AiCSO智能化安全运营实践

演讲人：肖志康

杭州安恒信息技术股份有限公司 副总裁

目录

CONTENTS

01、智能化安全运营背景

02、智能化安全运营实践-AiCSO

03、AiCSO智能化安全运营生态

Part 01

智能化安全运营背景

安全运营面临的困境

运营作业层面

- ✓ 大规模数据的分析带来巨大的挑战；
- ✓ 安全告警**分析、研判需大量人工干预**；
- ✓ 每日**海量误报**大幅度**降低运营效率**；
- ✓ 安全事件**响应工作需要大量安全专家**；
- ✓ 安全漏洞运营管理，资产、漏洞割裂；
- ✓ ……

运营管理层面

- ✓ 安全运营人员缺口，工作繁杂，**管理混乱**；
- ✓ 责任不清晰，安全工作**难协同**，工作推动受阻；
- ✓ 服务过程不可见，**难以**对安全人员**工作跟踪和审计**；
- ✓ 操作**流程不标准**，运营效率低下，安全管理不闭环；
- ✓ 运营**流程没固化**，运营质量因人而异，用户体验差；
- ✓ ……

对外

对内

安全运营中心

安全运营发展路线

基于“安全运营成熟度模型”，安全运营的发展，是**运营智能化从无到有，再到全面智能化的过程。**

安全运营成熟度模型

参考网络安全成熟度模型认证(CMMC)框架

智能化安全运营是大势所趋

针对当前安全运营建设过程中普遍存在的作业和管理层面问题，结合安全运营成熟度模型的发展路径可知：

安全运营发展的趋势是智能化安全运营。随着大数据、人工智能等技术的发展，安全运营智能化建设的时机已逐渐变得成熟。通过对安全运营作业和管理过程中的信息进行数据化，结合工具开展运营活动从而实现自动化，最终通过智能化分析等技术实现运营的智能化转变。

Part 02

智能化安全运营实践-AiCSO

AiCSO概述

AiCSO是一个针对性解决在网络安全运营管理中所存在的痛点的解决方案。通过平台与服务相结合的方式，为客户提供一位智能的首席安全运营官（CSO），帮助客户实现网络安全运营**数字化、自动化、智能化**。

1个安全运营支撑系统

安全运营支撑系统即SOOS，实现统一身份认证、统一权限管理、统一消息交换、多协议接入、服务能力编排、能力平台智能调度。

\+

N*

N个安全应用

各种安全能力平台（不限于安恒产品），诸如漏洞扫描、基线核查、威胁情报、资产稽查、云防护、事件管理、日志分析等。

=

AiCSO安全运营支撑平台

基于SOOS快速集成其他安全能力平台，提供信息安全统一门户，实现对信息网络和和重要信息集中式安全纳管与信息共享。

AiCSO智能化的核心基础能力

AiCSO核心基础能力

统一认证

平台提供了基于IAM（Identify Access Management）体系的统一身份认证模块，全面接入其他安全平台，为客户**提供的统一的信息安全管理门户。**

能力集成

底层技术架构采用松耦合的方式进行设计，基于1个安全运营支撑系统（Security Operation Operating System，简称SOOS）**快速集成其他诸如SIEM、IRP、TI、CMDB等安全能力平台。**

