工业网络安全监测预警平台(INSP)

Industrial Network Security Monitoring and Warning Platform

--面向工业生产，保障客户业务顺畅运行

绿盟科技 ICS产品部

NSFOCUS

目录

1 产品背景

工业网络面临挑战

新型安全威胁

工业网络威胁越来越严重，各类安全攻击手段层出不穷，新型威胁发现和处理时间长，如何处理

工业数据孤岛

日志、工业网络流量和业务流程数据中存在着很多信息，但是各自隔离，如何充分利用

运维难度大

缺少梳理工控网内的各类设备和节点，集中维护工控网络基本信息以及安全信息的解决方案。

安全态势未知

各类安全设备和系统投资巨大却看不到效果，如何直观感受安全态势

安全事件响应慢

安全事件响应慢，缺乏和生产业务相关联的生产监控网络安全应急响应体系

监管合规

网络安全法的实施，对日志存储，信息安全事件处理，安全态势感知等方面均提出相关要求

国家层面网络与信息安全相关要求

《中华人民共和国网络安全法》

第四十五条，负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

网络安全和信息化工作座谈会

国家主席习近平提出“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力……”

工信部 工业控制系统信息安全行动计划（2018-2020年）

到2020年，全系统工控安全管理工作体系基本建立，全社会工控安全意识明显增强。建成全国在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台（一网一库三平台），态势感知、安全防护、应急处置能力显著提升。

工信部【2016】203号

加快构建关键信息基础设施安全保障体系。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。

针对工业网络的APT攻击与病毒

高级持续威胁定义：

Gartner

- ✓ 高级：可绕过目前的防御系统；
- ✓ 持续：会不断尝试，直到进入目标系统，并且一旦进入，就可成功躲避目前的检测系统，直到实现其目的；
- ✓ 威胁：可造成极大危害；

主要动机：针对工业网络的APT攻击，多为政府支持的攻击

APT杀伤链及防护模型：

杀伤链

进入			潜伏			盗取
侦察	武器化	传输	利用漏洞	木马安装	C & C	目标达成

防护方案

事前预警检测	事中攻击拦截	事后应急响应和可视化
• 基于工业网络安全的黑白名单防护技术，对恶意行为进行事前主动防护； • 攻击/漏洞检测、威胁情报预警、建立资产清单库；	• 发现内网被感染主机的扫描探测行为； • 发现内网被感染主机的回连行为并及时拦截； • 拦截已知攻击； • 拦截未知攻击行为，多维度关联检测；	• 基于关联分析，回溯展现整个攻击全过程； • 安全态势分析； • 资产威胁等级分析；

工业网络APT 攻击与病毒实例

震网(Stuxnet)攻击：
席卷全球工业界的病毒，伊朗核工业基础设施遭到重创(APT)，延缓伊朗核进程。

2010/6

2011/2

代号夜龙(Night Dragon)的APT攻击：
5家跨国能源公司遭到攻击，超过千兆字节的敏感文件被窃，包括油气田操作的机密信息、项目融资与投标文件等。

2015/5

“海莲花”APT：
境外黑客组织“海莲花”被爆自2012年4月起，通过特种木马针对我海事机构、海域建设部门、科研院所和航运企业,展开了精密组织鱼叉式攻击。

blackenergy APT：
乌克兰多家电厂设施被感染，，造成大面积停电，整个城市陷入恐慌，损失惨重。

2015/12

2018/08/03

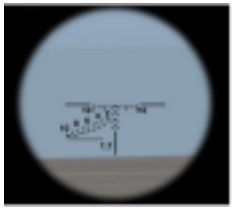
台积电病毒：
台积电由于技术人员软件安装过程的误操作，导致内部网络感染病毒引起部分工厂生产中断。经确定所感染的病毒为WannaCryptor（又名WannaCry）的变种类型。

Gartner对未来安全管理平台的定义

定义智能是下一代安全管理平台的核心特征，它能够具备自动防御、检测、响应和预测自适应的体系架构。更能高效地基于特殊的情境上下文和外部情报，协助安全专家发现安全问题，并通过运维手段实现闭环管理。

威胁情报

高级分析



猎捕和调查

自适应

自动化

2

产品介绍

产品概述

工业网络安全监测预警平台

（Industrial Network Security Monitoring and Warning Platform）

定义绿盟INSP产品是对工业网络中资产的日志和网络攻击流量数据进行采集和分析、计算，通过数据聚合、去重、标准化、建模、索引和关联，通过数据可视化的方式将分析和计算结果进行展示，建立和完善工业网络安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力，利用情报和智能分析成果，实现企业发布早期预警信息，评估工业企业内部可能受影响的设备或资产，避免核心业务系统遭受的攻击和预防潜在的安全隐患的专用软件安全产品。

