SMARTEAGLE
慧鹰

安全设备运维管理平台

——新型异构化网络安全环境保障系统

常州慧鹰信息科技有限公司

SMARTEAGLE
慧鹰

目录

Contents

目录

Part.

1

SMARTEAGLE
慧鹰

关于慧鹰

常州慧鹰信息科技有限公司是一家专业从事运维管理软件的研发、销售、咨询和服务的一体化高新技术软件企业，致力于为用户提供全面优质的运维产品及整体解决方案。

1.1 关于慧鹰

常州慧鹰信息科技有限公司是一家专业从事运维管理软件的研发销售、咨询和服务的一体化高新技术软件企业，致力于为用户提供全面优质的运维产品及整体解决方案。

慧鹰科技秉承“以用户需求为导向，以用户满意为宗旨”的经营理念，积极自主研发创新，极力构造良好运维生态，做到“人人都是运维工程师”

常州高新
技术企业

“龙城英才”
重点扶持企业

深耕运维行业
8+年

1.2 服务客户

UnionPay 银联
华泰证券 HUATAI SECURITIES
南京银行 BANK OF NANJING
东吴期货 SOOCHOW FUTURES
江苏·农村商业银行
国家电网 STATE GRID
中国能建
中煤集团
港华燃气 Towngas
SERES 赛力斯
协鑫 GCL
山东海化 SHANDONGHAIHUA
NVCC
cxmt 长鑫存储技术有限公司 ChangXin Memory Technologies, Inc.
洋河股份 YANGHE
EYE 爱尔眼科 AIER OPHTHALMOLOGY
赣锋锂业 GanfengLithium
固德威 GOODWE
ARISTON 阿里斯顿
东南大学 SOUTHEAST UNIVERSITY
无锡学院
连云港市第二人民医院
无锡市妇幼保健院
徐州市儿童医院
常州市金坛区中医医院
江南大学附属医院 AFFILIATED HOSPITAL OF JIANGNAN UNIVERSITY
江苏监狱 JIANGSU PRISON
江苏省常州监狱
射阳县公安局
太仓市财政局
宿迁人力资源和社会保障局
浙江大学图书馆
东南大学 SOUTHEAST UNIVERSITY
南京信息工程大学 Nanjing University of Information Science & Technology
滨江学院

Part.

2

SMARTEAGLE
慧鹰

产品介绍

安全设备运维管理平台SDOM（SmartEagle Security Operation Platform）是常州慧鹰最新研发的一代适用于异构化安全设备环境的运维平台。通过全面的多数据源采集能力，实时检测网络安全设备的运行状态，加强网络安全保障能力。基于DevOps为核心理念，为网络安全建设过程持续赋能，提升网络安全防护能力。

国内首家，致力为异构化网络安全环境打造“安全设备智能巡检及预警系统”

