



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



1

关于慧鹰

2

产品介绍

3

产品价值

4

未来方向

目录

Contents

Part. 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。



SMARTEAGLE
慧鹰

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
80+年





1.2 服务客户



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



长鑫存储技术有限公司
ChangXin Memory Technologies, Inc.



洋河股份
YANGHE



爱尔眼科
AIER OPHTHALMOLOGY

赣锋锂业
GanfengLithium

赣锋锂业



固德威
GOODWE



ARISTON
阿里斯顿



东南大学
SOUTHEAST UNIVERSITY



无锡学院



镇江市第二人民医院



无锡市妇幼保健院



徐州市儿童医院



常州市金坛区中医院·正骨医院



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

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。

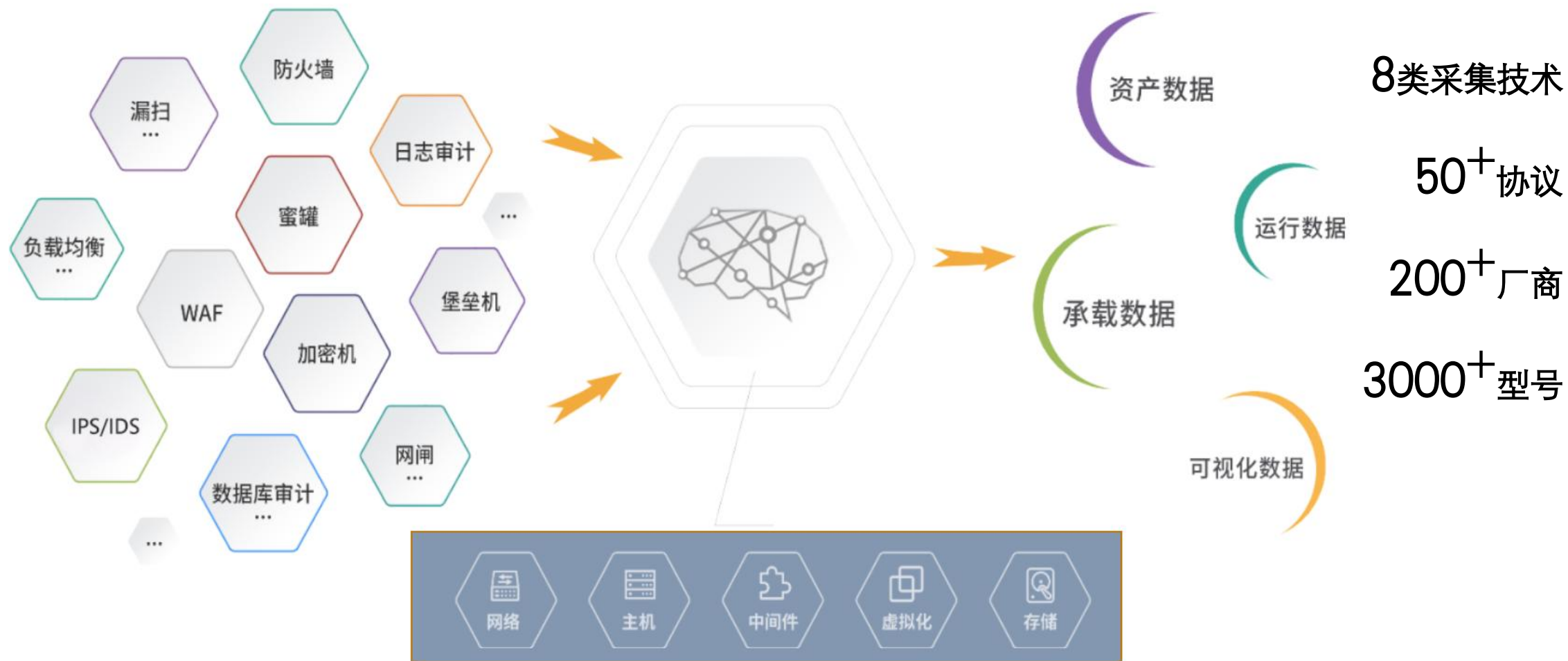
国内首家，致力于为异构化网络安全环境打造“安全设备智能巡检及预警系统”