数据调用

具备以低代码方式对数据进行抽取与调用的高性能模块，通过该模块能对所需要的数据进行抽取、清洗、传输与加载，**为上层流程跟踪、可视化展示提供调用接口。**

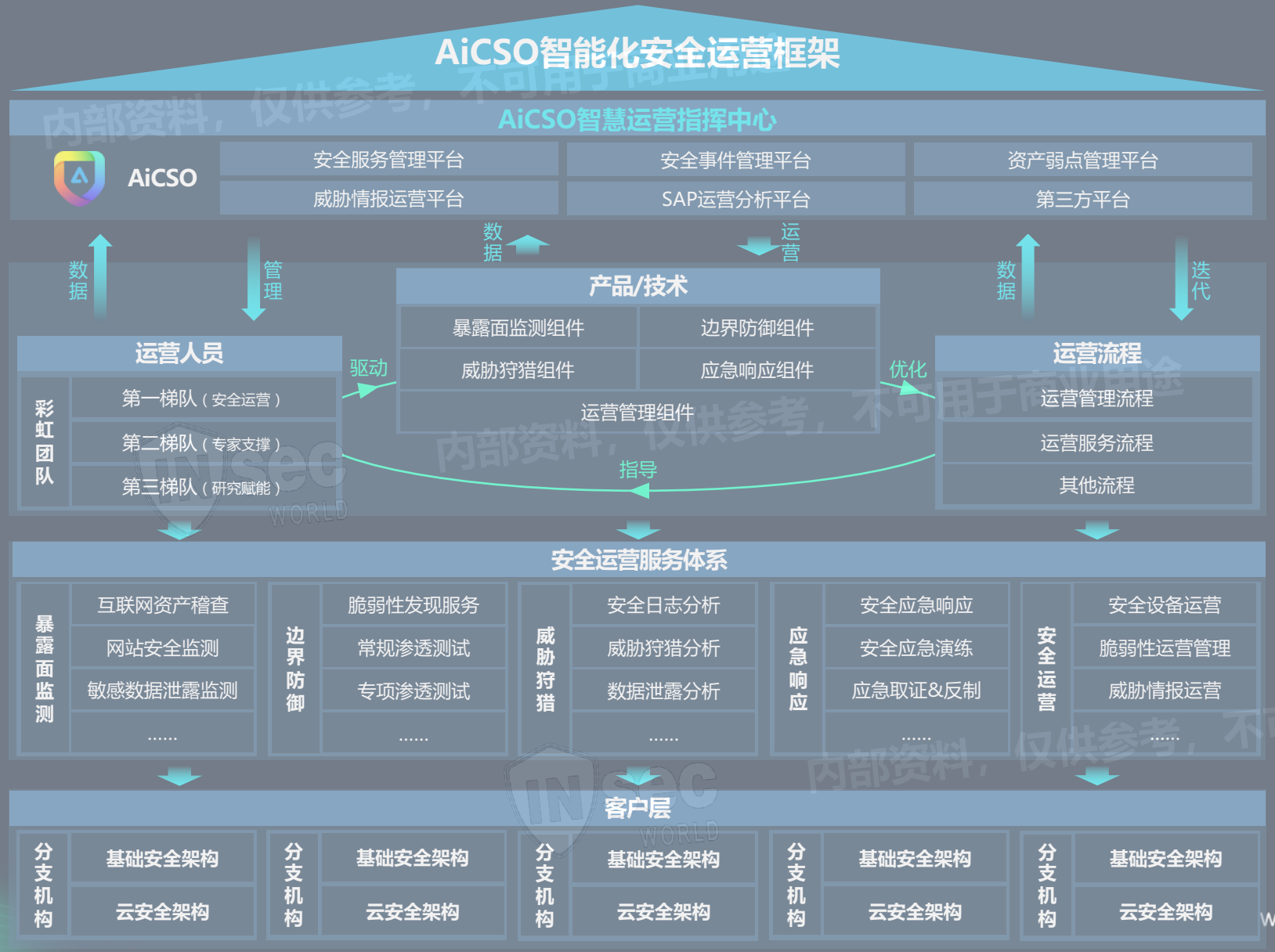
流程管理

提供流程管理功能，能对安全业务流程智能编排，创建出符合实际场景的安全运营业务流程，**提高运营工作效率和质量。**

数据利用

提供报告管理功能，能记录所有服务和工单产生的记录，规范化管理，便于对数据回溯，对服务工作审计，**加强人员绩效考核。**

以AiCSO为核心的智能化安全运营框架



Part 02-1

运营作业智能化

安全事件智能化运营

采集

日志
设备/系统/应用/中间件/.....

流量
TCP流量/UDP流量/.....

