奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

面向资配漏补的系统安全平台

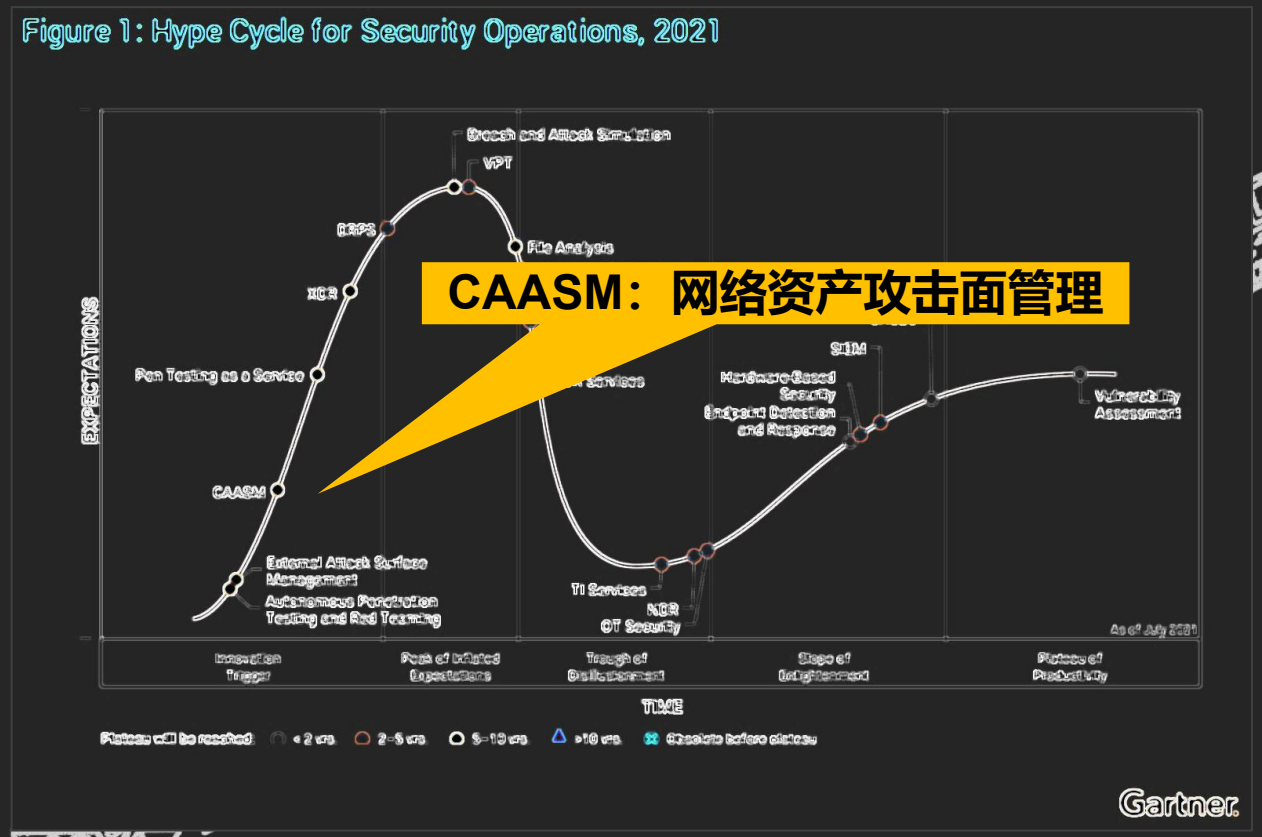
张勇 奇安信集团系统安全负责人

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

理念构想

Gartner于2021年Hype Cycle中提出了CAASM



网络资产攻击面管理 (CAASM) 是一项新兴技术，其核心是通过使用新兴技术，使安全团队能够解决持续存在的资产可见性和漏洞挑战。

主要特点：