安全数据整合难

实现安全资源数据统一监管，实时监控保障设备**稳定**运行

设备巡查不及时

对安全设备健康性实时巡查，保障安全设备功能**有效**工作

安全事件甄别难

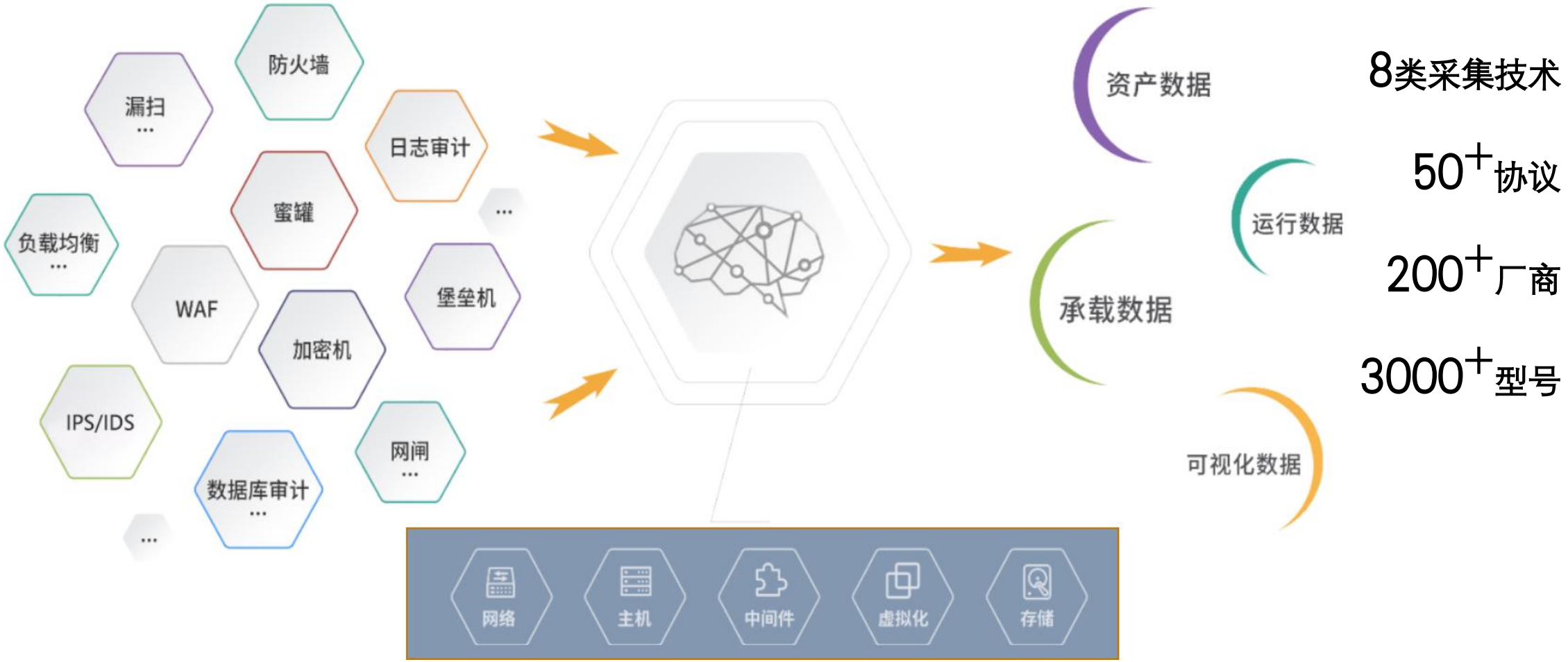
建立安全事件关联模型分析，实时保障安全策略**正确**执行

缺乏持续服务增值

提供信息安全事件分析的SAAS服务，落实安全**持续**性服务

平台提供“软件+服务”一体化解决方案

13年磨一剑，无感知采集来自安全资源的实时数据，构建全息数据视角



8类采集技术

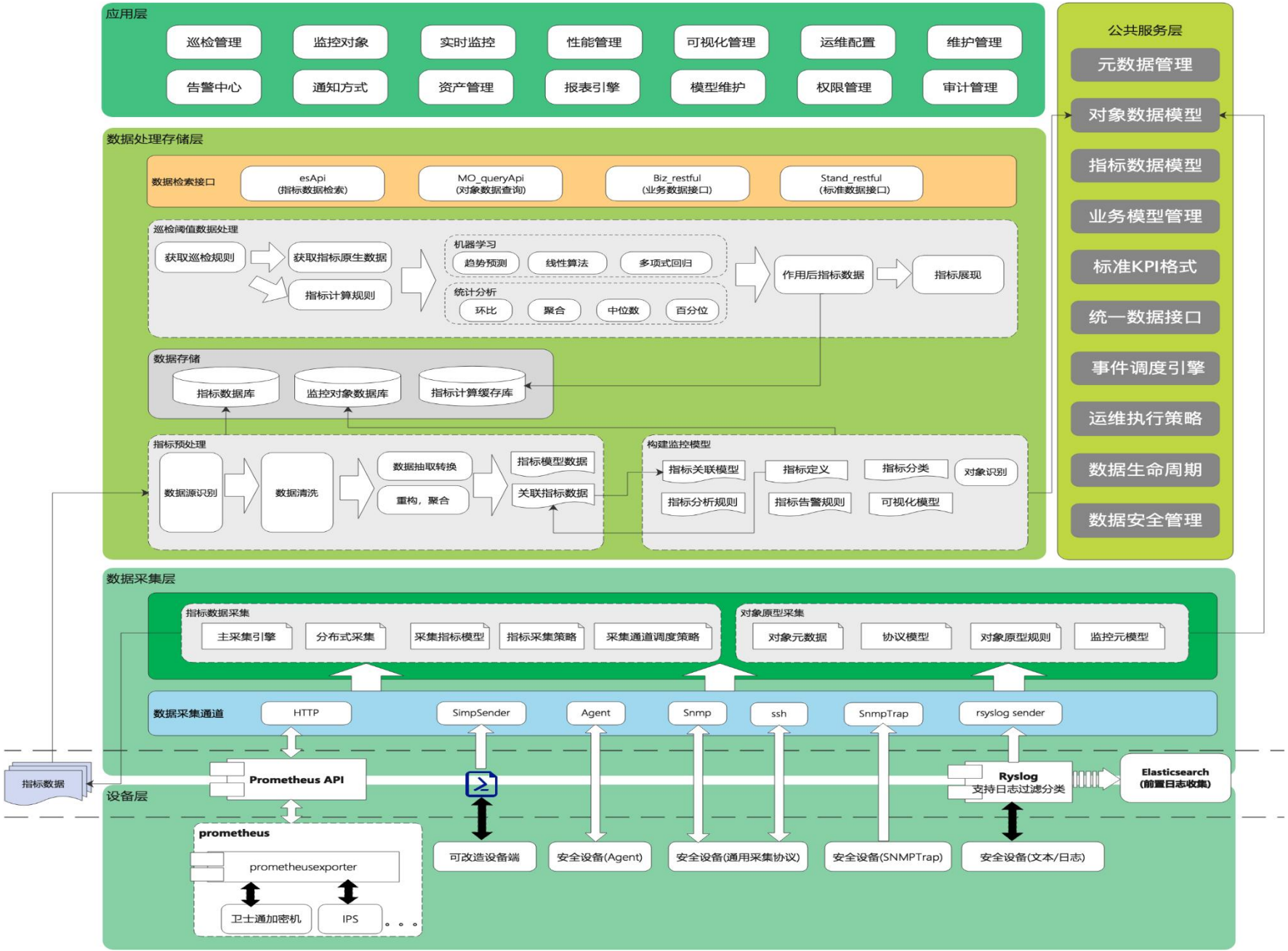
50+协议

200+厂商

3000+型号

基于安全资源数据分析，为用户的安全设备提供保障类平台

2.3 产品介绍 — 功能架构


应用层
巡检管理
监控对象
实时监控
性能管理
可视化管理
运维配置
维护管理
告警中心
通知方式
资产管理
报表引擎
模型维护
权限管理
审计管理
公共服务层
元数据管理
对象数据模型
指标数据模型
业务模型管理
标准KPI格式
统一数据接口
事件调度引擎
运维执行策略
数据生命周期
数据安全管理
数据处理存储层
数据检索接口
esApi (指标数据检索)
MO_queryApi (对象数据查询)
Biz_restful (业务数据接口)
Stand_restful (标准数据接口)
巡检阈值数据处理
获取巡检规则
获取指标原生数据
指标计算规则
机器学习
趋势预测
线性算法
多项式回归
统计分析
环比
聚合
中位数
百分位
作用后指标数据
指标展现
数据存储
指标数据库
监控对象数据库
指标计算缓存库
指标预处理
数据源识别
数据清洗
数据抽取转换
重构，聚合
指标模型数据
关联指标数据
构建监控模型
指标关联模型
指标定义
指标分类
对象识别
指标分析规则
指标告警规则
可视化模型
数据采集层
指标数据采集
主采集引擎
分布式采集
采集指标模型
指标采集策略
采集通道调度策略
对象原型采集
对象元数据
协议模型
对象原型规则
监控元模型
数据采集通道
HTTP
SimpSender
Agent
Snmp
ssh
SnmpTrap
rsyslog sender
指标数据
Prometheus API
Ryslog
支持日志过滤分类
Elasticsearch (前置日志收集)
设备层
prometheus
prometheusexporter
卫士通加密机
IPS
可改造设备端
安全设备(Agent)
安全设备(通用采集协议)
安全设备(SNMPTrap)
安全设备(文本/日志)

2.4 产品介绍 — 功能介绍

安全资源管理

自动发现各种安全相关设备系统，包括安全设备、以及关联的网络资源、操作系统等，并进行全面统一的管理。

安全设备监控

多种数据采集手段和监控方式，保障设备指标监控的实时性和准确性，支持指标DevOps构建。

安全预警中心

灵活的告警规则设立，支持数据预测告警以及SLA升级。多告警通道输出，保证告警及时送达。

安全事件分析

基于关联的安全事件分析模型，实现事件的智能关联以及甄别机制对安全事件精准降噪、降低误报率和漏报率

安全自动化巡检

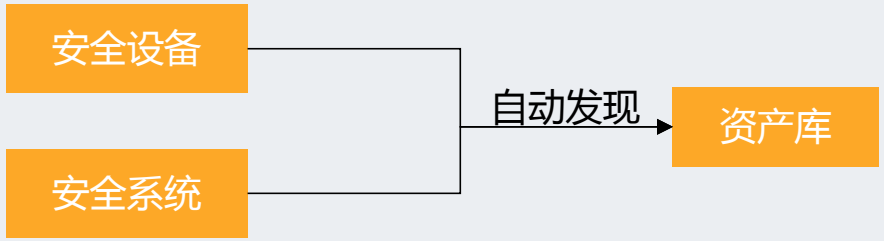
收集网络环境中不限于安全设备等的日常运行状态数据并根据预设巡检策略分析其健康情况

运维生态集成

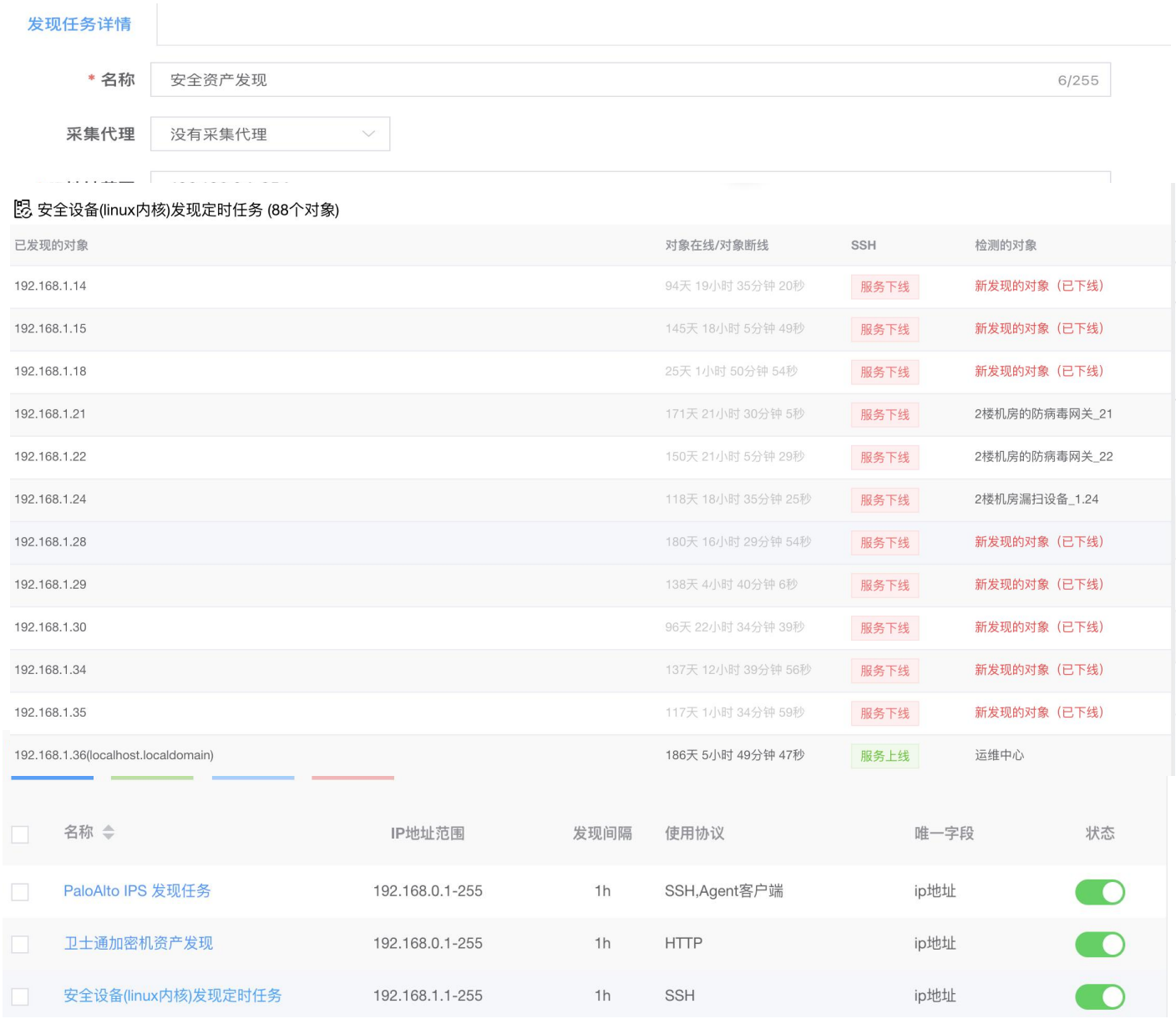
开放式架构，支持和运维生态其他产品服务快速集成，更好地完善运维规范化管理以及有效落实运维的闭环流程

