绿盟工控入侵检测系统

产品白皮书

【绿盟科技】

■ **文档编号**	NSF-IDS-ICS 产品白皮书	■ **密级**	内部使用
■ **版本编号**	V1.2	■ **日期**	2019-05-13
■**撰 写 人**		■ **批准人**	

■ **版权声明**

■ **版本变更记录**

时间	版本	说明	修改人

一. 产品概述

绿盟工控入侵检测系统是一款面向工业控制领域的入侵检测类产品。通过分析从网络关键节点处收集到的信息，发现是否存在违反已知或者自定义安全策略的异常行为，这样扩展了安全维护人员的管理能力。

入侵检测的流程大致分为：“信息源”、“信息采集”、“预处理”、“检测模型”、“检测结果”、“响应处理”六个模块，系统能够快速捕获批量数据包，并进行深度解析。如果获取的数据包存在已知的安全隐患或恶意迹象，入侵检测系统就会在系统受到危害之前进行报警操作；针对未知威胁，工控 IDS 通过绿盟云识别。

可以对工业控制系统可能面临的攻击行为进行有效检测，并通过事前告警、事中防护、事后取证三个角度，为工业企业用户提供一套可视化的适用于工业企业业务特性的解决方案，提升工业企业生产运营的安全性。

绿盟工控入侵检测系统可以适用于电网、发电、石油石化、市政、烟草等行业，供热，水利水务，智能制造等多种工控场景，为相关行业的业务稳定运行保驾护航。

二. 客户价值

面对新一代工控网络威胁的挑战，绿盟科技根据多年攻防研究积累、以及产品研发经验，推出了工控网络入侵检测系统（NSFOCUS IDS-ICS）。NSFOCUS IDS-ICS 具备国际领先的攻击特征库和即时更新的信誉库；为应对高级威胁，集成了云沙箱检测能力，实现了对已知和未知威胁的立体检测；采用流式病毒检测技术，捕获热点病毒，极大地增强防病毒能力；绿盟 IDS-ICS 为用户提供了一套“看得见、检得出、防得住”的全新工控入侵检测解决方案

绿盟工控入侵检测系统可以：

- 及时发现生产系统中潜在的攻击行为：绿盟工控 IDS-ICS 内置了多达 9600 多条规则库，检测覆盖 2~7 层的各种入侵攻击，可实时预警工控网络中发生的病毒木马后门等，通过工业流量分析、工业应用识别和工业攻击检测功能，用户可以清晰、直

观地感知网络内的流量异常变化、应用构成情况以及存在的攻击行为，为制定安全策略提供有力的信息支撑；

- 及时发现生产系统中潜在的异常操作行为：绿盟工控 IDS 支持多种工控协议的深度解析，可量身定制来监测工控网络中的敏感操控，可通过自学习的方式建立默认模板，客户也可以在自学习模板的基础上手动修改深度解析工控协议中的阈值，从而建立业务安全度更高的异常操作检测；
- 多样异常日志统计分析：多维度的 IDS 异常日志时间记录分析报表，给事件追朔提供强力的证据。
- 满足相关的合规性要求：如发改委 14 号要求、等保要求；
- 图形化的“组态级”的配置，有效减轻客户运维负担。

三. 产品优势

绿盟工控入侵检测系统的优势集中体现在以下几个方面：

- 工业通信协议的深度过滤

绿盟工控入侵检测系统可以针对工业协议进行深度解析，可以针对工业网络协议的内容和数据进行细致的合规性检查，对于操作指令中包含的针对点表、寄存器的异常操作进行报警，最大限度地保护控制系统的安全。

- 符合工业用户使用习惯的配置方式

工业中广泛应用的组态软件将专业的工艺流程、复杂的数据反馈封装成简单的图形化界面，直观的反映工业现场的生产情况。组态软件以其图形化、直观性和易用性深受广大工业用户的喜爱，也成为工业用户习惯的使用方式。绿盟工控入侵检测系统设计和开发时也力求作到专业，简单、直观、易用。

- 涵盖利用主流漏洞库中漏洞进行攻击的检测

绿盟工控入侵检测系统可以针对西门子、施耐德、ABB、AB，和利时，上海新华，倍福等主流工业控制系统的控制器的漏洞利用过程进行有效检测，可以针对主流上位机 WellinTech、Advantech、WINCC，citect等漏洞利用的过程进行检测。

- 工业级产品可靠性保障

为了适应工业网络环境对于产品可靠性的要求，绿盟工控入侵检测系统采用工业级产品设计，在环境适应性、散热、故障处理等方面进行了全面的优化。

绿盟工控入侵检测系统硬件平台专门面向工业应用场合设计，对PCB、电源、机箱结构、散热进行全面优化，采用低功耗、宽温、宽压电子元器件，无风扇传导散热，充分的减少产品的发热量，提高产品的稳定性和环境适应性，保证设备在各种恶劣环境下可以持续、稳定的运行。

四. 关键功能

4.1 智能协议识别和辅助规则生成

工业网络中设备众多、网络通信复杂，用户很难全面的掌握网络中所必须的业务通信需求，这会给入侵检测的规则配置带来很大的困难。为了方便用户进行入侵检测规则配置，提高规则配置的准确性，减少规则配置的工作量，绿盟工控入侵检测系统开发了智能协议识别和辅助规则生成功能。

智能协议识别功能采用被动检测的方式从网络中采集数据包，并进行数据包的解析，智能的与系统内置的协议特征、设备对象等进行匹配，生成可供参考的网络交互信息列表，通过对协议分布和流量信息的匹配，形成“网络流量行为基线”，帮助用户以最捷的方式了解和掌握网络中的业务通信状态，发现网络潜在的安全。

