绿盟工业网络安全监测管理平台

白皮书

■ **文档编号**	请输入文档编号	■ **密级**	请输入文档密级
■ **版本编号**		■ **日期**	

© 2022 绿盟科技

■ **版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ **版本变更记录**

时间	版本	说明	修改人

■ **适用性声明**

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

一. 工业网络安全管理的新需求和挑战 1

1.1 需求分析 1
1.2 面临的挑战 3
1.3 如何应对挑战 4

二. 绿盟工业网络安全监测管理平台 5

2.1 产品概述 5
2.2 产品架构 6
2.3 产品亮点 7
2.4 关键技术 9
2.5 产品功能 ..... **错误!未定义书签。**

三. 典型部署 11

3.1 部署方式 11
3.2 运行环境 ..... **错误!未定义书签。**

四. 结论 13

一. 工业网络安全管理的新需求和挑战

1.1 需求分析

随着工业 4.0，互联网+以及深度两化融合地发展，越来越多的信息技术应用到了工业领域。网络化，开放化以及数字化已逐渐成为工业控制系统发展的目标。工业控制系统已广泛应用于电力、水利、关键制造业，石油化工、交通、市政和食品制药等工业领域。其中，大多数的基础设施实现自动化作业时依赖工业控制系统。可见，在国家基础设施中越来越体现工业控制系统的重要性，对于工业控制系统来说，如果出现信息安全的漏洞，将直接影响到工业领域以及国家基础设施的安全，因此工业控制系统和国家的战略安全密不可分。

工业控制系统是由各种关键性设备对网络中传输的实时信息数据进行监测与采集，实现对自动化运行设备地监控以及对整个流程的规范化管理，它的主要特点实时性数据传输、数据驱动事件以及数据源主动推送。一般情况下，由通用的软件和网络设施组成工业控制系统，与开放的企业网和互联网等相互集成。由于传统的工业控制系统看重系统本身的物理防御，对软件以及系统的网络安全缺乏认识，因此，没有针对其形成专门的应对措施。工业系统网络化的快速发展，系统所面临的安全风险系数也在增大，网络安全问题也尤为明显，再加上工业网络普遍采用流行的以太网以及通常采用 TCP/IP 技术进行通信，以及 WALN 和 GPRS 等无线网络，使用标准的 Windows 操作系统，逐渐将工业控制协议迁移到应用层，工业控制系统的开放性，利用传统的 IP 协议安全漏洞能够攻击工业控制网络，使得工控系统的安全隐患愈加严重。工业控制系统目前大多采用 IT 技术，互联开放性逐渐加强，因此，黑客以把工业控制信息安全作为攻击目标之一，攻击手段多样，工业控制系统面临的威胁也日趋严重。

工业安全影响远超过商业和名誉保护。在多数情况下，当涉及到工业系统威胁、攻击、破坏时，往往首要考虑生态、社会和宏观经济因素。因此，工业系统等关键基础设施的关键节点和网络保护需要足够高的防护等级才能对抗日益增长的网络安全威胁。同时，工业环境需要一套的综合的解决方案通过安全预警响应和纵深防御策略提升技术流程的可用性。同时，工业互联技术及攻防技术的不断演进，企业对信息安全技术人员的依赖日益加深，对技术人员的安全能力也有了更高的要求。这不仅加剧了技术人员的需求缺口，也增加了管理人员使用成本。企业在转变生产方式和业务拓展的大背景下，运维和人员数量和人员成本的与日俱增，又使得企业预算捉襟见肘。

© 2022 绿盟科技

密级：请输入文档密级

过去，工业控制系统所采取的措施主要是通过隔离的手段进行安全防护，主要是把各个重要子系统之间的网络流量进行隔离控制，如今，工业控制系统不仅面临传统意义上的 IT 与病毒攻击，而且工业控制协议的信息漏洞与控制器的入侵等问题也日渐增多。据 SANS 研究所发现，35%的工业网络故障事件由网络攻击引起。在 2021RSA 大会上，“如何保证工业互联网安全”依旧是大会的热点话题。众所周知，国内工业产业链中 ICS 安全产业起步明显晚于国外的，而近年来以工业环境为目标的恶意攻击出现显著增长。供应链和业务中断的风险在过去三年里一直高居全球企业风险的榜首，而面向生产的网络安全成为能源、制造工业企业首要新兴问题。对于运营工业或关键基础设施的企业，风险日益壮大。由此可以看出信息安全问题已严重影响工业控制系统，需要工业领域以及国家给予足够的重视来积极应对。