平台提供 “软件+服务” 一体化解决方案

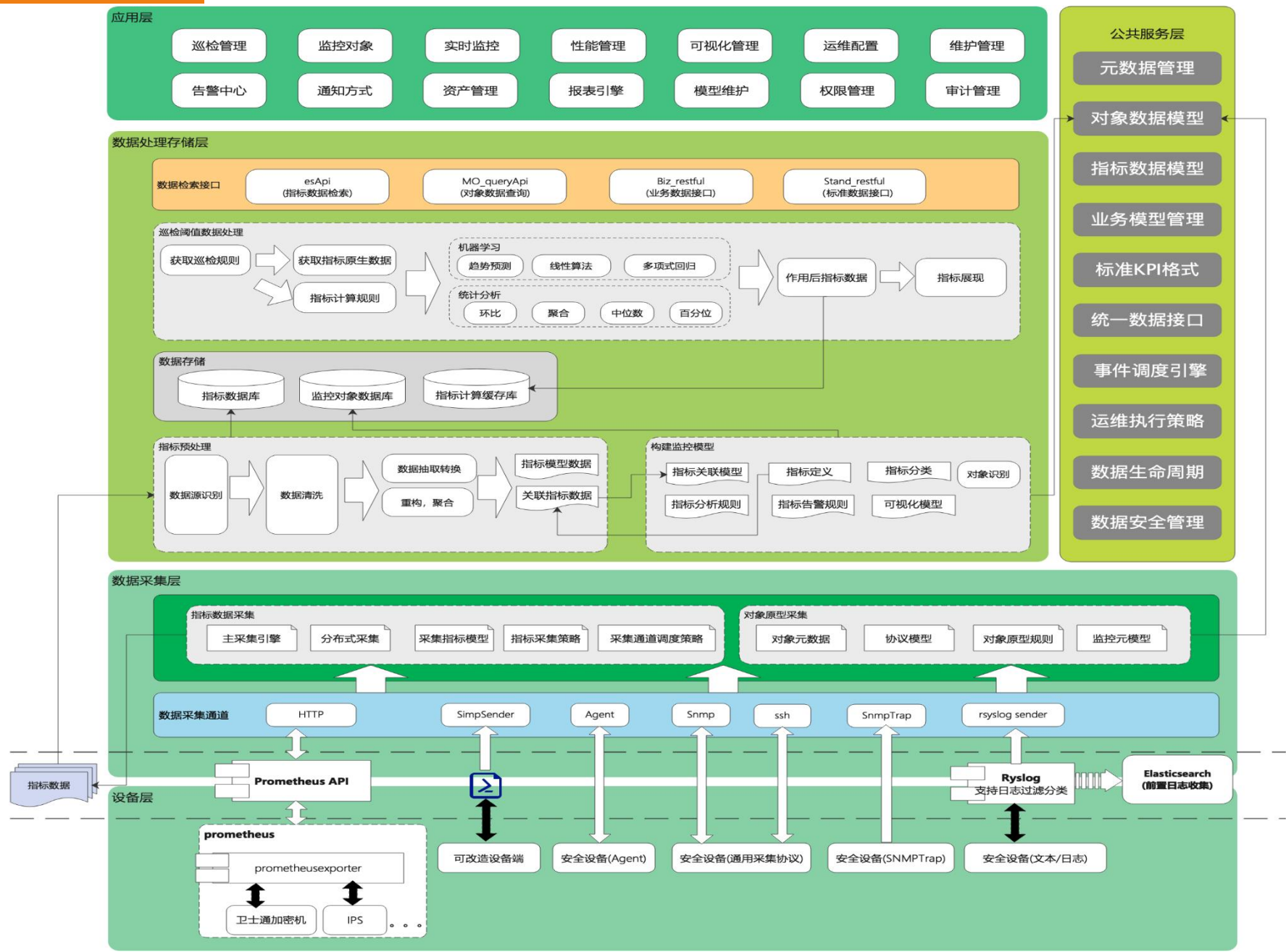
2.2 平台概述

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



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



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

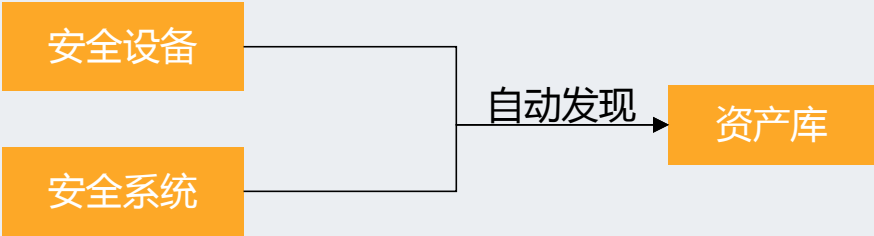
安全自动化巡检

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

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

发现任务详情

名称

安全资产发现

6/255

采集代理

没有采集代理

安全设备(linux内核)发现定时任务 (88个对象)

已发现的对象	对象在线/对象断线	SSH	检测的对象
192.168.1.14	94天 19小时 35分钟 20秒	服务下线	新发现的对象 (已下线)
192.168.1.15	145天 18小时 5分钟 49秒	服务下线	新发现的对象 (已下线)
192.168.1.18	25天 1小时 50分钟 54秒	服务下线	新发现的对象 (已下线)
192.168.1.21	171天 21小时 30分钟 5秒	服务下线	2楼机房的防病毒网关_21
192.168.1.22	150天 21小时 5分钟 29秒	服务下线	2楼机房的防病毒网关_22
192.168.1.24	118天 18小时 35分钟 25秒	服务下线	2楼机房漏扫设备_1.24
192.168.1.28	180天 16小时 29分钟 54秒	服务下线	新发现的对象 (已下线)
192.168.1.29	138天 4小时 40分钟 6秒	服务下线	新发现的对象 (已下线)
192.168.1.30	96天 22小时 34分钟 39秒	服务下线	新发现的对象 (已下线)
192.168.1.34	137天 12小时 39分钟 56秒	服务下线	新发现的对象 (已下线)
192.168.1.35	117天 1小时 34分钟 59秒	服务下线	新发现的对象 (已下线)
192.168.1.36(localhost.localdomain)	186天 5小时 49分钟 47秒	服务上线	运维中心

☐	名称 ◆	IP地址范围	发现间隔	使用协议	唯一字段	状态
☐	PaloAlto IPS 发现任务	192.168.0.1-255	1h	SSH,Agent客户端	ip地址	☒
☐	卫士通加密机资产发现	192.168.0.1-255	1h	HTTP	ip地址	☒
☐	安全设备(linux内核)发现定时任务	192.168.1.1-255	1h	SSH	ip地址	☒

- 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。

导航花名册

应用名称

筛选

重置

搜索条件

SDP

资产详细视图

资产查询视图

SSLVPN

testHSM

testweb

资产模板设计器[设备类型：防火墙]

预览

查看json

保存视图

清空

查询属性设置

查询表单设置

输入型组件

单行文本

多行文本

计数器

选择型组件

★所属环境

请选择★所属环境

★所属室

请选择★所属室

★区域

请选择★区域

★C类别

请选择C类别

★T子类

请选择T子类

★I项目

请选择I项目

属性字段

ATTR206

属性名称

●序列号

组件类型

单行文本

修改属性

×

★名称

系统版本

Map Code

分组

请选择

类型

文本

默认值

单位

显示格式

描述

必填

启用

- 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

同步设置

历史记录

* 名称

XXcmdb同步

系统代码

unionPay

通知方式

信息模板

选项

* 名称

ITop

类型

Webhook

参数

名称

alert_message

名称

alert_subject

名称

event_recovery_value

名称

event_source

名称

event_update_status

JavaScript

```
1 var Itop = {
2   params: {},
3
4   setParams: function (params) {
5     if (typeof params !== 'object') {
6       return;
7     }
8
9     if (params.log !== 'private_log' && params.log !== 'public_log') {
10      throw 'Incorrect "itop_log" parameter given: ' + params.log + '\nMust be "private_log" or "public_l
11    }
12  }
13  itop_params = params;
```

上传资产信息

下载导入模板

导入

已创建(0)

已更新(0)