资产
资产编号/地址/归属人/.....

脆弱性
漏洞信息/暴漏面/.....

威胁情报
开源/商业/社区/.....

新型检测日志
EDR/蜜罐/沙箱/.....

其他信息
用户信息/地理信息/.....

第三方系统
SIEM/日志审计/流检测/.....

分析

人工分析
结合大数据查询进行人工分析

关联分析
结合体系化关联规则检测威胁

情报关联
通过情报碰撞发现威胁

UEBA
结合算法发现异常偏离行为

威胁狩猎
专家利用工具深度挖掘威胁

响应

告警通知
针对安全威胁触发告警通知

SOAR
与响应剧本关联，自动响应

专家响应
针对尚未有剧本的威胁，进行专家响应处置

常规手段

新型手段

数据采集层面

全面数据采集

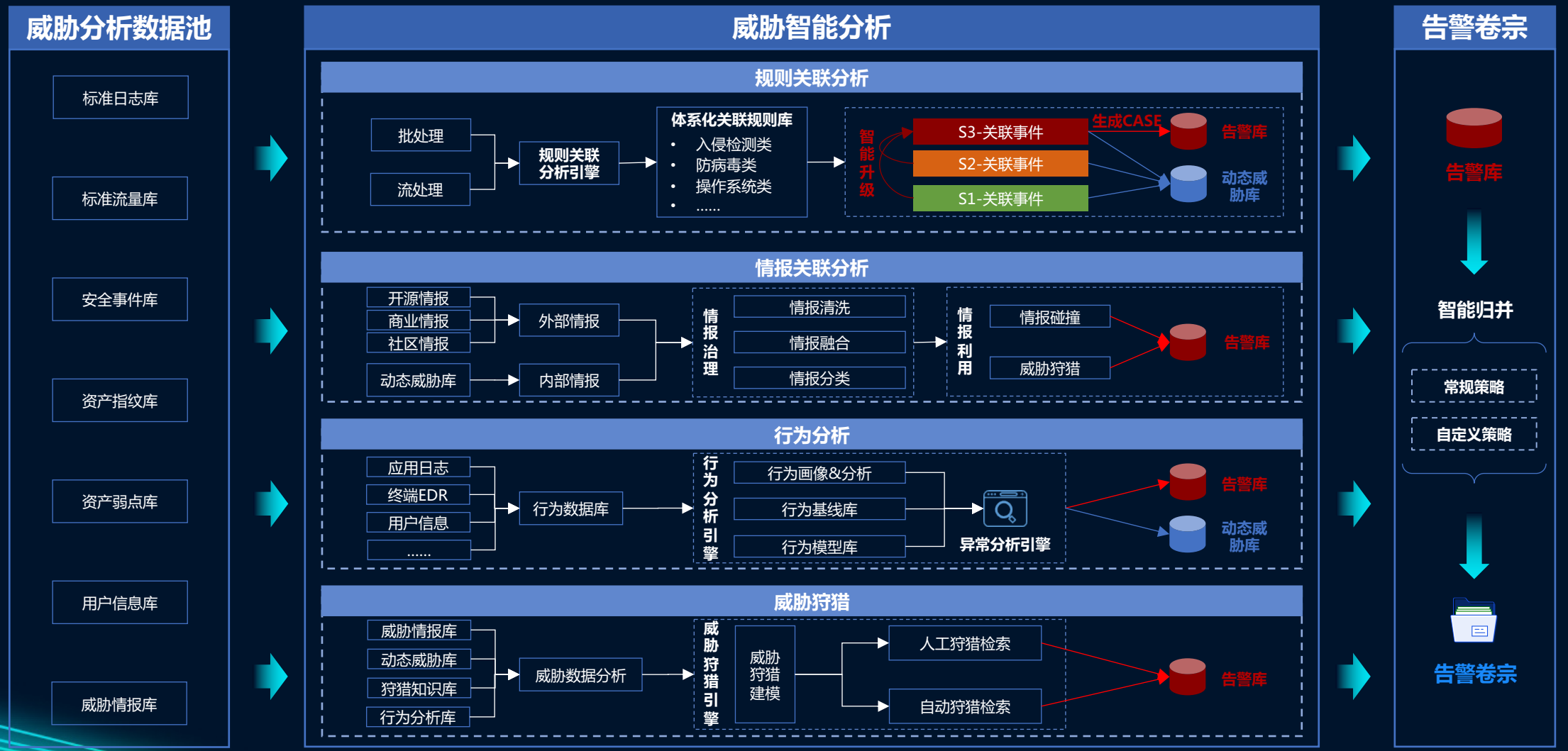
智能数据治理

- 主流网络协议解析