2.4.1 安全资源管理—资产发现

内置自动发现框架，支持安全设备系统的自动发现

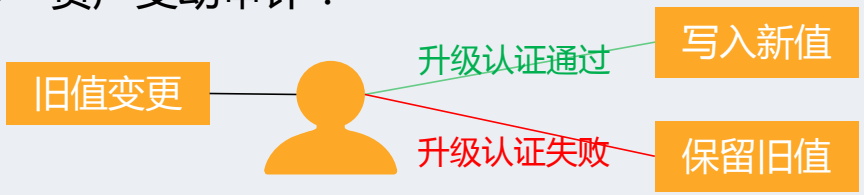


- 自动发现模板：提供发现内容定制化，允许用户自行配置条件组合域、IP端、发现方式等内容。
- 自动发现任务：提供发现任务定制化，支持自定义执行周期和时间。允许用户指定资产特征标识机制。
- 自动发现策略：
  - ✓ 最新发现结果自动同步资产库
  - ✓ 发现新资产及时通知运维人员
  - ✓ 支持数据同步到第三方CMDB

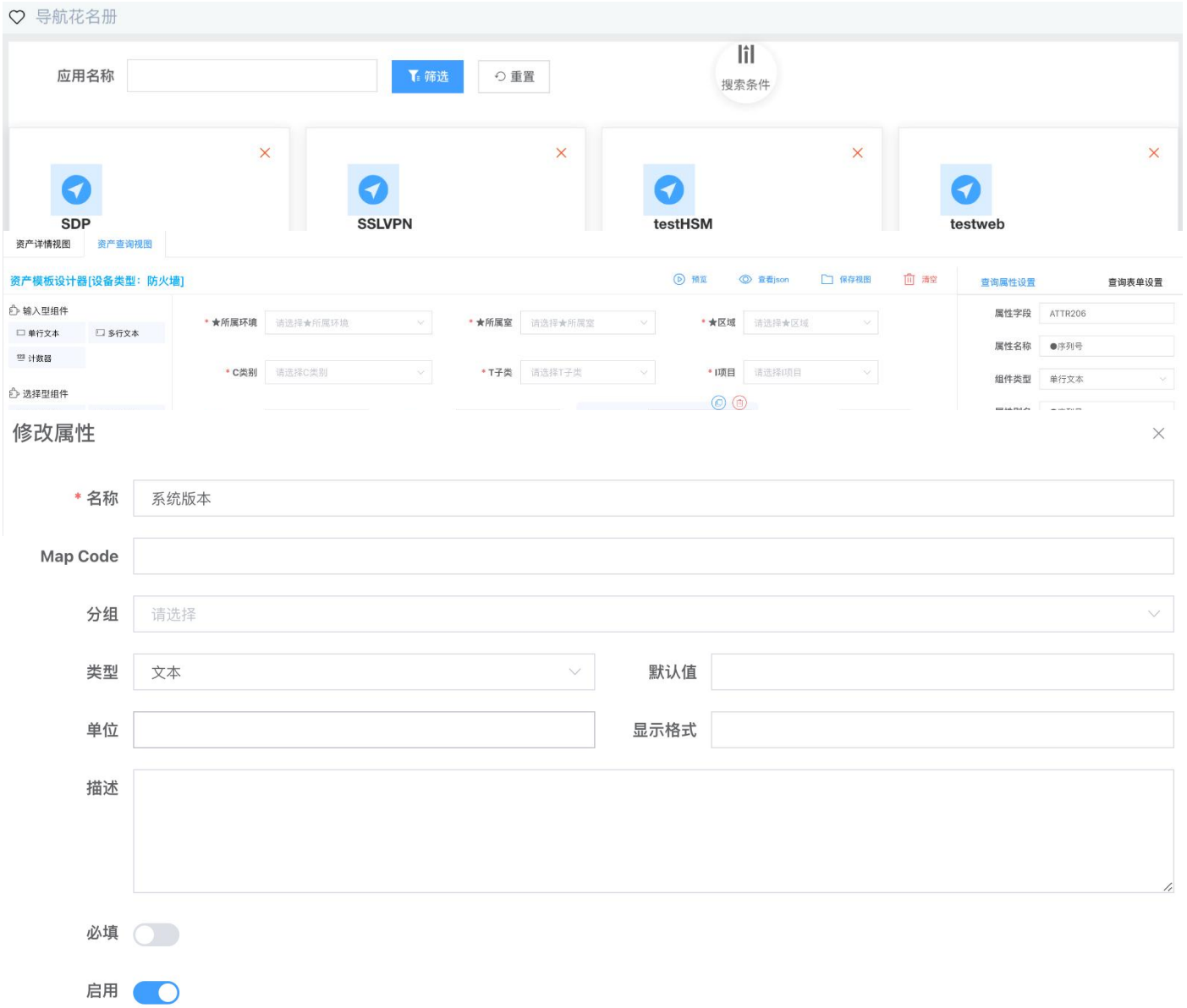


2.4.1 安全资源管理—资产维护

- 资产花名册：提供发现资产花名册一览，统一维护各个专用安全设备系统的登录导航。
- 动态的资产模型数据库：
  - ✓ 自定义资产详细视图及检索视图，针对不同类型资产定制专项数据呈现。
  - ✓ 所有的资产类型属性可以动态扩展，满足用户资产维护的增长性需求。
- 资产变动审计：

