CYBERBIT
PROTECTING A NEW DIMENSION

SCADAShield

The first OT security platform to go live. Ever.

Visibility, security, asset management and continuity for ICS/SCADA networks

ICS Security is Years Behind

Designed long before the days of the internet, with flat architectures and no plans for online access, automation, or remote management, ICS/OT environments present pointed challenges for IT and OT professionals:

- **Poor visibility and OT blind spots**
- **OT threats entering from IT networks**
- **Non-applicability of existing IT solutions**
- **IT-OT ownership conflicts**

SCADAShield – Proven, Battle-hardened OT-IT Security

To address these threats, SCADAShield has been securing the most sensitive infrastructures since 2010, with proven, battle-hardened technology that detects and mitigates cyber threats across the entire OT and IT stack—stopping known and unknown "zero-day" threats before they can cause physical harm.

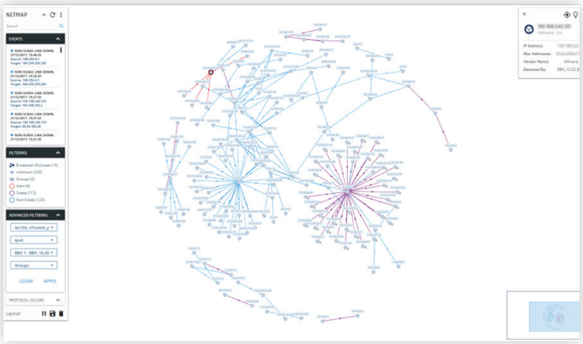
Unrivaled Visibility of your entire OT-IT Environment

Almost immediately upon deploying SCADAShield, ICS managers gain complete, real-time visibility into all IT and OT assets, network architecture and activity. For most, this mapping is the first time they are able to see all devices on all networks; a vital first step in securing them.Using passive, non-intrusive port mirroring and 7-layer granular deep packet inspection (GDPI), SCADAShield provides:

- **Full visibility of the OT network** by automatically generating a real time network map based on OT-IT communication paths and protocol analysis of all IP and non-IP network assets.
- **Quick identification of risky communications** allowing network and operations managers to quickly identify IT/OT touchpoints, analyze alerts and initiate investigation.

Use SCADAShield to:

- **Gain full visibility** into your OT and IT networks and assets
- **Detect known threats** and mitigate vulnerabilities in OT and IT devices
- **Detect unknown 'zero-day' OT threats**
- **Detect and mitigate** operational malfunctions and misconfigurations
- **Comply with regulations**

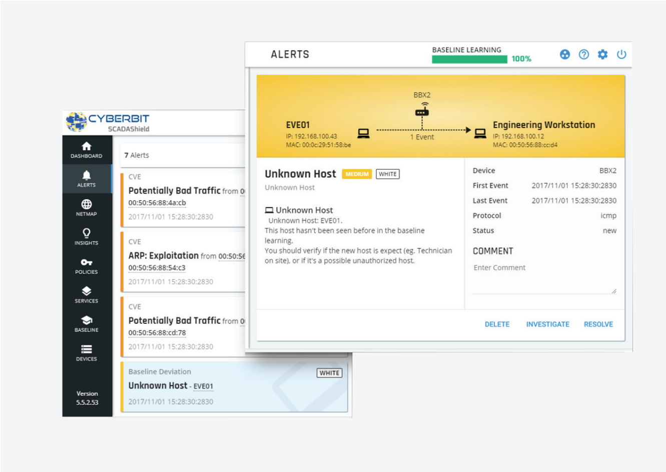


SCADAShield auto-generated network map

Detection of Known and Unknown OT & IT Threats

Once connected to the ICS/OT environment, SCADAShield automatically:

- **Baselines the customer's network**
- **Auto-generates operational policies;** others can be added or customized as required
- **Detects known vulnerabilities in IT and OT devices**, and provides clear guidelines for remediation and response
- **Detects anomalous behavior**, including deviant communications or commands that may indicate a cyber attack
- **Detects operational risks** such as malfunctions and misconfigurations, allowing OT staff to take remedial action



Version 5.5.2.53

7 Alerts

CVE
Potentially Bad Traffic from 0
00:50:56:88:4a:cb
2017/11/01 15:28:30:2830

CVE
ARP: Exploitation from 00:50:56
00:50:56:88:54:c3
2017/11/01 15:28:30:2830

CVE
Potentially Bad Traffic from 0
00:50:56:88:cd:78
2017/11/01 15:28:30:2830

Baseline Deviation WHITE
Unknown Host - EVE01
2017/11/01 15:28:30:2830

EVE01
IP: 192.168.100.43
MAC: 00:0c:29:51:58:be

BBX2
1 Event

Engineering Workstation
IP: 192.168.100.12
MAC: 00:50:56:88:cc:d4

Unknown Host MEDIUM WHITE
Unknown Host

Unknown Host
Unknown Host: EVE01.
This host hasn't been seen before in the baseline learning.
You should verify if the new host is expect (eg. Technician on site), or if it's a possible unauthorized host.