智能化的流量自学习规则，还可以辅助系统自动生成相关的异常检测规则，对现有的规则进行调优等。

4.2 “组态化”的配置模板

工业控制系统与传统 IT 系统在配置上和业务类型上存在较大的差异性，绿盟工控入侵检测系统可以提供基于组态的配置模板，可以针对客户的业务场景通过模板进行场景化的配置，方便现场的操作人员对规则进行配置和使用，使用上符合现场操作人员对工控系统的使

用习惯。通过预制的设备类型和应用场景，用户无需关注具体的规则设备，只需要配置场景就可以实现在应用场景内的规则配置和应用。

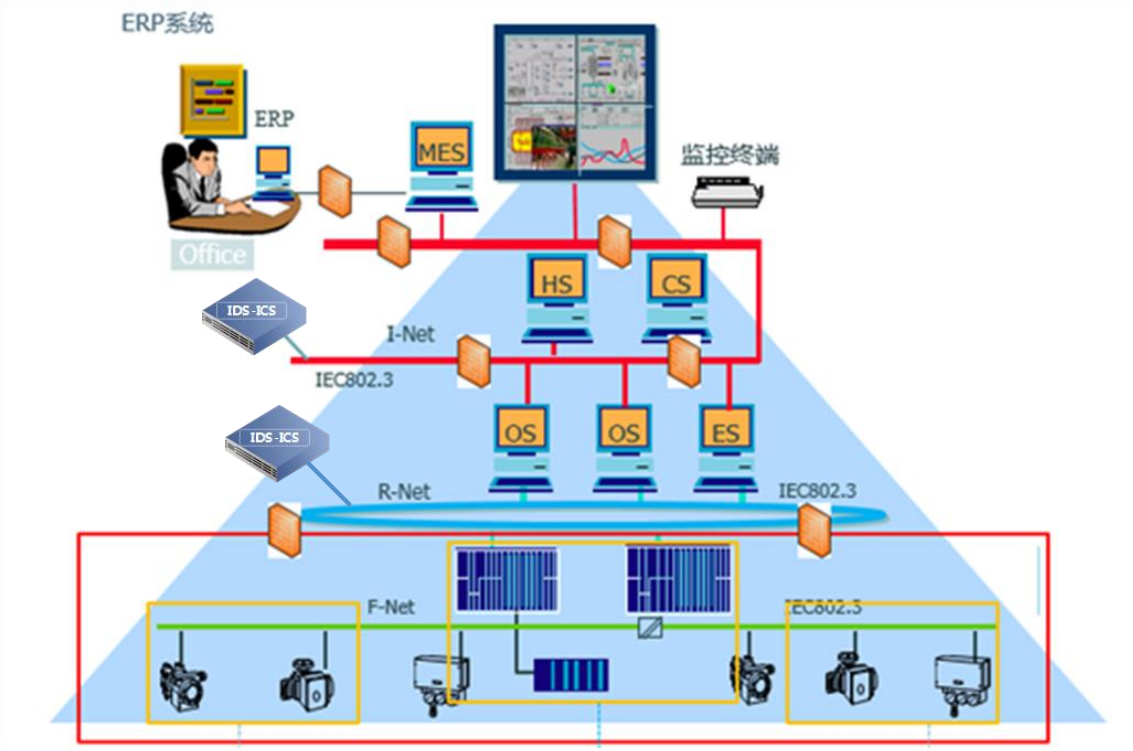
4.3 强大的安全防护能力

- **工控协议识别：**绿盟工控入侵检测系统支持 ModBus TCP、IEC-60870-5-104、C37.118、OPC UA、profinet、DNP3 等协议的解析和识别，解析内容包括源目的 IP、源目的端口、协议名称、协议内容等。
- **工控入侵检测：**绿盟工控入侵检测系统可以对 PLC 等控制设备的拒绝服务攻击漏洞（CVE-2013-2784）、缓冲区溢出攻击漏洞（CVE-2014-0768）等典型工控漏洞的攻击行为进行有效识别，并产生告警信息。
- **深层攻击发现：**绿盟工控入侵检测系统提供基于流的应用识别技术，可准确识别非标准端口应用、以及 HTTP 协议隧道中 Web2.0 应用，发现隐藏在应用中的攻击行为。
- **高级威胁检测：**绿盟工控入侵检测系统能够基于敏感数据的外泄、文件识别、服务器非法外联等异常行为检测，实现内网的高级威胁防护功能。
- **减少虚假告警：**传统 IDS 单纯分析数据包，脱离数据所处环境信息的检测方式，导致诸如：目标系统运行的是 Apache 软件，却产生了大量针对 IIS 的虚假告警事件的情况发生。绿盟工控入侵检测系统结合信誉机制、用户身份、地理位置、用户资产等上下文信息进行检测，能够显著减少虚假告警事件的产生。
- **快速威胁响应：**作为微软 MAPP 成员，绿盟科技可在 24 小时内快速发布入侵检测规则，并第一时间分发到用户设备中，实现快速威胁响应。

五、典型应用

部署在生产控制区域与信息系统区域的边界处，实现从信息系统到控制系统流量的安全性检测，发现潜在的攻击和异常行为。

部署在生产区域内部，旁路部署于 DCS、PLC 系统内部网络柜网络交换机上，对可能针对 DPU、PLC 等控制装置发动的攻击行为进行有效检测和预防。


ERP系统
ERP
MES
监控终端
Office
HS
CS
IDS-ICS
I-Net
IEC802.3
OS
OS
ES
IDS-ICS
R-Net
IEC802.3
F-Net
IEC802.3