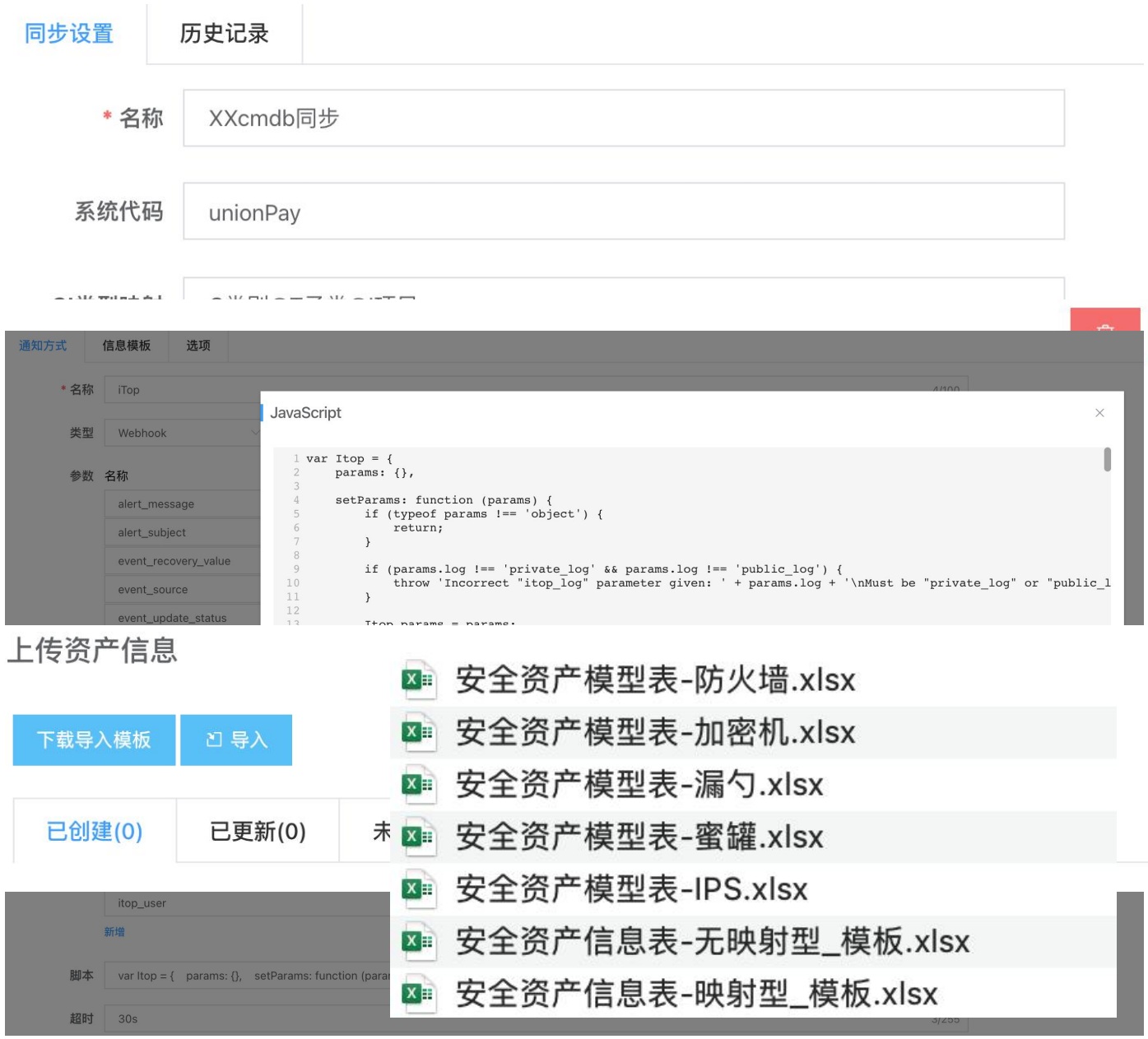


  - ✓ 所有资产的数据变化，记录在库，实现资产变更的可追溯。
  - ✓ 采用升级密码保护机制，对于危险性的操作需要权限提升审核才能操作。



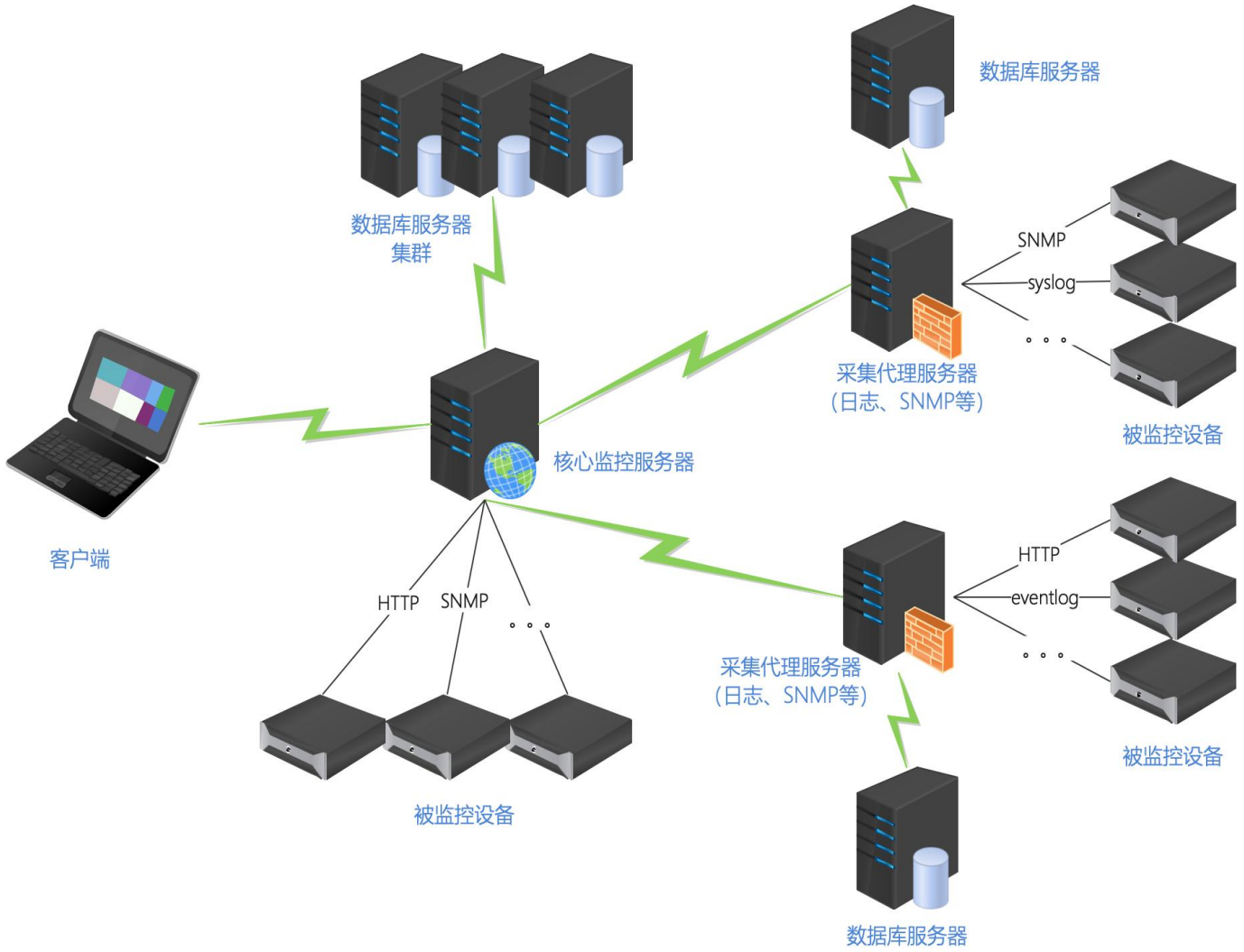
2.4.1 安全资源管理—资产同步

- 资产数据同步适配
  - ✓ 动态资产数据模型适配：支持与第三方CMDB、监控系统、资产系统动态资产适配。
  - ✓ 扩展性资产适配器：支持脚本引擎开发扩展资产适配器。
  - ✓ 自动适配同步：提供适配任务定制，支持自定义执行周期时间、支持自定义适配参数，进行自动更新同步
- 资产库建立：支持从Excel模板文件，实现资产类型的构建以及资产信息的快速录入
- 资产同步接口，Restful形式提供以下接口，
  - ✓ CIT生命周期管理API
  - ✓ CI生命周期管理API
  - ✓ CIR生命周期管理API