系统脆弱性管控

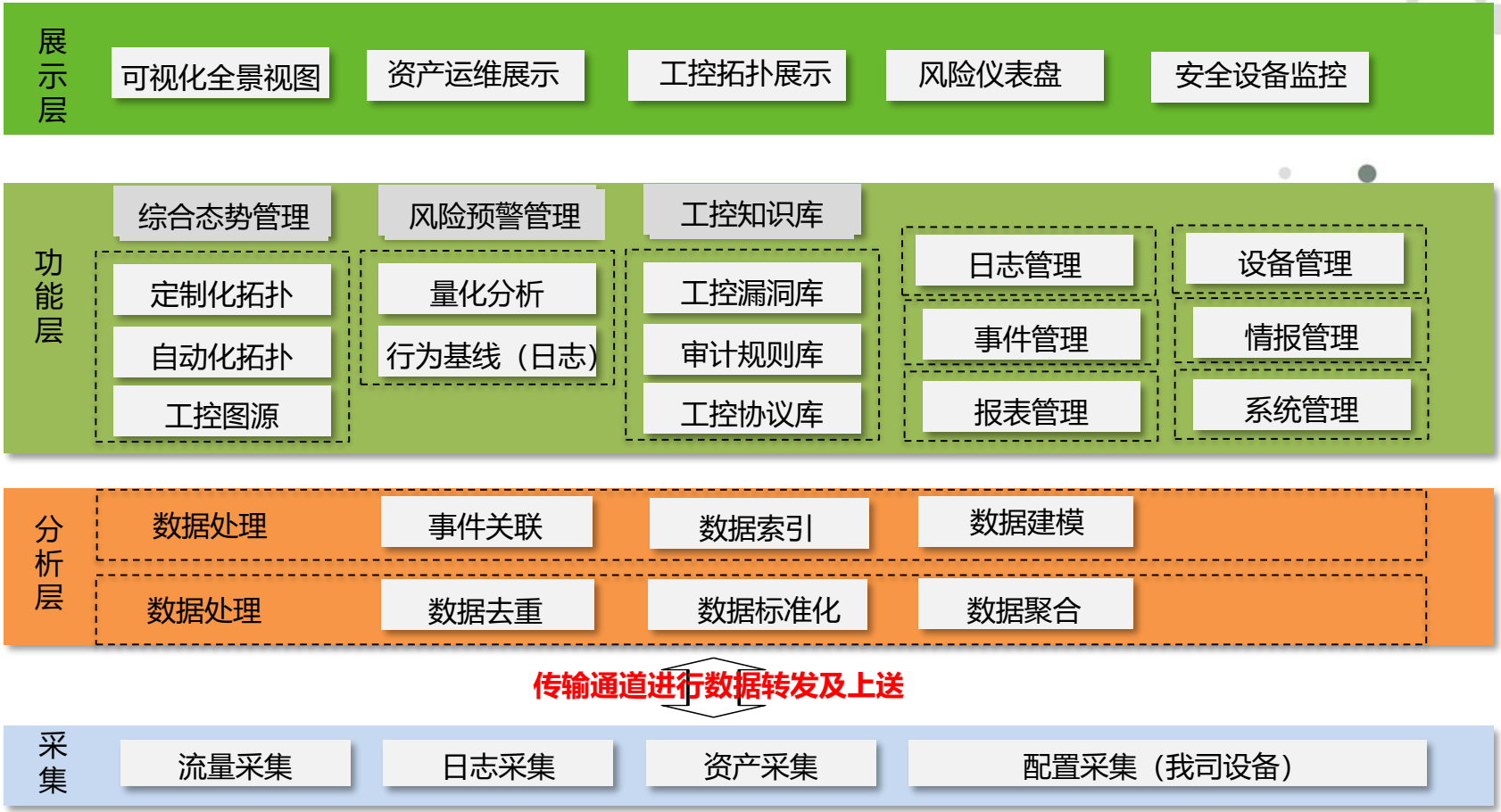
日志分析

攻击预警

运维监控

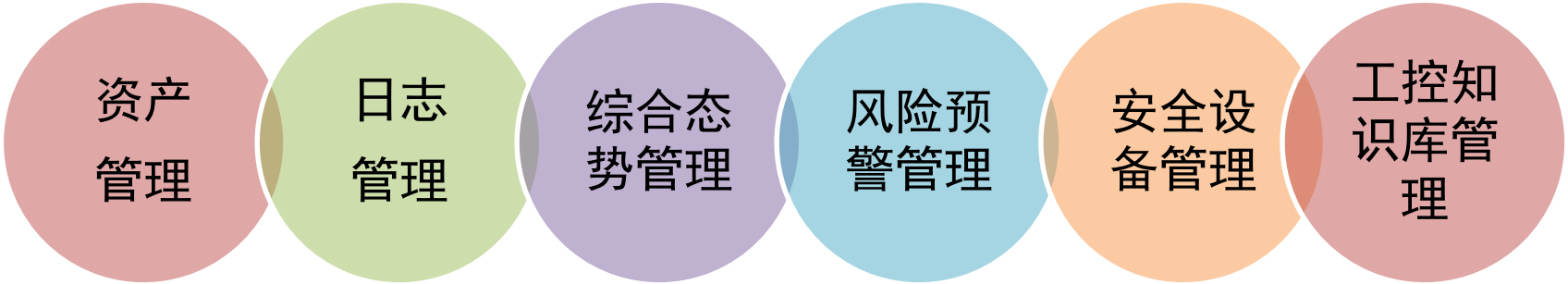
误操作告警

平台架构


展示层
可视化全景视图
资产运维展示
工控拓扑展示
风险仪表盘
安全设备监控
功能层
综合态势管理
风险预警管理
工控知识库
日志管理
设备管理
定制化拓扑
量化分析
工控漏洞库
事件管理
情报管理
自动化拓扑
行为基线（日志）
审计规则库
报表管理
系统管理
工控图源
工控协议库
分析层
数据处理
事件关联
数据索引
数据建模
数据处理
数据去重
数据标准化
数据聚合
传输通道进行数据转发及上送
采集
流量采集
日志采集
资产采集
配置采集（我司设备）

NSFOCUS INSP产品功能

INSP以大数据框架为基础，通过攻防场景模型的大数据分析及可视化展示等手段建立和完善工业网络安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力。



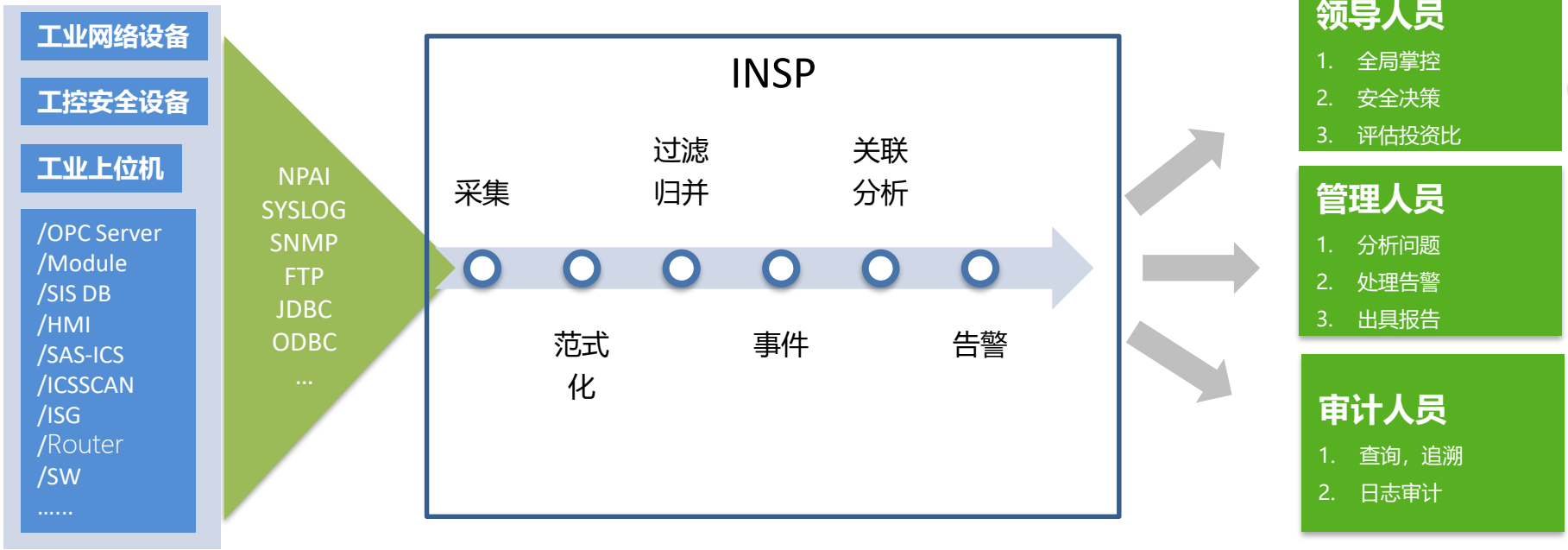
- 工控拓扑图
- 分区分域
- 资产信息管理和赋值
- 报表管理
- 综合分类管理
- 业务设备日志
- 安全设备日志
- 可视化统计
- 风险指数
- 安全事件列表
- 工控图源
- 资产风险分布
- 工作台
- 资产风险
- 风险计算
- 风险趋势
- 风险等级
- 脆弱性分析
- 工业安全网关
- 工控安全审计
- 工控漏扫系统
- 全局策略管理
- 工控漏洞库
- 规则审计库
- 工控协议库

与传统SOC/SIEM的差异

比较因素	绿盟工业网络监测预警平台	传统SOC/SIEM
定位	工业、工控专用	传统IT
数据存储和计算方式	大数据方式/Hadoop/Spark/分布式存储	关系型数据库，MySQL、Oracle，PG等
数据源	Flow流量数据、网络日志，安全设备日志、系统日志、应用日志	网络日志，安全设备日志、系统日志、应用日志
数据采集	40000条/秒	15000条/秒
面向工业生产场景	支持	不支持
态势感知	综合态势展现，支持工业场景拓扑定制	无
脆弱性管理	支持	下发扫描任务，生成脆弱性报告
资产管理	工控资产暴露面监控、资产安全区划分，资产对比、资产增删改查	资产增删改查
威胁分析	规则管理引擎/机器学习	规则管理引擎
工控安全设备管理	工业安全网关、工控审计、工控漏扫等	不支持

集中管理-工业网络安全事件监控、分析、处置

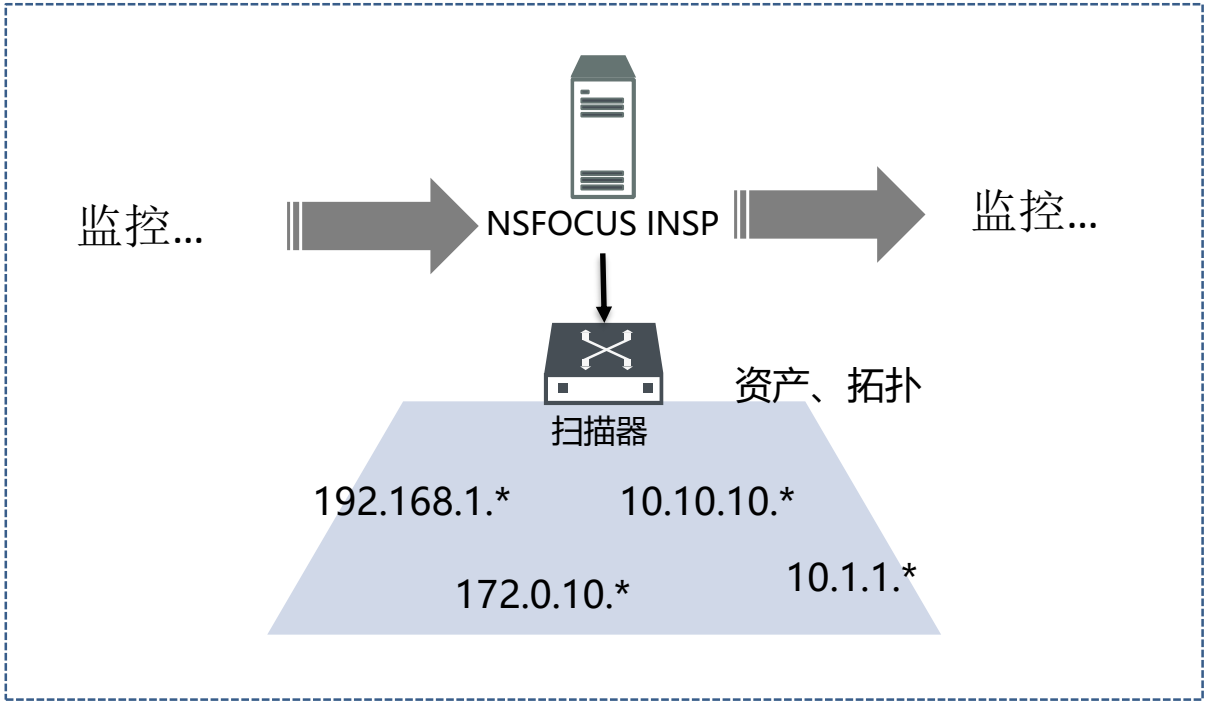
事件(日志、网络流)统一管理，提供安全事件的监控, 分析, 处置和风险评估的统一平台；