- 日志自动标准化
- 日志语义分类
- 字段信息智能补全
- 语义智能分类/标签
- 异常数据清洗过滤
- 数据编码自动转换

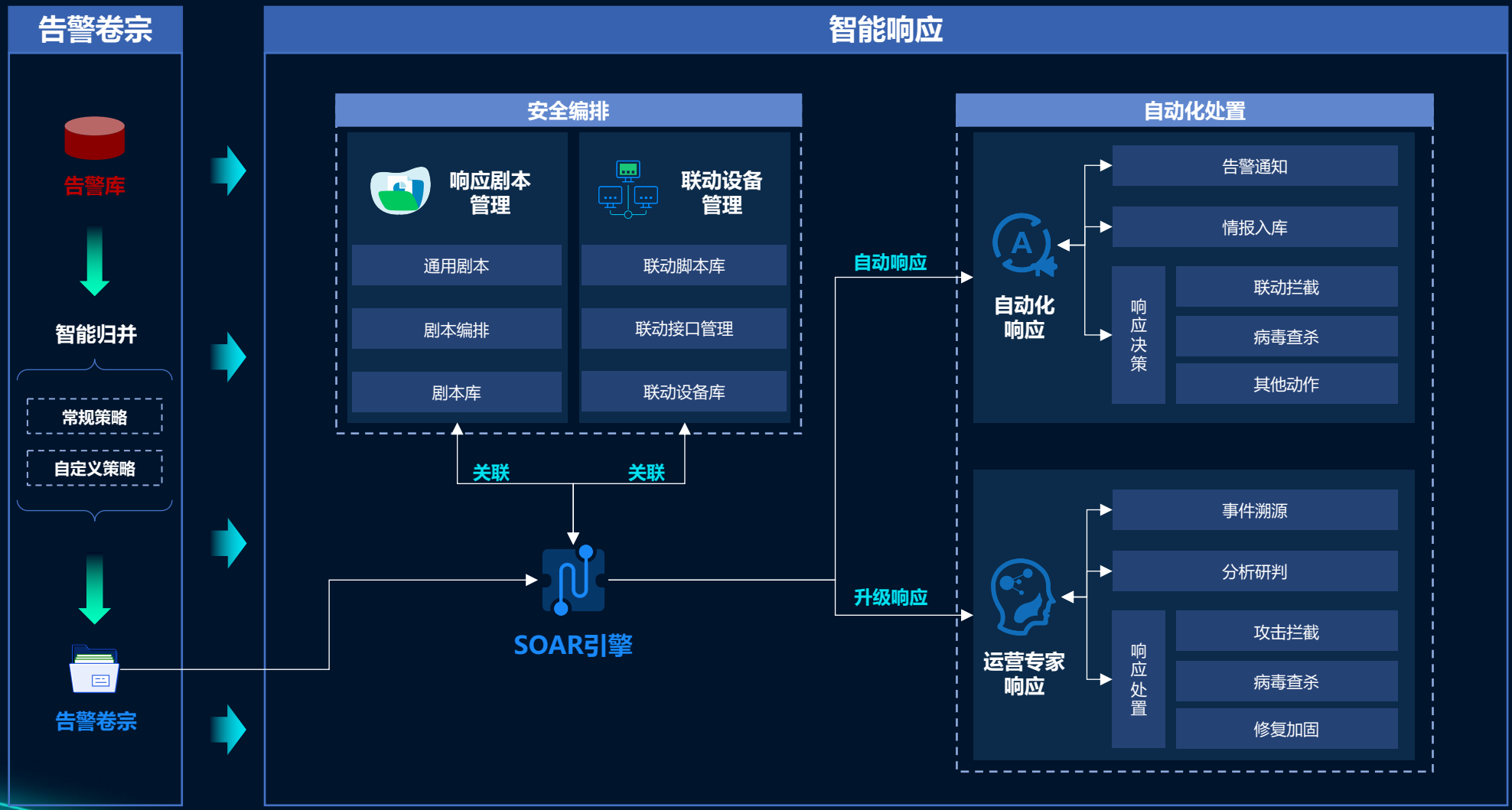
威胁分析数据池

- 标准日志库
- 标准流量库
- 安全事件库
- 资产指纹库
- 资产弱点库
- 用户信息库
- 威胁情报库

安全分析层面


威胁分析数据池
标准日志库
标准流量库
安全事件库
资产指纹库
资产弱点库
用户信息库
威胁情报库
威胁智能分析
规则关联分析
批处理
流处理
规则关联分析引擎
体系化关联规则库
入侵检测类
防病毒类
操作系统类
.....
智能升级
S3-关联事件
S2-关联事件
S1-关联事件
生成CASE
告警库
动态威胁库
情报关联分析
开源情报
商业情报
社区情报
外部情报
动态威胁库
内部情报
情报治理
情报清洗
情报融合
情报分类
情报利用
情报碰撞
威胁狩猎
告警库
行为分析
应用日志
终端EDR
用户信息
.....
行为数据库
行为分析引擎
行为画像&分析
行为基线库
行为模型库
异常分析引擎
告警库
动态威胁库
威胁狩猎
威胁情报库
动态威胁库
狩猎知识库
行为分析库
威胁数据分析
威胁狩猎引擎
威胁狩猎建模
人工狩猎检索
自动狩猎检索
告警库
告警卷宗
告警库
智能归并
常规策略
自定义策略
告警卷宗

响应处置层面


告警卷宗
告警库
智能归并
常规策略
自定义策略
告警卷宗
智能响应
安全编排
响应剧本管理
联动设备管理
通用剧本
剧本编排
剧本库
联动脚本库
联动接口管理
联动设备库
关联
关联
SOAR引擎
自动响应
升级响应
自动化处置
自动化响应
告警通知
情报入库
响应决策
联动拦截
病毒查杀
其他动作
运营专家响应
事件溯源
分析研判
响应处置
攻击拦截
病毒查杀
修复加固

