绿盟工控安全入侵检测系统产品彩页

1. 产品概述

绿盟工控安全入侵检测系统（NSFOCUS IDS-ICS）实时检测网络通信，精确识别缓冲区溢出、扫描攻击、DoS/DDoS、SQL 注入、蠕虫病毒、木马、间谍软件等传统攻击行为也可以根据内置规则库中的工控规则库，实现专门针对工控的攻击行为检测，采用自学习基线模型方式，可自定义已深度解析的工控协议安全策略，深度业务关联检测异常操作，生成多样化的告警方式，及时向管理员发送预警信息，并能够与工业防火墙等网关防护产品形成纵深防护体系。

2. 客户价值

- **攻击预警**

  内置超过 9600 多条的攻击特征库，实时检测 2~7 层的各种入侵攻击及违规行为，第一时间通知管理员采取进一步的防护措施。

- **攻击取证**

© 2019 绿盟科技
密级：内部使用

提供详细的日志保存及报表展示功能，可作为针对入侵者采取进一步法律行动的有力证据。

- **流量可视**

  通过 NSFOCUSIDS-ICS 的流量分析、应用识别和攻击检测功能，用户可以清晰、直观地感知网络内的流量异常变化、工控协议匹配，工控业务应用，流量分类情况以及存在的攻击及违规行为，为制定工控安全策略提供充分的数据支撑。

- **法规遵从**

  提供 2~7 层双向深度入侵检测解决方案，有助于组织用户满足等级保护、分级保护以及相关行业法规的要求，增强合规能力。

3. 产品优势

- **卓越的数据处理性能**

  系统采用业界领先的多核计算平台，融合绿盟科技自主研发的专业安全操作系统，拥有高吞吐量、低延时的卓越处理性能。

- **先进的智能协议分析技术**

  独有的智能协议识别技术，通过动态分析网络报文中的协议特征，准确识别各类攻击行为和异常网络流量，高速、准确地检测出通过动态端口或者智能隧道实施的恶意入侵，全面覆盖国内外主流工控厂家：西门子，施耐德，罗克韦尔，ABB，和利时，倍福等，支持：IEC-61850-MMS、GOOSE、SV， IEC-60870-102/103/104，ModbusTCP、S7、DNP3、ProfinetIO ，M5，M6 协议的识别和深度解析。

- **强大的抗攻击规避能力**

  完备的协议异常控制结构，高效的 IP 数据包重组策略，以及独特的协议数据汇聚体系，能够有效识别各类攻击规避技术，为用户提供最可靠的安全防护能力。

- **领先的用户身份识别技术**

  国内首创基于用户身份识别的入侵检测技术，有别于传统基于 IP 地址的检测方式，可以快速、准确定位内网攻击及违规行为责任人。

- **可扩展的入侵防护能力**

  灵活的、易于扩展的产品架构设计，为用户提供可自定义的威胁检测能力，丰富的安全响应能力，同时支持向工控网络入侵防护系统的无缝平滑升级，为用户提供更可靠的保护。

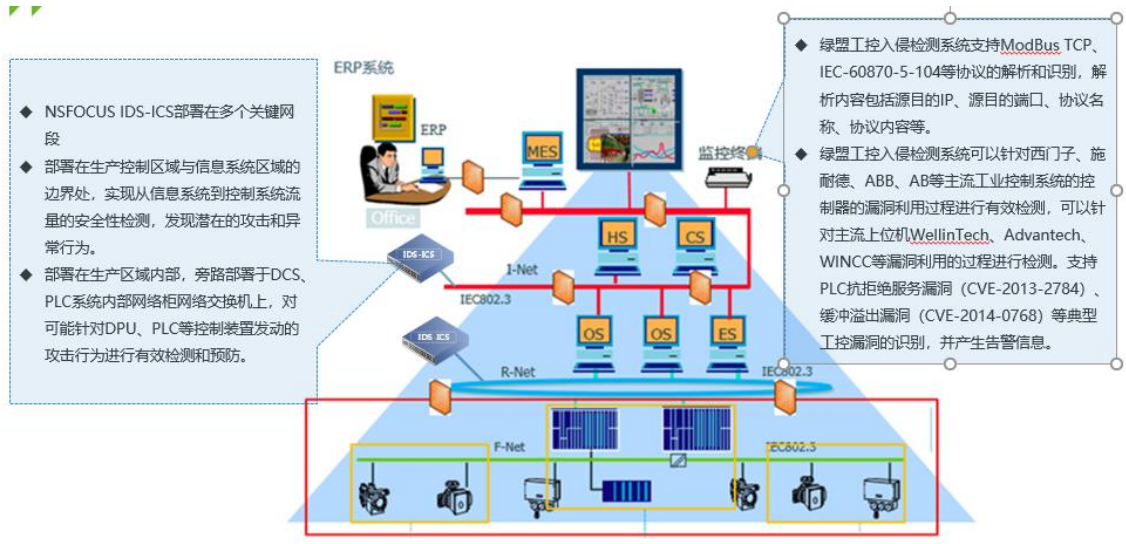
© 2019 绿盟科技
密级：内部使用

4. 关键功能

- 入侵检测
  - 可检测缓冲区溢出、SQL 注入、XSS 跨站脚本、暴力猜测、DoS 攻击、扫描探测、非授权访问、网页挂马、蠕虫病毒、后门木马、间谍软件、僵尸网络、零日攻击、可疑网络活动等各类攻击；检测分析工控网络中资产漏洞，系统漏洞，典型工控攻击性行为，
  - 支持自定义规则
- Web 安全监测
  - Web 信誉监测，URL 分类过滤监测
- 流量分析
  - 总流量监控、上下行协议流量监控、上下行 IP 流量监控
  - 深度协议解析监控
- 管理方式
  - 单机管理、集中管理、主辅管理
- 升级管理
  - 支持在线升级、离线升级
- 日志&报表
  - 缺省内置丰富的报表模板
  - 支持自定义报表
  - 支持 Word、Excel、Html 等多种文件格式
  - 支持自动生成报表

5. 典型应用

绿盟科技针对越来越复杂的工业网络环境，提供了可管理的工控入侵检测解决方案，将 NSFOCUS IDS-ICS 部署在工控网的多个关键网段，如：生产区、管理区、数据转送区，同时通过绿盟安全中心实现对多台工控安全入侵探测器的集中管理，实时掌握全网安全状况。



© 2019 绿盟科技
密级：内部使用