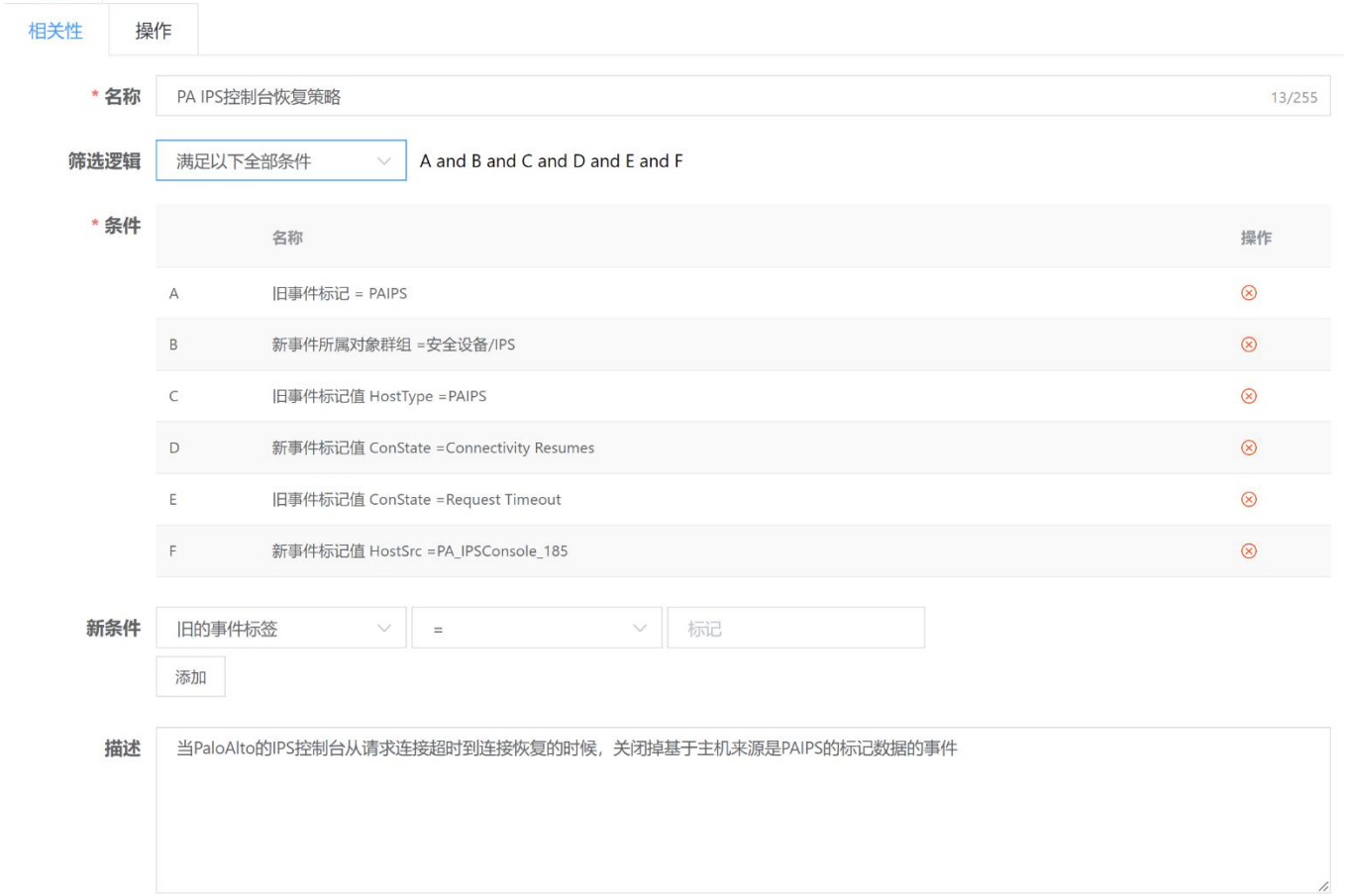
2.4.2 安全事件分析—日志采集

- 集中采集：对各类生产环境的日志数据进行采集、清洗、存储，这些数据包括不限于安全设备、网络设备、中间件、操作系统、数据库、应用层等所有日志。
- 采集方式：支持有代理采集与无代理采集。
- 过滤器设计：
  - ✓ 事件收集筛选器：在前置收集以及后置处理阶段，分别设计过滤机制，只负责传输业务所必要的事件日志，这样日志检索也变得更加方便，也大大地优化数据库容量。
  - ✓ 数据转换过滤器：用于减少事件日志收集过程中日志干扰信息，并且将日志数据指标化、精简化，然后存储到数据库中，大大提高日志的可读取性。
- 输出方式：支持多种输出方式
  - ✓ 内置TCP方式输出SDOM服务端
  - ✓ 输出到Elasticsearch、Kafka...
- 日志归档：可以根据合规性要求和内部审计要求来决定日志归档任务。比如存档时间、删除时间。



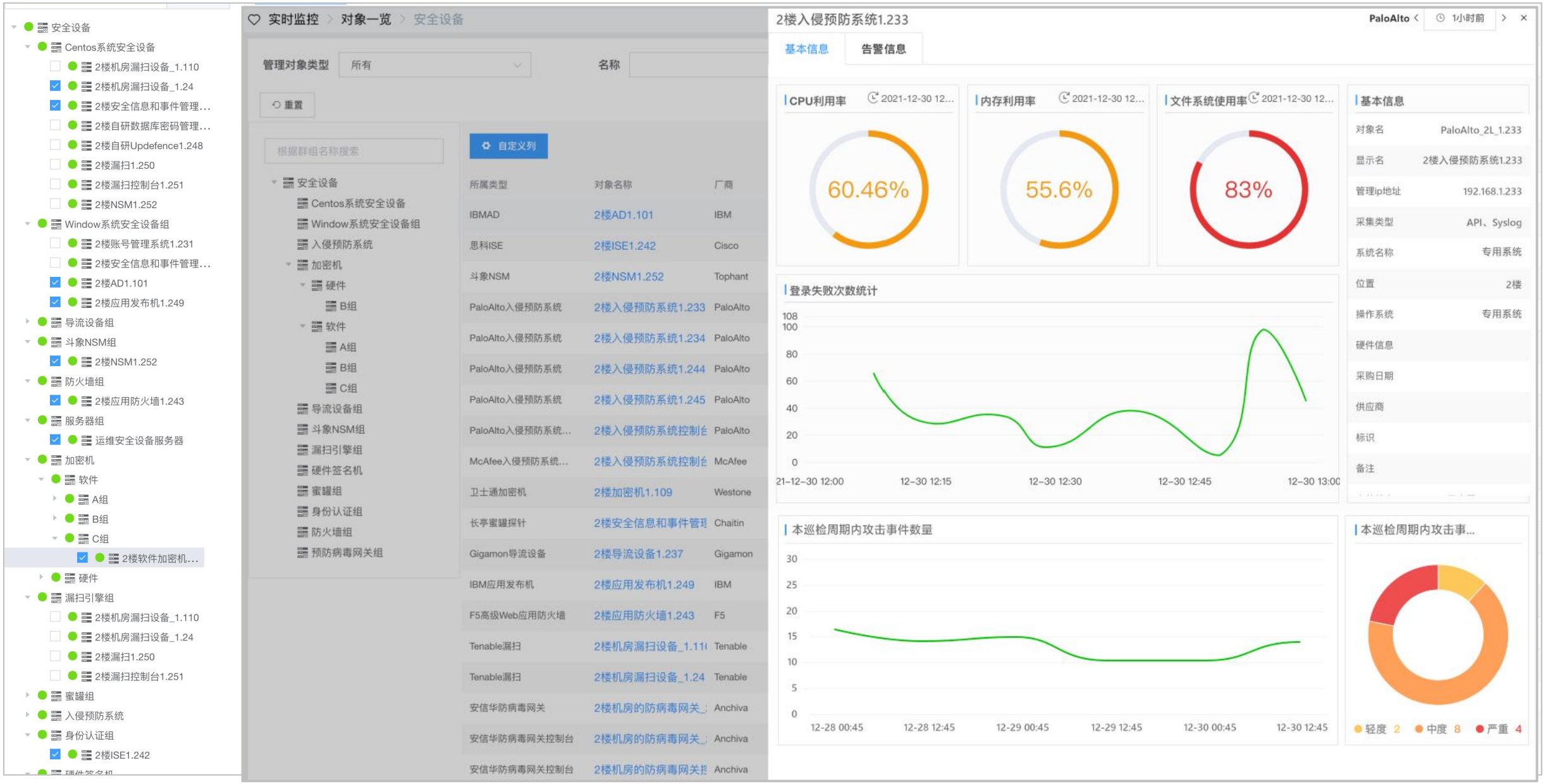
2.4.2 安全事件分析—事件关联

- 标准化指标模型设计：为了从收集的事件日志中获得最大收益，日志管理工具解析事件日志至关重要。SDOM内置的事件日志解析器，采用指标模型体系对事件日志进行规范化、解析和索引。
- 事件标签：
  - ✓ 便于识别日志文件中的细节问题，更加容易识别硬件设备、应用系统、服务
  - ✓ 用于日志过滤，基于事件标签的自动化运维
- 事件关联的应用：
  - ✓ 创建事件智能关联规则：可以避免告警洪灾现象，更加有利于问题的定位和溯源。
  - ✓ 基于告警规则的事件关联：对于日志的监控，应对多个日志的应用源的情况，采用事件关联机制可以更加细致处理日志的告警信息。
  - ✓ 全局事件关联规则：自定义创建新的网络攻击模式规则。
  - ✓ 跨日志分析，可以发现网络上多个设备的日志序列，快速构建网络安全问题的事件路径链，可以识别存在可能性攻击，并会迅速反馈运维人员，并主动采取措施来抵御攻击



