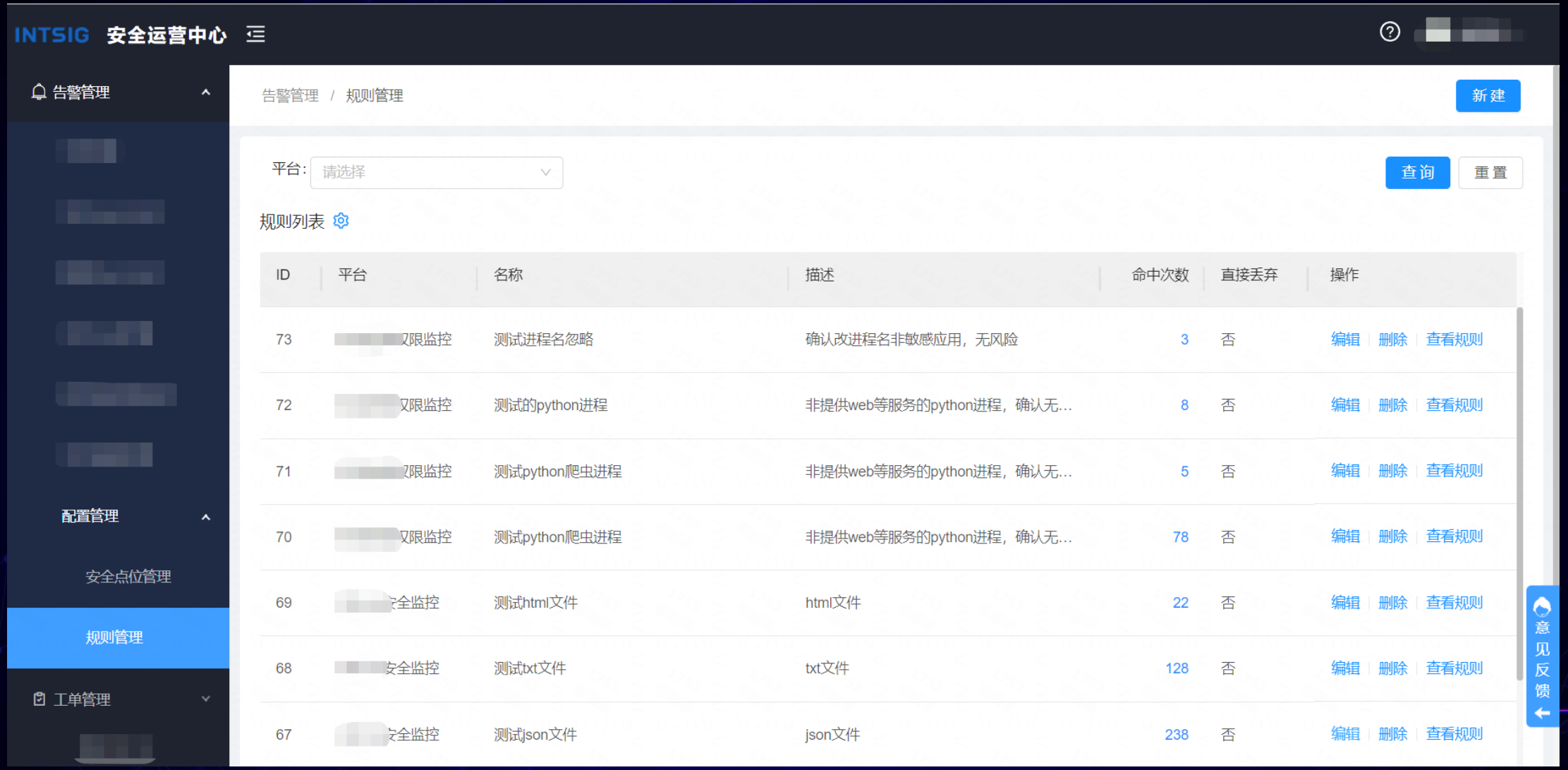
安全点位联动-点位&规则可持续运营



安全点位联动-点位&规则可持续运营



安全点位联动-点位&规则可持续运营



安世加

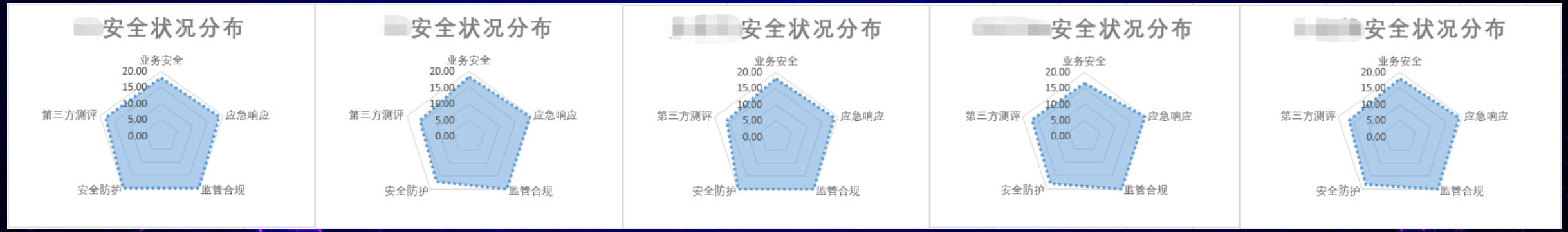
智能化运营-基于平台&数据&规则探索运营模式

安世加

智能化运营-业务方安全建模

基于SOC平台的元数据，参考CVSS等专业安全模型，通过5个维度，20+项衡量标准，并且以向上延申一个季度为梯度进行建模，加权计算出各业务线在指定的时间内最终的综合安全系数及各个维度安全状况分布，以此反映各业务线该周期内的整体安全态势。

业务安全：主要从安全漏洞视角，根据业务线周期内各类测试及漏洞情况按照公式加权计算出最终分值；
应急响应：主要根据业务线周期内是否存在安全事件、漏洞逾期、专项整改等维度进行加权计算出最终分值；
监管合规：主要根据业务线周期内是否存在内外部合规隐患事件进行加权计算出最终分值；
安全防护：主要根据业务线周期内安全防护设备或安全防护机制覆盖率及有效性等情况计算出最终分值；
第三方评估：主要根据第三方专业安全工具进行应用漏洞、SSL健壮性、网站有效性等检测结果进行相关计算得出最终分值；



智能化运营-专项治理

安全运营中心

Hi,

近期多次出现"设计缺陷/逻辑错误"相关的漏洞，按照专项行动治理启动规则，安全团队和业务方将一起配合启动"设计缺陷/逻辑错误"类问题专项治理行动，详情如下：

专项治理名称： 启信宝个人版第四季度测试