安全事件智能化运营场景

外部情报库
威胁情报库，用于情报关联模型，来源于开源、商用威胁球情报库。

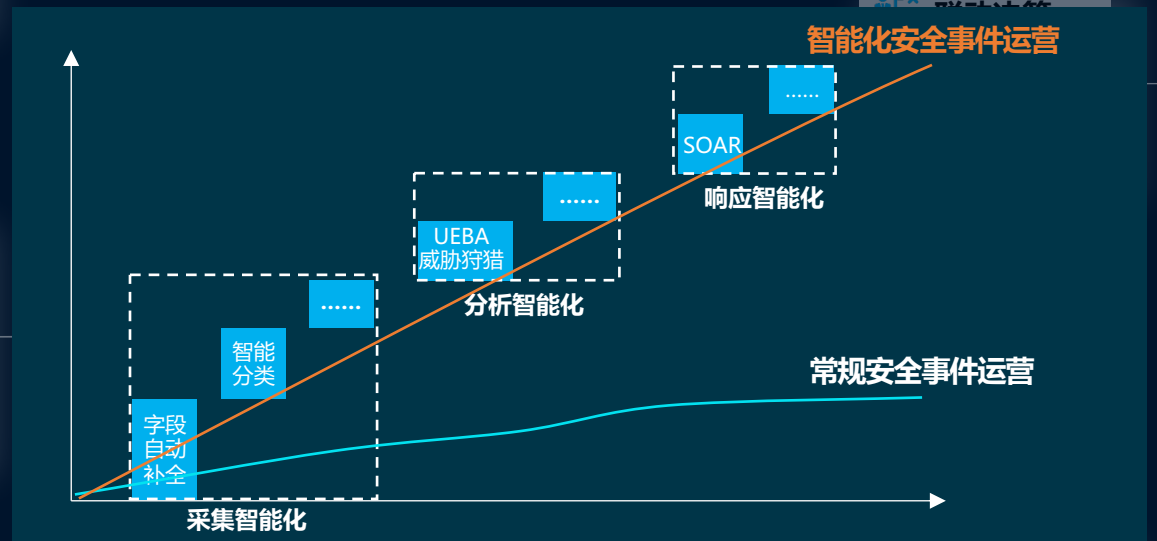
情报入库

情报关联

威胁数据池
安全日志、流数据，通过智能分类、字段智能补全等智能处理，形成**威胁分析数据池。**

检测

威胁检测模型
- 规则关联
- 行为分析
- 威胁狩猎
- 情报关联



智能化安全事件运营，通过采集、分析、响应三个维度的智能化技术应用，实现人员投入减少70%，且效率提高80%以上。

设备联动
海量网关型设备联动及响应策略。

结果通知
针对尚未具有响应剧本的告警，通报运营团队进行分析研判。

应急响应
针对尚未具有响应剧本的告警，通报运营团队进行分析研判。

情报关联

动态威胁库
动态威胁库，针对风险较低的威胁自动入库，用于持续监测。

Playbooks
动态威胁库，针对风险较低威胁自动入库，用于持续监测。

剧本入库

参考&积累

知识库
为专家研判提供依据，为应急响应提供参考案例。

Part 02-1

运营管理智能化

运营管理智能化架构

运营管理中心层

运营管理中心

运行监控			运营管理			流程管理	
服务总览	服务动态	服务健康监控	绩效管理	项目管理	工作计划	流程编排	流程可视化
值班状况	绩效监控	服务SLA	简报管理	智能调度	……	流程关联	流程智能优化

基础支撑-AiCSO

安全服务管理平台	安全运营支撑系统	数据分析引擎	开放接口	管理数据池

管理数据层

运营人员信息	任务信息		能力接入平台	
个人信息	任务基础信息	任务执行时长	SIEM平台	资产弱点管理平台
值班信息	任务执行进度	……	应急响应平台	……

运营服务层

暴露面监测能力域	边界防御能力域	威胁狩猎能力域	应急响应能力域	运营管理能力域
互联网资产稽查	专项渗透测试	安全威胁分析	安全应急演练	安全运维服务
第三方漏洞收集	协助加固服务	威胁狩猎服务	安全应急响应	能力提升服务
敏感数据泄露监测	常规渗透测试	用户行为分析	应急取证服务	安全管理服务
……	……	……	……	……