未

itop_user

新增

脚本

var Itop = { params: {}, setParams: function (para

超时

30s

安全资产模型表-防火墙.xlsx

安全资产模型表-加密机.xlsx

安全资产模型表-漏勺.xlsx

安全资产模型表-蜜罐.xlsx

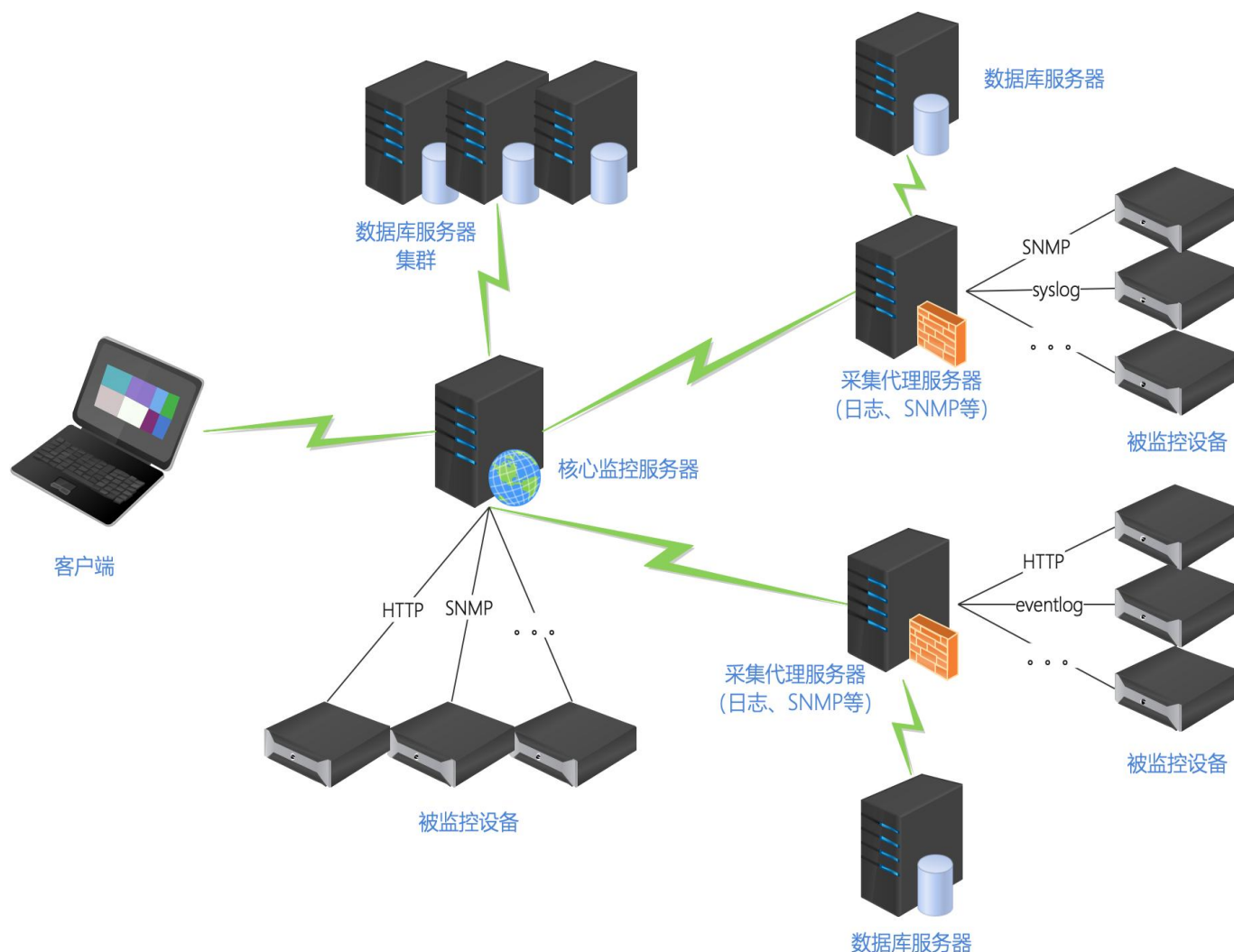
安全资产模型表-IPS.xlsx

安全资产信息表-无映射型_模板.xlsx

安全资产信息表-映射型_模板.xlsx

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，这些数据包括但不限于安全设备、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。



- 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

相关性

操作

* 名称

PA IPS控制台恢复策略

13/255

筛选逻辑

满足以下全部条件

A and B and C and D and E and F

* 条件

	名称	操作
A	旧事件标记 = PAIPS	✖
B	新事件所属对象群组 = 安全设备/IPS	✖
C	旧事件标记值 HostType = PAIPS	✖
D	新事件标记值 ConState =Connectivity Resumes	✖
E	旧事件标记值 ConState =Request Timeout	✖
F	新事件标记值 HostSrc =PA_IPSConsole_185	✖

新条件

旧的事件标签

=

标记

添加

描述

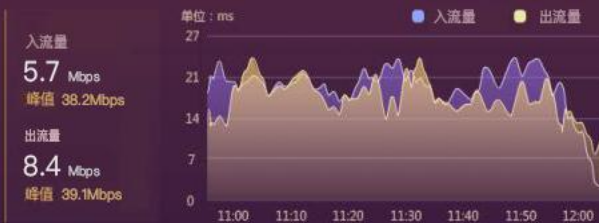
当PaloAlto的IPS控制台从请求连接超时到连接恢复的时候，关闭掉基于主机来源是PAIPS的标记数据的事件

