

# 谛听——工业网络空间安全态势感知系统

DIRECTING THE INDUSTRY NETWORK SPACE  
SECURITY SITUATION AWARENESS SYSTEM

为工业 4.0 保驾护航 · 助您赢在工控安全



辨工控网间之万物 探恶意漏洞以补天




电话: 4000-680-620 传真: 010-62971782

邮箱: support@winicssec.com 邮编: 100085

微博: <http://weibo.com/winicssec>

微信公众号: 威努特工控安全

地址: 北京市海淀区上地三街9号嘉华大厦F座907室

 北京威努特技术有限公司  
[www.winicssec.com](http://www.winicssec.com)

## 系统概述 / Product Overview

“谛听”（DITECTING）工业网络空间安全态势感知系统（www.ditecting.com）是为顺应国家网络空间安全形势，由东北大学“谛听”网络安全团队基于自身传统安全研究的优势，与国内工控安全领军企业北京威努特技术有限公司联合开发，意在辨识暴露在工业网络空间里的工业控制系统联网设备，帮助安全厂家维护工控系统安全、循迹恶意企图人士。

谛听工业网络空间安全态势感知系统支持 Siemens S7、Modbus、IEC 60870-5-104、DNP3 等 12 种工控服务的指纹识别，可实现对全球工控设备信息和开放常规服务的隐匿探测和全局采集，同时准确定位工控设备。该搜索引擎为用户提供了查看工控服务、厂商、设备的搜索入口，用户也可根据搜索语法自定义搜索，通过可视化统计报告直观展示全球工控设备的区域分布情况、十二种工控系统服务的使用和工控系统上常规服务开放情况，提供全球工业网络空间安全威胁态势感知，为工控安全发展提供真实的数据支持。

“谛听”系统定位于工业网络空间的搜索引擎，其搜索信息全面，信息丰富，范围广效率高，对于评估工业控制系统的安全性，推动国家关键基础设施的信息安全保障工作有极为重要的意义。

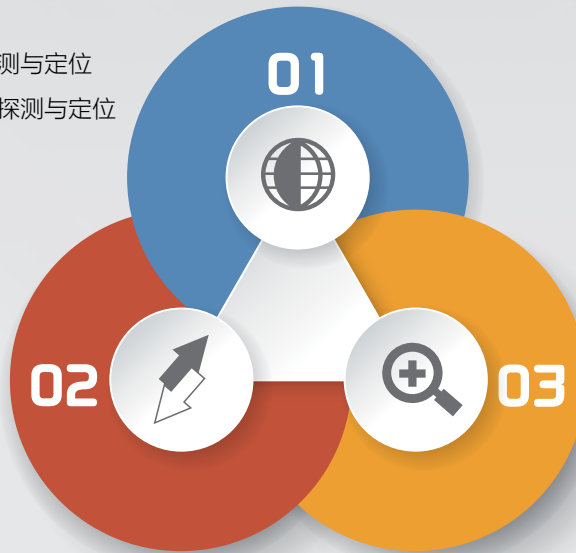
## 功能特性 / Features

### 工控设备全网在线探测

- 全球工控协议及设备的探测与定位
- 网络设备及物联网设备的探测与定位
- 常规服务的探测与定位

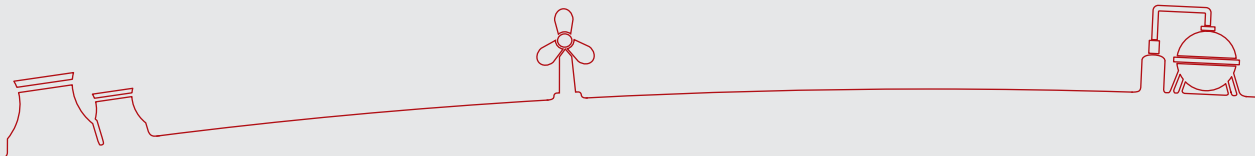
### 工控系统漏洞态势感知

- 工控系统漏洞扫描，漏洞库覆盖 CVE、CNNVD 等国际和国家级漏洞库
- 工控系统漏洞、设备资产智能分析及安全评分



### 全球威胁可视化

- 扫描全球网络的工控系统及常规服务
- 多维度展示扫描分析结果，并以地域图、柱状图、饼图、多层饼图等形式呈现



## 系统优势 / Product Advantages

### ★ 广泛的工控协议支持

支持 Siemens S7、Modbus、IEC 60870-5-104、DNP3、EtherNet/IP、BACnet、Tridium Niagara Fox、OMRON FINS、PCWorx、ProConOs、MELSEC-Q、Crimson V3 等多种工控服务协议指纹识别，能获取使用这些协议的工控设备的基本信息，同时也可识别常规服务。

工控协议主题简介  
Protocols

Service	Records	Port	Wiki
Siemens S7	Port 102	TCP 102	Wikipedia
Modbus	Port 502	TCP 502	Wikipedia
IEC 60870-5-104	Port 2404	TCP 2404	Wikipedia
DNP3	Port 20000	TCP 20000	Wikipedia
EtherNet/IP	Port 44818	TCP 44818	Wikipedia
BACnet	Port 47808	TCP 47808	Wikipedia
Tridium Niagara Fox	Port 1911	TCP 1911	Wikipedia
OMRON FINS	Port 9600	TCP 9600	Wikipedia
PCWorx	Port 1962	TCP 1962	Wikipedia
ProConOs	Port 20547	TCP 20547	Wikipedia
MELSEC-Q	Port 5007	TCP 5007	Wikipedia
Crimson V3	Port 789	TCP 789	Wikipedia