Device: BBX2
First Event: 2017/11/01 15:28:30:2830
Last Event: 2017/11/01 15:28:30:2830
Protocol: icmp
Status: new

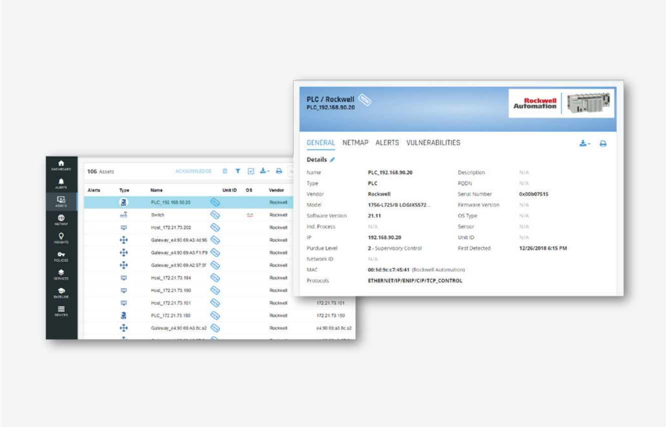
COMMENT
Enter Comment

SCADAShield detection and alerts

Granular Asset Management

SCADAShield enables granular asset management by providing the following information:

- **Attributes of all IT and OT assets** connected to the network, including device type, vendor, model, Purdue level, role, MAC address, IP address, serial number, OS, software/firmware version and associated vulnerabilities, as well as time last seen, last configuration change and more.
- **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.



106 Assets

Alerts	Type	Name	Unit ID	OS	Vendor	
		PLC_192.168.90.20			Rockwell	
		Switch			Rockwell	
		Host_172.21.73.202			Rockwell	
		Gateway_e4:90:69:A3:4d:96			Rockwell	
		Gateway_e4:90:69:A3:F1:F9			Rockwell	
		Gateway_e4:90:69:A2:97:5f			Rockwell	
		Host_172.21.73.194			Rockwell	
		Host_172.21.73.190			Rockwell	
		Host_172.21.73.101			Rockwell	172.21.73.101
		PLC_172.21.73.150			Rockwell	172.21.73.150
		Gateway_e4:90:69:A3:8c:a2			Rockwell	e4:90:69:a3:8c:a2

PLC / Rockwell
PLC_192.168.90.20

Details

Name	PLC_192.168.90.20	Description	N/A
Type	PLC	FQDN	N/A
Vendor	Rockwell	Serial Number	0x00b07515
Model	1756-L72S/B LOGIX5572...	Firmware Version	N/A
Software Version	21.11	OS Type	N/A
Ind. Process	N/A	Sensor	N/A
IP	192.168.90.20	Unit ID	N/A
Purdue Level	2 - Supervisory Control	First Detected	12/26/2018 6:15 PM
Network ID	N/A		
MAC	00:1d:9c:c7:45:41 (Rockwell Automation)		
Protocols	ETHERNET/IP/ENIP/CIP/TCP_CONTROL		

SCADAShield asset management

SCADAShield Optional Active Prevention Mode

SCADAShield can be **optionally** deployed in active prevention mode as an Intrusion Prevention System, allowing for active blocking of OT threats in real-time.

Support for Single Pane IT-OT-IoT Security

For single pane IT-OT-IoT security automation, orchestration and response (SOAR), SCADAShield can be integrated with Cyberbit SOC 3D.

Support for Diverse ICS and OT Organizations

SCADAShield offers out-of-the-box support for over 40 industry-wide and custom-developed protocols for the verticals listed below. New and proprietary protocols can be supported in a matter of days.

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

ABOUT CYBERBIT™

Cyberbit provides a consolidated detection and response platform that protects an organization's entire attack surface across IT, OT and IoT networks. Cyberbit products have been forged in the toughest environments on the globe and include: behavioral threat detection, incident response automation and orchestration, ICS/SCADA security, and the world's leading cyber range. Since founded in 2015, Cyberbit's products have been rapidly adopted by enterprises, governments, academic institutions and MSSPs around the world. Cyberbit is a subsidiary of Elbit Systems (NASDAQ: ESLT) and has offices in Israel, the US, Europe, and Asia.

sales@cyberbit.com | www.cyberbit.com

US Office:
Cyberbit Inc.
3571 Far West Blvd #168 | Austin, TX 78731 | Tel: +1.512.676.8731

Israel Office:
Cyberbit Ltd.
22 Zarhin St. Ra'anana | Israel 4310602 | Tel: +972-9-7799800

PROPRIETARY INFORMATION
The information 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