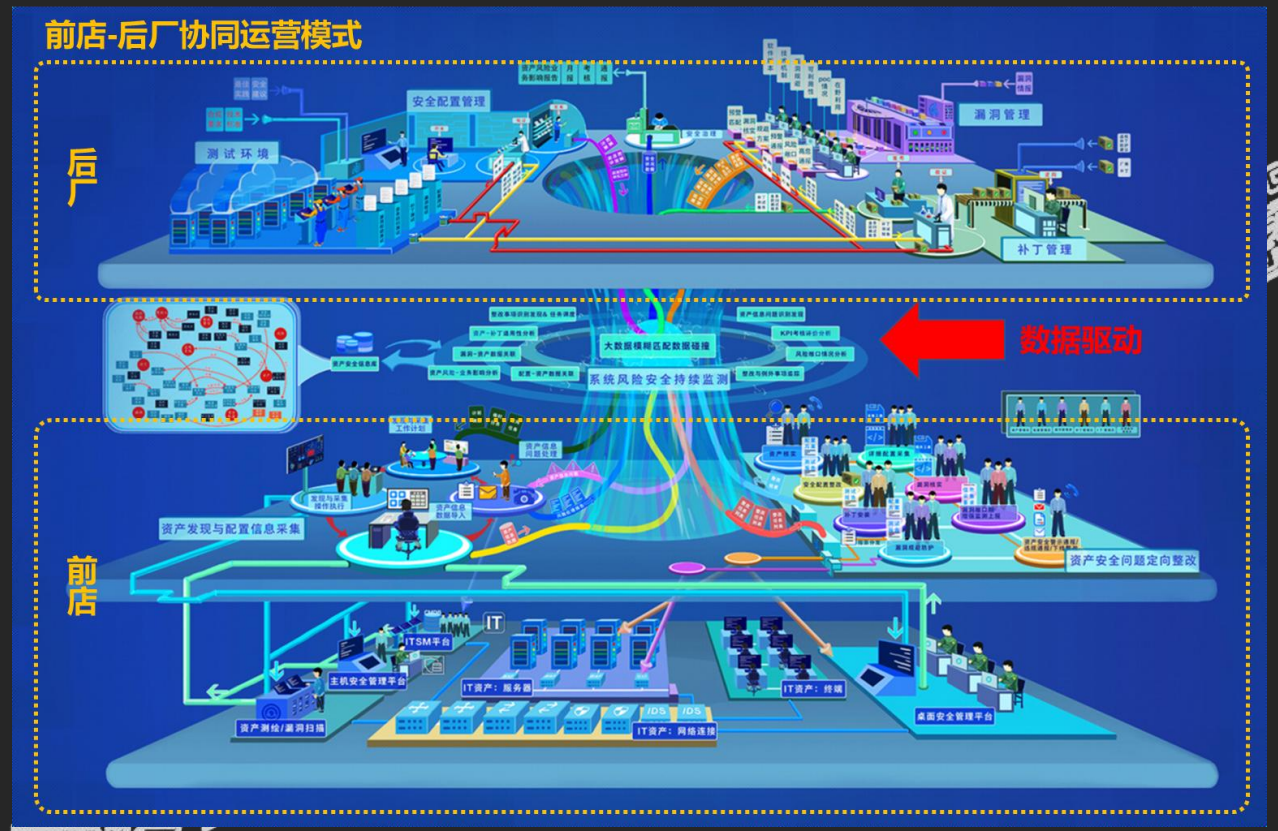
- 多源数据集成
- 全面资产视图
- 为脆弱性整改提供支撑能力

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

理念构想

系统安全运行构想



以“**数据驱动**”的实战化安全运行模式，打通资产管理、配置管理、漏洞管理和补丁管理四大基础安全流程，环环相扣融入整个大运维环境。

通过**数据碰撞**产生配置、漏洞和补丁相关运营工作任务。各运营角色以“前店-后厂”的协同运营模式输出运营成果，从而收敛资产攻击面、保持安全姿态，实现资产安全管理的闭环。