互连设备的引入，IT 和 OT 的整合，给 ICS 系统带来了新的安全挑战。企业希望能够知道在 ICS 中，什么是正常的操作，同时通过正常操作建立基线来判断什么是不正常的、意外的或者潜在的恶意操作。这就需要在工控环境中建立态势感知系统。态势感知是在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

专精于工业网络的态势感知系统的三大特征是：

- ✓ IT 和 OT 的深度融合
- ✓ 结合跨行业业务场景的行为基线
- ✓ 可视化的预警与感知

不同行业客户对工控平台有着不同的需求特性。大致分为以下几个方面：

① 针对不同行业的安全场景模型(行为基线建模），工控的业务操作流程进行梳理，形成各个工业操作业务流的健康性监控

② 工业网络的工控场景数据收集、处理和分析

③ 主动防御和安全预警

④ 全面了解工控网络的全局风险，以工控领域常见的拓扑或直观呈现的方式表现网络环境及各设备的运行状态和安全状态

⑤ 需要协助运维人员快速解决故障及事件

⑥ 指导安全工作和决策

⑦ 符合等保及合规要求

© 2022 绿盟科技

密级：请输入文档密级

1.2 面临的挑战

当前主流的工业网络管理系统主要面临着以下几种挑战：

1）多源异构数据采集需求

随着公司信息安全水平的提升，公司安全防护产品越来越多，安全品牌也也各式各样，同时对于后续的安全分析，已经不仅仅只是安全设备的职责，本次平台建设需要做好多源异构全数据采集规划，对于所有网络内可用的安全分析辅助信息进行收集，包括但不限于安全设备日志、业务系统日志、网络流量等等，为后续平台数据挖掘及关联分析做好数据准备。

2）工业网络数据存储与分析需求

由于采集数据的多元性、异构性和工业网络性，还会包括对于网络流量的采集，因此平台所采集的数据量将是一个巨大的数字，并且涉及到今后对于数据的挖掘以及关联分析和历史查询分析，存储的时间至少要六个月，因此工业网络数据的存储问题在平台设计之初就应该重点考虑，且为保障平台运转的延续性和对于 APT 等新型攻击的深度挖掘，还要考虑到存储空间不足时数据存储的可扩展能力。

工业网络数据采集后，对于已知攻击的实时分析、历史数据的挖掘分析，以及对工业网络内外网数据、事件、文件等的关联分析、检索、实时在线检测、离线检测，发现高级的 APT 攻击和信息泄漏行为能力要成为平台具备的基本能力，计算能力的强弱直接决定着平台今后的实用性。

3）安全指标及态势的可视化展现需求

作为大数据安全分析平台，在分析能力基础上应有一个人性化的、简单实用的展示界面，平台分析结果需采用量化指标形式呈现，直观展示当前网络攻击、病毒木马、主机漏洞、终端异常行为等重点安全监控指标，在出现高威胁攻击时可通过实时攻击地图进行展示，同时结合历史数据分析，展示全公司安全态势及发展趋势。

4）信息安全一体化建设和监管需求

在安全运维工作中，安全运维人员面对不同类型并且部署于不同位置的安全设备，难以在全局上了解全网存在的脆弱性是如何分布的、面临的安全威胁有哪些，也难以判断第一时间应该优先对哪些脆弱性进行修补和控制，对哪些威胁进行诊断和分析。按照设备告警时间的顺序处理威胁告警、控制和修补资产脆弱性，往往会导致运维人员错过真正需要诊断分析的威胁和真正需要控制和修补的漏洞，无法及时有效地降低网络安全风险。

© 2022 绿盟科技

密级：请输入文档密级

安全设备集中管理工具可以对安全威胁告警及其分类，并帮助安全运维人员识别最需要进行诊断分析的威胁。同样，通过安全设备集中管理工具，安全运维人员才能查看全网资产脆弱性分布情况，从而进一步根据资产重要性和脆弱性的风险级别识别出最需要控制和修补的脆弱性。

5）如何保障企业业务系统协同管理

无论是传统企业环境中，还是在未来的“云计算”环境中，不可避免的存在一个或者多个业务系统并存的情况。 这些业务系统可能是网管、SOC 、SIEM 或者 CMDB 等。它们自身定位不同，并且负责着不同类型信息的收集、汇总以及展示。如何与这些相关业务系统协同运维，打破各自为战的“信息孤岛”是摆在企业面前的另一道障碍。

6）如何保障业务平台系统的可用性

业务系统的可用性体现在：对新兴的威胁防御以及资产维度上的威胁感知。传统的工业网络管理系统强调对单个设备和性能的可用性管理，缺乏通过多设备联动，对复杂网络威胁攻击（APT 攻击）的检测和防护。同时，从设备监控视角出发，过渡地强调设备故障的及时诊断，已经不能够从根本上保障核心业务系统的可用性，更缺乏从核心资产维度的监控和分析。