2.4.3 安全设备监控—监控可视化

运维监控一览



核心网络设备端口分析



张家港核心



徐州核心

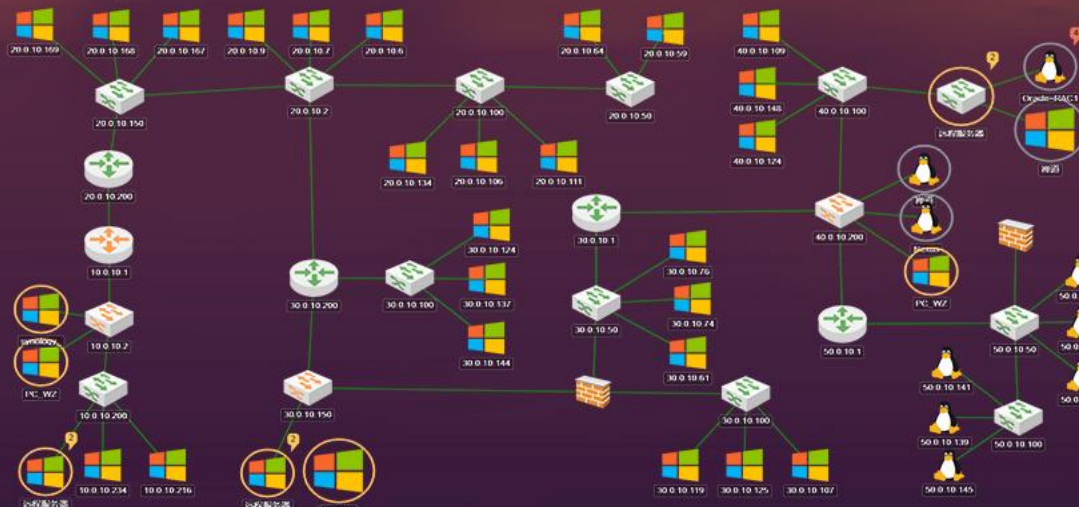


收费系统交易量



2020-11-12 18:32

运维监控分析平台



问题列表

时间	等级	状态	所属群组	对象	名称
🕒 2020-11-12 15:31:47	中级	问题	服务器	TELNET_LINUX	ICMP PING 不可用
🕒 2020-11-12 15:31:26	中级	问题	中间件	TOMACT_1	无法采集到数据
🕒 2020-11-12 15:31:46	警告	问题	服务器	OA服务器SSH	磁盘空间不足
🕒 2020-11-12 15:31:47	高级	问题	服务器	WEBLOGIC服务器	ICMP PING 不可用
🕒 2020-11-12 15:31:47	高级	问题	服务器	ORACLE业务系统	ICMP PING 不可用
🕒 2020-11-12 15:31:47	警告	问题	服务器	ORACLE_RAC1	磁盘空间不足
🕒 2020-11-12 18:31:47	高级	问题	服务器	ORACLE_RAC2	ICMP PING 不可用

高负载设备占比



张家港CPU使用率TOP10



徐州CPU使用率TOP10



数据库CPU使用率



安全设备

Centos系统安全设备

2楼机房漏扫设备_1.110

2楼机房漏扫设备_1.24

2楼安全信息和事件管理...

2楼自研数据库密码管理...

2楼自研Updefence1.248

2楼漏扫1.250

2楼漏扫控制台1.251

2楼NSM1.252

Window系统安全设备组

2楼账号管理系统1.231

2楼安全信息和事件管理...

2楼AD1.101

2楼应用发布机1.249

斗象NSM组

2楼NSM1.252

防火墙组

2楼应用防火墙1.243

服务器组

运维安全设备服务器

加密机

软件

A组

B组

C组

2楼软件加密机...

漏扫引擎组

2楼机房漏扫设备_1.110

2楼机房漏扫设备_1.24

2楼漏扫1.250

2楼漏扫控制台1.251

蜜罐组

入侵预防系统

身份认证组

2楼ISE1.242

实时监控 > 对象一览 > 安全设备

管理对象类型

所有

名称

重置

根据群组名称搜索

自定义列

安全设备

Centos系统安全设备

Window系统安全设备组

入侵预防系统

加密机

硬件

软件

A组

B组

C组

导流设备组

斗象NSM组

漏扫引擎组

硬件签名机

蜜罐组

身份认证组

防火墙组

预防病毒网关组

所属类型

对象名称

厂商

IBMAD

2楼AD1.101

IBM

思科ISE

2楼ISE1.242

Cisco

斗象NSM

2楼NSM1.252

Tophant

PaloAlto入侵预防系统

2楼入侵预防系统1.233

PaloAlto

PaloAlto入侵预防系统

2楼入侵预防系统1.234

PaloAlto

PaloAlto入侵预防系统

2楼入侵预防系统1.244

PaloAlto

PaloAlto入侵预防系统

2楼入侵预防系统1.245

PaloAlto

PaloAlto入侵预防系统...

2楼入侵预防系统控制...

PaloAlto

McAfee入侵预防系统...

2楼入侵预防系统控制...

McAfee

卫士通加密机

2楼加密机1.109

Westone

长亭蜜罐探针

2楼安全信息和事件管理

Chaitin

Gigamon导流设备

2楼导流设备1.237

Gigamon

IBM应用发布机

2楼应用发布机1.249

IBM

F5高级Web应用防火墙

2楼应用防火墙1.243

F5

Tenable漏扫

2楼机房漏扫设备_1.111

Tenable

Tenable漏扫

2楼机房漏扫设备_1.24

Tenable

安信华防病毒网关

2楼机房的防病毒网关

Anchiva

安信华防病毒网关控制台

2楼机房的防病毒网关

Anchiva

安信华防病毒网关控制台

2楼机房的防病毒网关

Anchiva

2楼入侵预防系统1.233

PaloAlto < 1小时前 > x

基本信息

告警信息

CPU利用率

2021-12-30 12...

60.46%

内存利用率

2021-12-30 12...

55.6%

文件系统使用率

2021-12-30 12...

83%

基本信息

对象名

PaloAlto_2L_1.233

显示名

2楼入侵预防系统1.233

管理ip地址

192.168.1.233

采集类型

API、Syslog

系统名称

专用系统

位置

2楼

操作系统

专用系统

硬件信息

采购日期

供应商

标识

备注

登录失败次数统计

21-12-30 12:00

12-30 12:15

12-30 12:30

12-30 12:45

12-30 13:00

本巡检周期内攻击事件数量

12-28 00:45

12-28 12:45

12-29 00:45

12-29 12:45

12-30 00:45

12-30 12:45

本巡检周期内攻击事...

