

产品概述

天融信工控安全検査工具箱系统简称“工具箱”是等级保护2.0大背景下，为工业控制系统信息安全検査工作推出的一款安全评估产品。工具箱结合多年技术积累，支持市场上主流的工控设备识别、工控协议分析、工控漏洞定位、工控风险评估检查；能帮助用户发现工业控制网络中的资产信息，包括工控设备、服务器、网络通信设备、安全防御设备等，支持生成工业控制网络拓扑，帮助客户梳理现有网络架构。结合天融信专用的工业漏洞库、工控设备库、工控威胁特征库、工控协议库等，帮助用户完成多维度安全风险评估，同时生成详实的漏洞分析报告和安全风险解决建议，协助提升工业控制系统整体安全防护能力。



产品特点

检查指标灵活多样

工具箱集成《GB/T22239-2019信息安全技术网络安全等级保护基本要求》、《工业控制系统信息安全防护指南》、《电力监控系统安全评估规范》、《工业控制系统信息安全评估规范》等常见评估标准，支持通信流量、无线网络、漏洞扫描、配置核查等多种组合检查模型，可实施多重、快速、自定义的安全检查评估。

网络信息全面掌握

工具箱内置丰富的工控设备指纹库、威胁特征库、工控协议库、工控漏洞库，可识别工业控制网络中的资产信息，生成资产清单，生成工控网络拓扑图，帮助客户全面掌握工业控制系统运行状态信息。

安全漏洞无损探测

工具箱结合专用的工控漏洞库，可以采用无损式漏洞探测技术，智能匹配工控设备指纹信息，自动发现系统资产的漏洞信息，保证执行检查过程中不影响网络设备的稳定运行和正常通讯。

异常行为及时发现

工具箱采用被动接收网络流量的方式，激活流量分析引擎，实现流量统计、数据分析、文档生成、DNS查询及威胁检测，同时匹配专用的威胁特征库和异常行为检测规则库，可快速识别网络中的异常行为。

配置核查 洞察基线

工具箱内置核查引擎，快速获取系统配置信息，帮助用户了解终端威胁情况，支持多种协议远程登陆目标系统远程基线核查，同时支持Agent本地检测，不对系统配置进行任何修改，确保业务持续性和业务安全。

军工级 便携加固硬件

工具箱依托军工级加固笔记本，采用便携式软硬件一体化设计，适应各种工业生产控制场景；结合安全评估内容和流程，提供简易的操作界面，可快速完成工业现场的安全评估工作。

典型应用

工业控制系统安全评估典型应用

工具箱旁路部署的接入方式可以以最高的效率和精度对工控系统的安全风险评估检查，并根据工业控制系统实际运行环境，依据专业的工控系统漏洞库完善漏洞库，提升工控系统安全。高效的评估工作，采用工控系统漏洞库对工控系统进行漏洞扫描并生成详细的漏洞分析结果和安全风险的解决方案，帮助工业企业客户提升工控系统整体安全性能。