2.4.3 安全设备监控—监控可视化

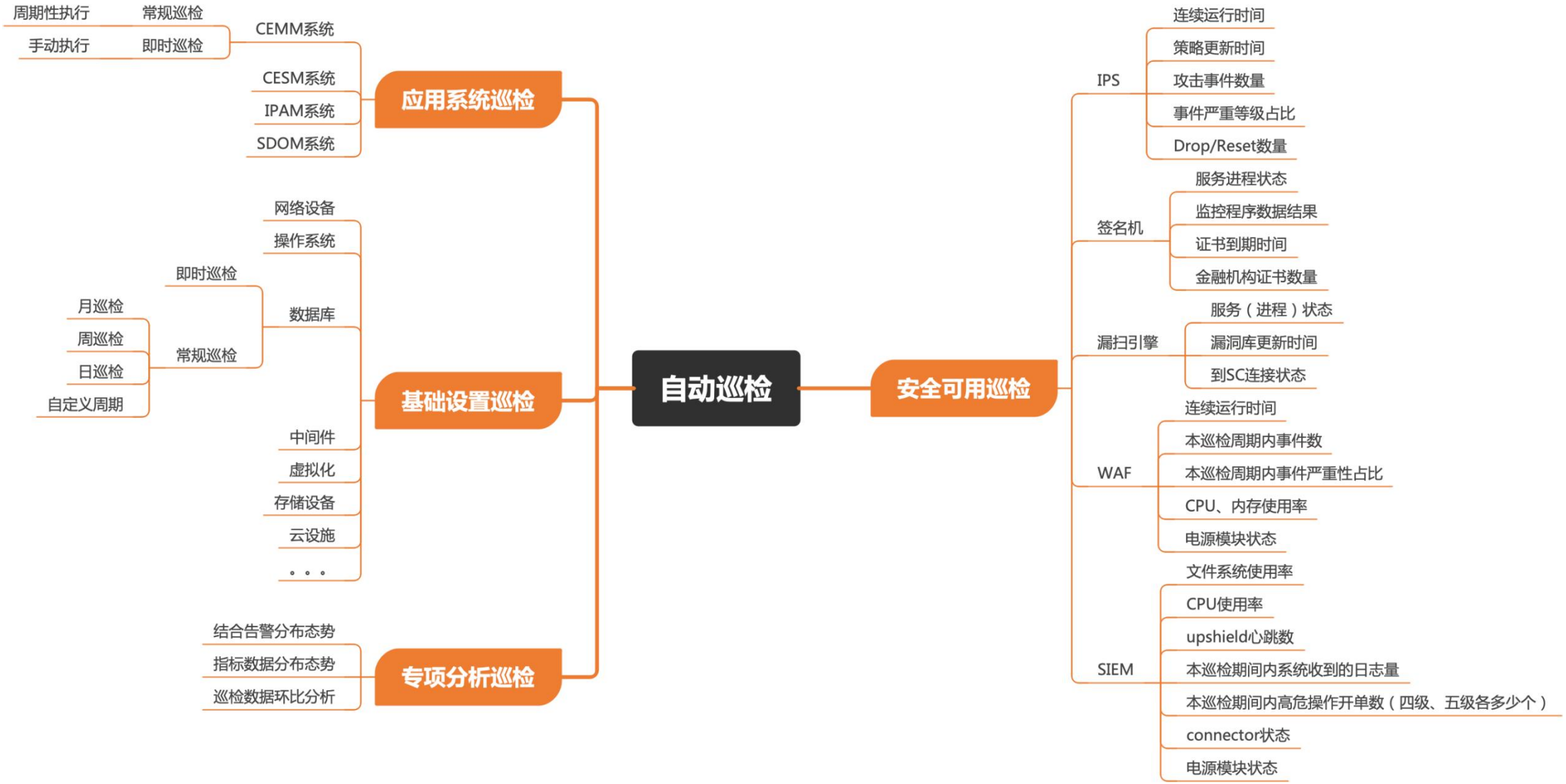
2.4.3 安全设备监控—指标综合分析



2.4.3 安全设备监控—DevOps指标构建

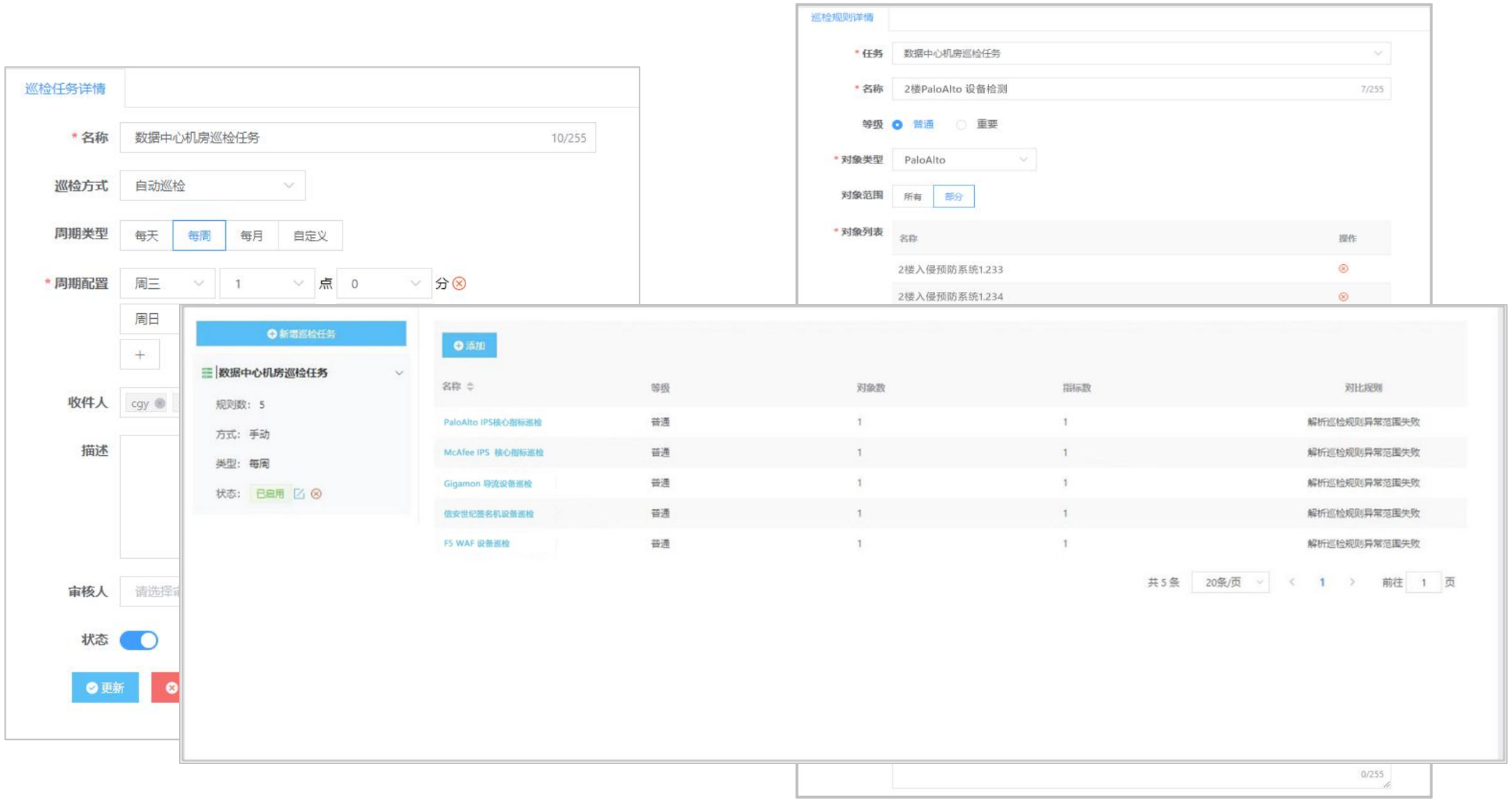
- 系统内置开发者模式，用户可以自行开发更多指标扩展，通知支持指标可视化GUI显示模型定义