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

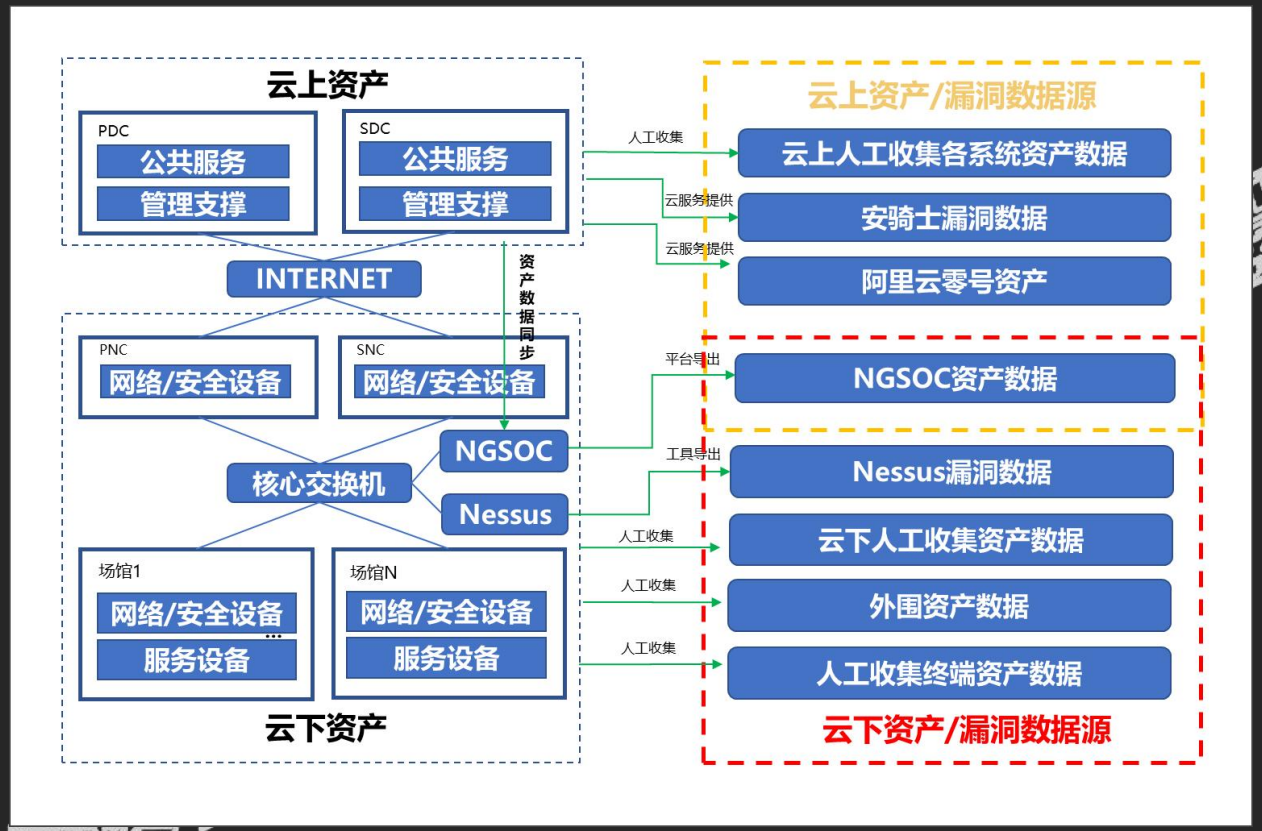
北京2022年冬奥会和冬残奥会

系统安全落地实践

BCS2022系列活动-冬奥网络安全“零事故”宣传周

建设背景

资产安全闭环管理面临的挑战



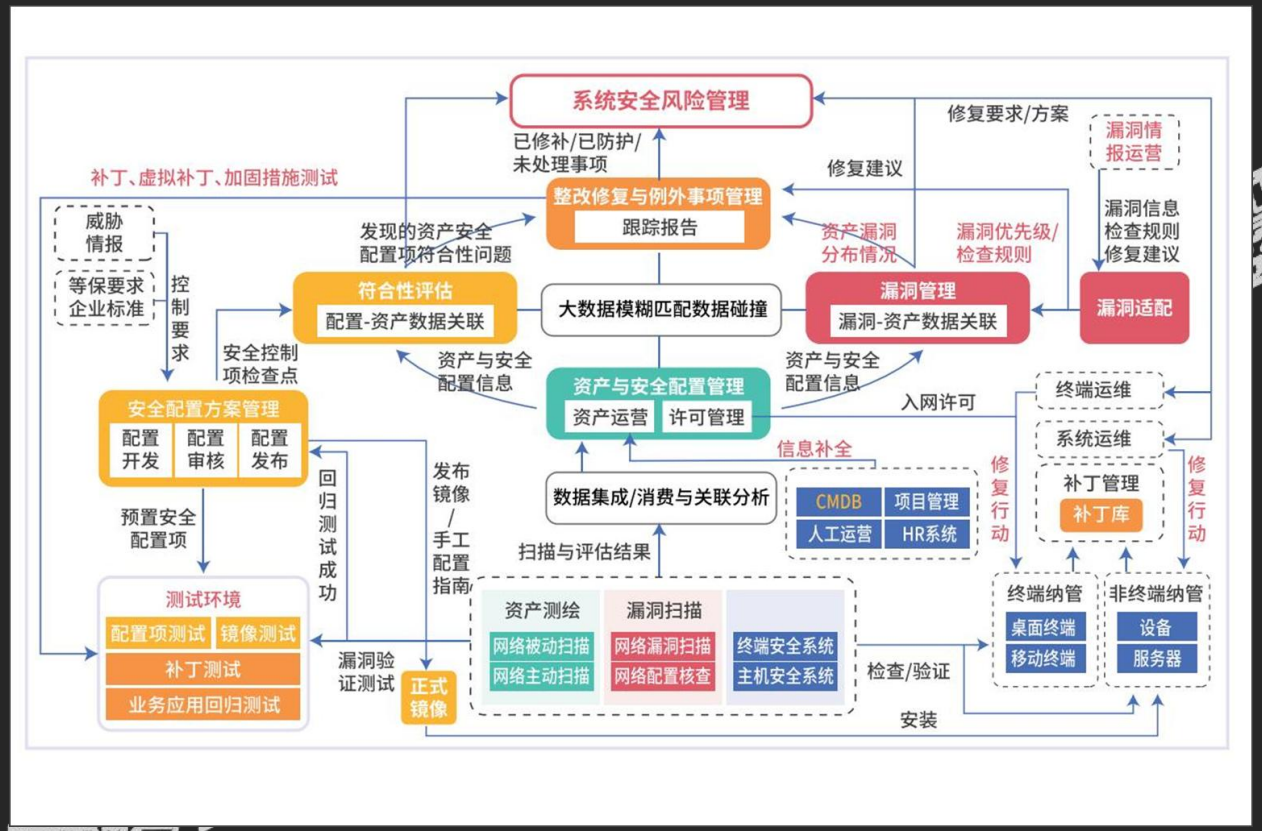
冬奥资产安全管理范围涵盖云上公共服务和管理支撑系统、云下网络中心资产、场馆资产、业务系统资产和外围资产。

