绿盟工业网络安全合规评估工具

产品白皮书

目录

一. 引言

随着工业信息化进程的快速推进以及工业互联网、工业云等新兴技术的兴起，信息、网络以及物联网技术在智能电网、智能交通、工业生产系统等工业控制领域得到了广泛的应用，极大地提高了企业的综合效益。为实现系统间的协同和信息分享，工业控制系统也逐渐打破了以往采用专用系统、封闭运行的模式，开始在系统中采用一些标准的、通用的通信协议及硬软件系统，甚至有些工业控制系统也能以某些方式连接到互联网中。这使得工业控制系统必将面临病毒、木马、黑客入侵、拒绝服务等传统的信息安全威胁，由于工业控制系统多被应用在电力、交通、石油化工、核工业等国家重要的行业中，攻击行为所导致的安全事故造成的社会影响和经济损失会更为严重。出于政治、军事、经济、信仰等目的，敌对的组织、国家以及恐怖犯罪分子都可能把工业控制系统作为达成其目的的攻击目标。

近年来，以“伊朗布什尔核电站遭到‘震网病毒’攻击”为代表的一系列针对工业控制系统的信息安全事件表明，攻击者正普遍采用被称为高级持续性威胁（Advanced Persistent Threat，简称 APT）的新型攻击手段。攻击者不仅具有明确的攻击目标，而且在攻击时也多采用有组织的多攻击协同模式。显然，这种新型的攻击手段更难防御，对安全厂商及相关研究机构的安全服务能力提出了更高的挑战。由于国内工业控制系统及其工作环境的相对封闭性，国内安全研究团队的研究对象多集中在互联网和传统的信息系统上，在工业控制系统安全方面缺乏研究成果和实践经验。另一方面，工业控制系统提供商提供的系统或者应用软件更加关注工业控制系统的功能实现，往往忽视信息安全的因素。

工业控制系统脆弱的安全状况以及所面临的日益严重的攻击威胁，已经引起了国家的高度重视，提升到‘国家安全战略’的高度，在政策、标准、技术、方案等方面展开了积极应对。根据工业网络安全合规标准和国内外的最佳实践，通过常态化的工业网络安全评估，查找突出问题和薄弱环境，排查安全问隐患和安全漏洞，分析安全状况和防护水平，有针对性地采取管理和技术防护措施，是提升工业企业网络安全保障能力，切实保障网络安全的有效途径。无论是监管机构的安全检查还是工业企业自查，复杂多样的工业环境和数量巨大的评估对象都对评估人员的技术水平和工作量提出了很大的考验，所以亟需一款针对工业网络环境的综

合安全评估工具，可以方便评估人员现场开展评估工作，快速定位工业网络风险，指导工业企业进行网络安全防护

二. 产品概述

绿盟工业网络安全合规评估工具（NSFOCUS Industrial Network Security Compliance Assessment Toolkit，简称：NSFOCUS ISCAT）配置一体化、便携式、高性能专用硬件装备，集检查对象信息收集、合规评估、资产安全评估（资产管理、漏洞扫描、配置核查、视频设备评估）、流量安全评估（流量收集、流量审计、流量统计）、无线 WiFi 评估、主机恶意代码评估于一体的综合评估工具集，为用户提供标准、专业的检查指导，多样的评估功能，并支持对评估结果数据的关联分析、统计对比，可帮助用户快速分析展示合规现状，定位工业网络安全风险。系统架构

NSFOCUS ISCAT V1.0 采用模块化的设计，主要由系统接入层、系统核心层、系统服务层、基础平台层四个部分组成，每个部分划分为不同的功能模块，整体系统架构如图 2-1 所示：

