工业安全隔离网闸系统

产品概述

工控漏洞扫描系统能够全面、精准地检测信息系统中存在的各种脆弱性问题，包括各种安全漏洞、安全配置问题、不合规行为等，在信息系统受到危害之前为管理员提供专业、有效的漏洞分析和修补建议。并结合可信的漏洞管理流程对漏洞进行预警、扫描、修复、审计，防患于未然。

产品特点

- 空间资产探测

自动生成网络拓扑，方便用户快速发现、统计全网信息资产，了解安全风险等级。

- 系统漏洞扫描

全方位、多侧面对系统进行实时、定期的系统漏洞扫描和分析。

- WEB 漏洞扫描

全面支持 OWASP TOP 10、敏感关键字、挂马、暗链、钓鱼等漏洞检测。

- 数据库漏洞扫描

支持十余种数据库，内置扫描芜略超 2000 条，并可发现数据库中潜藏的木马。

- 基线配置核查

对目标系统进行自动化的基线检测、分析，并提供专业的配置加固建议与合规性报表。

- 工控漏洞扫描

支持对主流的工业控制系统进行漏洞扫猫和分析，支持远程检测及离线比对方式。丰富的漏洞知识库方便用户及时发现漏洞，通过安全加固降低因工控漏洞带来的经济风险。

- 内 WIFI 安全检测

支持对 WIFI 无线网络进行安全检测并生成 WIFI 安全检测报告。

- Docker 漏洞扫描

可检测 Docker 漏洞、Docker 镜像漏洞、木马后门以及不安全配置。

- 大数据漏洞扫描

支持对主流大数据平台组件进行漏洞扫描和安全 配置合规性检查。

- 视频监控安全检测

可以对视频监控系统进行漏洞扫描，涵盖了视 频监控系统的各种操作系统、网络服务、弱口令。

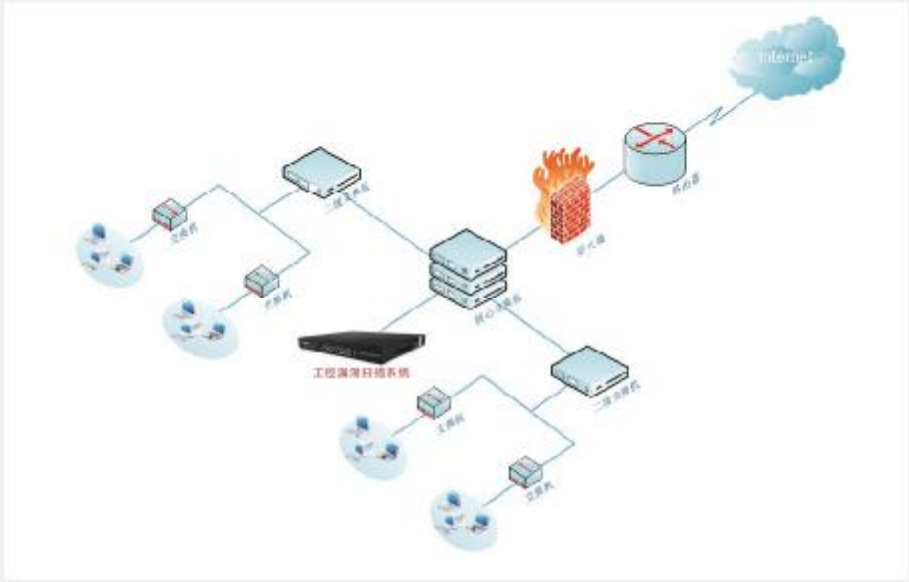
- Windows 安全加固

支持对 Windows 操作系统的配置网络、接入、日志、防护等方面进行自动和手动安全加固。

- 全网分布式管理

提供全网分布式管理功能，从而实现了对大规模网络实时、定时的漏洞扫描和风险评估。

典型部署



江南三体河北信息安全技术有限公司

地址：河北省廊坊市广阳区友谊路462号

网址：http://www.stiot.net

邮箱：jnst@jnsanti.net