CYBERBIT
PROTECTING A NEW DIMENSION

SCADAShield

Industrial Grade Operational Continuity & Security

Challenges

OT and IT managers of critical infrastructure facilities are accountable for the security and continuity of their operational network. However, OT networks pose unique challenges: familiarity with network topology, IT/OT convergence points which expose the OT network to attacks originating in the IT network, and the use of old, unsecured and non-standard protocols.
To address these challenges and reduce downtime, OT managers need to gain back control over their network by using technologies that will improve monitoring, detection, visibility and forensic investigations, and allow mitigation of potential security and continuity risks.

YOUR RELIABLE ICS PARTNER

CYBERBIT is a wholly owned subsidiary of Elbit Systems (NASDAQ: ESLT), a global provider of defense and homeland security solutions. With offices across 4 continents, CYBERBIT is trusted by utilities, airports, manufacturers and governments as their long-term partner for securing their operational networks.

SCADAShield - ICS Visibility and Security

SCADAShield is a non-intrusive solution for OT network monitoring, detection, forensics and response. It discovers and visualizes all OT network components and communications, monitors both OT and IT protocols, and enables OT and IT managers to detect, analyze and respond to network anomalies, vulnerabilities and threats.

How Does It Work?

By using granular Deep Packet Inspection (DPI), SCADAShield knows the specific fields which should be analyzed in each layer of the inspected protocol. SCADAShield analyzes both IP and serial protocols, taps all network activities and maps all assets. As a result, it provides IT and OT managers with unmatched visibility and security of their OT network and facilitates advanced detection, easy analysis, and faster response.

SCADAShield BlackBox

Easy & Quick Deployment

SCADAShield is easy and fast to deploy. Its BlackBox smart sensor is installed out-of-band in a non-intrusive mode and passively monitors the SCADA network by tapping the network's communication hubs. SCADAShield automatically generates whitelist rules and blacklist rules to identify security vulnerabilities, misconfigurations, malfunctions or policy breaches. The SCADAShield BlackBox can optionally be installed inline, with active blocking capabilities. SCADAShield can integrate with any SIEM, and report its alerts.

ICS Network Security and Continuity

1. Discover, map and control all your industrial network assets
2. Visualize your entire network and identify changes
3. Monitor your network and receive real-time alerts on suspicious activity
4. Track unauthorized devices, communications and actions
5. Mitigate equipment and protocol vulnerabilities, exploits and security issues
6. Conduct forensics and investigations and analyze root cause
7. Customize dashboards and reports easily and quickly
8. Align with ICS network control standards and industry regulations

SCADAShield Main Dashboard

SCADAShield Network and Communications Map

SCADAShield Capabilities:

NetMap: Discover and Visualize Your Entire Network

SCADAShield's NetMap allows OT and IT managers to have a full understanding of network topology and communications, identify OT and IT touch points and initiate forensic investigations. Once SCADAShield is deployed, NetMap immediately generates a network map and provides full visibility of your entire OT network. It maps both IP and serial assets, indicates the specific protocols used between the devices and highlights potential risks.

Granular Deep Packet Inspection (DPI)

Unlike traditional systems, which analyze RTU and PLC or historian logs to look for potential threats, SCADAShield uses granular Deep Packet Inspection (DPI), which wisely inspects communication packets at byte-level and exposes anomalies at higher, more reliable rates. SCADAShield supports over 20 of the most widely used ICS protocols, and continuously adds support for new protocols according to customer requirements.

Automatic Base-Line and Rule Generation

By continuously monitoring network traffic, SCADAShield automatically learns which communication patterns are legitimate and which are non-standard and may indicate malicious activity or potential downtime. It employs auto-learning mode to generate whitelists automatically and detect anomalies and zero day threats.

SCADAShield Capabilities:

Signature-Based Detection

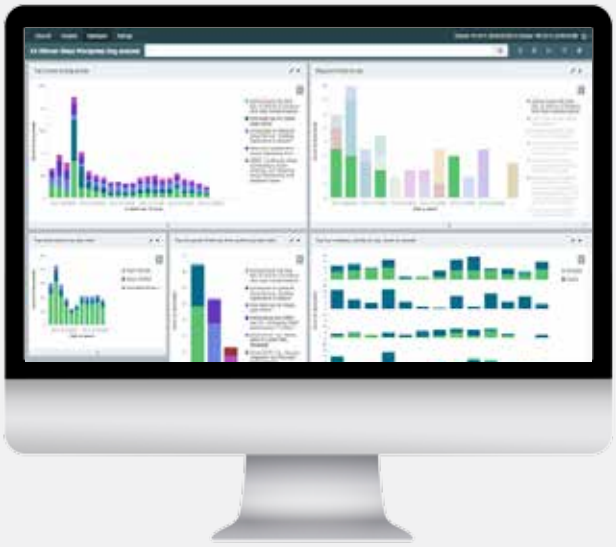
SCADAShield identifies signatures of known ICS\SCADA CVE's, devices and protocol vulnerabilities, exploits and security issues, flagging actionable alerts for mitigation.