轻度 2

中度 8

严重 4

✓ 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

输入名称过滤

安全设备 0 0

Arcsight安全信息和事件管理器

F5高级Web应用防火墙

Gigamon导流设备 10

IBMAD 9 1

IBM应用发布机 9

IBM账号管理系统 6

McAfee入侵预防系统

McAfee入侵预防系统控制

PaloAlto入侵预防系统

PaloAlto入侵预防系统控制

Tenable漏扫 3 3

Tenable漏扫控制台 2

安信华防病毒网关 3

安信华防病毒网关控制

长亭蜜罐控制台 2

长亭蜜罐探针 4 2

斗象NSM 1 1

思科ISE 6 1

卫士通加密机 12

信安世纪签名机 6

PaloAlto入侵预防系统模板

指标分类

功能指标 (4)

性能指标 (3)

设备状态信息 (3)

监测类型

Tarp (7)

简单检查 (3)

HTTP (1)

数据类型

数字类型(浮点型) (5)

字符 (1)

数字类型(整型) (5)

有效性

有效 (11)

有无告警规则

无告警规则 (5)

有告警规则 (6)

模板

非模板的指标 (8)

模板的指标 (3)

历史记录

7天 (3)

3个月 (8)

趋势记录

0 (1)

1年 (10)

间隔

0 (7)

1分钟 (3)

5分钟 (1)

添加

启用

停用

删除

清除历史

	Wizard	名称	告警规则	键值
		CPU利用率	1	cpu.avg.load
		ICMP ping组件模板: ICMP ping检测	1	icmpping
		ICMP ping组件模板: ping丢失率	1	icmppingloss
		ICMP ping组件模板: ping响应时间	1	icmppingsec
		与控制台连接状态	1	console.connect.status
		内存利用率	1	memory.avg.load
		包转发率	0	packet.forwarding.rate
		当前会话数	0	system.current.session
		指标采集器	0	cemmexec.sh[ce-mm-security-mock.sh,"{
		策略最近更新时间	0	policy.last.updated

PaloAlto入侵预防系统模板

对象群组

所有

对象

PaloAlto入侵预防系统模板

高级筛选

指标

指标处理

* 名称

策略最近更新时间

8/255

取数方式

Tarp

* 键值

policy.last.updated

允许的对象

0/150

指标值类型

数字类型(整型)

单位

unixtime

* 历史值保留

90d

3

* 趋势值保留

365d

3

显示值

选择

显示值映射

指标分类

功能指标

关联资产

无

描述

状态

开关

更新

删除

复制

返回

0

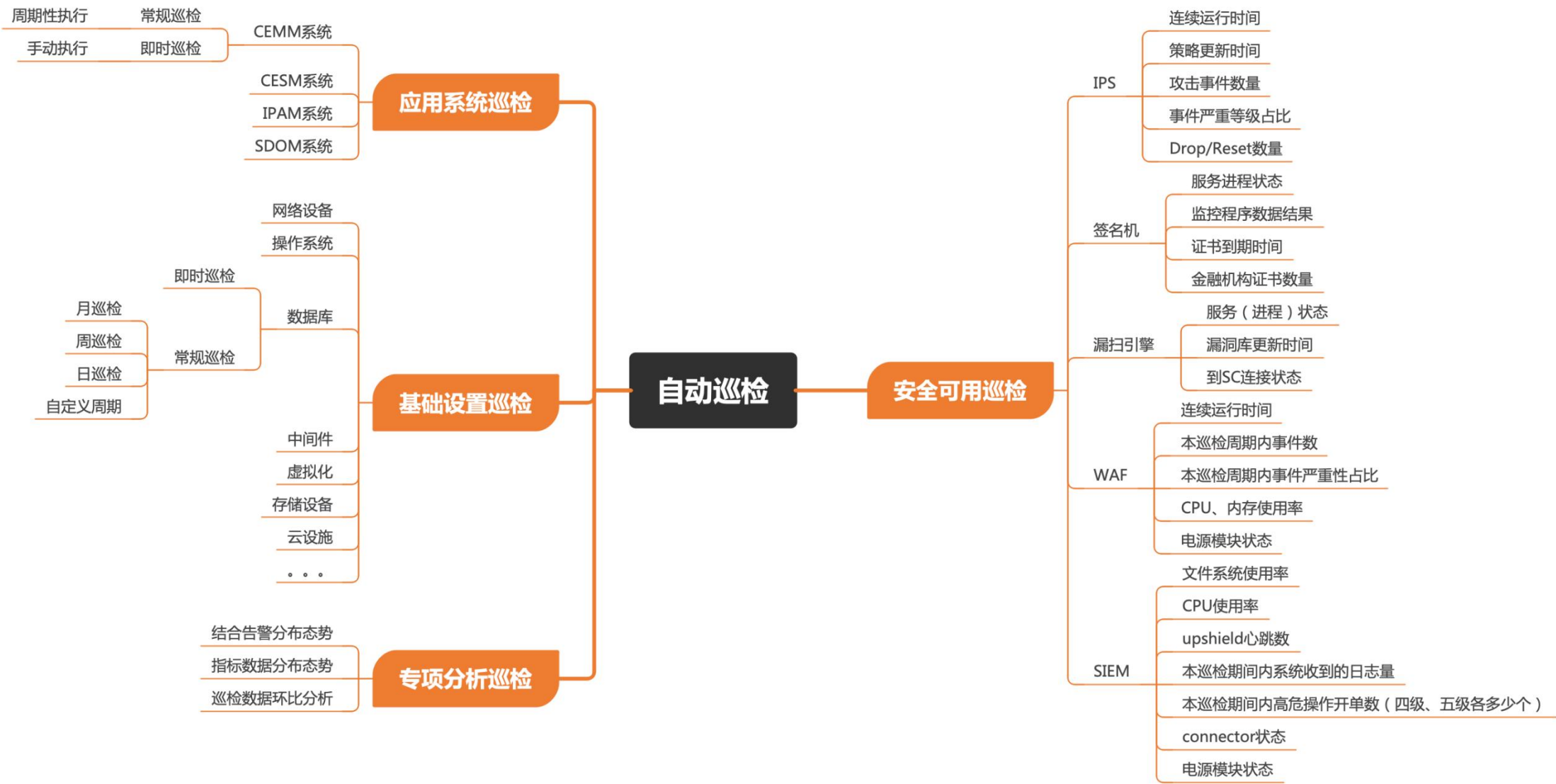
3个月

1年

tarp

功能指标

安全自动化巡检-巡检任务树



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

巡检任务详情

* 名称

数据中心机房巡检任务

10/255

巡检方式

自动巡检

周期类型

每天

每周

每月

自定义

* 周期配置

周三

1

点

0

分

收件人

cgy

描述

审核人

请选择

状态

更新

新增巡检任务

数据中心机房巡检任务

规则数: 5

方式: 手动

类型: 每周

状态: 已启用

添加

名称	等级	对象数	指标数	对比规则
PaloAlto IPS核心指标巡检	普通	1	1	解析巡检规则异常范围失败
McAfee IPS 核心指标巡检	普通	1	1	解析巡检规则异常范围失败
Gigamon 导流设备巡检	普通	1	1	解析巡检规则异常范围失败
信安世纪签名机设备巡检	普通	1	1	解析巡检规则异常范围失败
F5 WAF 设备巡检	普通	1	1	解析巡检规则异常范围失败