虽然已经通过云安全管理系统、资产台账等方式对资产和脆弱性进行统一管理，但仍面临巨大挑战：

- 未建立统一的**资产数据标准**；
- 不同来源的资产台账存在**数据差异与冲突**；
- 缺乏**全局视角的统一资产风险管理**。

建设背景

系统安全建设目标



汇聚冬奥资产及其安全状况数据，建立信息系统的**动态资产清单**，保障资产数据的全面性与准确性。

构建冬奥资产安全管理体系，制定**资配漏补安全运行流程**，并持续在实际运营工作进行优化。

开展**常态化资产安全运营**，通过资产数据治理和碰撞分析，驱动资产信息核实与属性冲突解决、漏洞修复状态跟踪及补丁协同安装等工作。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

安全输出

建立动态资产清单，实现资产安全闭环管理

汇聚冬奥资产“白账”与“探查账”数据，结合漏洞情报，对云上/云下/外围资产及其配置、漏洞、补丁等安全状况数据进行数据治理与数据碰撞分析，发现“白账”中未登记的资产及登记错误的数据，人工运营补全“探查账”中未核实的资产信息，判定资产安全状况与脆弱性缓解优先级，建立冬奥信息系统的动态资产清单。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

服务协同

运营流程与操作SOP文档设计

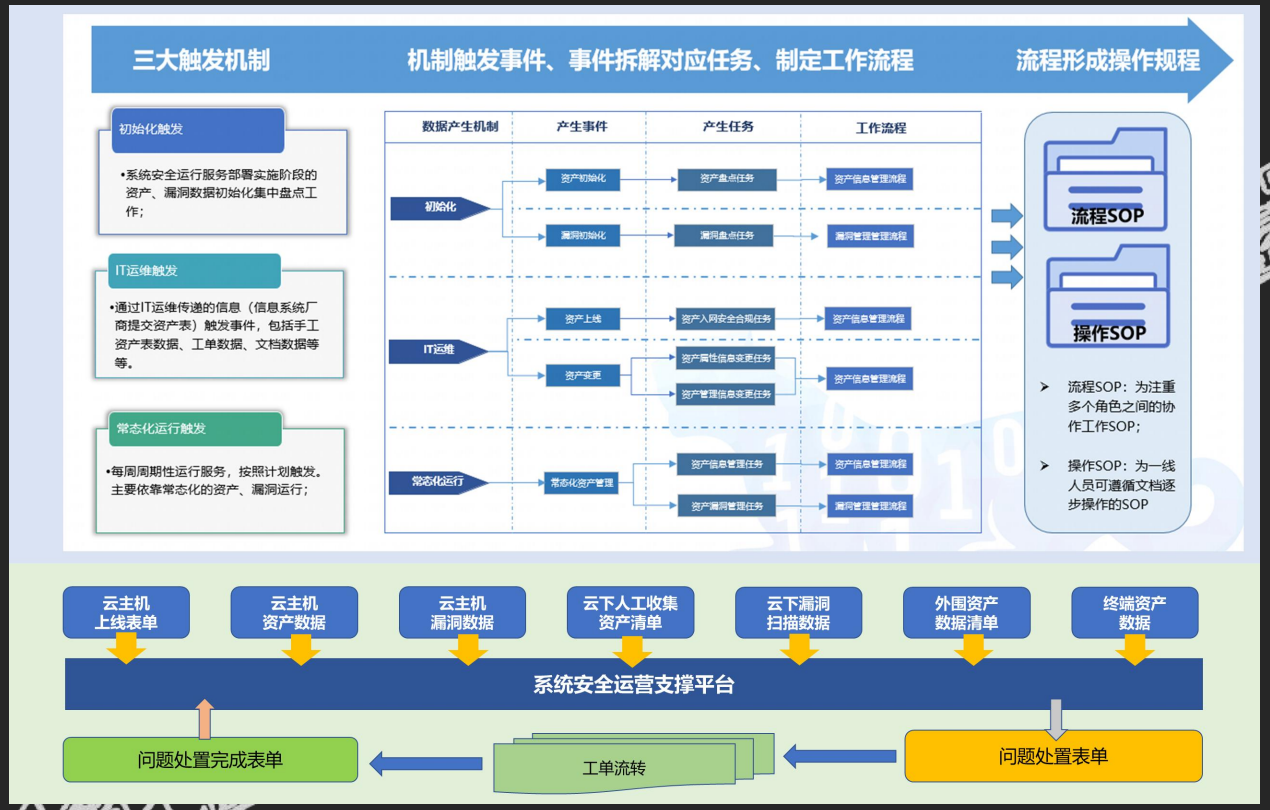
制定冬奥资产管理、漏洞管理、补丁协同安装等相关的运营流程与操作规程，定义资产管理工作中的角色、职责、工作范围和协同机制。

