CYBERBIT
PROTECTING A NEW DIMENSION

SCADAShield

The Only Full-Stack Security Solution for ICS Networks

Challenges

A major challenge faced by critical infrastructure facilities is the growing convergence between IT and OT, making IT security vulnerabilities become OT security vulnerabilities, as identified by Gartner (Market Guide for Operational Technology Security, May 2016). And indeed, recent ICS attacks exploited IT to OT attack vectors, and penetrated to the operational network through corporate IT or Industrial IT components, causing physical harm to the operational environment. So were the attacks on the Ukraine Power Grid (2016, 2015), the German Steel Mill (2016), and the infamous Stuxnet (2010).
Threat actors are exploiting the growing connectivity, together with "traditional" OT challenges: vulnerable and unsecured SCADA protocols, wide attack surface and lack of visibility.
To address these challenges, a new approach for securing ICS organizations must be applied – which addresses the full threat stack, and detects across the entire attack surface.

SCADAShield

SCADAShield is a layered solution for providing full stack ICS detection, visibility, forensics and response. SCADAShield performs continuous monitoring and detection across the entire attack surface for both IT and OT components, and applies smart analytics in order to detect security and operational threats.

YOUR SOLID AND RELIABLE 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.

Detection and Visibility Across the Entire Threat Stack

SCADAShield's layered approach allows it to detect IT to OT attack vectors, as well as Machine to Machine (M2M). SCADAShield sensors monitor the OT network, Industrial IT components (HMI, SCADA server, Historian server, etc.), and critical IT/OT touchpoints in the corporate network. All data is transferred to a central big data repository and analyzed to identify anomalous activity, combining OT and IT data. A real-time network map is automatically created, providing full visibility of the OT network, while all data is constantly available for investigation and analysis.

ICS Network Security and Continuity

1. Continuous detection and response across the entire threat stack – OT, Industrial IT and Corporate IT
2. Discover, map and control all your industrial network assets
3. Visualize your entire network and identify changes
4. Real-time alerts on suspicious activity
5. Track unauthorized devices, communications, and actions
6. Mitigate equipment and protocol vulnerabilities, exploits and security issues
7. Conduct investigations, analyze root cause and respond
8. Customize dashboards and reports easily and quickly, identify trends and extract operational value
9. Comply with ICS network control standards and industry regulations

Three Layers of Monitoring

SCADAShield consist of three sensors, to monitor and detect across the entire attack surface:

- **OT DPI Monitor –** passive and non-intrusive Deep Packet Inspection (DPI) of OT network transmissions, with granular analysis down to the field level, including both Ethernet and serial communications. Out-of-the-box support for all widely-used ICS protocols, and continuous support for new and proprietary protocols according to customer requirements.
- **Industrial IT Monitor –** a lightweight agent for industrial IT endpoints and servers (such as Historian Server, Domain Controller, SCADA Server, HMI) which collects granular host data including application and user behaviors, applies behavioral analysis and transfers all data to the central big data repository for further analysis and advanced forensics.
- **Corporate IT Monitor –** continuous monitoring of critical IT/OT touchpoints in the corporate IT network, collecting granular data from the host. Response and prevention measures can be easily executed by the kernel-level agent to quickly remediate the threat.

Central Big Data Security Analytics

SCADAShield applies behavioral analytics, machine learning algorithms whitelisting and blacklisting rules in order to detect anomalies and threats across the entire threat stack. Correlating and analyzing OT and IT data together, allows detection of abnormal behaviors using advanced behavioral analytics and machine learning, together with auto-baselining and rule creation, SCADA CVEs and protocol policies. The Big Data security analytics engine is adaptive to the customer's network and adapts its detection mechanisms according to the routine network patterns.

Main Capabilities

Detection and Response - for the Entire Threat Stack

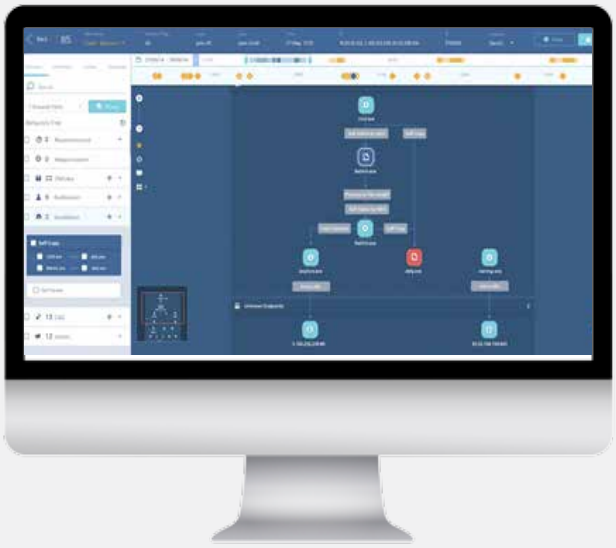
Quickly identify and respond to high-priority threats including M2M and IT to OT attack vectors. SCADAShield detects and automatically prioritizes anomalous activities in the SCADA network and on the IT assets. It correlates IT and SCADA data for improved detection and identification of threats. All alerts provide granular data for investigation and analysis, providing analysts and operators with detailed visibility. Response can be easily executed on IT assets using the IT monitors, enabling analysts to quickly act and remediate threats. IOC-based prevention, together with SCADA CVE detection, assures that known threats are identified and will not be able to act, while behavioral analytics and machine learning algorithms detect and alert on unknown threats.

Main Capabilities

Netmap - Real Time Automatic Discovery and Visualization

SCADAShield's Netmap allows OT and IT managers to have a full understanding of network topology and communications, identify OT and IT touchpoints and initiate forensic investigations. Netmap 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, highlights potential risks and indicates of network changes.

SCADAShield Network and Communications Map



SCADAShield Forensics - automatic visualization of the entire attack story

Forensics – Real Time and Historical Data Combined With Powerful Visualization to Quickly Identify Root Cause and Respond

SCADAShield collects valuable and granular data from the OT network and the IT hosts, and provides the forensics tools for analyzing and investigating it over big data. Analysts and network 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 Forensics provides advanced graph visualization of the entire attack story for both M2M and IT to OT attack vectors, allowing analysts to quickly identify root cause and respond to threats immediately.

Analytics - Advanced Dashboards, Reports and Visualization Tools to Extract Operational Value

SCADAShield's Analytics provide customized dashboards and reports to identify trends, and gain an overview of important data and measurements. Terabytes of monitoring data transform into actionable insights allowing users to slice and dice data based on any desired combination. SCADAShield Analytics supports construction of visual modules for all network layers.

SCADAShield Analytics

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 | www.cyberbit.net

US Office:
CYBERBIT Inc.
3800 N. Lamar Blvd. Suite 200
Austin, TX 78756
Tel: +1-737-717-0385

Israel Office:
CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra'anana
Israel 4310602
Tel: +972-9-7799800

CYBERBIT
PROTECTING A NEW DIMENSION