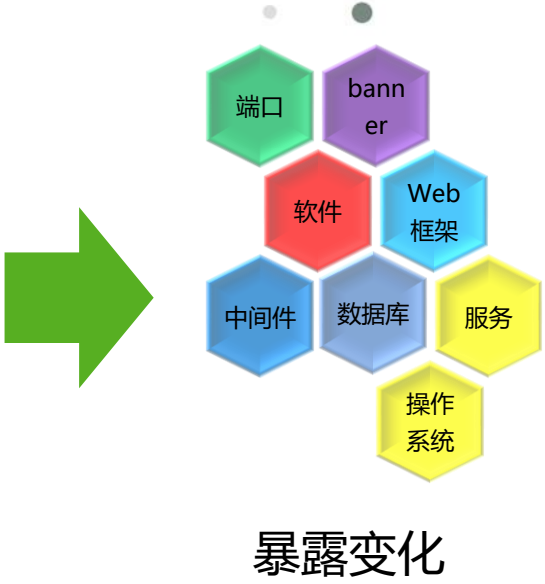


基于大数据框架，通过主/被动结合的获取手段，实时地采集用户工业网络中各种不同厂商的工控安全设备、工业网络设备、工业上位机、操作系统、以及各种应用系统产生的日志信息，并将这些信息汇集到中心平台，进行集中化的存储、备份、查询、审计、告警、和分析，并出具相应的日志报告，实现日志的全生命周期管理。

工业网络资产生命周期管理

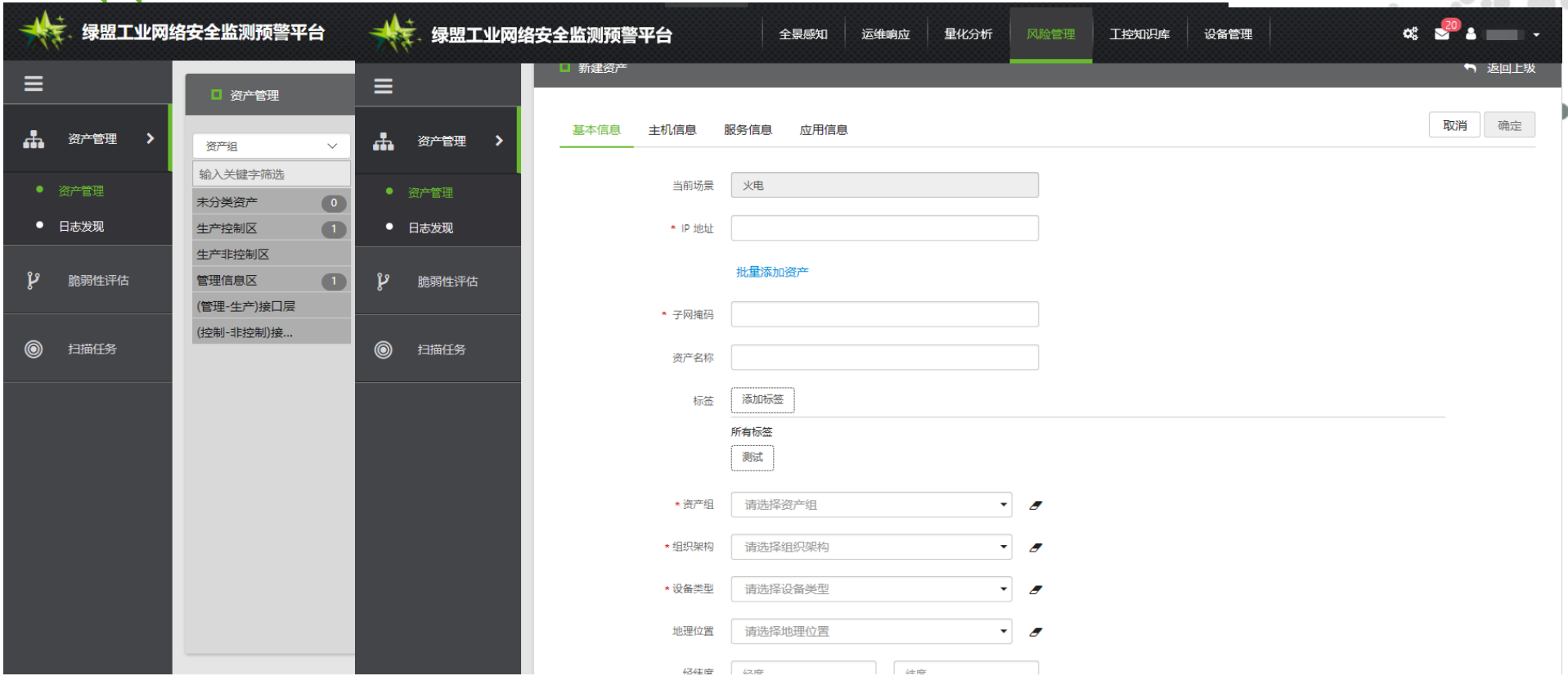
基于工业网络安全监测预警平台可建立企业内网的资产基线，通过持续监控的手段，了解工业内网资产变化情况，对合法资产和非法资产进行有效稽查。





暴露变化

资产管理



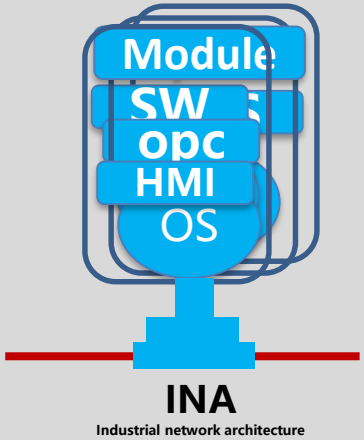
- 内置具有行业特性的工控安全监控拓扑
- 内置工控图元库，可进行组态化的拓扑图人工绘制
- 根据项目进行拓扑的定制化绘制
- 工控资产业务拓扑+工控安全设备部署拓扑

INSP:一站式综合管理-内容分类

设备及策略管理

- 工业安全网关
- 工控安全审计
- 工控漏洞扫描

日志管理



事件管理

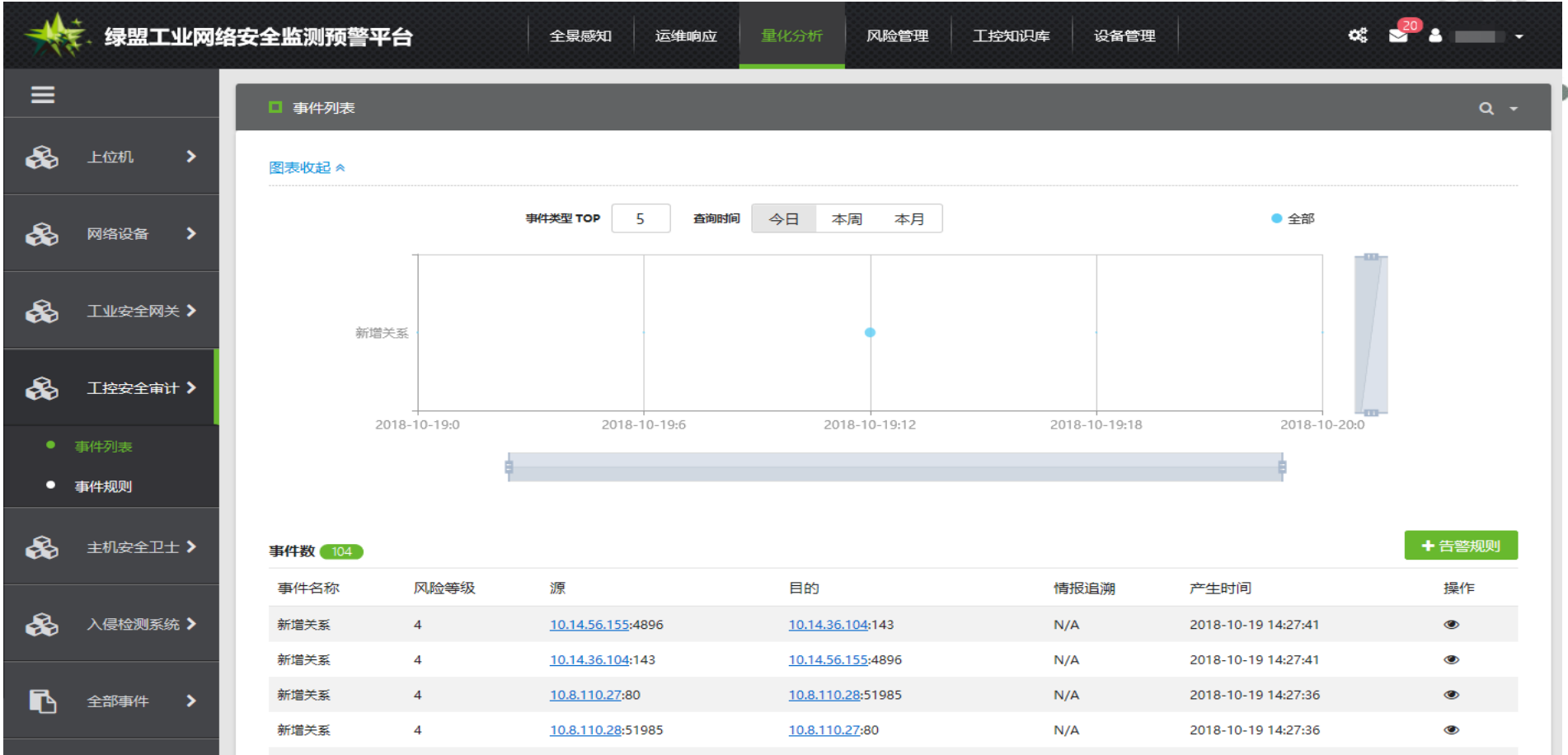
- 业务交互的两个控制节点产生了业务交互
- 关键业务发生的时间与基线有较大的差异
- 资产关系和新增

