CYBERBIT
PROTECTING A NEW DIMENSION

SCADAShield - OT Security Platform

Asset management, visibility, security and continuity for ICS/SCADA networks

ICS Networks Are in Constant Risk of Downtime

Growing connectivity and complexity of ICS/SCADA networks and lack of monitoring and analysis tools make ICS organizations be at risk of operational failures and malicious activity resulting in expensive downtime. Malformed packets, unauthorized devices and activities, changes in network volumes and anomalous commands can cause harm and disruption. To achieve continuous operations, derived from secured and trusted networks, visibility and anomaly detection must be applied.

Passive, DPI monitoring of SCADA communications

SCADAShield uses Granular Deep Packet Inspection (GDPI) to thoroughly analyze packets and detect OT, IT/OT and IT attack vectors. Traffic analysis is used also for building a real-world network map and for asset management. SCADAShield uses mirror port for passive and non-intrusive monitoring.

Use SCADAShield to:

- Achieve network visibility and manage your OT and IT assets
- Detect and mitigate known vulnerabilities in OT and IT networks
- Detect and respond to unknown ICS threats
- Detect and mitigate operational misfunctions and misconfigurations
- Comply with regulation

Visibility

SCADAShield provides full visibility of the OT network by automatically generating a live real-world network map based on traffic analysis.
The network map presents all IP and non-IP network assets and their communication paths and protocols, allowing network managers and analysts to quickly identify IT/OT touchpoints, initiate investigations and analyze alerts.

SCADAShield automatic network map

Detection

SCADAShiled detection and alerts

SCADAShield automatically baselines the customer's network and alerts on anomalous security and operational behaviors. It alerts on malfunctions and misconfigurations, and helps enforce operational policies and regulation. The engine provides clear guidelines for remediation and response, allowing network managers and analysts to achieve remediation in a timely manner.

Asset and Layer Management

SCADAShield asset and layer management

SCADAShield automatically maps and identifies all OT and IT assets and their types, presenting them in Purdue Model for OT layer management. It graphically shows the operational and organizational layers, identifying device types, vendors, model, serial number, operating systems, firmware and software versions, vulnerabilities, MAC address, IP, last seen, last configuration change, and more.

SCADAShield Advanced

SCADAShield can also be provided in an active mode for inline installations, to block malicious commands and prevent attacks from executing. Additionally, it can integrate to Cyberbit EDR to provide advanced malware protection, detect, respond and prevent IT/OT attacks and malware on HMI and SCADA servers.

Vast Industrial Processes and Vendors Support

SCADAShield has out-of-the-box support for over 40 protocols, including vertical-designated protocols for energy companies, oil & gas, building management, automation & production, manufacturing and pharmaceutical. New and proprietary protocol support can be provided on-demand.

YOKOGAWA · EMERSON · ABB · Schneider Electric · MITSUBISHI · Honeywell · General Electric · Rockwell Automation · SIEMENS

SCADAShield for Smart Buildings and Data Centers

Smart devices and IoT infrastructure are increasingly becoming an integral part of our physical environment. SCADAShield for smart buildings secures IT, OT and IoT infrastructure such as data centers and building management systems, allowing network managers to identify security and functional anomalies, and track regulation requirements.

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 mid-2015 Cyberbit's products were 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.
3800 N. Lamar Blvd. Suite 200 | Austin, TX 78756 | Tel: +1-7377170385

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

CYBERBIT
PROTECTING A NEW DIMENSION