1.3 如何应对挑战

在优化工业网络现有安全防护能力方面,利用相关技术,对安全态势感知进行建设,具有重要意义。在现行规范及产业需求的指导下,对感知平台的架构与能力进行设计,通过对预警通报、安全监测等技术加以利用的方式,确保企业态势始终处于可感可知状态,为日后监管工作的开展提供便利。对感知平台能否发挥应有功能起决定作用的主体为管理人员,详细来说,就是以感知平台得到高效建设为前提,通过全面监管的方式,确保异常情况、安全威胁可获得及时预警。除此之外,还有两方面内容需要引起重视:

(1)加大管理网络运营安全性的力度,以实际情况为依据,调整现有管理制度,酌情引入预警机制,确保安全决策科学、应急响应有效。

(2)面向管理人员定期组织培训,使管理人员拥有良好的素质与能力,可快速处理安全事件,真正做到事中阻断威胁和事后追溯威胁产生源头,避免类似情况再次出现。

综上可知，客户需要一套全新的安全管理系统来应对传统网络和工业网络数据带来的所有挑战，该系统能够通过数据采集和大数据分析，利用机器学习等先进技术，协助企业 IT 运维人员和安全分析人员快速发现威胁。以情报为驱动，针对企业工业网络资产情况进行全方位的监控和告警，协助用户进行网络安全威胁的统一管理。同时，这个系统应该是一个开放的平台，能够与客户的其他管理系统实现协同工作。

二. 绿盟工业网络安全监测管理平台

2.1 产品概述

绿盟工业网络安全监测管理平台从工业控制系统安全的角度，对工控系统的各类 IT 和 OT 设备数据进行采集，包括业务设备日志采集、安全设备事件收集、网络流量数据采集、安全设备配置采集等功能。平台对采集得到的结果进行统一分析与展示，发现工控网络内部的异常行为，如新增资产、时间异常、新增关系、负载变更、异常访问等行为，实现对工控现场安全事件的预警与响应。

绿盟工业网络安全监测管理平台可以对工业网络中各类上位机服务器、工控终端、网络交换设备、工控安全设备进行集中化的性能状态监控、安全事件的集中展示、安全风险的评估、工控分区分域的健康等级，以及依赖于工控知识库的安全响应与处置。