数据采集和展示

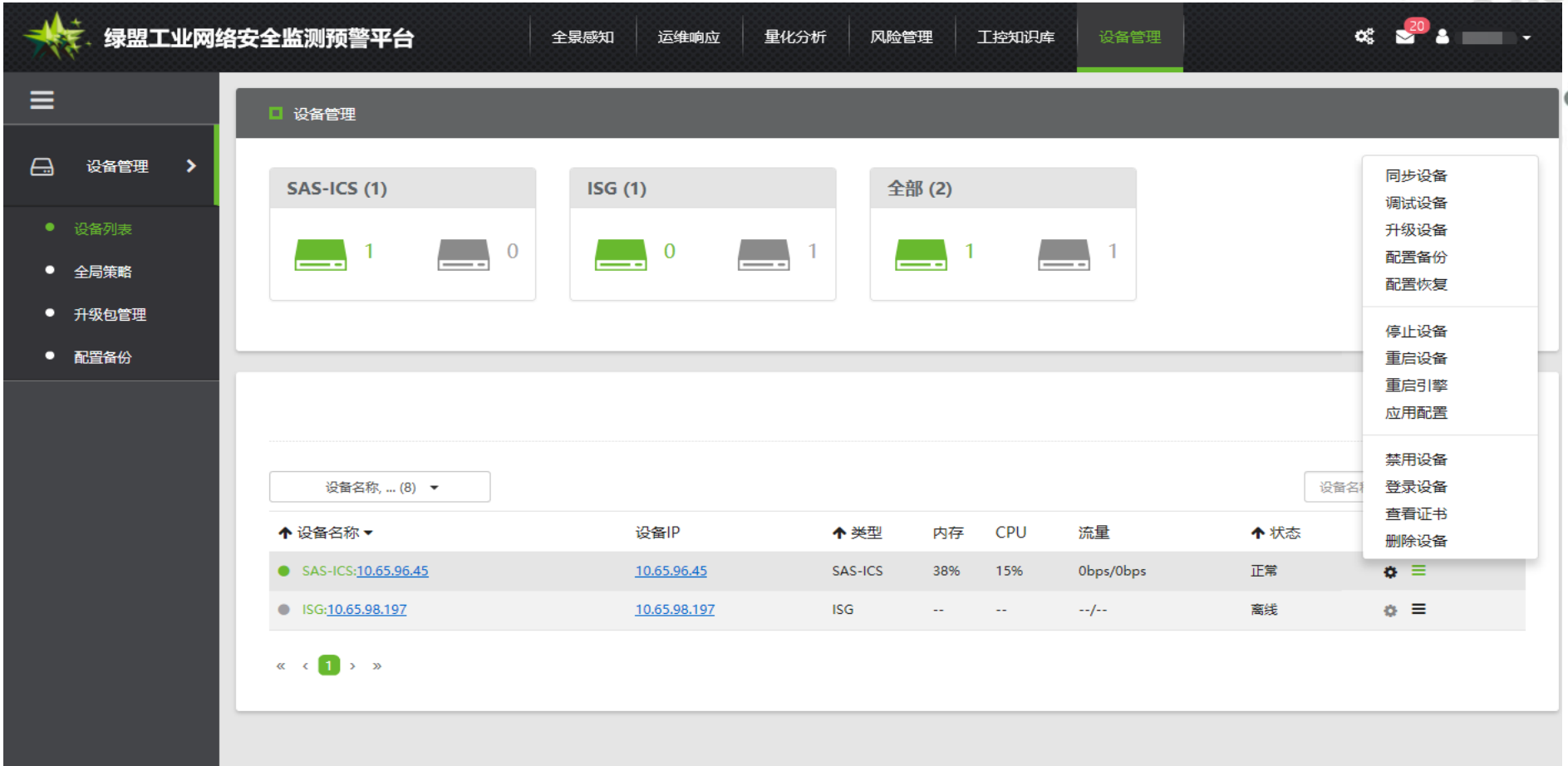
- 前后端分离，后端灵活配置安全能力的同时又能保证界面统一呈现。
- 多源异构数据接入

- ✓ **提供并支持包括Syslog协议等8种数据协议类型数据采集能力，具备包含深度流检测探针在内的多种安全采集工具，；**
- ✓ **提供了绿盟自身对日志理解的分类，方便用户直接查询；**

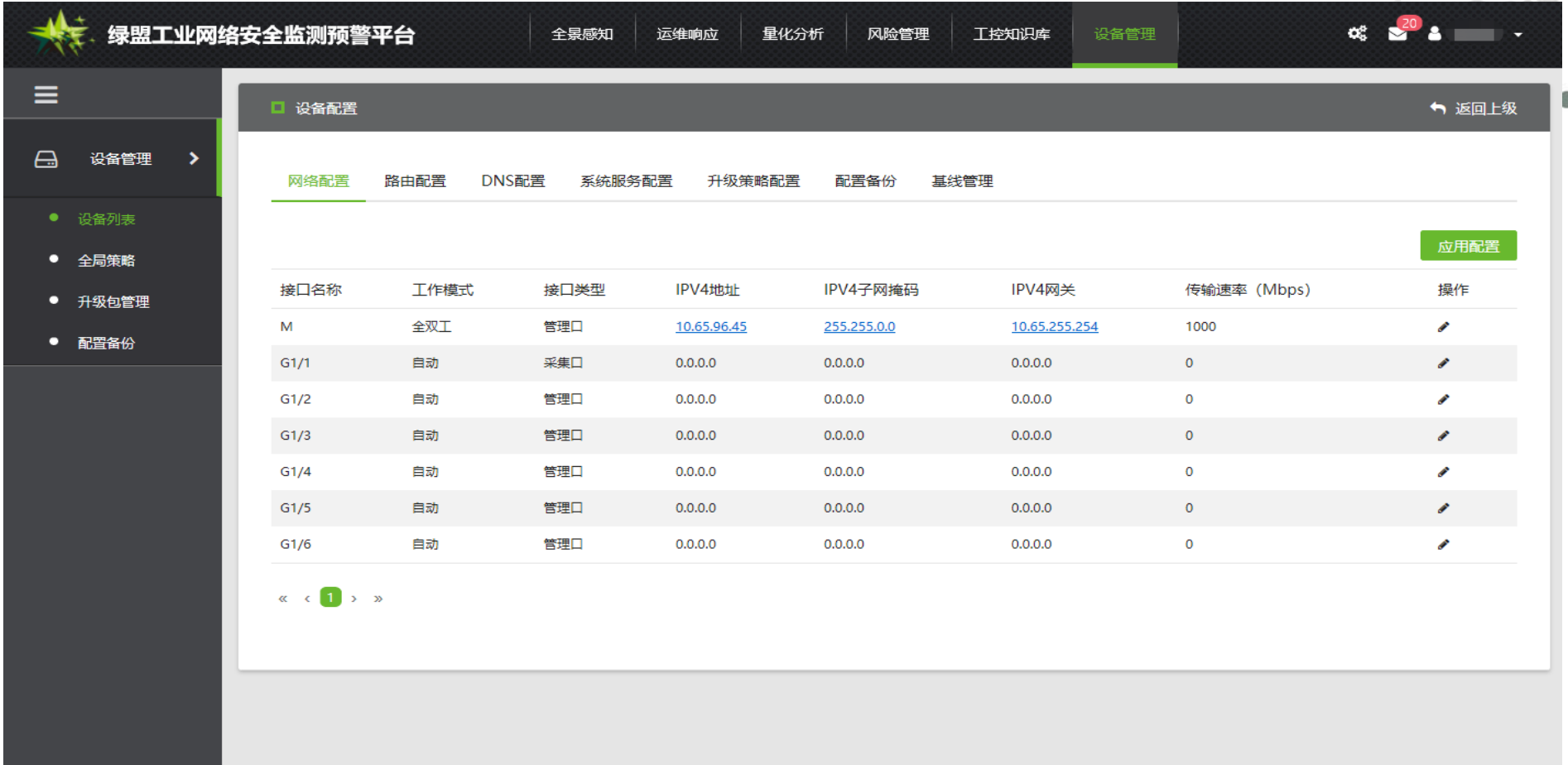
一站式综合管理


绿盟工业网络安全监测预警平台
全景感知
运维响应
量化分析
风险管理
工控知识库
设备管理
20
上位机
网络设备
工业安全网关
工控安全审计
事件列表
事件规则
主机安全卫士
入侵检测系统
全部事件
事件列表
图表收起
事件类型 TOP
5
查询时间
今日
本周
本月
全部
新增关系
2018-10-19:0
2018-10-19:6
2018-10-19:12
2018-10-19:18
2018-10-20:0
事件数 104
+ 告警规则
事件名称 风险等级 源 目的 情报追溯 产生时间 操作
新增关系 4 10.14.56.155:4896 10.14.36.104:143 N/A 2018-10-19 14:27:41
新增关系 4 10.14.36.104:143 10.14.56.155:4896 N/A 2018-10-19 14:27:41
新增关系 4 10.8.110.27:80 10.8.110.28:51985 N/A 2018-10-19 14:27:36
新增关系 4 10.8.110.28:51985 10.8.110.27:80 N/A 2018-10-19 14:27:36

