NSFOCUS

ICSScan

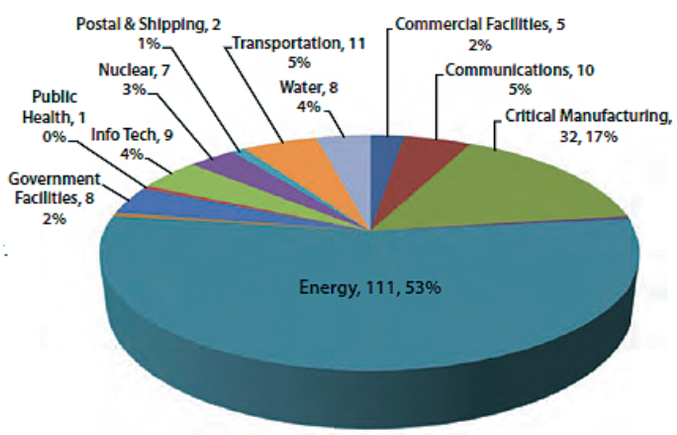
绿盟工控漏洞扫描系统
NSFOCUS Industrial Control Systems Vulnerability Scanning System

THE EXPERT BEHIND GIANTS

一. 工控安全态势日益严峻

工业控制系统（Industrial Control Systems，ICS）广泛应用于工业、电力、能源、交通运输、水利、公用事业和生产制造业。工业控制系统通过对机械装置、交通工具、实验装置、仪器仪表等工业设备进行自动化监测、指挥、控制和调节，保证工业设施的正常运转，是国家关键基础设施和信息系统的重要组成部分。

根据ICS-CERT监测，仅是2012年10月至2013年3月期间，就发生200多起工业控制系统安全事件，其中主要集中在能源、关键制造业、交通、通信、水利、核能等领域，而能源行业的安全事故则超过了一半。



近年来，工业控制系统相关的安全事件正在呈快速增长的趋势。但广大工控系统使用者因为缺乏相关的工控漏洞检测手段，不能及时有效的发现工控系统中的安全隐患，为系统上线后的安全埋下了隐患。

二. 绿盟工控漏洞扫描系统

绿盟科技作为国内最具实力的网络与信息安全产品和服务提供商，为协助客户尽早发现工控系统中存在的安全隐患，凭借自身十多年的漏洞挖掘与分析检测经验，研发了国内首款工控漏洞扫描系统。

绿盟工控漏洞扫描系统（NSFOCUS Industrial Control Systems Vulnerability Scanning System，简称NSFOCUS ICSScan）可以通过远程安全评估的方式，批量发现工控设备、工控软件以及支撑他们运行的服务器、数据库、网络设备的安全风险。

三. 产品功能

3.1 工业控制及网络系统安全漏洞扫描

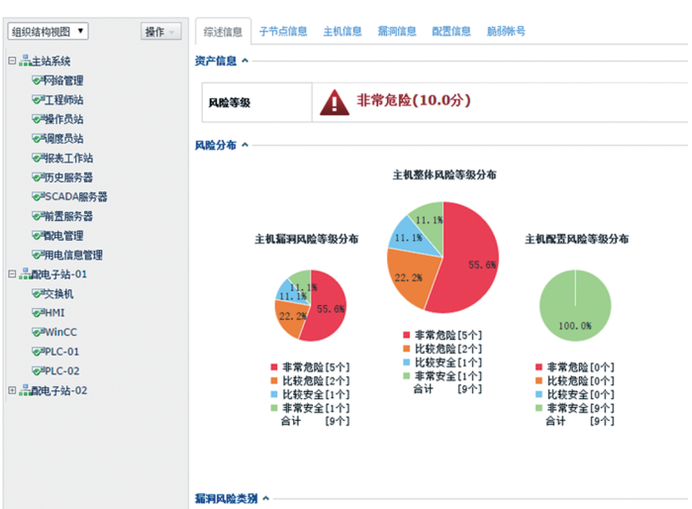
- 对二十余个品牌的工业控制设备/系统，比如SCADA、DCS、PLC

等，以及处于上游的数字化设计制造软件进行漏洞扫描；支持Modbus TCP、西门子S7等主流工控协议。

- **12000+**：IT系统漏洞扫描插件，涵盖主流操作系统、数据库、中间件、通信协议、应用系统、虚拟化系统、网络设备、安全设备、办公自动化产品。
- **3000+**：检查项目，涵盖七大类三十余种产品的近百个版本：操作系统、网络与安全设备、数据库、应用系统、虚拟化产品。
- **600+**：WEB应用漏洞扫描插件，全面检测SQL注入、跨站脚本运行、信息泄露、越权等WEB应用系统安全漏洞。
- 弱口令检测功能：支持操作系统、应用服务、数据库等十余种协议或系统的弱口令检测。支持内置字典与外挂字典。

3.2 资产管理

- 建立工控资产组织树形结构，定义工控资产信息与责任人信息。
- 可手工导入或自动发现各类资产，并自动归入相应组织结构。
- 可实现下发任务、查看结果、查看安全状态、查看资产信息等全部业务功能。



3.3 风险分析与展现

- 仪表盘：在首页展示当前工控系统安全状态，第一时间获得工控系统安全风险态势数据。
- 告警平台：将发现的工控系统安全风险全部展现在告警平台上。
- 任务报表：简明直观的任务报表，可以自定义报表内容和报表输出格式。

四. 应用场景与部署模式

绿盟工控漏洞扫描系统应用场景：

- 协助工控系统用户顺利完成等保安全建设和日常安全检查；
- 协助国家/行业监管机构完善工控系统安全检查能力；
- 协助评估/测评机构强化对工控客户服务能力，完善测评技术手段。

绿盟工控漏洞扫描系统采用远程访问的方式，网络可达即可；连接现有的网络，不做网络的任何修改；可覆盖传统的IT系统，也可覆盖工控系统，如下图所示：