以运营流程为指引，细化为运行团队可执行落地的操作规程，协同信息系统IT运维完成资产安全运营。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

服务协同

运营工作闭环与平台支撑



系统安全运营服务与运行平台有效结合，为冬奥网络安全保障工作提供了有力支撑：

- 多源异构资产和漏洞数据标准化；
- 实体识别、抽取、归一和融合；
- 通过数据碰撞发现资产安全问题；
- 生成运营工作任务并分发；
- 驱动由运营人员对安全问题进行处置；
- 运营绩效可视化、服务质量可度量。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

运营成效

资产的问题处置是一个由数据驱动的持续常态化的过程。伴随多源资产数据的不断更新，通过大数据分析平台碰撞产生资产事项，驱动资产管理处置流程，由一线运营经理及资产责任人交互处置资产事项，完成资产数据的闭环管理。

第一次常态化资产梳理结果

类别		云上资产	数据中心资产	云下场馆资产	外围资产	资产总数
无问题资产		224	1264	193	121	1802
有问题资产	冲突资产	427	51	24	0	502
	待补全资产	319	147	148	0	614
总数		970	1462	365	121	2918

问题资产处置

运营经理团队自行判断处置资产问题，核实并处置问题资产500余条

由资产责任人交互处置资产问题，核实并处置问题资产320条

常态化资产梳理结果

类别		云上资产	数据中心资产	云下场馆资产	外围资产	资产总数
无问题资产		835	1084	340	121	2380
有问题资产	冲突资产	0	0	0	0	0
	待补全资产	296	0	0	0	296
总数		1131	1084	340	121	2676

处置说明：

- 云上资产：主要处理资产属性信息冲突问题、关联字段问题、资产重要属性信息补全问题、新资产上线
- 数据中心资产：主要处理资产重要信息补全问题，其中删除无效资产信息，导致资产数减少
- 云下场馆资产：主要处理资产重要信息补全问题，其中删除无效资产信息，导致资产数减少

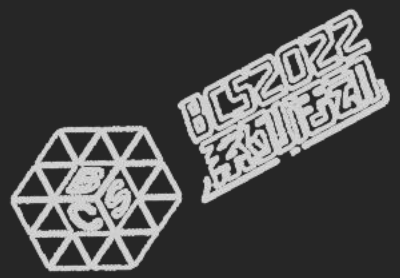
- 问题资产：存在属性冲突或属性信息待补全的资产
- 冲突资产：资产属性信息在多个数据来源中不一致，发生冲突
- 待补全资产：资产的属性信息值为空值的资产，隶属于国外IT公司资产，重要信息已经完备，少量信息未补全

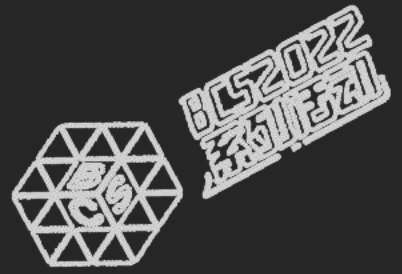
奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