### ★ 高并发、动态自适应的分布式隐匿探测

工控设备在网络空间分布广泛，地址空间巨大，本系统基于多线程技术建立分布式探测架构，整合优势网络资源实现工控设备的高并发扫描，研究并实现了基于时区 / 流量分布特性的优化扫描算法，实现了对全球工控设备信息和开放常规服务的隐匿探测和全局采集。

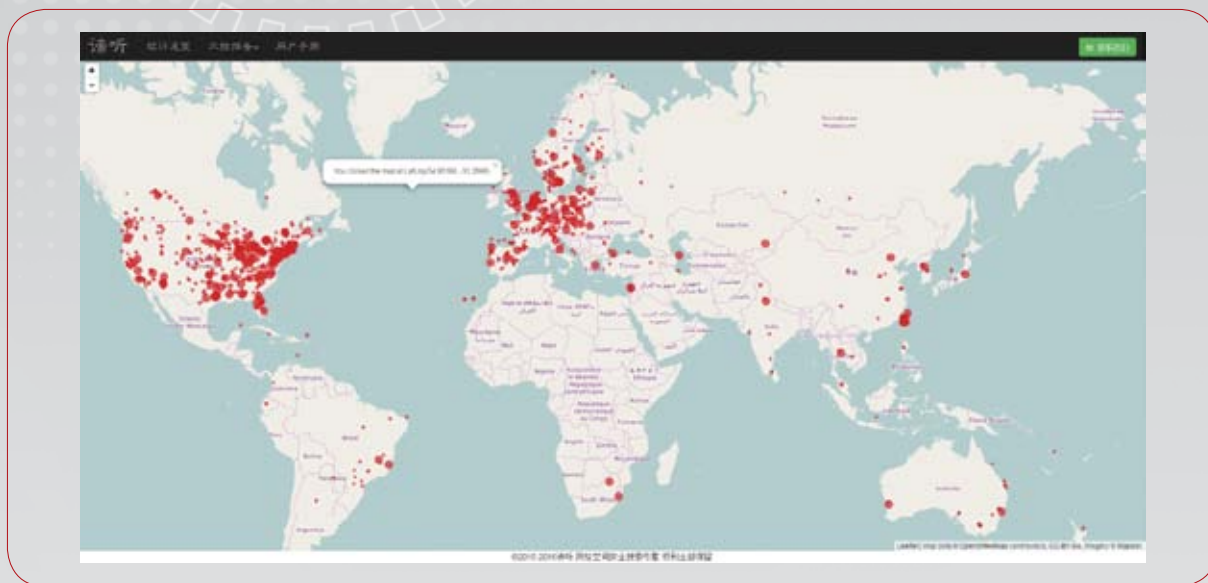
### ★ 工业控制设备的精确定位与综合分析

通过全面采集和分析工控设备信息，对其进行精准定位，最小粒度可定位到某一省份的具体某一企业 / 单位。



### ★ 全球工控设备态势感知

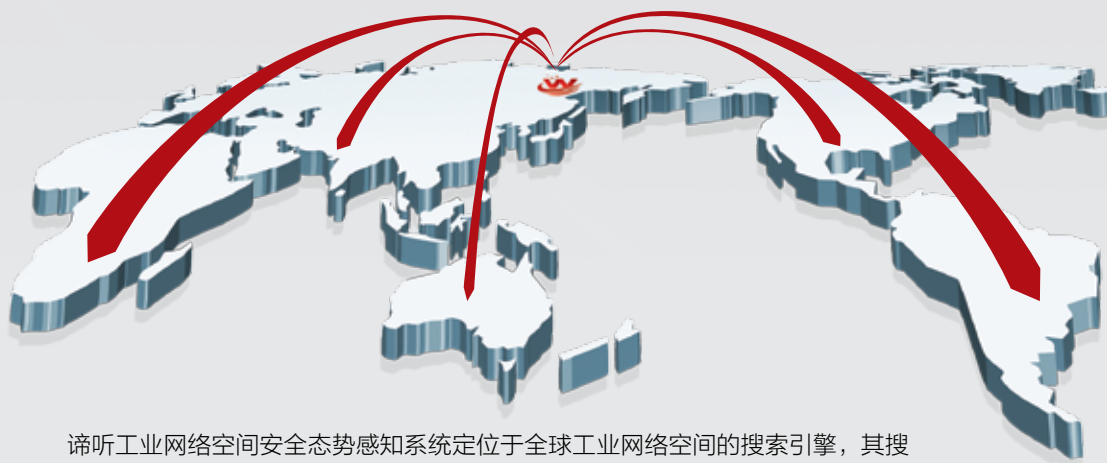
本系统研究并实现基于全球地理位置信息的工控设备可视化展示模块，实现了工控设备全球网络空间安全态势感知及威胁分布信息展示，同时从多维度展示工控设备属性的分析结果，并以地域图、柱状图、饼图、多层饼图等形式呈现。



### ★ 工控系统及常规服务的漏洞扫描与分析

本系统的工控系统漏洞库涵盖了 CVE、CNNVD 等国际和国家级漏洞库，以及威努特工控安全漏洞研究成果，针对 PLC 设备漏洞、上位机软件漏洞和弱点、VxWorks 系统漏洞、摄像头漏洞、应用程序 SQL 漏洞、系统文件上传漏洞等进行漏洞扫描，为厂商提供安全解决方案。

## —— 系统价值 / Product Values



谛听工业网络安全态势感知系统定位于全球工业网络空间的搜索引擎，其搜索维度多，信息丰富，范围广效率高，并提供多维数据分析结果，能够为维护工控设备及系统安全提供有效保障，对于评估工业控制系统的安全性，推动国家关键基础设施的信息安全保障工作有极为重要的意义。