CYBERBIT
PROTECTING A NEW DIMENSION

Providing OT Network Visibility and Security for a Leading European Energy Utility Using SCADAShield

Case study

The Utility

A major energy utility of a European country, with dozens of geographically dispersed electrical substations. The utility holds two SCADA command and control centers for the transmission grid – a main site and a disaster recovery site, Using different SCADA protocols, standard and proprietary, and multiple vendors' equipment.

The challenge

Assuring Operational Continuity

The utility operates, amongst new equipment, old and unsecured legacy equipment, which leaves it exposed to cyber security attacks, unknown malfunctions, human errors and tampering attempts with insufficient detection capabilities and network visibility. This combination of varied risks and deficient network visibility and detection directly influences system downtime, resulting in financial, reputational and even legal implications. Moreover, the utility worries about network policy violation performed by both employees and system technicians, that don't fully obey regulation restrictions and thus impose yet additional threats on the OT network.

Using no inspection and monitoring solution, network visibility and security remain neglected and unnoticeable, leaving the network unreliable and unsafe. The utility had no capability of monitoring and tracking any action performed in the network, moreover its consequences. There was a crucial need to obtain visibility and see what actually occurred in the network in order to assure continuous network operability and full ongoing functionality.

Industry:
Energy Utility
(Generation + Transmission)

The Challenge:
Gain full visibility and security of OT network activity to detect cyber threats, system malfunctions, and network and equipment problems.

The Solution:
SCADAShield

Why CYBERBIT
An easy and quick Plug&Play implementation, passive tapping of network traffic without interfering in network communication, with ability to customize to suit the customer's existing deployment and all legacy OT systems.

The Results
The utility operators now have full visibility of the OT network, full network in-depth analysis and forensic capabilities, and enhanced security assuring operational continuity and no unknown and unexpected surprises.

The Solution

SCADAShield

The utility understood it needed to combine a tool that will allow it to gain full OT network safety and reliability and add End Point security to it.

Cyberbit EDR is an end point detection and response solution.

By using SCADAShield, the utility's network operators gained visibility of their network for the first time – which included seeing and investigating network transmissions, mapping both SCADA and non SCADA network assets, and obtaining a real, updated, network map.

By using automated whitelisting and blacklisting capabilities, EDR for SCADA detects anomalous network activity, generates alerts, and allows the SCADA operators to conduct forensic investigation by breaking down the protocol using deep packet inspection (DPI). All network transmissions can be then investigated in order to understand and analyze all the data.

Cyberbit EDR seamlessly integrated to the organization's existing HP ArcSight SIEM, reporting its alerts directly to it.

The Results

The utility finally gained OT network visibility, reliability and security, and is now able to see, investigate and monitor all transmissions within the OT network.

The utility's network operators can now assure operational continuity and ascertain minimum downtime, by identifying policy violations and unauthorized communications and tracking anomalous network activity caused by security threats, system malfunctions and operational.

"The ability to see what is going on in our network enables us to follow for the first time after problematic transmissions and understand their origins and their cause. Seeing a true network map of our network allows us to be more efficient and knowledgeable when analyzing operational and security risks, and to respond to them better and more adequately."

Get in touch with us to see how we can help you assure operational continuity in your OT networks, and regain control over your operations.

Visit www.cyberbit.com

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.com | www.cyberbit.com

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

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

CYBERBIT
PROTECTING A NEW DIMENSION