共 5 条

20条/页

< 1 >

前往 1 页

巡检规则详情

* 任务

数据中心机房巡检任务

* 名称

2楼PaloAlto 设备检测

7/255

等级

普通

重要

* 对象类型

PaloAlto

对象范围

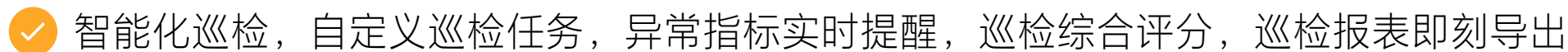
所有

部分

* 对象列表

名称	操作
2楼入侵预防系统1.233	
2楼入侵预防系统1.234	

安全自动化巡检-巡检视图



✓ 基于合理数据采样，通过不同算法，可以实现实时告警

2楼ISE1.242

已启用

AGENT

SNMP

JMX

IPMI

告警规则

告警规则依赖

* 名称

思科ISE登录失败超过5次

13/255

告警等级

未分类

信息

警告

中级

高级

灾难

* 告警表达式

表达式关系	对象	指标	计算方式	比较符	阈值	动作	信息
A:	2楼ISE1.242	ISE登录失败次数	最新值	大于	5	与 或 替换	

测试 表达式逻辑结果:A

恢复方式

表达式

恢复表达式

无

事件生成模式

单个

多重

对思科ISE登录失败次数进行告警

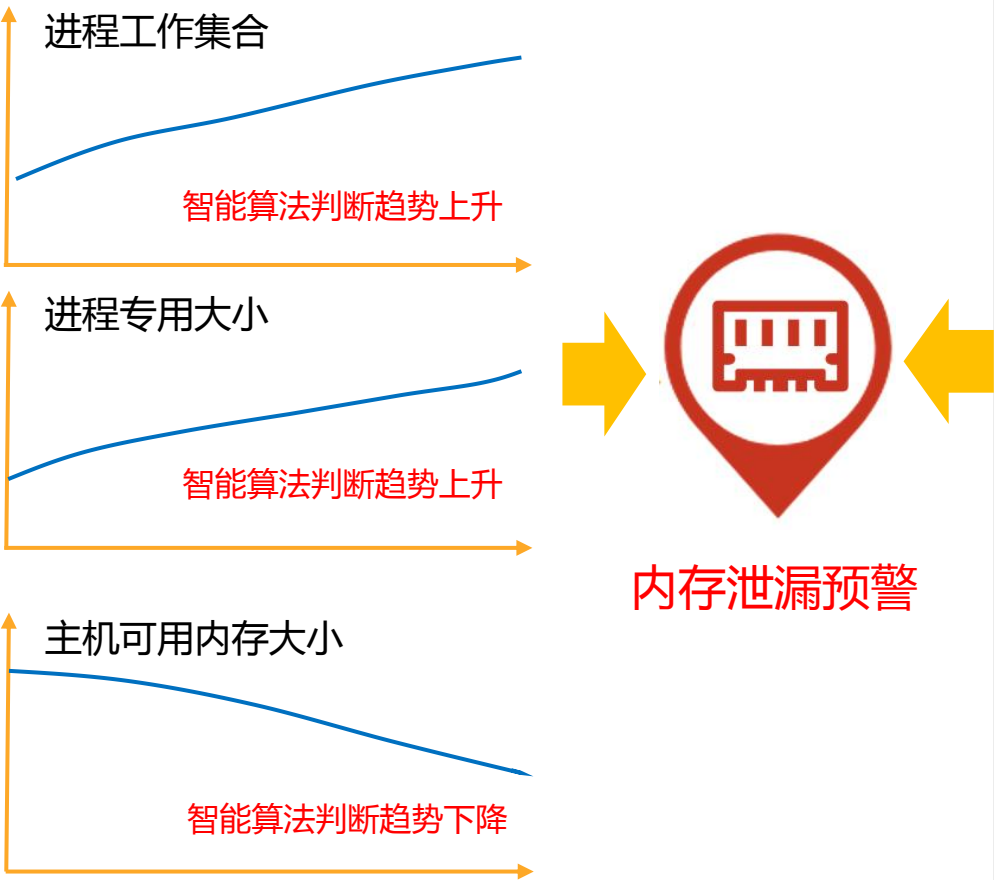
检测实时最新值

时间	告警等级	所属群组	对象	名称	触发的告警	持续时间	确认状态
19:38:34	中级	安全设备/身份认证组	2楼ISE1.242	ISE登录失败超过5次		26分钟 55秒	未确认
19:00							
18:53:34	中级	安全设备/身份认证组	2楼ISE1.242	ISE认证失败超过5次		1小时 11分钟 55秒	未确认

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



告警规则

* 名称

内存泄漏预防

告警等级

未分类

信息

警告

中级

高级

灾难

* 告警表达式

表达式关系	对象	指标	计算方式	比较符	阈值	动作	信息
与						与 或 自	
└ A:	OA服务器	进程工作集合趋势上升	最新值	>	0	与 或 替换 自	
└ B:	OA服务器	进程专用大小趋势上升	最新值	>	0	与 或 替换 自	
└ C:	OA服务器	主机可用内存趋势下降	最新值	<	0	与 或 替换 自	

测试

表达式逻辑结果:A and B and C

允许手动关闭

☐

描述

状态

☒

添加

返回

实时监控三指标变化关系是否同时成立，触发预警

2.4.5

安全预警中心—基于数据预测告警规则

步骤1：选择检测指标项以及计算类型

选择函数表达式

* 指标

WIN-746N3DN4GCE: #6:磁盘使用大小

选择

表达式类型

简单类型

高级类型

下一步

取消

步骤2：选择采集样本数据

选择样本数据

选择数据方式:

根据时间范围

根据最近值的个数

选择时间范围:

截止时间: 当前实时时间

起始时间: 相对于截止时间, 向前推 30d 时间

动态数据样本, 实时训练算法, 保证预测的准确性

上一步

下一步

取消

运维数据预测，提早风险防范

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

选择分析模型

名称	类型	用途
☒ 线性回归模型	预测模型	用于呈线性增长的数据分析
☐ 指数回归模型	预测模型	用于呈指数级增长的数据分析
☐ 对数回归模型	预测模型	用于二值分布的数据分析
☐ 幂函数回归模型	预测模型	用于幂函数曲线规律分析
☐ 一次多项式回归模型	预测模型	用于单指标单次的数据分析模型
☐ 二次多项式回归模型	预测模型	用于单指标二次的数据分析模型
☐ 三次多项式回归模型	预测模型	用于单指标三次的数据分析模型
☐ 四次多项式回归模型	预测模型	用于单指标四次的数据分析模型, 特殊分析可以高次多项式
☐ 五次多项式回归模型	预测模型	用于单指标五次的数据分析模型, 特殊分析可以高次多项式
☐ 六次多项式回归模型	预测模型	用于单指标六次的数据分析模型, 特殊分析可以高次多项式
☐ 神经网络异常检测模型	异常检测模型	利用神经网络数据分析模型对指标进行异常检测
☐ 自回归积分滑动平均模型	趋势预测模型	利用ARIMA模型进行指标的趋势预测
☐ 长短期记忆模型	趋势预测模型	利用网络模型LSTM模型进行指标的趋势预测

