



# SCADA Scan

Portable Plug & Scan ICS/SCADA Network Assessment System



## Introducing SCADA Scan

SCADA Scan is a portable ICS/SCADA network assessment system that conveniently plugs into a network switch, and within minutes of passive monitoring provides:

- Audit data for regulatory and regional critical infrastructure audit requirements (e.g. NERC, NIST, ISO)
- Security data for first responders
- Comprehensive network mapping
- Asset discovery
- Vulnerability assessment
- Real-time threat detection

## Portable Solution Ideal For:

- ICS-CERTs and first responders
- Regulators
- Auditors
- MSSPs and MSPs
- Multi-site ICS organizations

## Discover your entire OT network and manage your assets

SCADA Scan automatically generates a comprehensive network topology chart (netmap) that includes:

- All IT and OT network components connected to the scanner, and their attributes, including vendor, model, device type, Purdue level, role, MAC address, IP addresses, OS, software/firmware version and associated vulnerabilities.
- Communication protocol analysis, which details the protocols being used between every two nodes in the network, whether these are SCADA/OT protocols, non-SCADA (IT) protocols, or combined.
- IT/OT network touch points allowing to identify areas of risk.



Real-Time Netmap



SCADA Scan Critical Alert

## Understand your vulnerabilities

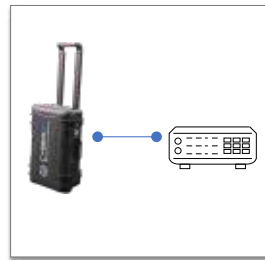
A detailed report provides you with a list of all the CVEs (Common Vulnerabilities and Exposures) observed in your network, and their location. Based on the actionable report, you may choose to fix or patch a vulnerability, or check whether it indicates malicious activity. To provide reliable vulnerability detection, SCADA Scan parses each packet and performs deep-packet inspection, resulting in the identification of dangerous commands and actions located deep in the protocol, such as attempts to exploit a vulnerability or risky commands and data that can adversely affect operational processes.

### Each alert details:

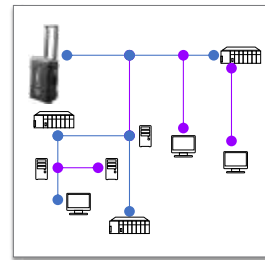
- The vulnerability type and the potential risk
- The CVE number
- Network location

## How It Works

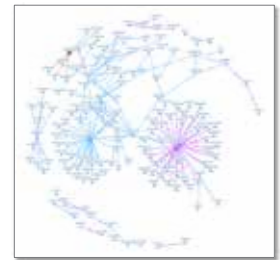
<b>Connect</b>	Easily plug-in SCADAScan to a mirror port in any of your network switches, without introducing any foreign data into the scanned network.
<b>Scan</b>	SCADAScan begins to passively monitor your network.
<b>Discover</b>	Within minutes, start receiving reports including network map, CVE assessment and more.
<b>Wipe</b>	Fully remove data from all components and move on to the next customer or ICS site.



1. Connect



2. Scan



3. Discover

## Support for Diverse ICS and OT Organizations

SCADAScan and SCADASHield offer broad OT and IT protocol support for the following verticals:

- Power grids
- Manufacturing
- Transportation
- Oil & gas
- Airports
- Pharma
- Smart buildings
- Military facilities
- Water and utility
- And more!

## Plug and Scan Integration

Fully portable and takes minutes to set up



## Upgrade to SCADASHield - Add continuous anomaly detection, policy enforcement and forensics across all required monitoring points.

Cyberbit SCADASHield has been securing the most sensitive infrastructures for over eight years, with proven, battle-hardened technology that detects and mitigates cyber threats across the entire OT and IT stack. Using 7-layer granular deep packet inspection (GDPI), SCADASHield provides unprecedented OT asset discovery and visibility, detecting known OT threats and vulnerabilities, as well as undocumented OT threats and anomalies. Ensuring continuity, SCADASHield detects deviations from operational restrictions and enforces operational policies and has been chosen to protect ICS/SCADA networks across verticals.

## ABOUT CYBERBIT™

CYBERBIT provides advanced cyber security solutions for high-risk, high-value enterprises, critical infrastructure, military and government organizations. The company's portfolio provides a complete product suite for detecting and mitigating attacks in the new, advanced threat landscape, and helps organizations address the related operational challenges. Cyberbit's portfolio includes advanced endpoint detection and response (EDR), SCADA network security and continuity, security incident response platform, and security team training and simulation. Cyberbit's products were chosen by highly targeted industrial organizations around the world to protect their networks.

CYBERBIT is a wholly-owned subsidiary of Elbit Systems Ltd. (NASDAQ and TASE: ESLT)

[sales@cyberbit.net](mailto:sales@cyberbit.net) | [www.cyberbit.net](http://www.cyberbit.net)

**Israel Office:**  
Cyberbit Ltd.  
22 Zarhin St. Ra'anana | Israel 4310602  
Tel: +972.9.779.9831

**US Office:**  
Cyberbit Inc.  
3571 Far West Blvd #168, Austin, TX 78731  
Tel: +1.737.717.0385

**Singapore Office:**  
Cyberbit Singapore Pte. Ltd.  
Temasek Avenue Centennial Tower, #21-23  
Singapore 039190 | Tel: +65.6679.5771

### PROPRIETARY INFORMATION

The information here in is proprietary and includes trade secrets of CYBERBIT Commercial Solutions Ltd. It shall not be utilized other than for the purpose for which it has been provided.



**CYBERBIT**  
PROTECTING A NEW DIMENSION