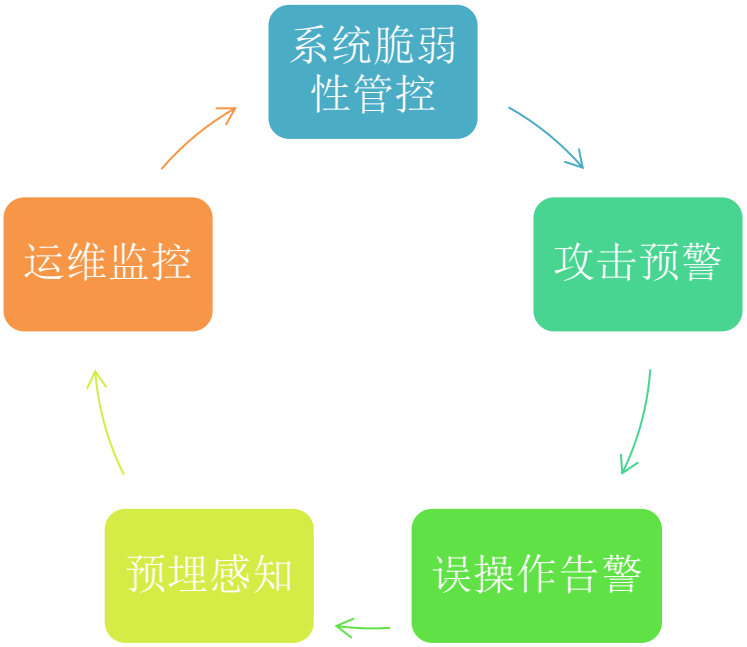


图 2.1 融合业务的安全保障闭环

2.2 产品架构

NSFOCUS INSP 主要由展示层、功能层、分析层、数据层、采集层共五个部分组成，可以在各种不同场景的工业网络环境中进行灵活的部署和管理,如图所示：

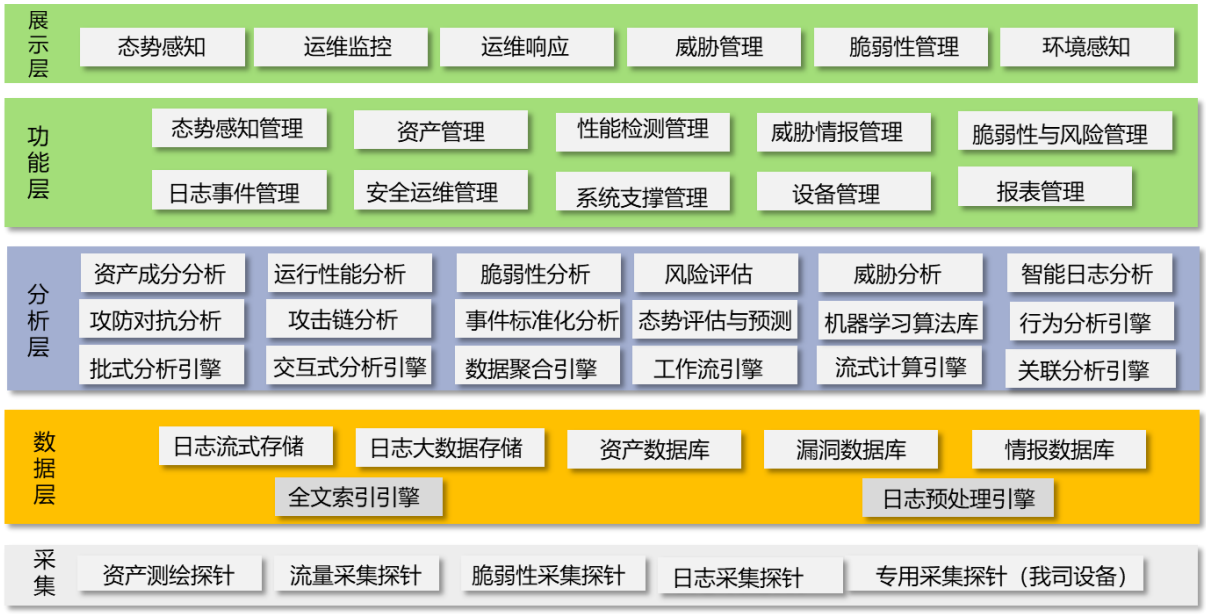


图 2.2 NSFOCUS INSP 系统架构图

1、采集层主要是采集影响系统网络安全的内外部要素数据，包括企业内部 IT 环境数据、资产数据和外部情景数据。内部态势数据包含了资产、业务、性能、配置、漏洞、日志、流/包数据等，外部态势要素包括安全情报数据和安全合规要求等。系统数据摄取不仅支持海量、异构、高速的安全态势要素数据还支持分布式数据采集，提供分布式消息队列保证数据采集性能。 平台主要流量探针是工控审计设备。

2、数据层将收集到的内外部安全态势要素数据按照数据处理的需要存储在相应的数据库中。数据存储层可以兼容不同类型的大数据，这些数据包括结构化和非结构化数据、关系型和非关系型数据、实时数据和历史数据。存储的数据服务于系统后续的监测分析操作，系统使用多种数据存储技术。

3、分析层提供多种智能安全分析方法对网络安全态势进行全天候多方位的感应，并且拥有安全监测和分析预警能力。安全分析的途径包括实时流量式分析、曾经访问记录的批量分析、交互式分析和回放分析等。此外，网络安全态势感知系统还提供持续监测、关联分析、情境分析、机器学习、行为分析、威胁猎捕、风险评估、态势理解与预测等功能。

© 2022 绿盟科技

密级：请输入文档密级

4、功能层提供系统的应用功能的实现。包括基于工控网络拓扑的综合态势管理、基于攻击链和业务行为基线的风险预警管理、基于工控事件库和处置预案库的工控知识库以及其他核心功能模块。

5、展示层是系统实现安全态势呈现和系统人机交互的关键部分，不仅可以为各类安全管理人员提供安全态势可视化呈现和安全处置响应界面，还可以通过各类仪表板，报表报告和功能操作实现整个安全态势感知与安全防护的技术支撑。

2.3 产品优势

强大的日志模式识别技术

系统通过机器学习技术对获取到的日志进行分析、理解和挖掘，运用聚类算法对数据信息进行清洗，然后在根据日志相关信息进行自动化归类合并的基础上形成一个个日志数量不同的数据集，且每一个数据集包含类型相似的日志。企业安全分析人员在查看数量繁多、种类复杂的搜索结果时，可以通过数据集模式进行查看和分析。这种技术可以帮助安全分析人员优先分析数量最少的日志集，从统计学的角度来说，这种小概率分布的数据往往是异常分析的入口线索；安全分析人员也可优先处理数据量最大的日志集，并且可对其进行范式化，解决了最大概率分布的日志的范式化，方便后续分析和审计。