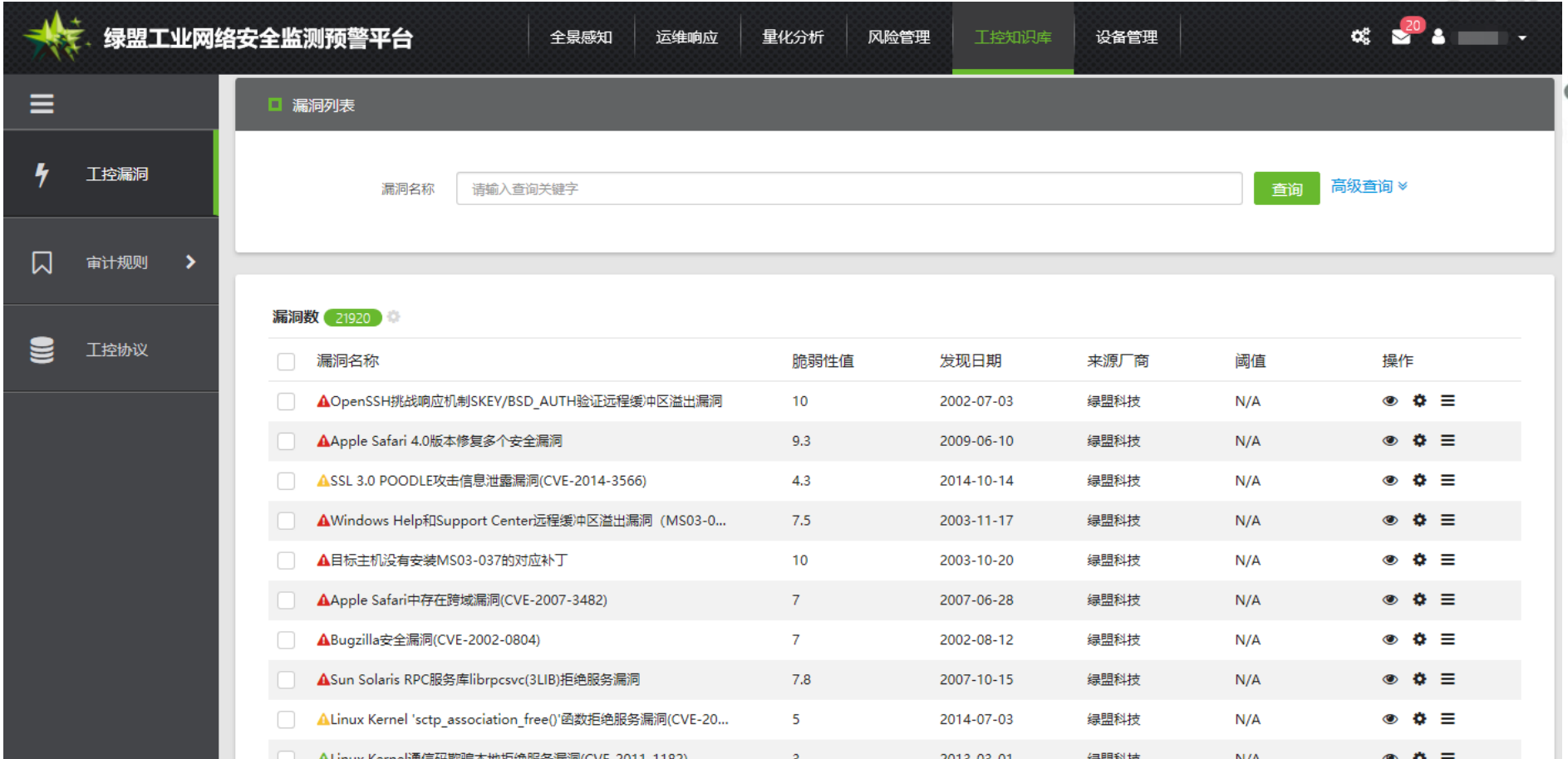
设备及策略管理


绿盟工业网络安全监测预警平台
全景感知
运维响应
量化分析
风险管理
工控知识库
设备管理
20
设备管理
设备管理
设备列表
全局策略
升级包管理
配置备份
SAS-ICS (1)
1
0
ISG (1)
0
1
全部 (2)
1
1
同步设备
调试设备
升级设备
配置备份
配置恢复
停止设备
重启设备
重启引擎
应用配置
禁用设备
登录设备
查看证书
删除设备
设备名称, ... (8)
设备名称
设备IP
类型
内存
CPU
流量
状态
SAS-ICS:10.65.96.45
10.65.96.45
SAS-ICS
38%
15%
0bps/0bps
正常
ISG:10.65.98.197
10.65.98.197
ISG
--
--
--/--
离线
1

设备及策略管理


绿盟工业网络安全监测预警平台
全景感知
运维响应
量化分析
风险管理
工控知识库
设备管理
20
设备管理
设备列表
全局策略
升级包管理
配置备份
设备配置
返回上级
网络配置
路由配置
DNS配置
系统服务配置
升级策略配置
配置备份
基线管理
应用配置
接口名称 工作模式 接口类型 IPV4地址 IPV4子网掩码 IPV4网关 传输速率（Mbps） 操作
M 全双工 管理口 10.65.96.45 255.255.0.0 10.65.255.254 1000
G1/1 自动 采集口 0.0.0.0 0.0.0.0 0.0.0.0 0
G1/2 自动 管理口 0.0.0.0 0.0.0.0 0.0.0.0 0
G1/3 自动 管理口 0.0.0.0 0.0.0.0 0.0.0.0 0
G1/4 自动 管理口 0.0.0.0 0.0.0.0 0.0.0.0 0
G1/5 自动 管理口 0.0.0.0 0.0.0.0 0.0.0.0 0
G1/6 自动 管理口 0.0.0.0 0.0.0.0 0.0.0.0 0
« ‹ 1 › »

工控知识库管理


绿盟工业网络安全监测预警平台
全景感知
运维响应
量化分析
风险管理
工控知识库
设备管理
20
工控漏洞
审计规则
工控协议
漏洞列表
漏洞名称
请输入查询关键字
查询
高级查询
漏洞数 21920
漏洞名称
脆弱性值
发现日期
来源厂商
阈值
操作
OpenSSH挑战响应机制SKEY/BSD_AUTH验证远程缓冲区溢出漏洞 10 2002-07-03 绿盟科技 N/A
Apple Safari 4.0版本修复多个安全漏洞 9.3 2009-06-10 绿盟科技 N/A
SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566) 4.3 2014-10-14 绿盟科技 N/A
Windows Help和Support Center远程缓冲区溢出漏洞（MS03-0... 7.5 2003-11-17 绿盟科技 N/A
目标主机没有安装MS03-037的对应补丁 10 2003-10-20 绿盟科技 N/A
Apple Safari中存在跨域漏洞(CVE-2007-3482) 7 2007-06-28 绿盟科技 N/A
Bugzilla安全漏洞(CVE-2002-0804) 7 2002-08-12 绿盟科技 N/A
Sun Solaris RPC服务库librpcsvc(3LIB)拒绝服务漏洞 7.8 2007-10-15 绿盟科技 N/A
Linux Kernel 'sctp_association_free()'函数拒绝服务漏洞(CVE-20... 5 2014-07-03 绿盟科技 N/A

