onward SECURITY
a DEKRA company

HERCULE
SecDevice

物联网设备漏洞检测工具

SecDevice 是针对连网产品所设计的自动化安全评估工具，具备模糊测试，网页安全测试与后門扫描等功能，并采用专利 AI 学习技术，加速漏洞检测时间与正确性。测试评估的范围涵盖 IEC 62443、OWASP TOP 10 及 CWE/SANS TOP 25 等网络安全标准。

Global InfoSec Awards 2022
• Most Innovative Compliance Automation

2022 IT World Awards
• Hot Technology of the Year
• Security Software

产品特色

- **针对物联网产品安全：**
  针对连网产品的安全检测而设计，通过以太网络或无线网络与待测设备连接，可自动化分析与测试待测设备的安全性，同时支持自动化连续性测试，减少人工介入时间。
- **多样化漏洞测试手法：**
  采用模糊测试、网络漏洞扫描、网页漏洞扫描及 DoS 等测试手法，可发掘已知与未知漏洞，涵盖操作系统、网络应用程序、网络协议、网页及无线安全漏洞等。
- **TCF 智能化检测技术：**
  使用 AI 技术学习网络封包，协助测试人员检测各种客制化网络协议漏洞，提升检测的覆盖程度与完整程度。
- **完整的测试纪录：**
  可记录检测过程中的攻击封包与测试方法，提供明确的漏洞发生原因与相关佐证数据，以协助用户快速审查产品安全问题。

简单	整合	高覆蓋
三个步骤开始扫描	包含连网设备 所需的安全测项	超过 170+ 个安全测项 与专利精准测试方法

步骤一 选择测试项目 步骤二 选择测试目标 步骤三 开始测试	· 埠自动识别 · 网页安全测试 · 模糊测试 · 无线网路测试 · 漏洞利用	· 系统层漏洞 · 网路层漏洞 · 协议层漏洞 · 网页层漏洞 · 无线层漏洞

产品效益

- **降低人力与工具成本：**
  节省网络安全工作人员的养成时间，并降低多套工具的采购负担。
- **减轻专业依赖：**
  简单的操作设计，让测试人员能轻易上手，并通过详细的测试纪录， 有效协助开发人员解决问题。
- **提升产品安全测试的完整性：**
  专利 AI 学习技术可支持检测客制化协议安全性，弥补传统安全测试方法的不足。

Contact us - contact@onwardsecurity.com
Learn more at - www.onwardsecurity.com.cn

产品技术规格

SecDevice 使用已知与未知漏洞检测技术，针对待测设备的下列目标进行网络端的漏洞检测：

网络安全	基于 IPv4 或 IPv6 的寻址技术，通过网络对目标发送安全测试封包，其测试范围涵盖待测设备的操作系统与应用程序。
网页安全	基于网址 (URL) 定义的测试目标，针对多数连网设备提供的网页式操作介面，检测其网站应用程序的安全性。
无线安全	基于服务设置标识符 (SSID) 定义测试目标，针对设备提供的无线联机服务，分析是否存在安全漏洞。

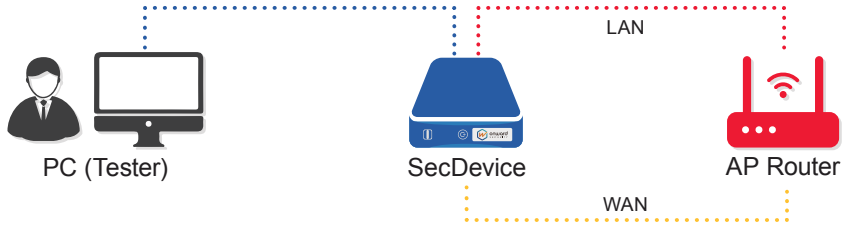
支持通讯协议

Core Network	ARP, ETHERNET, ICMP(v4/v6), IGMPv3, IP(v4/v6), TCP(v4/v6), UDP(v4/v6)
IIoT	BACnet, CoAP, DNP3, EtherNet / IP, FINS, S7comm, IEC 60870-5-104, IEC 61850(Goose/MMS/Sampled Value), Modbus, OPC UA, ProfitNet
Network Management	CWMP, DHCP(v4/v6), DNS, LDAPv3, NTP, OCSP, PPTP, SIP, SNMP(v1/v2/v3/trap), SSHv2, TFTP, Telnet, TLS 1.2, UPnP, IPsec, RADIUS, IKEv2, IPMI, NFSv4, VLAN, FTP, BGP, BFD

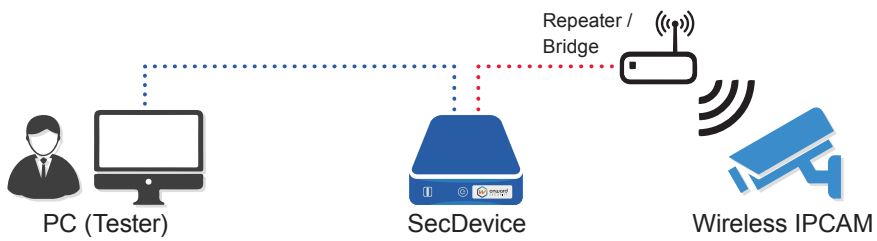
File System	CIFS/SMB
Web Application	HTTP, WEB Fuzz(Including XML and JSON format)
VoIP/IMS	RTP, RTCP, RTSP
Wireless	802.11 WLAN Client / AP 802.11 WPA Client / AP

产品使用情境

单一个网络联机接口的连网设备
例如：工控设备或医疗设备



两个网络联机接口的连网设备
例如：网通设备



无线网络的连网设备
例如：监控设备