PB 级的日志处理能力

平台使用 Spark 技术，在并发内存内处理机制方面能够带来数倍于其它采用磁盘访问方式的解决方案，借助离线计算引擎在小时级别内，即可完成对 PB 数量级的数据挖掘。可以为大规模、超大规模网络提供高性能的日志采集，存储和审计功能。例如：6 个月内的安全事件之间的相关性，安全事件之间的影响程度，安全事件之间的规律性等并以报表形式进行输出。

先进的可视化范化技术

平台还采用了可视化范式化技术，针对安全运维人员的范化需求，系统提供了可视化操作界面，运维人员可直接在页面完成编辑正则表达式和显示所需信息提取结果的操作，可视化范化技术不仅大幅简化了传统范化工作的流程，降低了编写正则表达式的难度，还提升了工作人员日志范化的日常工作效率，使平台变得更方便更高效。

可视化的综合态势管理

工业网络安全监测管理平台可以通过网络拓扑或直观呈现的方式表现网络环境及各设备的运行状态和安全状态，从而达到对工控网络中的各类设备进行集中的状态及性能监控的目

© 2022 绿盟科技

密级：请输入文档密级

的。平台态势呈现支持两种拓扑呈现，一是面对全网设备的普渡模型拓扑，让客户对全网资产的分布状态更清晰直观。二是可自定义绘制的网络拓扑，主要来呈现网络结构和网络安全建设的情况。

综合态势管理还包括可视化的攻击链状况展示、风险仪表盘展示、告警事件类型分布展示、资产风险分布展示、最新安全事件列表等可视化模块。

一站式的信息综合管理

工业网络安全监测管理平台提供一站式的信息综合管理功能。一站式综合管理包括对安全设备上传的事件类日志信息、业务系统上传的操作等日志信息、采集的安全设备配置策略信息进行统一的分析和呈现。

日志管理功能模块支持上位机服务器、数据库服务器、工业网络通信设备的日志采集和接入。采集服务器、工作站的用户登录、操作信息、运行状态、移动存储设备接入、网络外联等事件信息；采集数据库的操作信息、运行状态等事件信息；采集网络设备的用户登录、操作信息、配置信息变更、流量信息、网口状态等信息。

安全设备管理模块支持对绿盟安全设备的状态监测。其中对绿盟工控审计设备、工控入侵监测设备、边缘计算网关的策略配置与下发。可联动绿盟防火墙设备进行一键封堵的操作。以及支持在平台对工控漏扫下发资产扫描与漏洞扫描的任务。

融合业务特性的工控知识库

工业网络安全监测管理平台基于多类型的工控知识库进行事件的关联分析。深入到不同行业的工控网络特性当中，产生融合业务特点的场景告警。同时又具备工业网络全行业属性的通用性告警，如针对资产新增、路径异常、未知协议、越权操作、关键控制等操作产生的告警。

工控知识库包括工控事件库、处置预案库、工控漏洞库、工控协议库。平台主要依据工控事件库和处置预案库将多种设备收集的日志进行整合关联分析，产生告警并给出处置建议。工控漏洞库包含了 IT 信息系统漏洞及 OT 工控环境漏洞，方便运维人员进行风险分析和管控。工控协议库囊括了 Modbus Tcp、S7、S7 PLUS、Profinet、DNP3、IEC 60870-5-104、IEC 61850-MMS 等主流工控厂商使用的工控通信协议。通过工控知识库的建立可以达到强大的关联分析效果。比如平台从生产控制网络的资产行为中建立了一组正常行为基线，即到一组 PLC 的 Modbus 所有通信都是来自于相同的 3 个 HMI 工作站，标记为基线 A。在运营过程中发现监控系统报警，与基线 A 出现分歧，出现了第 4 个系统与 PLC 进行通信，判断其可能的表现有四种：一个新的未被授权的设备被插入网络中（如一台管理员的笔记本电脑）；一个使用欺诈 IP 地址的恶意 HMI 正在运行；新的系统安装上线。通过对近期公网

的威胁情报及生产控制网络近期操作行为的整合分析，得知该异常是由于未被授权的设备接入网络所导致。

多层次智能安全分析技术

系统提供多层次的智能安全事件分析技术，本技术根据安全事件对人工依赖度从高到低分为关联分析、行为分析和专项深度分析三个层次。其对安全事件的分析具体包括以下五个方面：