2.4.4 安全自动化巡检–巡检任务树



2.4.4 安全自动化巡检–巡检模板

- 系统内置多种巡检模板、同时可以自定义巡检任务、巡检指标、巡检执行策略



2.4.4 安全自动化巡检–巡检视图

- 智能化巡检，自定义巡检任务，异常指标实时提醒，巡检综合评分，巡检报表即刻导出

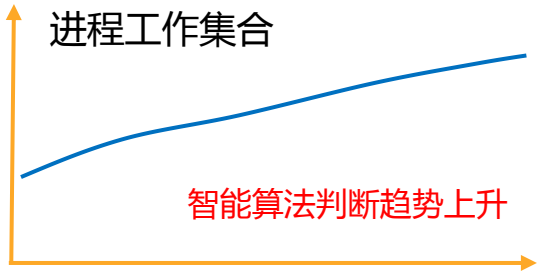
2.4.5 安全预警中心—实时告警测试

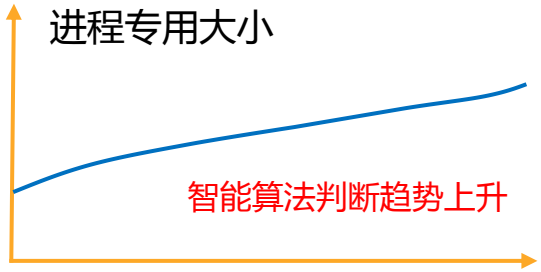
- 基于合理数据采样，通过不同算法，可以实现实时告警

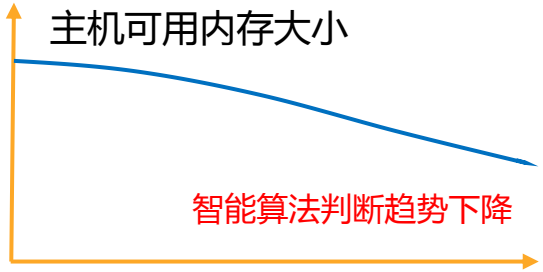
2.4.5 安全预警中心—动态复合告警规则

适用场景：早期风险防范——内存泄露预防

详细描述：对内存相关的多项指标进行智能分析做趋势数据预测，从运维角度梳理预测指标的相关关系，从而进一步判断预警是否成立，可早期判断内存泄漏







内存泄漏预警

2.4.5 安全预警中心—基于数据预测告警规则

运维数据预测，提早风险防范

步骤1：选择检测指标项以及计算类型

步骤2：选择采集样本数据

动态数据样本，实时训练算法，保证预测的准确性

步骤3：选择相应的预测算法模型，包括机器学习的统计分析以及概率分析

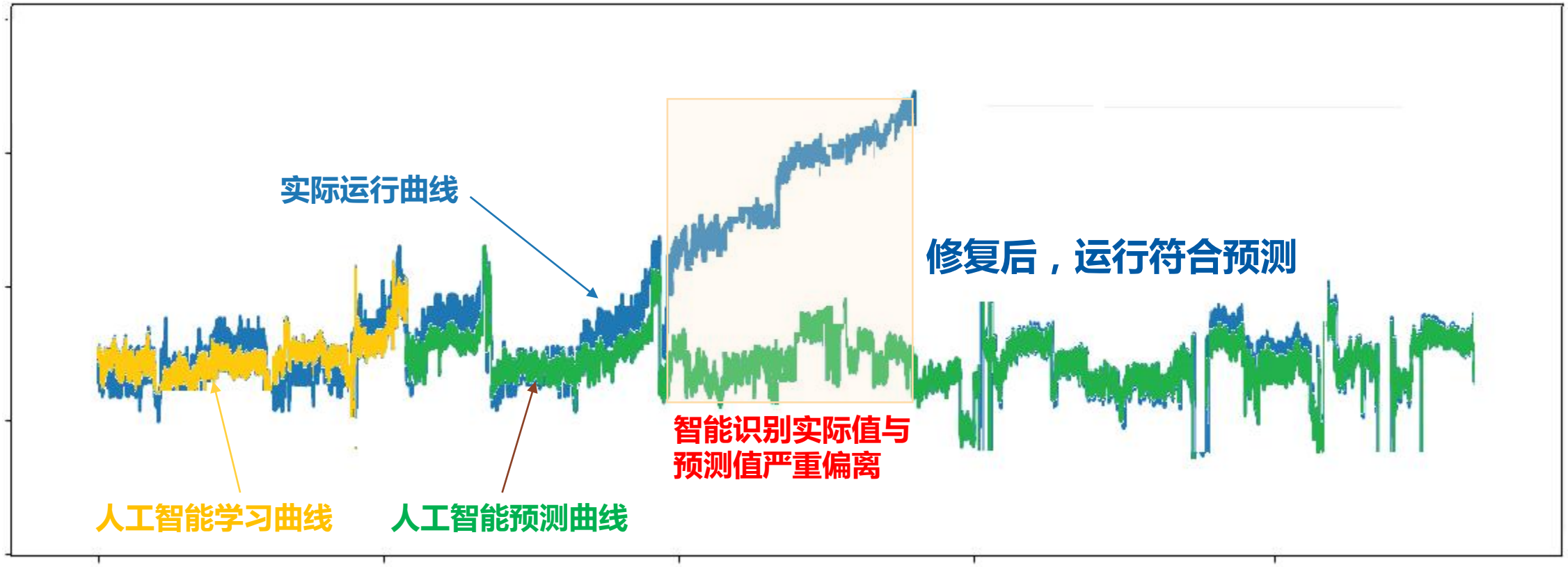
步骤4：选择告警判别依据，包括对预测的时间和预测值类型的设置

2.4.5 安全预警中心—基于数据预测告警规则

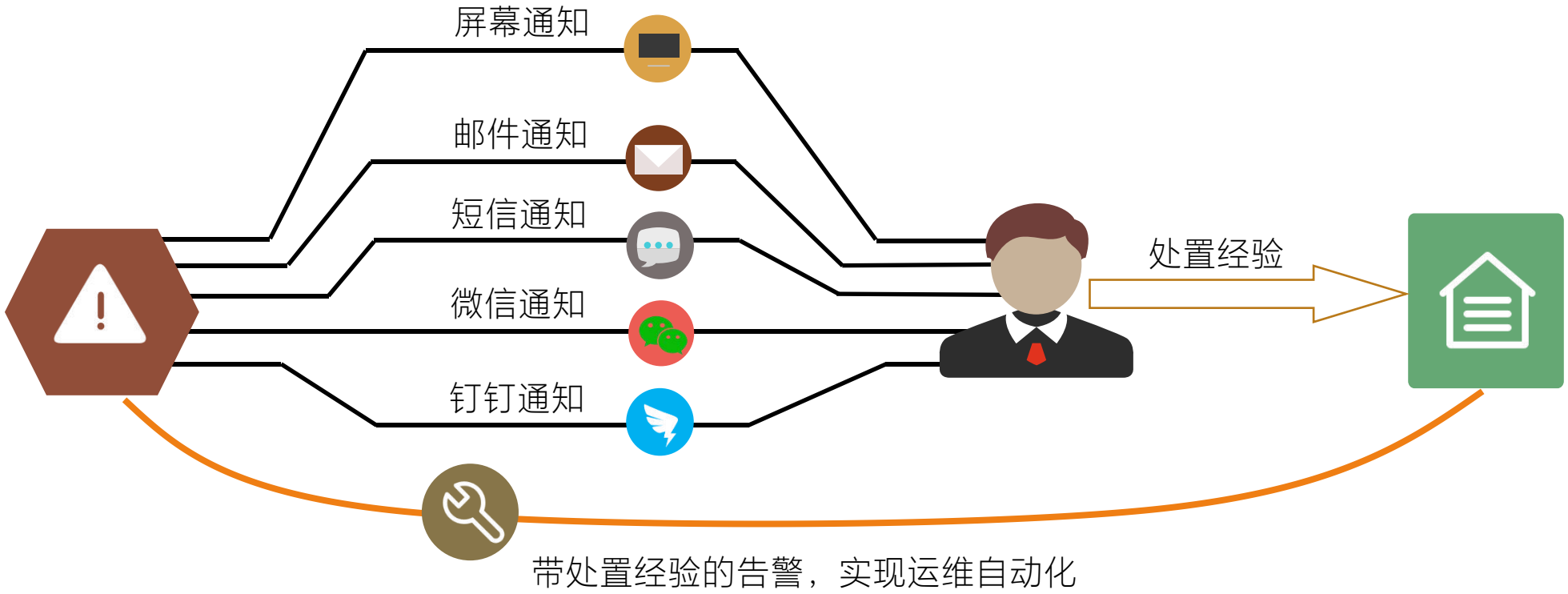
适用场景：早期风险防范——检测未来磁盘空间剩余可用量

规则用途：根据历史磁盘使用的数据情况，预测未来磁盘使用量的潜在风险

详细描述：选择指定数据区域作为训练数据样本，同时根据预测算法，预测未来某一个时间点的磁盘使用的预测数据大小。
比较磁盘实际可用容量大小与预测数据的判断情况，提前预警，提早规划磁盘容量使用