流程管理层面

AiCSO流程管理智能化，主要提供以下能力：

□ 流程编排

AiCSO具备智能流程编排能力，主要功能：**可视化编排、流程组件化、拖拽式编排**。

□ 流程关联

AiCSO具备高效的流程关联能力，能快速**实现主流程、子流程的关联**，从而将**复杂流程简单化**。

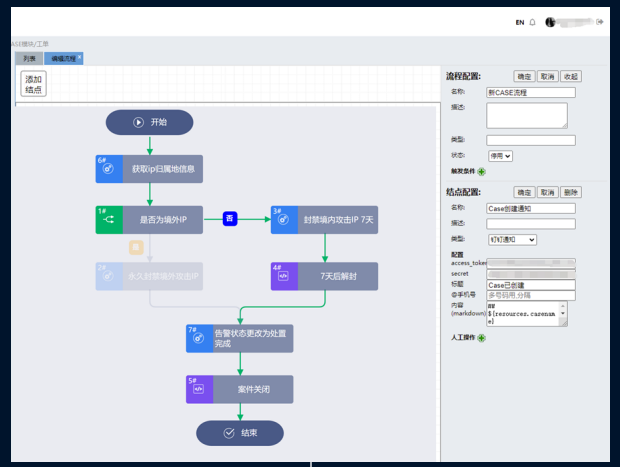
□ 流程可视化

AiCSO能对流程进行可视化，从而实现运营服务的**全流程可视**，便于对运营服务进行跟踪和管理。

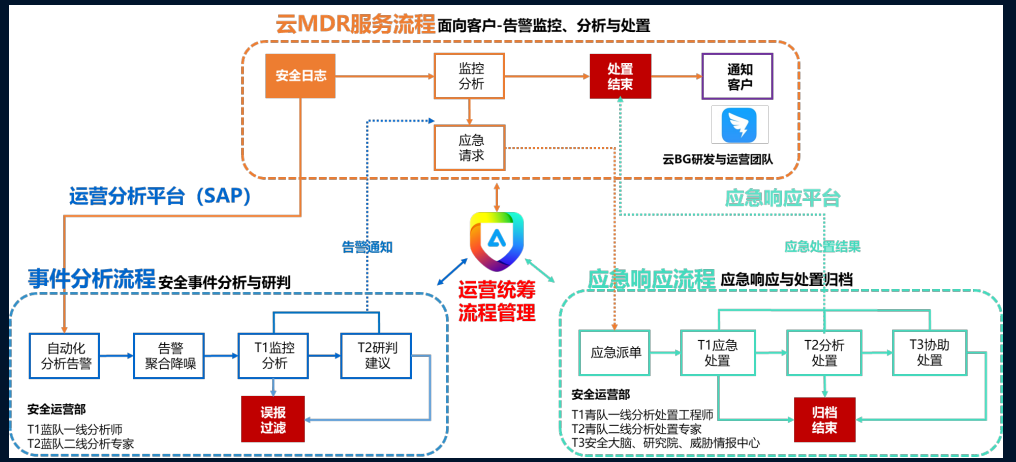
□ 流程智能优化

AiCSO通过对**流程进行数据化**，通过流程优化模型对服务数据（服务关键节点耗时、服务总耗时、服务平均耗时等）进行分析，为**流程优化提供依据**。

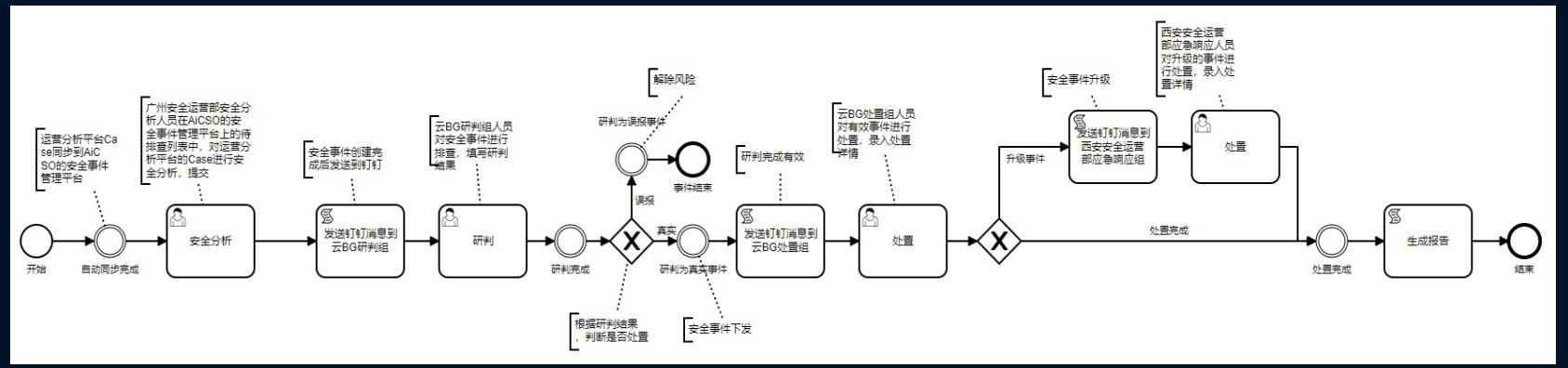
流程编排工具



设计流程



编排



标准化流程

运行监控层面

通过AiCSO的数据化、可视化能力，实现安全运营服务管理的整体监控：

□ 服务总览监控

对各个安全运营服务的关键服务指标进行实时监控，便于了解**整体安全运营服务状况**。

□ 服务动态监控

对安全运营服务的**关键动态进行监控**，便于了解关键运营服务实时动态。

□ 服务健康监控

服务健康监控，通过对安全运营服务的关键指标进行综合评分和计算，获得**服务健康度排行**。

□ 局部服务监控

局部服务监控，支持对**单个安全运营服务的状态监控**。

安全服务响应服务监控

运营管理层面

AiCSO运营管理智能化，基于管理者角度，提供运营服务项目从建立到终止的闭环管理，主要能力：

□ 绩效考核

AiCSO安全服务管理子平台，能对运营人员的**工作关键指标进行监控**，通过KPI算法结合任务完成时长、关键节点时长、响应速度、结果评分等数据**自动计算KPI分值**，并排行。

□ 项目管理