1）敏捷分析：对多源异构数据动态建模，实时检测。

2）精细化分析：以强大的数据模型和精确到字段的分析规则，帮助安全人员精细化安全分析。

3）追溯分析：对发生的安全事件追踪溯源，提供分析证据。

4）策略化分析：将安全分析策略化，可以很好将机器分析、用户业务和人的分析能力进行结合，同时，分析策略的可配置化为企业提供旺盛的生命力。

5）水平扩展能力：集群上的安全分析计算可以进行灵活的水平扩展。

APT 是一种高级持续性威胁，通过长期潜伏找到有价值的特定目标，利用网络中受信的应用程序漏洞，发起持续性网络攻击，窃取核心资料或篡改数据。但任何攻击行为都会有他的行为特点，如嗅探，提权，安装后门，扩散和逃逸等行为。绿盟根据多年工程经验结合美国 NASA 的攻击链条模型设计出针对攻击行为特征的安全分析模型，通过该模型，用户不必具有很高的专业安全能力就可以准确的对安全事件进行发现，预测和历史痕迹追踪，从而降低对专业安全分析人员的要求，减轻企业成本。

2.4 关键技术

工业网络数据采集

NSFOCUS INSP 可以支持代理日志采集方式和多种标准协议。通过数据采集、数据理解、数据抽取和数据清洗等操作，将各种应用系统和设备的日志进行预处理，帮助管理员把工业网络日志进行去噪，提取其中人们事先不知道，但有潜在有用的信息和知识。

独家数据强化技术

NSFOCUS INSP 根据绿盟科技对攻防研究的长期积累，提供一套简洁有效的日志统一分类，使用独有的技术将日志快速标准化，并基于安全分析需要进行数据的过滤和强化，丢弃无法用的噪音信息，提升日志查询和分析效率。

强大的分析引擎

平台中预制关联分析引擎，预制引擎构成分析平台的核心功能并且对专项分析提供基础能力，如风险分析、脆弱性分析、态势分析、资产分析、攻击链条分析等。

分析引擎采用分布式设计能够进行横向扩展，面临工业网络数据量时能够实现按需扩展，将分析引擎分散到其他更多的机器中，实现按需进行计算资源扩展。

高效的面向业务的插件化设计

NSFOCUS INSP 采用全新大数据框架，将上层业务模块插件化处理，使业务模块与平台功能进行一对一设计，业务模块的改善和增加就不会造成其他模块或平台功能的调整，也就是将业务模块抽象并与平台功能实现分离，从而提高研发效率，降低企业维护成本。

智能的资产发现技术

相比较于传统的 NMAP 资产扫描工具的主动介入式扫描（这种方式常常会违反组织安全策略，被安全系统识别为扫描类信息刺探），系统提供了主被动结合的方式进行资产发现。首先通过旁路采集的网络流量和日志数据发现网络中存在的未知资产及其开放的端口和服务。未知资产会触发平台驱动系统内部漏洞扫描系统进行扫描识别，助力企业进一步发现资产的类型和版本、开放的端口和提供的服务，以及存在的漏洞。针对非操作系统类和网络设备类资产，系统支持多种协议 SSH/Telnet/FTP/HTTP/HTTPS 等进行服务数据采集。

可靠的网络安全通报预警

NSFOCUS INSP 采用大数据组件，对数据对象弹性分布存储 3 个存储节点中，并采用线程级监控，一旦发现问题，可迅速恢复并告警，同时 3 备份可以提供完整的灾难恢复功能。网络安全通报预警系统将来自国家主管机构、系统厂商、第三方组织、安全厂商、上级单位等包括病毒、漏洞、安全通告在内的外部预警以及来自集团总部及其二级分支的内部预警的信息进行整合形成预警发布内容、采用技术手段、预警发布方式、预警发布结果等四个模块，系统支持安全监测预警和信息通报，可根据规范通过接口上报和下发安全信息。

（1）预警发布内容。安全检测、监测的研判结果，包括攻击信息、日志信息、性能指标分析结果、检查报告等相关内容；

（2）采用技术手段主要包括信息筛选、数据分类、分析结果、告警处理结果、行业排名、区域排名等；

（3）预警发布方式包括，大屏展示、信息滚动播放、邮件通知、短信通知、运维平台、应急处置平台等；

（4）预警发布结果，利用邮件短信发送告警信息，并提供解决方案，达到流程追溯、取证记录和事件管理的目的。

© 2022 绿盟科技

密级：请输入文档密级

丰富的威胁情报

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技依赖多年的安全经验和情报数据积累推出的一款威胁情报分析和共享平台，可为用户提供及时准确的威胁情报数据。