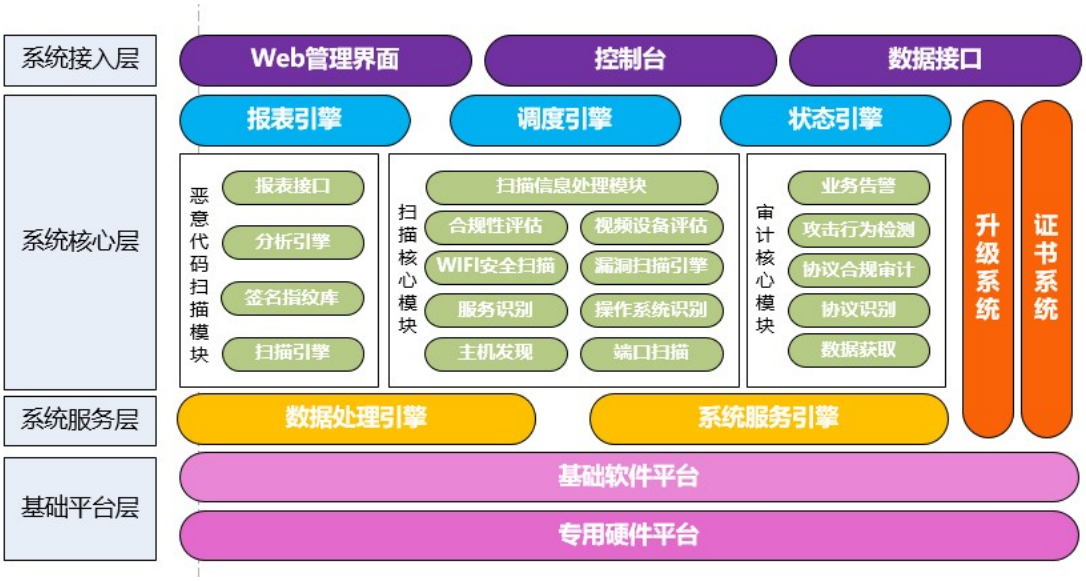

图 2-1：NSFOCUS ISCAT 系统架构图

1. 基础平台层

- 专用硬件平台提供可靠稳定的硬件环境,同时配置主机恶意代码扫描和主机配置核查两个独立的 U 盘评估工具;

- 基础软件平台包含了绿盟科技定制操作系统、文件系统、硬盘加密解密、应用程序加密解密、输入输出加密解密、IPv4/IPv6 网络服务、内置数据库、Web 服务、程序运行环境等功能。

2. 系统服务层

系统服务层包含数据处理引擎和系统服务引擎。

- 数据处理引擎是系统内部的数据接口，提供了数据库访问、数据缓存、数据同步等功能。数据处理引擎屏蔽了数据库系统操作的细节，减少数据库的连接，优化数据库的访问，缓存常用和计算复杂的数据，集中处理数据的逻辑，降低了其他功能模块的维护工作量；
- 系统服务引擎是系统内部的功能接口，提供了系统还原点备份与恢复、任务数据导入导出等功能。系统服务引擎解耦了前台操作和后台操作，后台功能以特定的权限运行，增加了系统的安全性。

3. 系统核心层

系统核心层是执行产品功能的核心，提供最具竞争力的功能，包含信息收集、合规评估、资产安全评估、流量安全评估、无线 WiFi 安全评估、主机恶意代码评估等功能。

- 报表引擎是报表展示的核心处理模块，能够提供 HTML、WORD、EXCEL、PDF 等多种报表格式。
- 调度引擎是评估工作的协调中心，根据用户操作的不同可能有正在执行的评估任务、未完成的评估任务、已完成的评估任务，协调各任务的执行状态。
- 状态引擎是系统状态的协调中心，主要包含系统资源状态信息、系统的授权证书信息、BDB 配置项、任务执行进度信息、升级进度信息等。
- 证书系统提供了产品可授权使用的信息，包含购买用户、设备 HASH 值授权、授权起止信息等。
- 升级系统提供了产品更新的能力，为扫描插件更新、入侵规则更新、产品功能更新、产品反馈修改等提供了可能。

4. 系统接入层

系统接入层包含了用户通过浏览器访问 Web 页面、通过串口访问控制台、通过数据接口进行数据交互等方式，其中数据接口包含第三方平台管理数据接口、SNMP Trap。