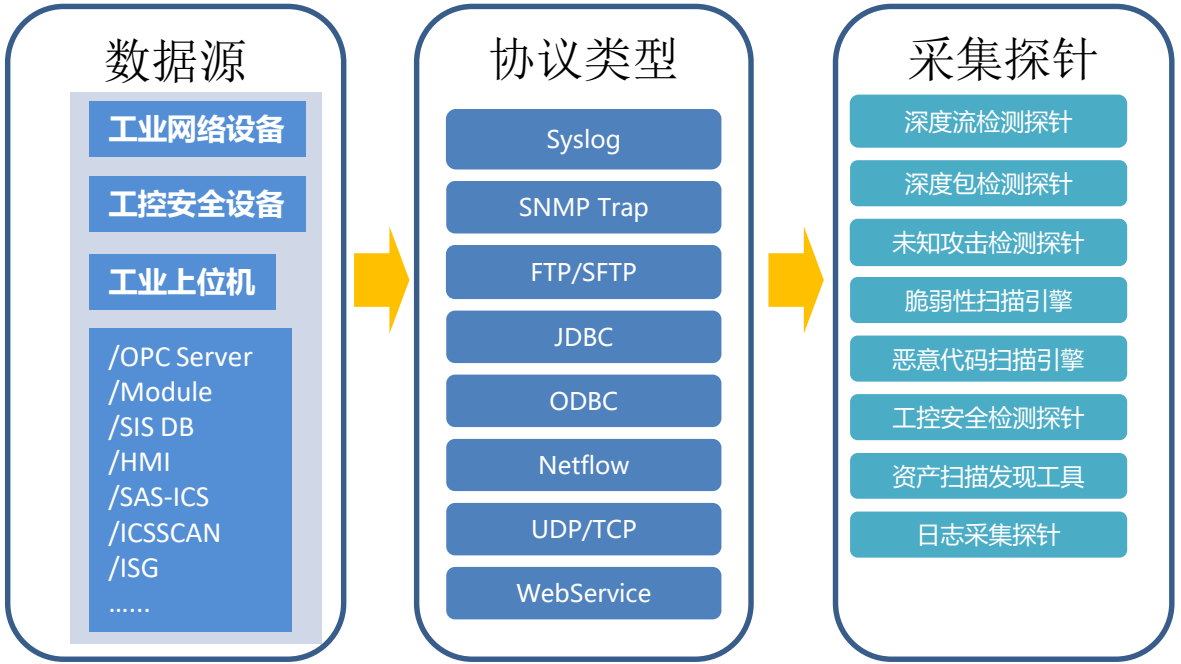
3 产品特性

数据采集能力

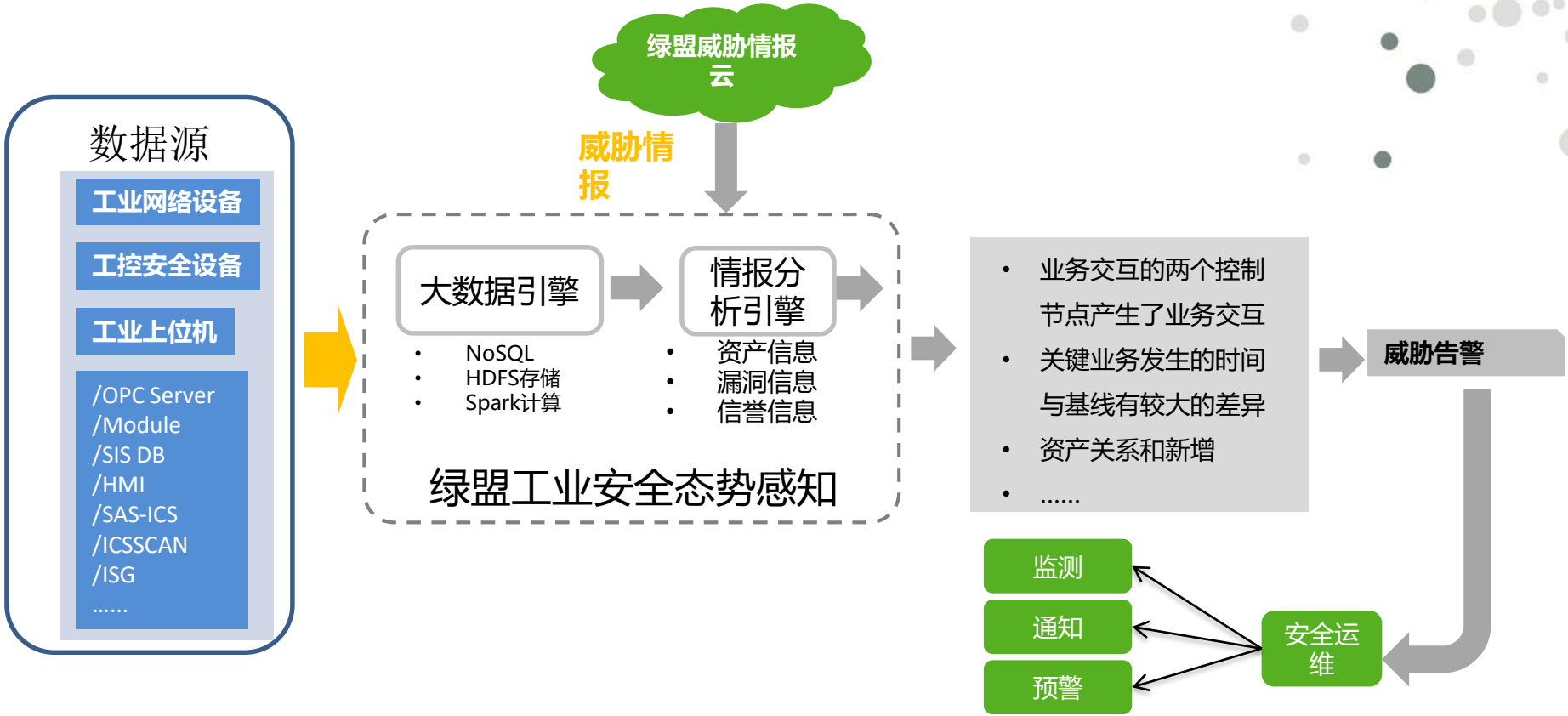
绿盟工业网络安全监测预警平台支持多源异构数据接入，并支持包括Syslog协议等8种数据协议类型数据采集能力，具备包含深度流检测探针在内的多种安全采集工具，为平台的上层分析研判业务提供有力的支撑。

各项性能指标如下：

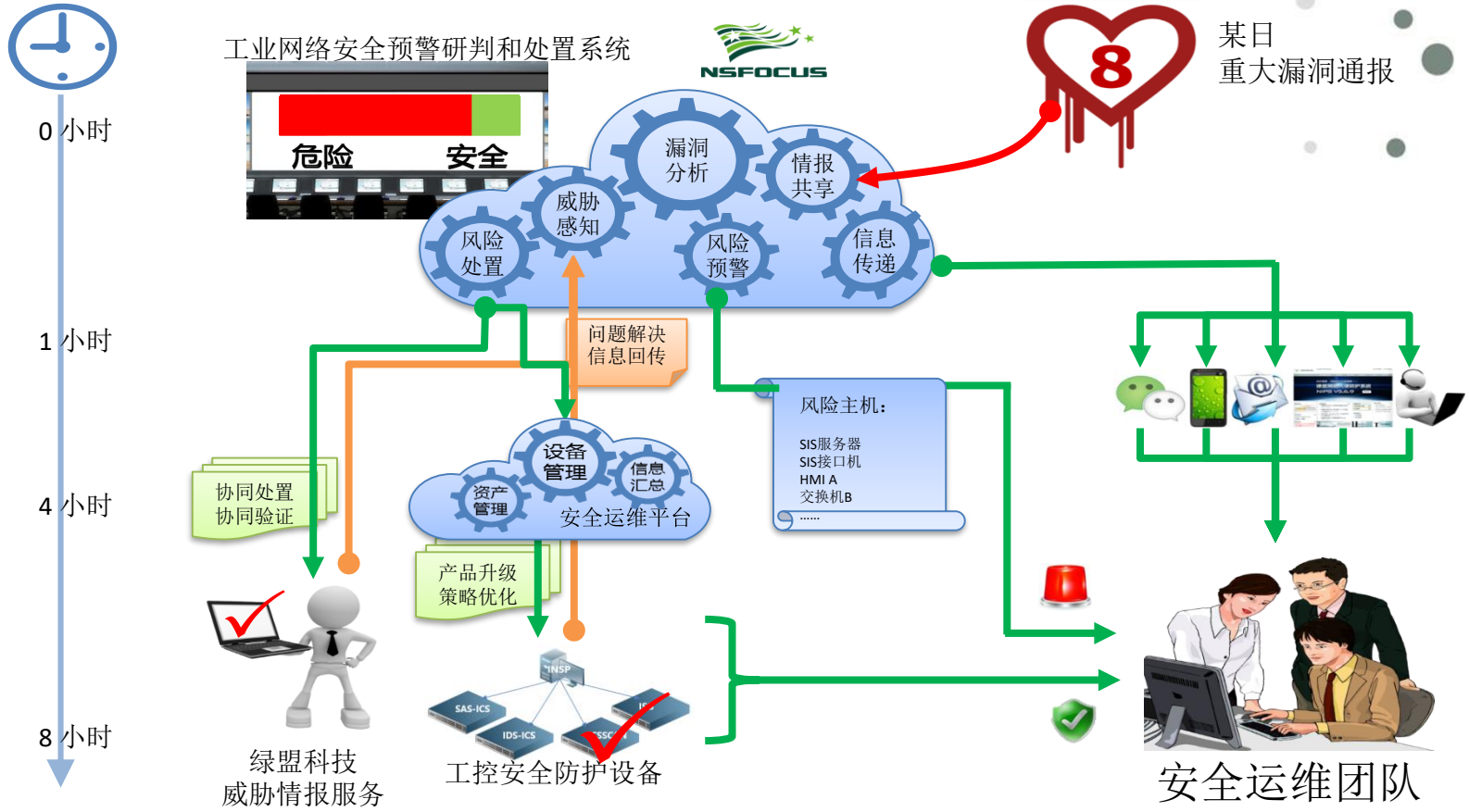
- 各类日志采集性能，4万/秒。
- 原始数据包采集性能，7万/秒。
- 网络流量数据采集性能，15万/秒。