绿盟工业网络安全监测管理平台接入基于绿盟威胁情报中心 NTI 的威胁情报数据。安全管理平台将本地告警数据、网络资产数据、漏洞数据与绿盟威胁情报数据按照多个维度进行关联分析，实时感知资产的威胁和脆弱性，通过平台安全规则的筛选和过滤最终形成漏斗效应，保证告警的更加精准和有效，并洞察新的威胁动向。借助 NTI 的威胁情报支撑，用户可及时洞悉资产面临的安全威胁进行准确预警，了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，提前预防 0day 漏洞和重大攻击的发生，减少安全损失， “主动预防”胜过“事后救火”。

2.5 客户价值

- 便携管理

IT 和 OT 的深度融合，安全设备状态可视策略可管，实现安全管理的集中化。

- 安全可视

多种可视化的态势模块，针对工业场景的专题分析，构建工业网络安全态势感知中心。

- 简化运维

减少威胁发现和响应时间，帮助安全人员降低工业网络安全运维难度。

- 满足合规

能够应对《等保 2.0》、《关基》等多项合规要求。

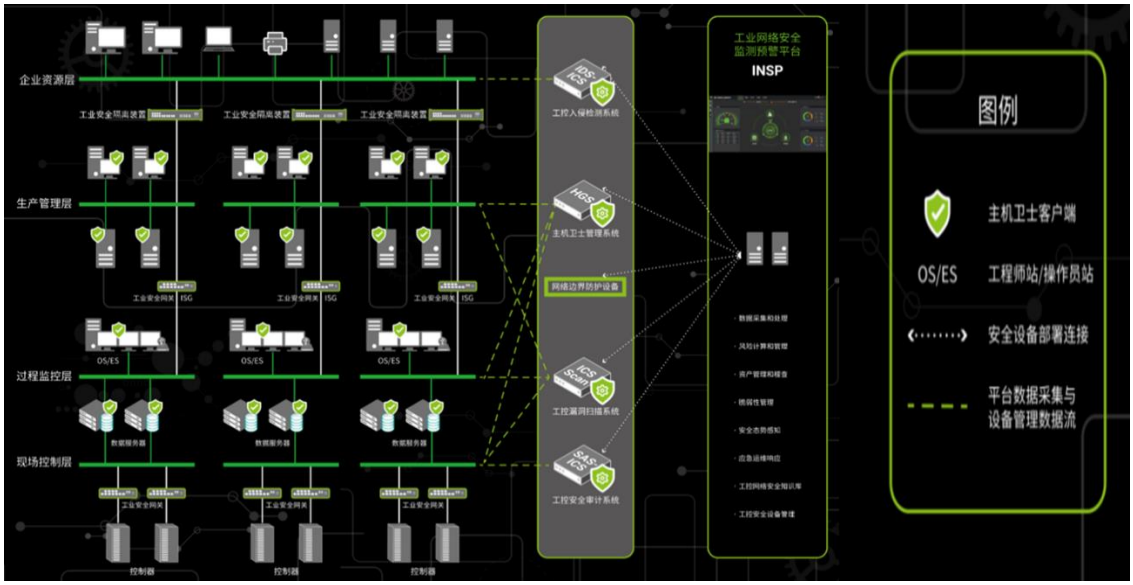
三. 典型部署

3.1 单极部署

在工业网络中就部署一个管理中心程序，所有的用户都登录到该管理中心进行访问，通过系统权限设置来区分不同的管理职责。

在单级部署模式下，又分为单机部署和集群部署。

单级单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分企业客户的工业网络环境。在单机部署场景中，用户仅需在一台服务器上部署 NSFOCUS INSP 系统。之后，管理中心可以收集设备对象的日志和性能信息。用户可以通过浏览器登录系统的交互界面，并根据相应的权限进行各种管理操作。



单级部署模式

3.2 多级部署

多级部署是指将 INSP 采用多地，按照分组的运行的方式进行部署的模式。一般地，当需要在分散在工业企业网络中进行较大规模的节点部署时，此时，大量的性能、日志数据通过网络汇总到集团管理中心，会给管理中心造成一定的性能影响。通过在将 NSFOCUS INSP 平台运行于工业企业集团不同数据管理中心的方式，上至业务层网络，下达生产现场，实现集团对工业生产网络安全的全局把控。提供从工业网络安全评估到事件响应在内的全周期安全服务。