业务线：

实施方式： 1）启动专项治理行动后，业务方梳理所有相关功能接口进行白盒代码Review；

2）同时将这些接口通过安全运营中心提交安全测试，由安全团队对这些接口进行全面的黑盒测试；

历史漏洞：

工单名称	风险名称	风险等级	风险状态	风险类型	风险处理人	风险责任人	安全检测人	业务线	风险来源
		中危	已修复	设计缺陷/逻辑错误					安全团队
		中危	已修复	设计缺陷/逻辑错误					ISRC
		中危	已修复	设计缺陷/逻辑错误					安全团队
		中危	已修复	设计缺陷/逻辑错误					安全团队

创建人：

启动时间： 2021-

专项行动治理规则详细如下：

启动规则：各业务线在1个自然年内相同类型中危及以上漏洞出现3次及以上启动专项治理行动；

实施方式：

1）启动专项治理行动后，业务方梳理所有相关功能接口进行白盒代码Review；

2）同时将这些接口通过安全运营中心提交安全测试，由安全团队对这些接口进行全面的黑盒测试；

漏洞后续跟踪：

1）在1个自然年内，若经过专项治理行动的漏洞类型在同一产品再次出现，则由安全团队对该业务所有相关研发人员进行一次整体的专项培训，同时业务方需全面分析再次出现的原因，并将原因分析通过填写复盘报告邮件抄送该产品线及安全团队leader；

- 基于SOC的应用漏洞数据，同一业务线在1个自然年内相同类型中危及以上漏洞出现3次及以上即启动专项治理行动；
- 专项治理行动由业务方和安全团队共同配合完成；
- 经过专项治理后若仍继续发生，则需进行专项安全培训+深度复盘；