AiCSO安全服务管理子平台，为**安全服务项目从立项到结束的全生命周期闭环管理**提供管理界面。具备工作台、项目管理、工作计划、简报管理、日程管理、系统管理等功能，一方面，能对**服务项目进行统筹、计划、任务拆解**等，另一方面，能对**服务实施进度、服务情况、服务结果进行跟踪和管理**。

运营管理智能化场景-漏扫闭环管理服务

服务流程编排

通过可视化编排、流程关联等技术进行漏洞闭环管理服务的流程建设

可视编排

流程编排智能化

项目监管

项目经理：
通过AICSO进行全流程跟踪监管，防止偏离，保障结果

可视监管

项目全生命周期监管

标准化流程

项目监管

1.项目建立

通过AiCSO进行：
- 项目建立
- 角色定义
- 权限分配
- 目标制定

任务计划

2.服务任务规划

项目经理执行：
- 项目拆解
- 里程碑制定
- 任务计划

任务执行

3.任务执行

第一梯队人员：
- 受理任务
- 根据计划执行漏扫任务

漏扫结束

4.结果上报

第一梯队人员：
- 漏扫报告上传
- 项目经理审核后下发修复工单

修复工单

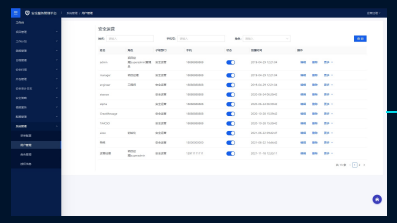
5.修复加固

资产管理员：
- 受理修复加固任务；
- 加固完毕后上报结果；

客户汇报

6.任务结束

客户：
- 通过AiCSO查阅结果以及服务过程



AiCSO
安全服务管理平台

任务智能催促

流程智能优化

绩效考核

绩效考核

管理者：
通过AiCSO综合执行效率和服务结果直接获得KPI值

智能考核

KPI智能计算

Part 03

AiCSO智能化安全运营生态

智能安全运营生态

在十四五、信创、新基建等背景下，没有任何一个安全厂商能独自满足安全运营整个框架建设所需要的所有安全能力，这就要求须持积极、开放、合作的心态构建智能化安全运营生态。

信息化、数据化、自动化、智能化是发展路线，而标准化是智能化运营生态建设的基础。**智能化安全运营生态的构建，需要数据、API的标准化，进行数据共享，实现安全能力的融合，合力共建安全运营生态。**

“数字经济 安全为钥”

智能化安全运营，助力数字化转型