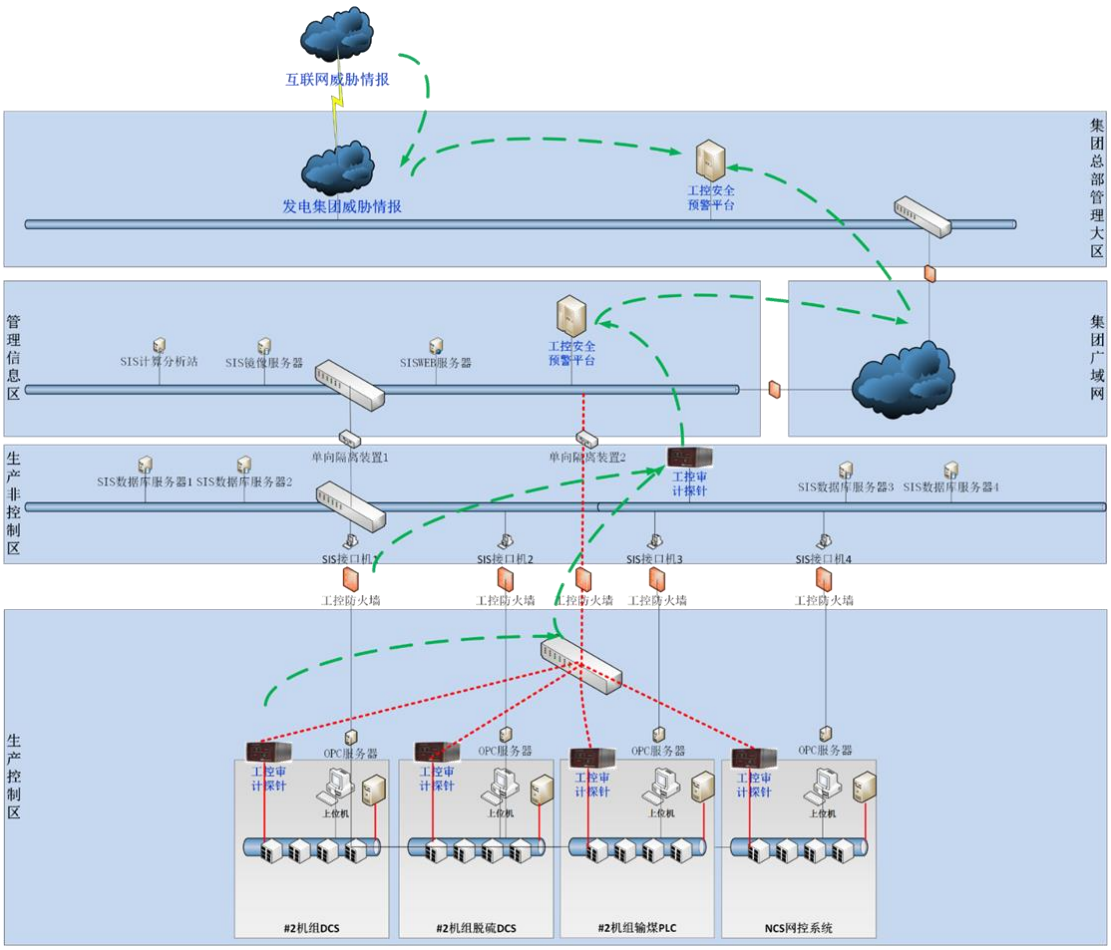


图 3.1 多级部署模式

四. 结论

现在已是大数据和云计算的时代，信息安全问题也正在演变成一个大的网络安全问题，也是现在 Internet 和政企行业安全运营系统亟待解决的问题。知己知彼，才能百战不殆。没有意识到风险是最大的风险。保护网络安全，首先要了解风险隐藏在什么地方，是一种什么类型的风险，会在哪种情况下发生风险，正所谓“聪者听于无声，明者见于未形”，预测网络安全态势是当前企业最基础性的任务，因此，要全面提高企业在网络安全要素感知、通报预警、评估风险、发现漏洞、通报结果，整改安全策略等方面的能力；要进一步完善合理有效的安全风险评估机制、情报共享机制、研判处置机制，精准掌握危害网络安全事件的运动

规律、基本动向、态势等信息，将已获取的各种数据资源进行有机结合，提高大数据挖掘分析功能，更好的感知网络安全态势，做好应对风险的防范策略。

由于工业控制系统所覆盖的行业重要性，比如油化、电力、核电厂、水利、交通、市政、军事、高端制造业等，其安全性问题也越发的重要，并且牵涉到国计民生。对于这些关键信息基础设施，如何进行安全监测及预警，如何及时有效的进行事前的防范，事中的监测以及事后的追溯，正成为工控安全领域亟待解决的问题。

基于全生命周期的工控系统安全综合保障手段的建设，给传统的单点安全防护提供了新的思路。将功能安全、信息安全进行深度融合的工业网络安全监测管理平台，连接了孤军奋战的单个结点，融入了故障诊断、异常告警、态势感知、攻击检测等持续可运营的安全防护理念，最大限度的保障工业控制系统稳定、高效、安全的运行。

© 2022 绿盟科技

密级：请输入文档密级