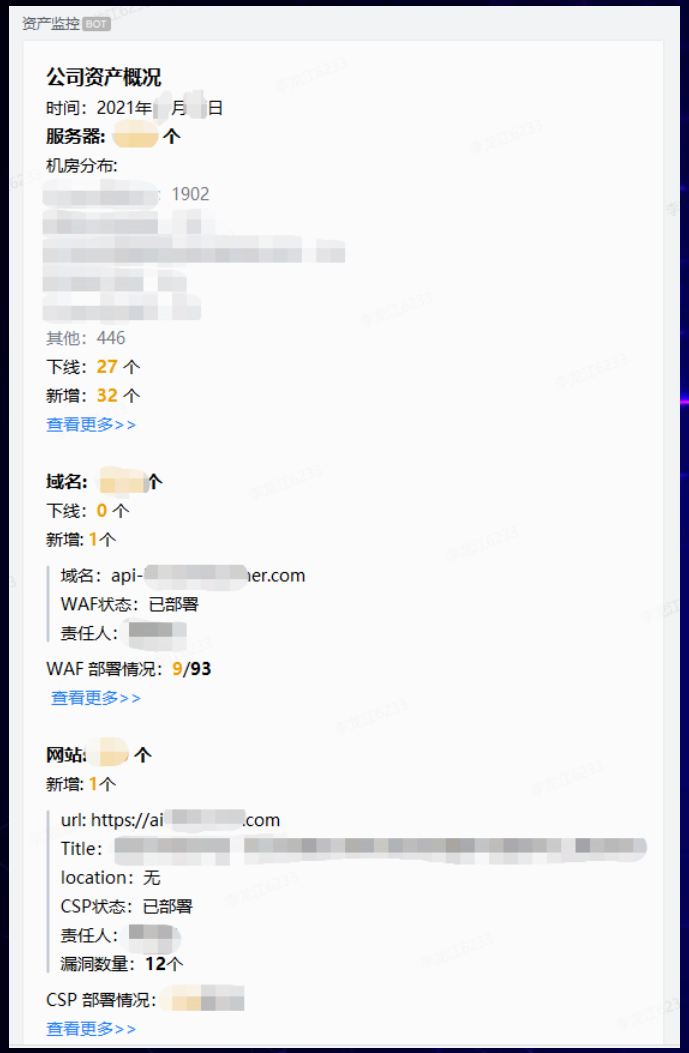
安世加

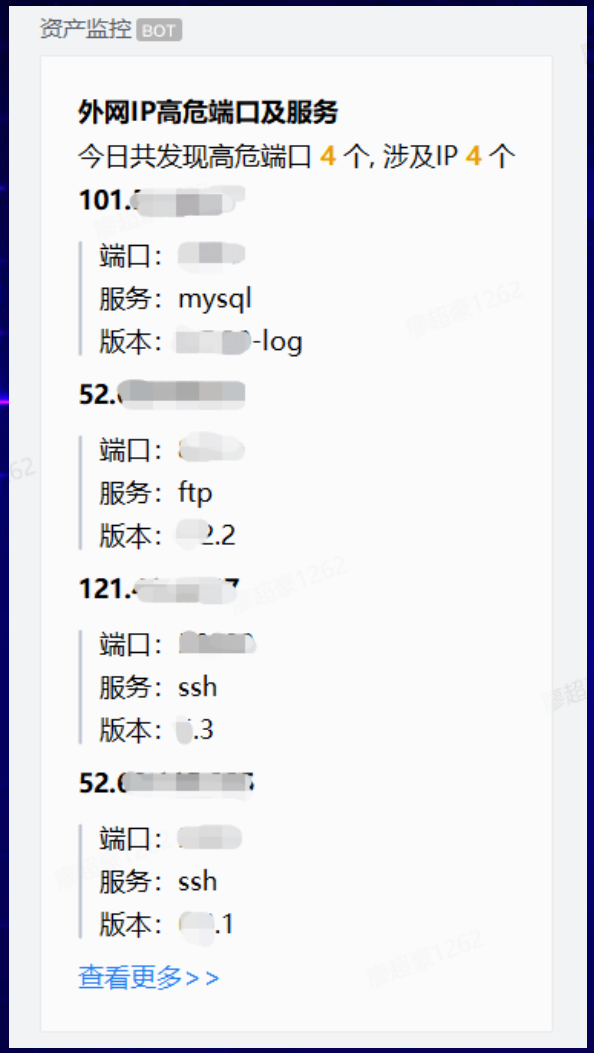
智能化运营-态势分析

- 业务线提测/风险分布
- 业务线风险占比
- 业务线风险分布
- 风险类型分布
- 业务线提测/风险趋势
- 风险类型Top10

安世加

智能化运营-安全巡检机器人





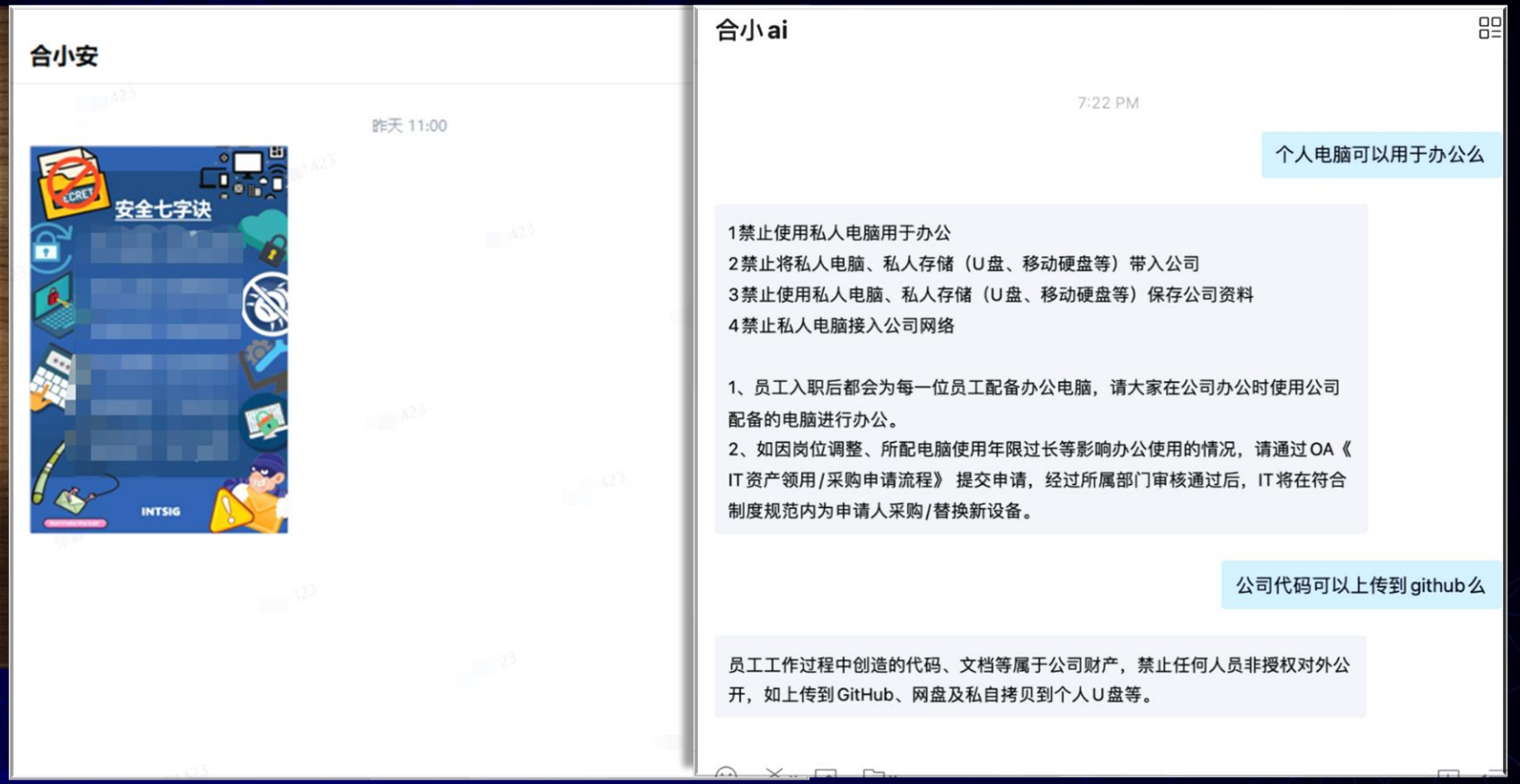
- 基于资产管理模块，每日对公司全量信息资产进行盘点和安全巡检后，通过机器人发送消息至安全团队，再由运营人员判断是否需要对相关风险或异常进行跟进

- 对所有接入SOC的告警进行日报统计及异常情况跟进

所有数据均为用于演示的测试环境，非真实数据

安世加

智能化运营-其他场景的运营探索



安世加

基于SOC的安全体系全景图

合规性

- 等级保护
- 法律符合
- 安全认证
- 政企合作
- 隐私保护
- 安全联盟

终端安全

- PC
- 智能手机
- 客户端

- 安全沙箱
- 安全加固
- 多因素认证
- SDK安全标准
- 终端病毒检测
- 代码安全规范
- 权限安全管控
- 加密与防篡改

网络与接入安全

- 运营商网络
- 终端网络
- 办公网络
- 服务内网

安全接入

- 安全域划分
- 网络链路加密
- 终端接入认证
- SSO单点登录
- IP黑/白名单

网络安全

- DDoS高防
- 网络入侵检测
- 分布式蜜罐
- 异常流量监测
- 网络安全审计

应用与数据安全

- 应用开发安全
- 大数据安全

应用安全

- SDL
- 应用分级分类
- Web应用防火墙
- APP/Web应用扫描
- 统一安全组件

数据安全

- 数据加密处理
- 数据脱敏、鉴权
- 数据存储备份

数据安全交换

- 数据安全存储
- 数据安全传输

安全管理

- 隐私保护
- 终端管理
- 应用管理
- 内容管理
- 安全制度
- 安全审计
- 风控体系
- 安全绩效考核

安全体系规范

统一身份认证

安全运营中心

- 资产管理
- 工单管理
- 监管合规
- 风险管理
- 告警管理
- 安全建模
- 知识库

感谢聆听

合合安全应急响应中心：
https://security.intsig.com/
微信公众号：合合安全应急响应中心

安世加

安世加专注于网络安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，以培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加