系统安全运行服务支撑平台

产品解决方案





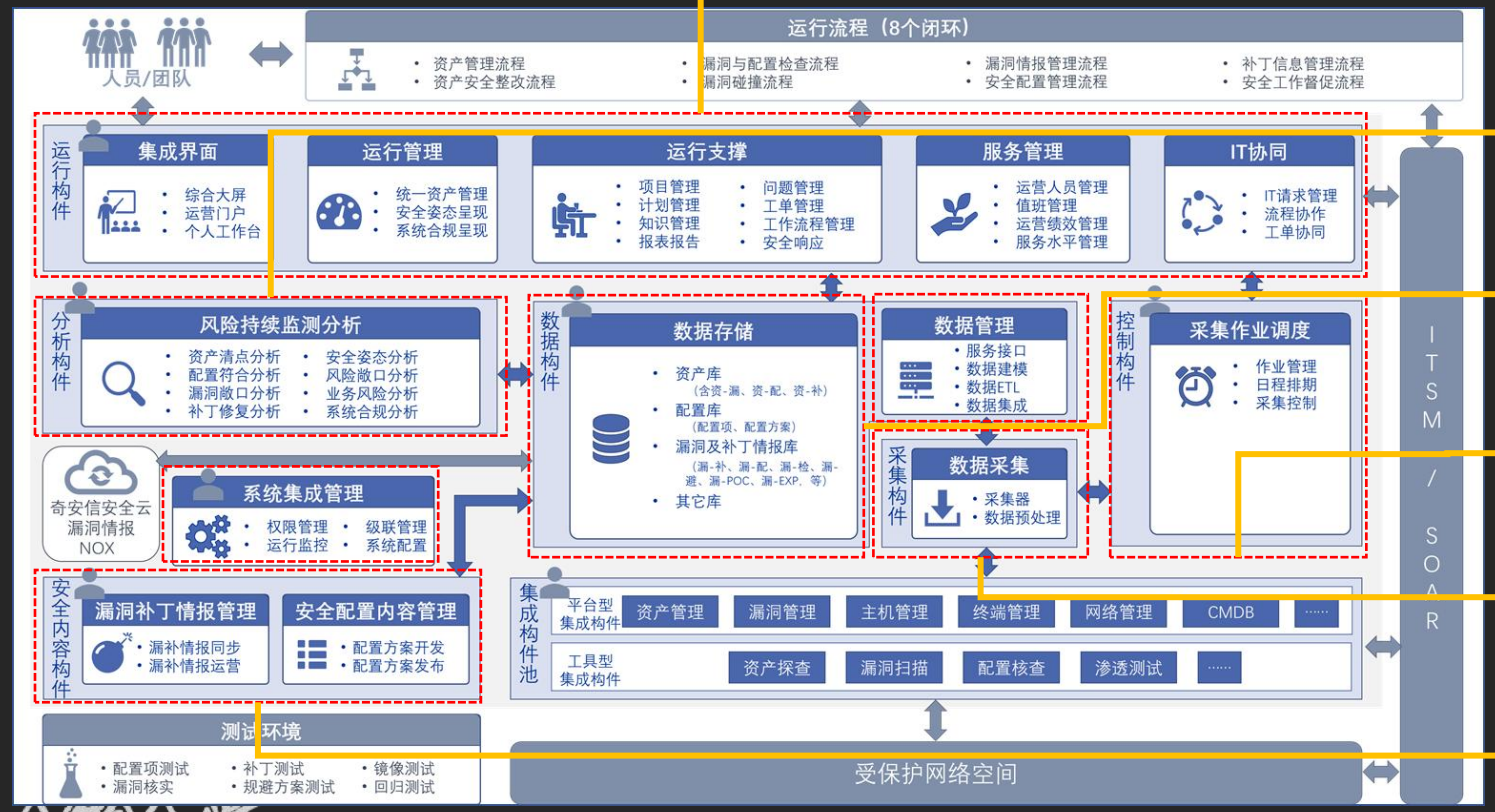
数据和运行双核驱动模式

通过聚合IT资产、配置、漏洞、补丁、漏洞情报等数据，持续监控信息系统的资产状态，进行多维度数据碰撞分析、关联分析，发现资产安全问题，驱动资产发现、配置采集、风险持续监测和资产安全整改等安全运行工作。

打通“资配漏补”安全运行流程与IT服务流程，形成跨团队、跨组织的协同运营机制，将传统事件驱动的、临时抱佛脚资产安全运营模式转变为以数据驱动的常态化运行模式，实现系统资产安全控制措施落地。

平台架构

运行架构



运行构件是运营人员的工作平台，通过灵活配置工作流程，实现资配漏补的运行闭环；

分析构件可以实现多维度的资产数据碰撞，实现资产风险的持续安全监测；

数据构件负责资产及配置、漏洞、补丁、情报等数据的存储和管理；

控制构件负责资产探查设备、漏洞扫描设备等安全设备的任务调度和管理；

采集构件以插件形式实现多源异构数据的集成和采集；

内容构件负责实现漏洞情报的本地化运营管理和安全配置管理。

核心能力

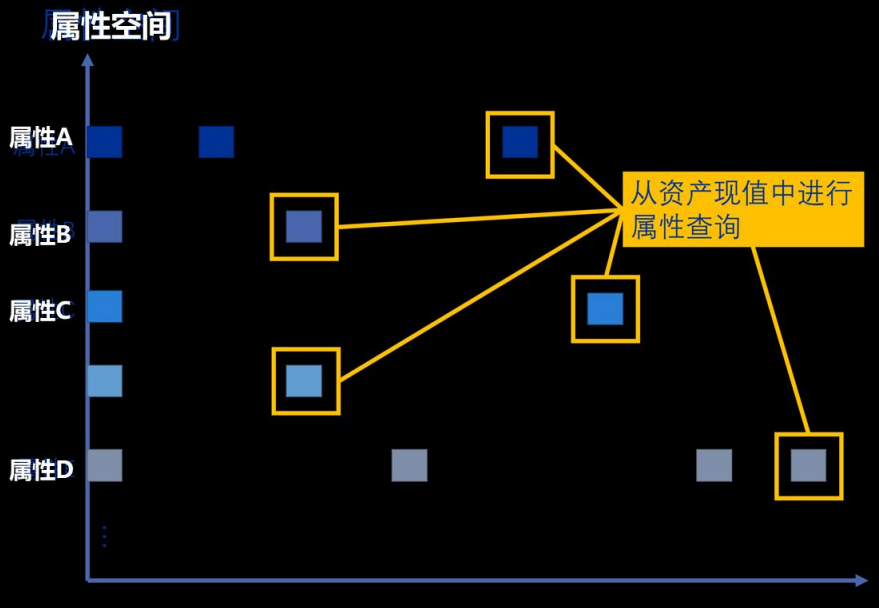
基于插件框架的多源数据集成

基于插件框架适配不同协议和接口的数据源，快速扩展数据采集能力。集成的目标系统除资产探查、漏洞扫描等**传统安全系统**外，还面向**IT基础设施**实现应用集成。如：通过负载均衡系统获取应用发布状况、通过HR/IAM获取组织架构、联系人信息等。