Customizable Dashboards and Actionable Reports

An extensive report builder enables users to create and tailor a variety of dashboards and reports according to their preferences, transforming terabytes of monitoring data into actionable insights. Users can slice and dice data based on any desired combination including ad-hoc reports for a specific need. For instance, to investigate the use of opcodes over time.

Real-Time Forensics

SCADAShield collects valuable network data across the network, and provides the forensic tools for analyzing and investigating it over big data. Analysts and managers easily access both historical and real-time data to investigate events in real-time, look at past events or proactively hunt for threats.



SCADAShield Customizable Dashboards

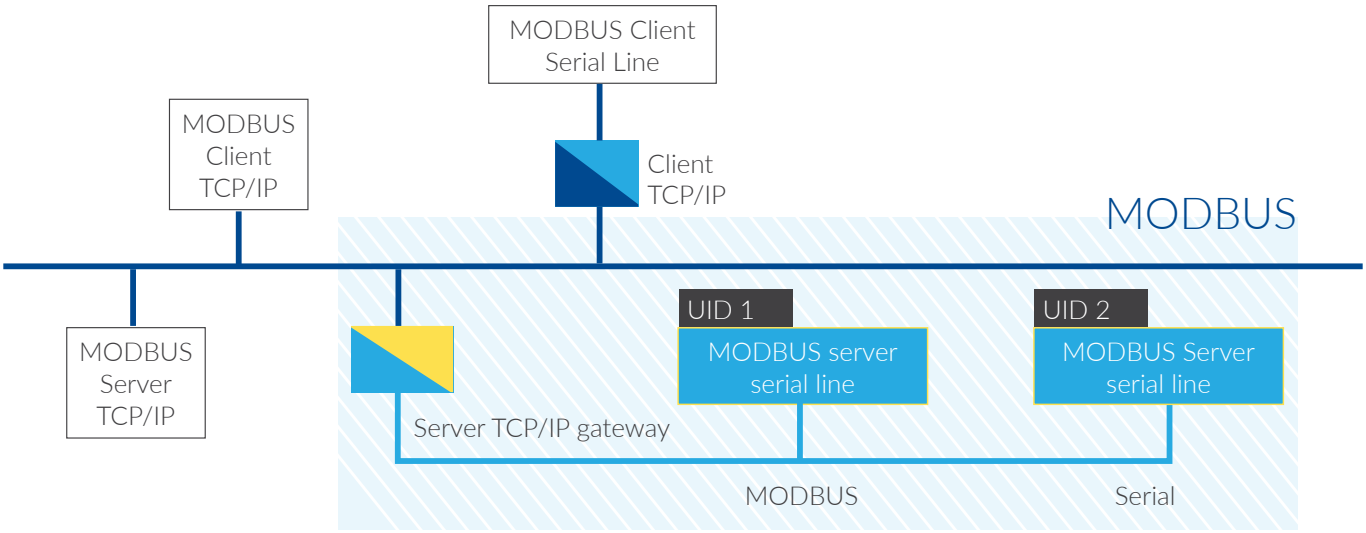
Out-of-the-box support for over 20 protocols

SCADAShield supports 20 of the major ICS protocols out-of-the-box with additional protocols being added on an ongoing basis. These include Modbus, IEC, DNP, CIP, SITA, Profibus, Profinet, MDLC, TIM, SITA, and more.

Granular DPI Examples

SCADAShield understands the specific structure of each ICS protocol. As a result it detects malicious behavior that would otherwise go undetected.

Protocol	Identifying malicious behavior: Sample
Modbus	Detect values set for specific registers, identify command types i.e. MEI (function code 43) type 14 which executes device scan (read device identification) to identify serial slave devices behind TCP/IP gateway
Ethernet/IP CIP	Identify request path (indicating to which internal resource in the target node the service is directed, e.g. HMI_SITE1), identify commands that cause PLC malfunction: Stop/Crash PLC (service code 0x07), reboot Ethernet controller in the PLC
ICCP/MMS	Detect all the 14 service codes and the bilateral table, and whitelist accordingly, identify MMS malform packets (malform payload structure) which may cause denial of service to ICCP servers



Unlike other tools, SCADAShield identifies serial slave devices behind TCP/IP gateways

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 cyber 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)

CYBERBIT Commercial Solutions Inc.
3800 N. Lamar Blvd. Suite 200 | Austin, TX 78756 | Tel: +1-737-717-0385
sales@cyberbit.net | www.cyberbit.net

CYBERBIT
PROTECTING A NEW DIMENSION