迅捷的预警通报能力


绿盟威胁情报云
威胁情报
数据源
工业网络设备
工控安全设备
工业上位机
/OPC Server
/Module
/SIS DB
/HMI
/SAS-ICS
/ICSSCAN
/ISG
.....
大数据引擎
NoSQL
HDFS存储
Spark计算
情报分析引擎
资产信息
漏洞信息
信誉信息
绿盟工业安全态势感知
业务交互的两个控制节点产生了业务交互
关键业务发生的时间与基线有较大的差异
资产关系和新增
.....
威胁告警
监测
通知
预警
安全运维

高效的应急响应体系


0 小时
1 小时
4 小时
8 小时
工业网络安全预警研判和处置系统
危险
安全
NSFOCUS
某日
重大漏洞通报
漏洞分析
情报共享
威胁感知
风险处置
风险预警
信息传递
问题解决
信息回传
风险主机：
SIS服务器
SIS接口机
HMI A
交换机B
.....
设备管理
资产管理
信息汇总
安全运维平台
协同处置
协同验证
产品升级
策略优化
SAS-ICS
IDS-ICS
绿盟科技
威胁情报服务
工控安全防护设备
安全运维团队

配置要求

主机硬件配置要求

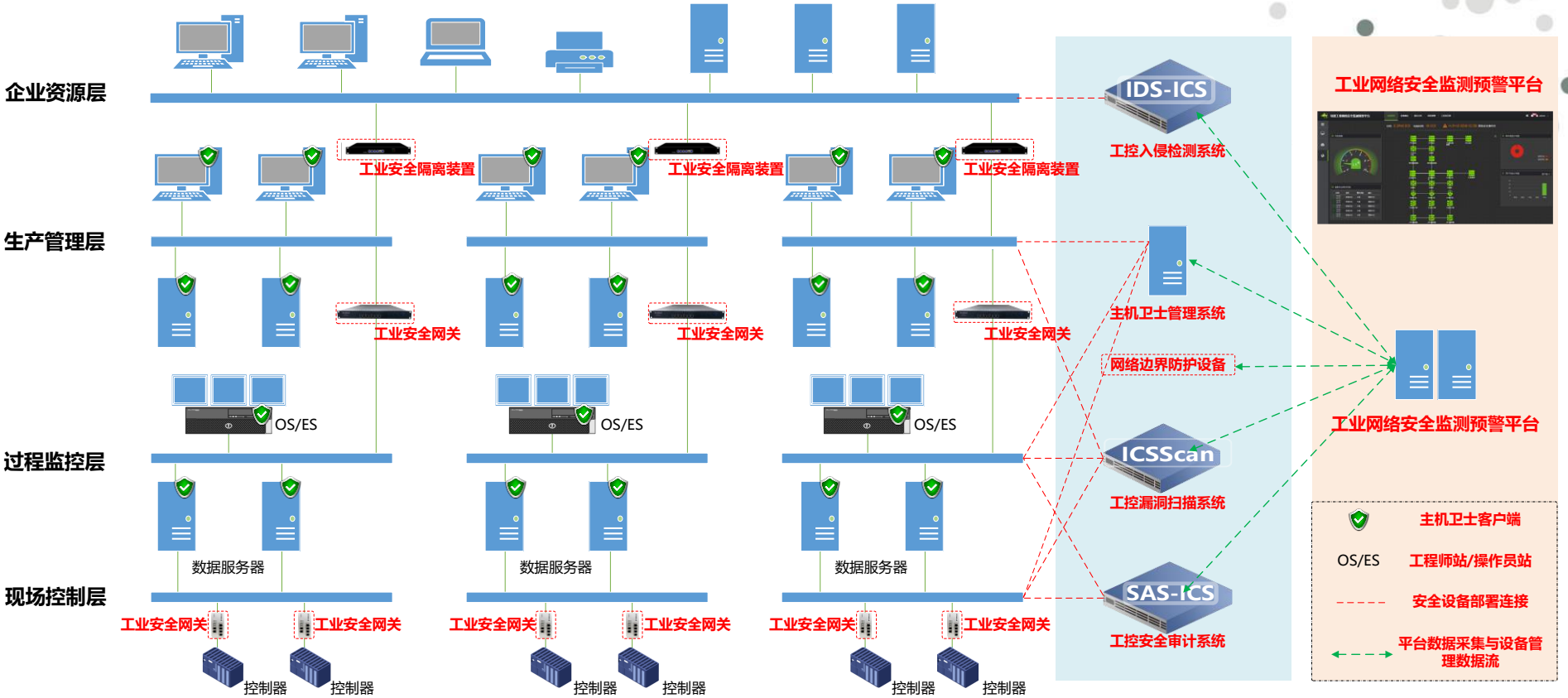
硬件	服务器（I）
CPU	2*E5-2630V2 （6核心12线程、2.6GHz）
内存	64GB DDR 3 1333MHz
硬盘	8*1TB（ext4文件系统格式、7200转），Raid5
网卡	千兆网卡
Raid卡	带缓存raid卡，推荐PERC H710p
光驱	内置光驱
电源	热插拔冗余电源（1+1）1100瓦

主机软件配置要求

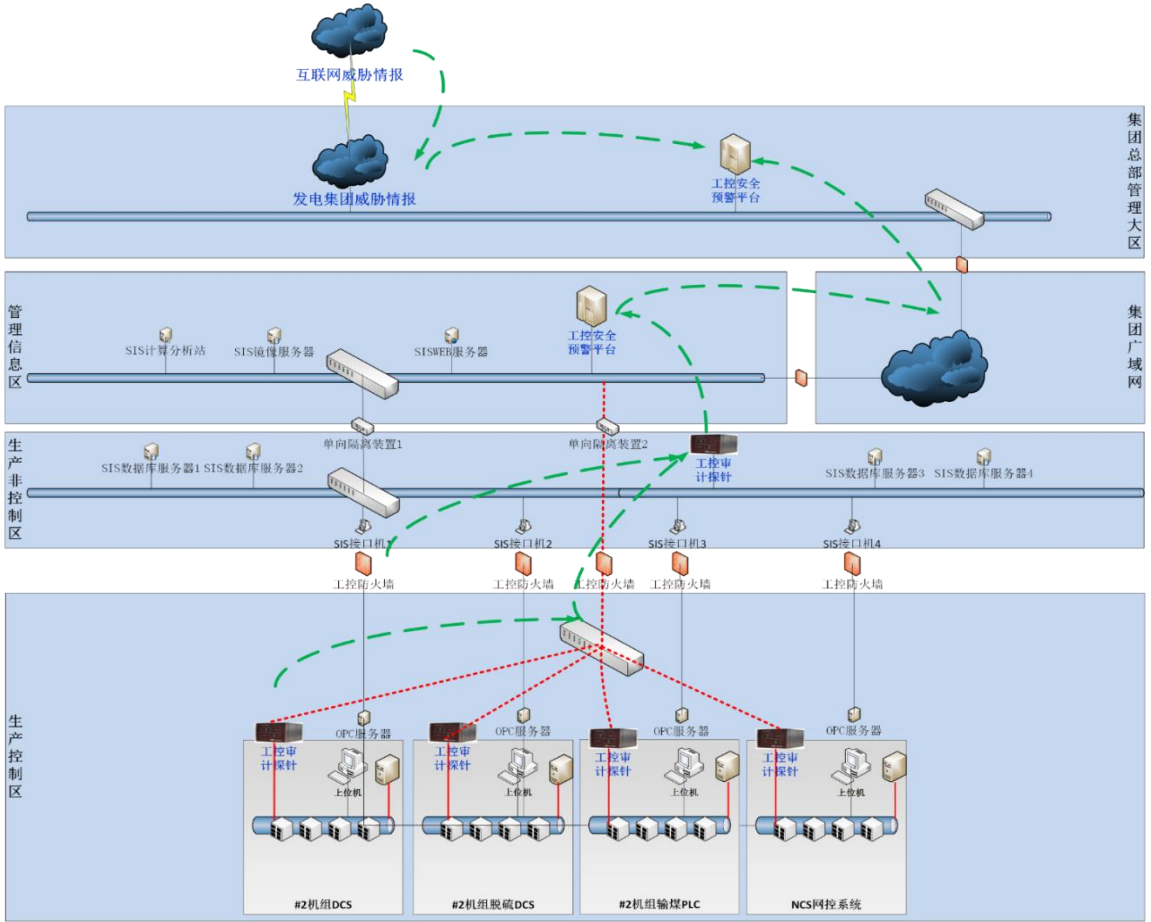
软件	要求
操作系统	目前只支持64位操作系统，要求安装时关闭SELinux。 • CentOS 6.5 x86_64，basic server模式。 • CentOS 7.3 x86_64，infrastructure server模式。

- ✓ INSP是软件形态，需要部署在Linux操作系统上，系统组成：安全分析中心、日志采集器和日志代理。
- ✓ 日志代理可以安装在Windows或Linux主机上，用来采集主机系统的日志和其他应用日志。
- ✓ 采集器支持本地部署方式。