2.4.5 安全预警中心—多通道告警输出



- 多样化告警通知方式，确保运维人员及时获取告警信息，第一时间处理告警。

2.4.6 运维生态集成

运维可视化

提供完善的数据接口，支持与Grafana、Graphite、DataV等可视化产品无缝对接，满足不同的运维呈现场景需求

运维监控

Zabbix、Prometheus、Elastic Stack等优秀的运维监控产品互相贡献生态和技术成果，持续助理运维行业

运维自动化

平台体系内置自动化运维作业平台组件，集成多个开源运维自动化工具，同时支持和用户方自动化平台对接

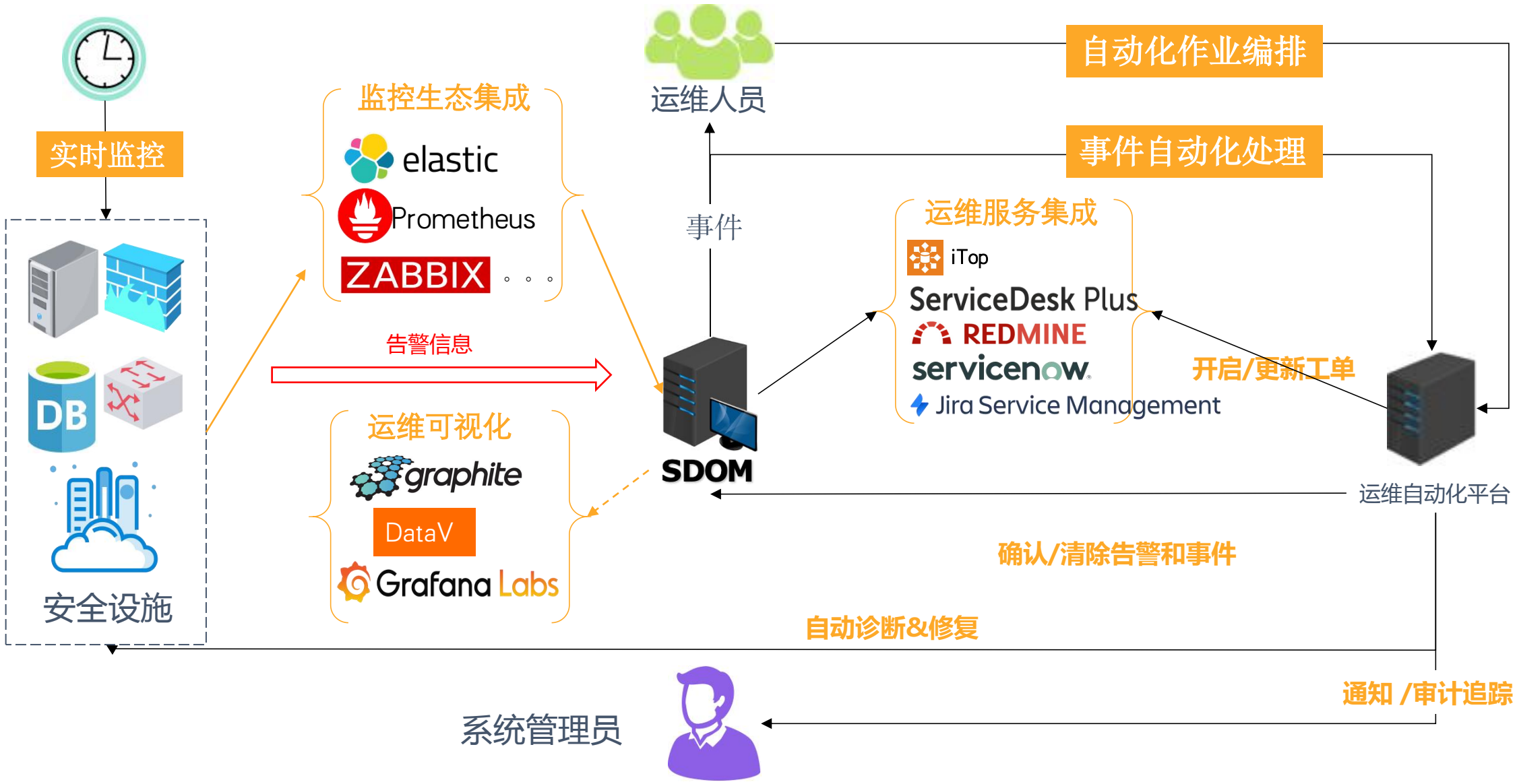
运维告警

提供对象数据、指标数据、告警数据是实时导出。支持输出到其他运维告警平台，比如OneAlert、AlertManager等

运维服务

支持和各类运维服务管理流程系统集成，比如ITop、ServiceDesk Plus、ServiceNow等

2.4.6 运维生态集成


实时监控
DB
安全设施
监控生态集成
elastic
Prometheus
ZABBIX
。。。
告警信息
运维可视化
graphite
DataV
Grafana Labs
运维人员
事件
SDOM
自动化作业编排
事件自动化处理
运维服务集成
iTop
ServiceDesk Plus
REDMINE
servicenow
Jira Service Management
开启/更新工单
运维自动化平台
确认/清除告警和事件
自动诊断&修复
通知 /审计追踪
系统管理员

目录

Part.

3

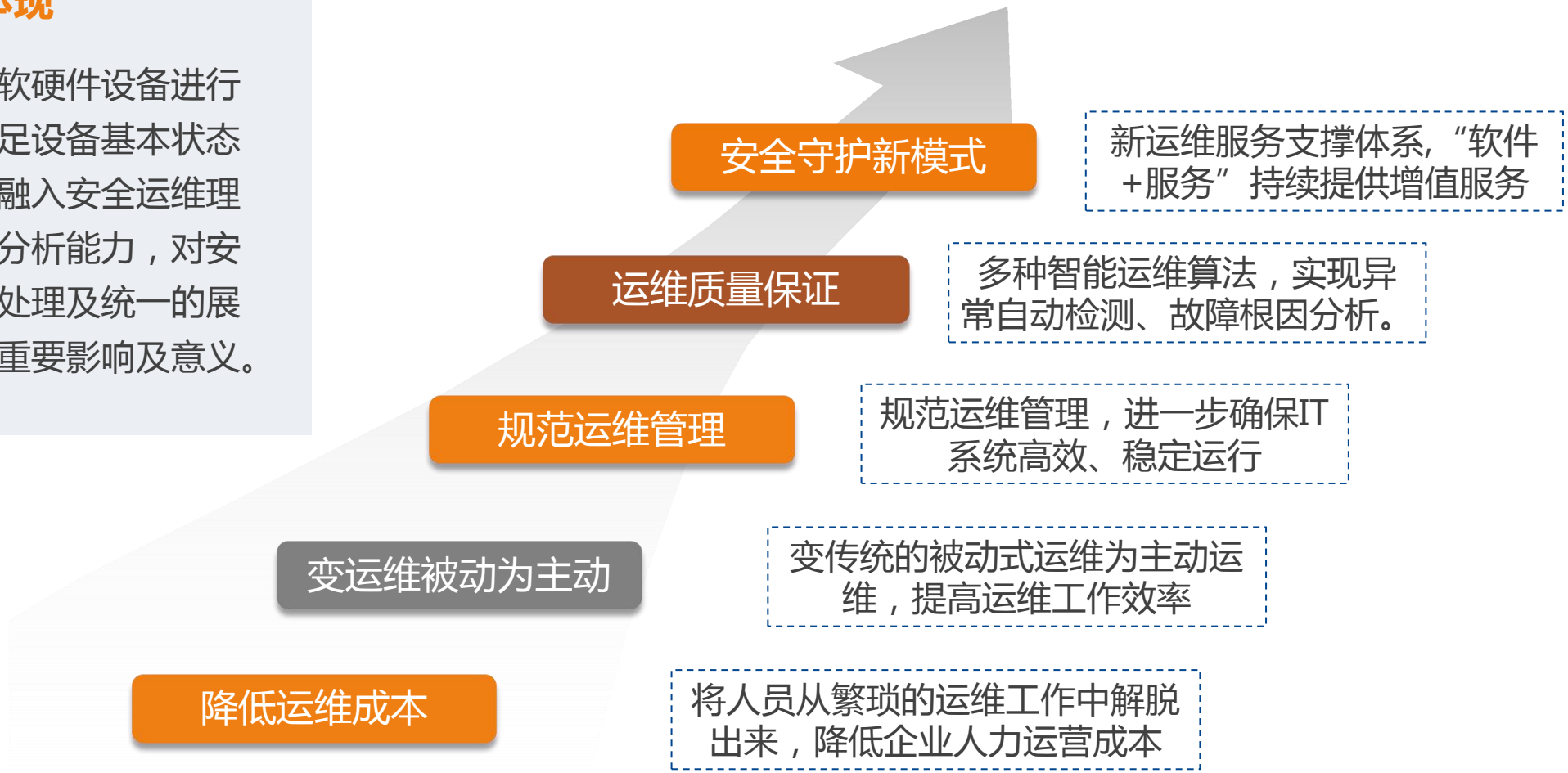
产品价值

通过ATOP实现智能自动化运维会给我们带来什么效益呢？

4. 产品价值

产品价值体现

慧鹰SDOM实现对IT软硬件设备进行统一监控管理，在满足设备基本状态和性能监控基础上，融入安全运维理念，通过强大的数据分析能力，对安全事件进行联动分析处理及统一的展现，对运维工作有着重要影响及意义。



SMARTEAGLE
慧鹰

感谢您的观看

THANK YOU FOR YOUR LISTENING