下一步

取消

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

选择告警判别依据

预测在 7d 时间后的指标 WIN-746N3DN4GCE: #6:磁盘使用大小 的 Δ 值

结果值 > 10G

上一步

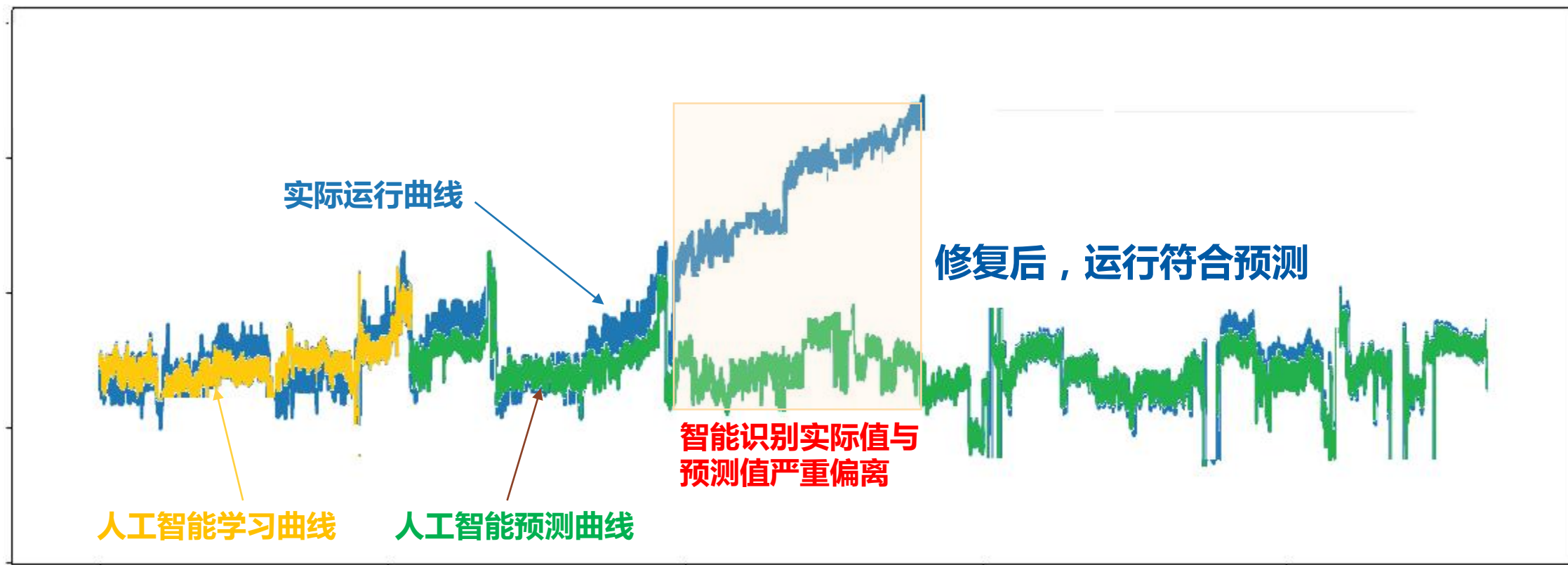
完成

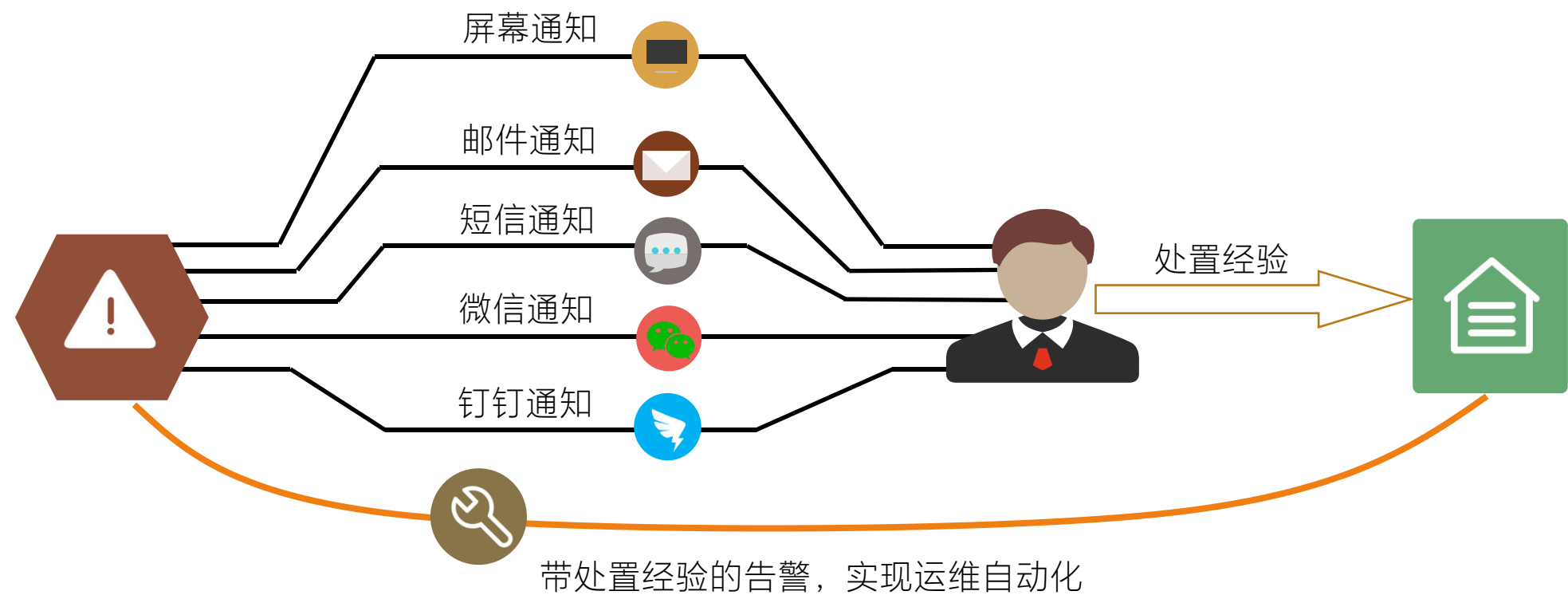
取消

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





✔ 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。

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



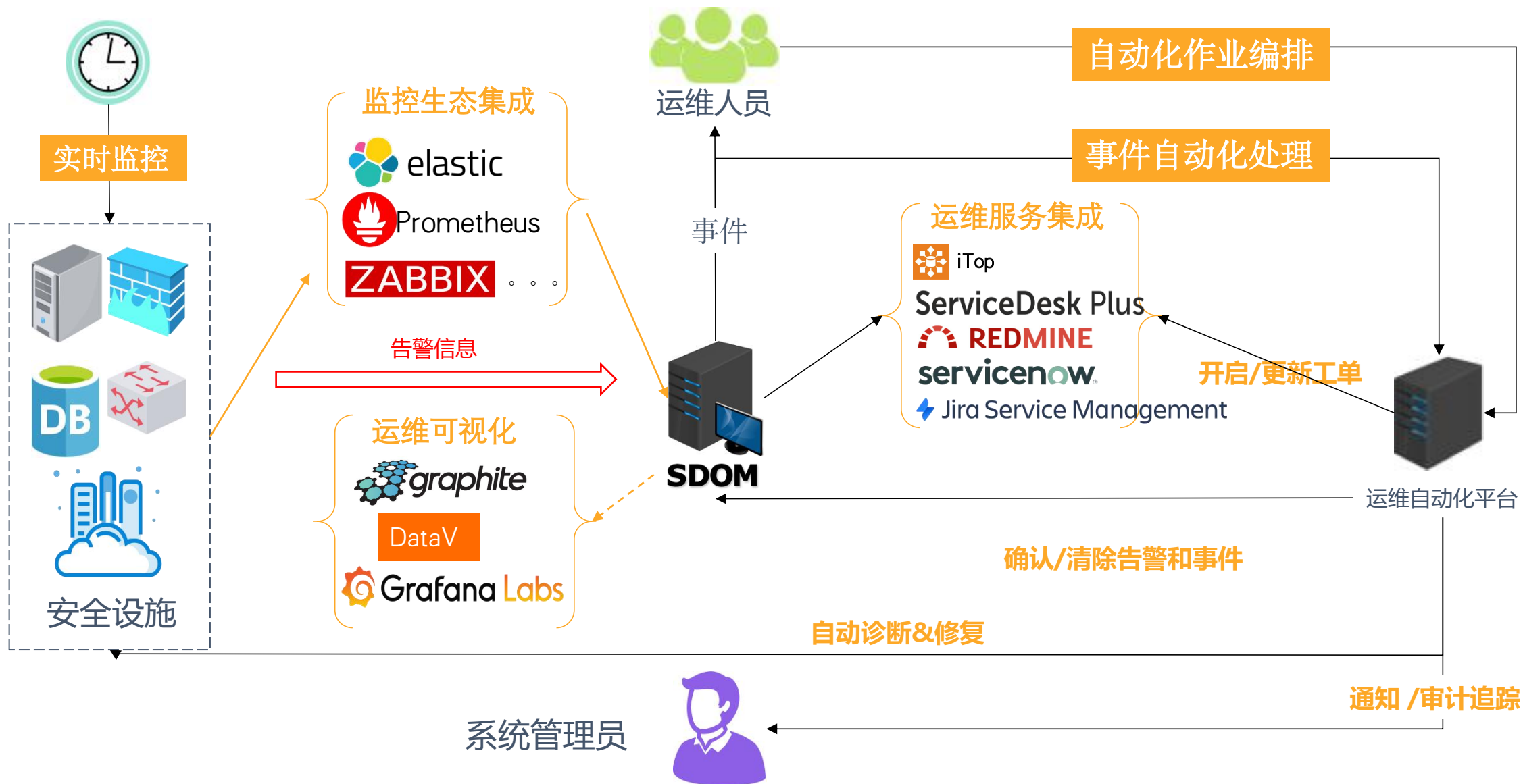
运维自动化

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



Part.

3

产品价值

通过ATOP实现智能自动化运维会带来什么效益呢？



SMARTEAGLE
慧鹰

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。

安全守护新模式

新运维服务支撑体系，“软件+服务”持续提供增值服务

运维质量保证

多种智能运维算法，实现异常自动检测、故障根因分析。

规范运维管理

规范运维管理，进一步确保IT系统高效、稳定运行

变运维被动为主动

变传统的被动式运维为主动运维，提高运维工作效率

降低运维成本

将人员从繁琐的运维工作中解脱出来，降低企业人力运营成本



SMARTEAGLE
慧鹰

感谢您的观看

THANK YOU FOR YOUR LISTENING