INSP整合工控安全解决方案-部署示意图



联动智能防御



情报数据流向

监测设备通道

工业互联网企业级平台

边缘计算安全网关

4 客户价值

客户价值

实现安全事件分析的统一化，集约化；

能够综合多种数据来源进行未知威胁分析；

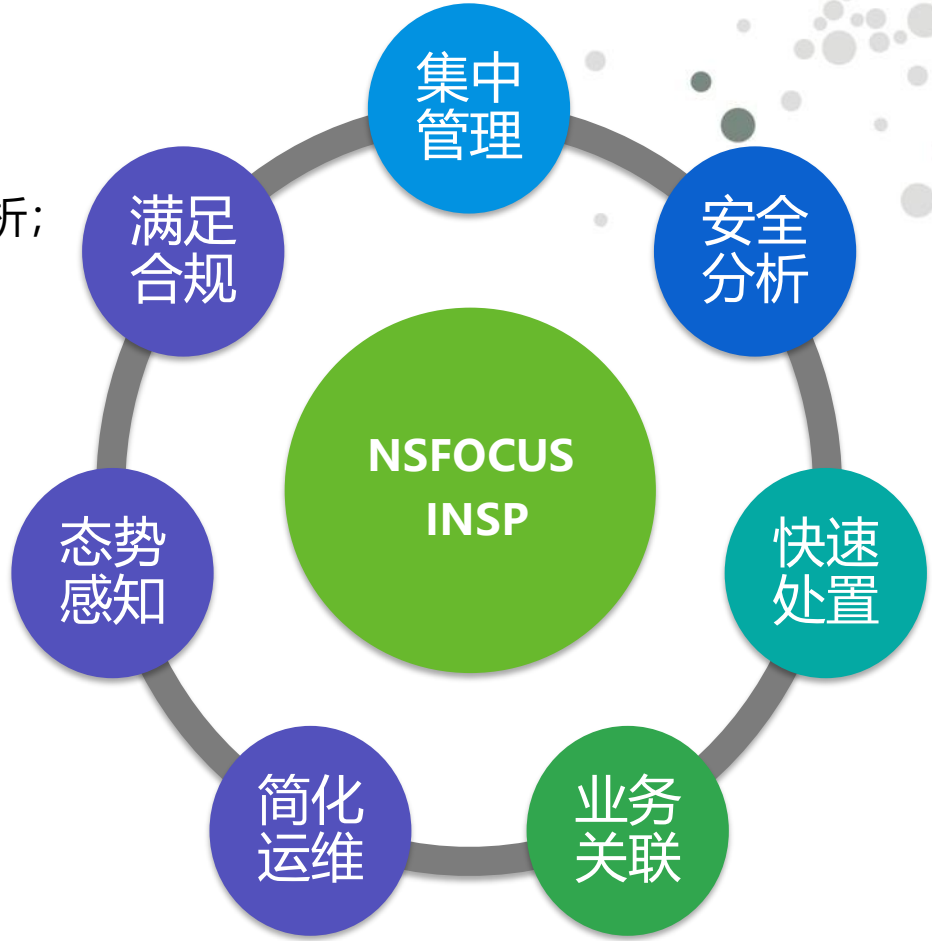
减少威胁发现和响应时间；

上至业务层网络，下达生产现场，全局把控；

能够帮助安全人员简化工业网络安全运维难度；

可以构建企业整体安全态势感知中心；

能够应对多项监管合规要求；



5 对比分析

友商产品对比分析(资质&案例)

内容/品牌	绿盟INSP	启明星辰	威努特USM	360网神	安恒信息	天地和兴HX-EICS
资质						
产品资质	《计算机信息系统安全专用产品销售许可证》《计算机软件著作权登记证书》	启明的工业soc使用的还是传统T-soc的产品资质，产品继承了启明星辰泰合信息安全运营中心系统（TSOC）	《计算机信息系统安全专用产品销售许可证》《计算机软件著作权登记证书》	360网神目前暂无工业级SOC，在研中，目前同威努特合作	安恒暂时没工业级SOC产品	《计算机信息系统安全专用产品销售许可证》《计算机软件著作权登记证书》
案例						
能源、政府	三板溪电厂、姚孟电厂、台州水务、温州水务等	国家工业信息安全发展研究中心牵头的工业转型升级专项项目、长庆油田二期、厦门烟草等等	属于绑定产品，作为自有产品的统一管理平台，威努特其他工控安全产品缺乏web独立管理界面，所以所有的项目都有USM产品	N/A	N/A	主要是电厂
电网	N/A	N/A	N/A	N/A	N/A	N/A
电厂	具备	N/A	具备	N/A	N/A	具备
能源	具备	具备	具备	N/A	N/A	具备
轨交	N/A	N/A	N/A	N/A	N/A	N/A
制造	N/A	N/A	N/A	N/A	N/A	N/A
其他	N/A	N/A	N/A	N/A	N/A	N/A

友商方案对比分析（主要技术规格）

内容/品牌	绿盟INSP	启明星辰T-soc	威努特USM	360网神	安恒信息	天地和兴HX-EICS
主要功能						
自有工控安全设备管理	√	√	√	N/A	N/A	√
日志收集	√	√	x	N/A	N/A	N/A
集成数据库	√	√	x	N/A	N/A	N/A
部署方式	√	√	N/A	N/A	N/A	N/A
工控设备类型	√	√	√	N/A	N/A	√
资产清单列举	√	√	√	N/A	N/A	√
工业网络资产拓扑	√	√	√	N/A	N/A	x
定制化工业网络资产拓扑	√	√	√	N/A	N/A	x
自动资产识别	√	√	x	N/A	N/A	x
提取流量攻击报文特征	√	√	√	N/A	N/A	√
网络设备日志收集	√	√	x	N/A	N/A	x
工控知识库	√	√	x	N/A	N/A	√
线形图、饼图、条状图等多种方式来显示信息	√	√	x	N/A	N/A	√
自动识别新的设备	√	√	x	N/A	N/A	x
日志量化分析	√	√	x	N/A	N/A	x
配置向导	√	√	x	N/A	N/A	x

业界领先的漏洞即时响应速度

Microsoft Active Protections Program

Microsoft

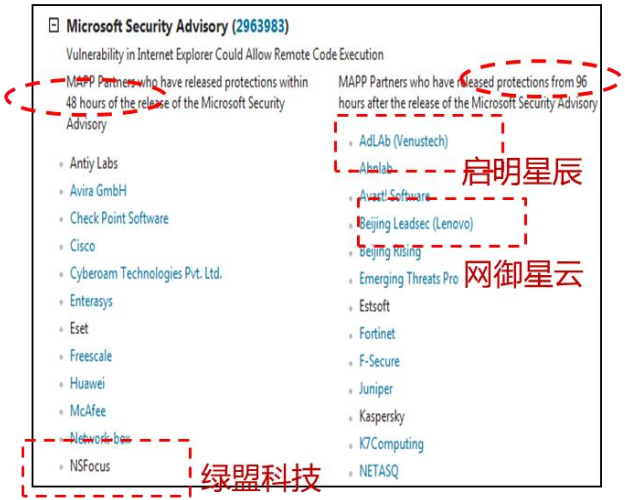
✓ **Microsoft Active Protections Program（MAPP）Partner**

The Microsoft Active Protections Program (MAPP) is a program for security software providers that gives them early access to vulnerability iNIPSormation so that they can provide updated protections to customers faster.

MAPP Partners who have released protections within 48 hours of the release of the Microsoft Security Advisory

Microsoft MAPP vulnerabilities	NSFOCUS	HP (TippingPoint)	FireEye	IBM	LastLine	Radware	Cisco	Fortinet	Juniper	Kaspersky	Mcafee	Palo Alto	Symantec	Trend Micro
Microsoft Security Advisory (2963983)	O	x	x	x	x	x	O	x	x	x	O	O	O	O
Microsoft Security Advisory (2934088)	O	x	x	x	x	x	O	O	x	x	x	O	x	x
Microsoft Security Advisory (2914486)	O	x	x	x	x	x	x	O	x	x	x	x	x	O
Microsoft Security Advisory (2896666)	O	x	x	x	x	x	O	x	x	x	O	O	O	O
Microsoft Security Advisory (2887505)	x	x	x	x	x	x	O	O	x	x	x	O	O	O
Microsoft Security Advisory (2847140)	O	x	x	x	x	x	O	x	x	O	x	x	O	x
Microsoft Security Advisory (2794220)	O	x	x	x	x	x	x	x	x	x	x	x	O	O
Microsoft Security Advisory (2719615)	O	x	x	x	x	x	O	O	O	x	O	x	O	O
Microsoft Security Advisory (2639658)	x	x	x	x	x	x	x	O	O	O	O	x	x	x
MAPP Partners who have released protections within 48 hours of the release of the Microsoft Security Advisory	78%	0%	0%	0%	0%	0%	67%	56%	22%	22%	44%	44%	67%	67%

Reference:
https://technet.microsoft.com/en-us/security/dn568129.aspx



微软漏洞48小时响应率，绿盟在24小时内响应，远超业内友商。

Thanks