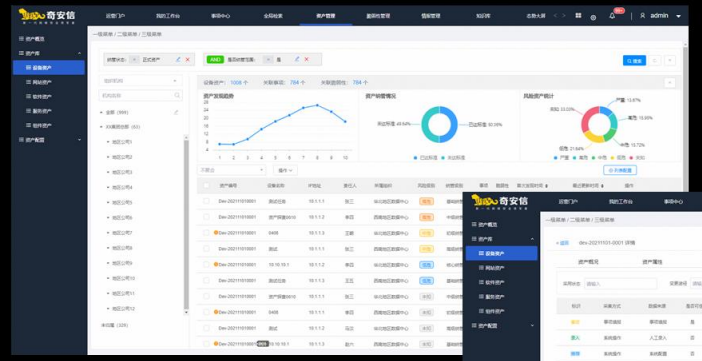
核心能力

基于时空建模的统一资产安全信息库

运营人员关注资产信息准确性、全面性，而且尤其关注资产信息的变化轨迹。因此，在资产模型设计方面以国家标准与国际最佳实践为基础，并延展了配置、漏洞和补丁等实体信息，留存了资产属性的历史值及数据来源和采集方式等关联信息，构建基于时间和网络空间的动态资产清单。

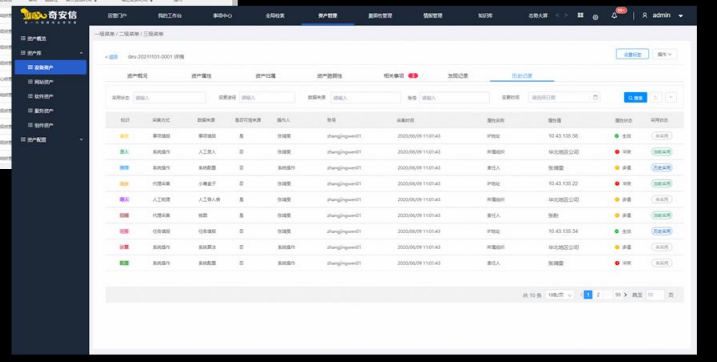


时空资产库



- ✓ 字段级历史信息查询
- ✓ 资产信息溯源

资产变化轨迹



- ✓ 属性推荐值算法
- ✓ 归属信息推荐算法

核心能力

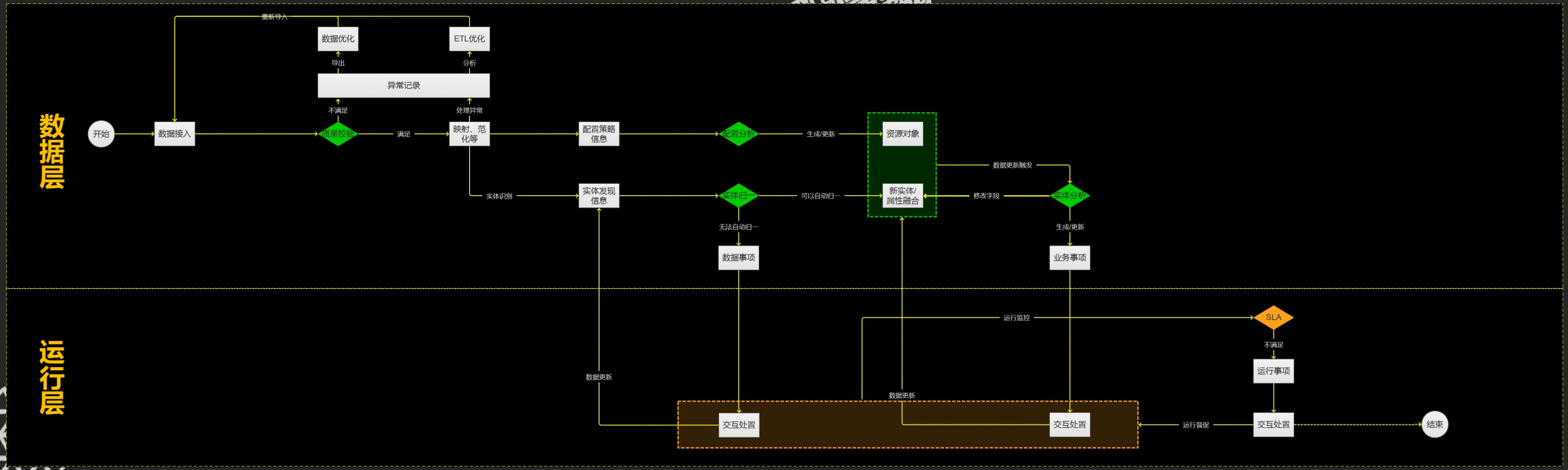
基于数据驱动的资产风险持续监测

在安全运营过程中，多数用户安全基础数据管理分散，关联分析难度大，且运营人员通过人工表格和脚本处理的方式分析安全问题准确性和时效性较低。通过实体分析算法模型，对资配漏补和情报数据碰撞分析，发现资产安全问题，驱动运营人员有针对性的开展实战化安全运营工作。