- 主要负责系统自身和任务下发的接入管理；
- 系统自身提供 Web 和 Consle 两种管理模式，更为完善的进行配置管理。

2.1 产品功能

2.1.1 计划管理

NSFOCUS ISCAT 支持快速创建、正常创建和自动导入评估计划，同时还支持历史评估计划复用；支持用户任意组合评估项。

- 快速创建：仅需输入计划名称及评估选项，方便评估人员日常评估工作或单项快速评估；
- 正常创建：需要输入详细的评估计划信息、评估人员信息及运营单位信息，适用于监管机构、评测结构或企业集团有计划地安全评估工作；
- 自动导入：适用于评估工具与平台对接场景，支持平台下发评估计划，直接导入评估工具。

2.1.2 信息收集

NSFOCUS ISCAT 支持收集评估对象信息，包括被检查单位的基本信息、区域信息、系统基本信息、系统服务信息、系统互联信息和系统数据信息等。

2.1.3 合规评估

NSFOCUS ISCAT支持三个合规性标准，并且支持用户自定义评估模板：

- 支持等保 2.0 通用要求和工控系统扩展要求、工信部《工业控制系统信息安全防护指南》、国能安全 36 号文--《电力监控系统安全防护方案》合规性评估；
- 支持用户自定义合规评估模板，允许通过选择各合规性指标而自定义评估内容，以便于完成专项评估任务评估项的快速集成；同时还支持离线自定义模板后自动导入评估工具，方便行业合规性模板接入。

2.1.4 资产安全评估

2.1.4.1 资产信息采集

NSFOCUS ISCAT支持手动录入和自动识别两种方式收集资产信息；支持资产树和网络拓扑两种方式进行资产管理。

2.1.4.2 资产安全评估

NSFOCUS ISCAT 支持基于资产的漏洞扫描和配置核查的全方位资产安全评估

- 漏洞扫描：支持对传统IT类设备和工控OT设备的主机发现、端口扫描、服务识别，支持Windows、Unix/Linux各类操作系统识别，支持各类网络设备及防火墙识别、支持各主流数据库（Oracle、MySql、Postgresql等）漏洞扫描，支持虚拟化组件漏洞扫描；同时为不支持接入扫描的工业场景提供静态扫描功能，通过离线特征比对完成扫描任务；
- 配置核查：支持对上位机设备信息配合核查功能，从账户管理、口令设置、端口管理、应用程序管理、网络服务管理、操作系统安全设置、磁盘管理、日志审计、更新设置、补丁管理等多角度进行配置安全基线核查。

2.1.4.3 视频设备安全评估

NSFOCUS ISCAT支持对在线视频监控设备的检查:

- 支持发现系统内是否有非法视频监控设备接入；
- 支持的测试功能包括但不限于缓冲区溢出、权限验证缺失及绕过；
- 支持的协议包括但不限于RTSP、ONVIF、SIP；
- 支持检查视频监控设备是否开启RTSP，RTSP是否存在弱口令，并检查RTSP视频流传输是否采取了相关加密措施；
- 支持检查视频监控设备是否开启SIP、ONVIF，SIP、ONVIF是否存在弱口令，并检查SIP、ONVIF设备接入是否采取了相关加密措施。

2.1.5 流量安全评估

2.1.5.1 通信流量采集

NSFOCUS ISCAT 支持采集网络流量信息：

- 支持从交换机镜像端口获取数据包用于流量分析；
- 支持在无人值守的情况下通过设置时长或数据总量来限制获取的数据包总量，当获取数据包的时长达到设置时长或设置的数据总量时应停止获取数据流量；

- 支持留档保存流量数据包；
- 支持将获取的流量数据包进行导出供取证归档处理；
- 支持删除获取的流量数据包。

2.1.5.2 流量安全审计

NSFOCUS ISCAT支持进行异常流量分析，包括：

- 支持工控系统组成单元的典型攻击行为检查，组成单元包括工控系统的核心控制单元及上位机软件等；
- 支持实时解析协议数据包，分析威胁异常结果应包括时间日期、规则（即威胁行为的特征表述）、源地址、目标地址、源端口、目标端口、协议类型等；
- 支持生成流量威胁分析综合结果信息。