核心能力

基于数据中台的实体识别、融合和分析

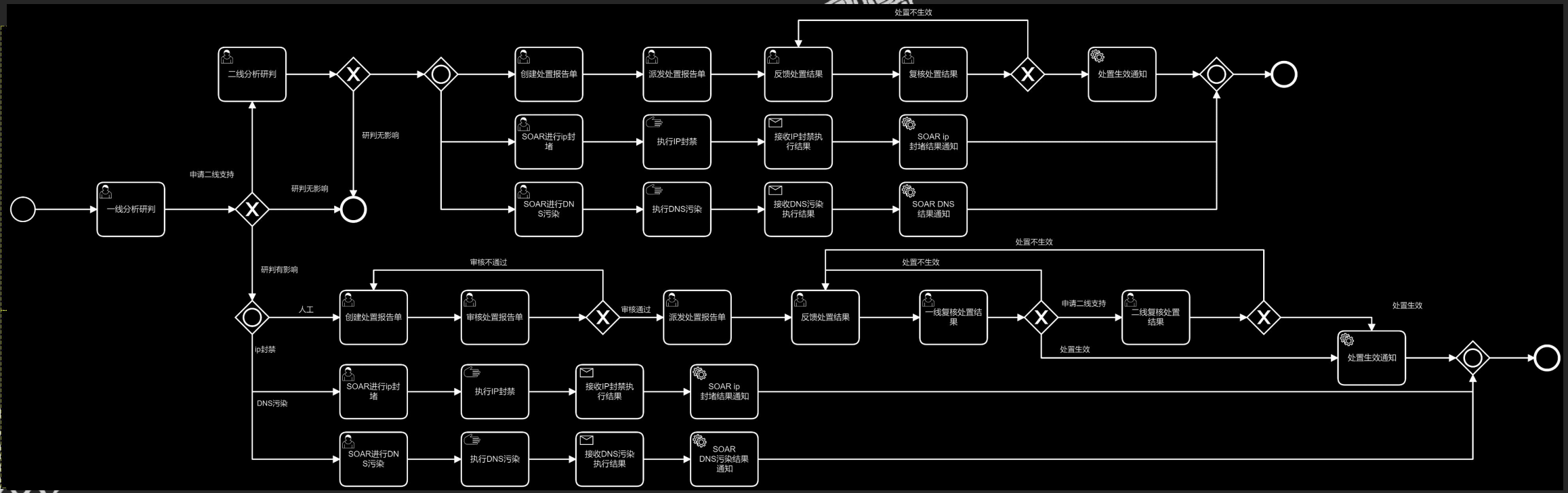
基于中台数据治理能力，对多源异构资产数据标准化，通过**实体数据模型**实现资产和漏洞实体数据识别和抽取。通过**实体相似度算法模型**，实现实体数据归一和融合。通过**实体分析算法模型**，对资产、漏洞和情报等数据碰撞分析，从而发现资产安全问题。



核心能力

基于流程引擎的运营流程定制化

基于支持BPMN2.0的工作流引擎，通过扩展实现定制化的任务列表和人工任务，以动态表单+命名空间的方式实现人机界面和节点数据在流程中的流转。将**运营流程标准化**，实现**运营绩效可量化**、**服务质量可度量**。



奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

启示

系统资产安全是将资产情况从“模糊”梳理“清晰”

问题从”不可控“到”可控“的持续运营过程

- 多源资产数据汇聚（白账、探查账）
- 资产数据治理
- 资产多维数据、历史数据分析碰撞
- 资产问题持续运营
- 形成动态资产清单（黑账）

……

- 汇聚多源漏洞情报数据实现漏洞库、补丁信息在企业的本地运营
- 建立漏洞与资产的关联关系
- 依据漏洞情报生命周期，评估影响程度与修复优先级
- 漏洞修复的常态化运营

1 资产发现及运营

2 漏洞、补丁持续运营

3 配置持续运营

4 安全状况持续监控

- 软件资产、服务资产配置信息的本地运营
- 采集资产生命周期配置信息，持续跟踪资产配置变化
- 建立软件组件配置与资产的关联关系
- 配置变更的持续运营

……

- 持续监控信息系统的资产状态
- 将不能修复漏洞、无法整改配置项的资产加入例外管理清单，纳入风险管理；
- 与态势感知联动，持续对例外管理清单中的资产加强监控
- ……

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周