2.1.5.3 通信流量诊断

NSFOCUS ISCAT支持流量统计分析、工控协议识别及合规性分析、数据包分布统计、诊断数据统计和IP流量统计：

- 流量统计：支持按照时间生成流量曲线图，并计算流量总量；支持按照不同的协议类型、不同的流量类型（包括广播流量、多播流量、单播流量）进行工控数据流量统计；
- 工控协议识别及合规性分析：支持识别和深度解析Modbus/TCP、OPC、S7、S7plus、DNP3.0、IEC104等主流工业协议；
- 数据包分布统计：支持按照数据包大小分段进行数据包大小分布统计；
- 诊断数据统计：支持对TCP会话的相关诊断数据（包括TCP连接被拒绝、TCP重复的连接尝试、TCP重传数据包、TCP重复确认等）、IP首部非法校验和、ICMP端口不可达、TCP端口扫描和ARP请求风暴等进行统计；
- IP流量统计：支持进行IP流量信息统计，统计的信息至少应包括接受数据包数量、接受流量字节数、发送数据包数量、发送流量字节数等。

2.1.6 无线 WIFI 评估

NSFOCUS ISCAT支持对无线WIFI进行安全评估，包括：

- 支持搜索无线WIFI的SSID名称以及对应的MAC地址信息；
- 支持隐藏无线WIFI的SSID搜索功能；
- 支持获取各无线节点所连接的设备相关信息；
- 支持发现无线安全事件以及安全策略配置；
- 支持无线弱密码检查，支持用户自定义无线密码字典。

2.1.7 恶意代码扫描

NSFOCUS ISCAT支持对工业主机进行恶意代码（例如病毒、木马）检查，包括：

- 支持快速检查功能，快速检查系统关键目录,快速检查和发现关键目录中所存在的恶意代码程序；
- 支持全盘检查功能，对系统所有的盘符下的文件进行全面深度检查，帮助发现系统中存在的恶意代码；
- 支持自定义检查功能，对选择的目录进行全面的检查，帮助发现指定检查的目录中是否含有恶意代码，支持快速选择桌面、文档、系统关键目录。

三. 产品特性

NSFOCUS ISCAT 秉持“安全防护从安全评估开始”的理念，始终致力于帮助用户快速、便捷地完成工业网络的合规风险评估，找到差距，以评促改，形成针对工业网络环境的闭环风险管理。产品将持续从纵深检测能力和至上用户体验出发，为用户提供一站式工业网络合规评估解决方案。

- **便携**：采用便携式的硬件设备，功能全、易携带，帮助用户在现场评估并全面评估风险；
- **标准**：集成多个合规性评估模板，包括等保 2.0、工信部指南和国能安全 36 号文；

- **准确**：强大的漏洞库、威胁特征库、设备指纹库、检查知识库以及工业协议库，提高评估的准确性和完整性；
- **易用**：基于用户体验的 UI 设计，采用引导式操作方式，降低用户学习成本，提升用户体验；
- **高效**：支持网络远程评估和离线非接触式评估，同时可以支持用户多人协同工作，提高工作效率。

四. 典型应用及客户价值

《网络安全法》第八条：国家网信部门负责统筹协调，县级以上地方人民政府有关部门的网络安全保护和监督管理职责，明确了监管机构的监管职责；第十七条：国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务，明确了测评机构、安全服务企业和机构的业务方向；第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，明确了关键设施运营企业的责任和义务。NSFOCUS ISCAT 兼具全面的评估功能、便携的硬件设备以及良好的扩展性适配于以下场景的安全评估：

监管机构和测评机构常态化检查：为监管机构和测评机构提供一站式便携评估工具，帮助用户快速、高效、准确的完成检查和测评工作；

工业企业定期自查：帮助工业企业快速定位技术、管理方面的安全风险，满足合规要求的同时，提升自身工控系统的安全性；

工控系统上线前的安全评估：帮助系统供货商、集成商对上线前的工控系统进行风险评估，实现工控系统全生命周期的安全。

五. 售后支持

业务类型	客户支持热线	服务时间
产品售后技术支持	400-818-6868 转接 0	周一至周日 7×24 小时全天服务

	13321167330	
产品服务购买咨询	400-818-6868 转接 1	周一至周五 9：00-17：30
客户意见建议及投诉热线	010-59610080	周一至周五 9：00-17：30
产品售后技术邮箱	support@nsfocus.com	周一至周日 7×24 小时全天服务