CASE STUDY

Securing a Global Chemicals Manufacturer

OVERVIEW

Securing a distributed manufacturing operation spanning multiple production facilities is always a challenge. The challenge is compounded when it comes to securing chemical manufacturing operations, due to the devastating environmental damages and threat to human life resulting from of a potential cyber-attack.

When a global specialty chemicals manufacturer, a market leader in its field, published a tender for implementing an enterprise-wide cybersecurity solution for its production lines, twelve of the most prominent OT security vendors applied.

SCOPE OF THE PROJECT

The tender specified the scope and the business objectives of the project:

- Continuous monitoring of all OT assets
- Detecting and alerting on OT cyber threats and anomalies
- Tracing logic & firmware changes on all industrial controllers
- Reporting OT cyber-alerts to the facility SIEM (Security information and event management system)

The tender selection process included a scoring of feature compliance, field proof-of-concept (for both network visibility and for anomaly detection) and visits to reference sites.

CUSTOMER'S CURRENT CYBER ECOSYSTEM

The customer's current cyber-security system deployment covers well its IT networks.

However, when these tools were applied to the OT network, key functional gaps arose such as the system's inability to handle OT-specific network protocols.

PROPOSED SOLUTION

Radiflow's proposed solution was based on the company's iSID Industrial Threat Detection System. The solution called for an instance of iSID to be installed locally at each production plant.

As each plant incorporated multiple subnets, an instance of Radiflow's iSAP Smart Collector was installed on each subnet to send a mirrored stream of all TCP/IP data traffic to the local iSID. And while sending such volumes of data over the plant's LAN would typically overload the network, iSAP's proprietary filtering and compression algorithms are able to greatly reduce data volume, saving the need to make changes to the customer's LAN.

The collected TCP/IP data is used by iSID to self-learn the network and construct a network topology model, which includes all assets, ports and protocols, along with their full properties, as well as mapping each to its appropriate business process.

Radiflow iSID's dashboard, displaying the network's security status

radiflow

This model serves to provide full visibility into the OT network and for detection of attempted attacks, violation of access policy to the industrial controllers, management of maintenance activities and monitoring of logic changes on controllers.

What's more, iSID is able to prioritize the risk associated with each specific controller by weighing in the criticality of each business process and analyzing the interplay between different systems.

iSID also integrates into SIEMs by different vendors at each plant, providing the customer with a unified alerting system.

iSID's Map View graphically displays all network components and enables users to drill down to each component's properties and threats.

CHALLENGES

As the customer operates dozens of facilities with different types of systems and topologies, the project, which is expected to take three years to completion, requires close cooperation between the customer and Radiflow to optimize the solution capabilities which may evolve over the project lifecycle.

Radiflow research team utilizes a machine-learning infrastructure to quickly parse additional protocols and provide full visibility for all the assets in each site where the system is deployed.

REASONS FOR CHOOSING RADIFLOW

The customer has stated the following reasons for selecting Radiflow:

- Technical solution to the customer's problem: Radiflow's solution fully met all stated requirements, providing a response to the customer's unique challenges. Specifically mentioned was the use of iSAP Smart Collectors to send data traffic to each site's iSID without overloading the network, which provides flexibility to the entire deployment architecture.
- General positive impression of the expertise of the Radiflow team throughout the extensive selection process, and the long-term commitment to support the customer throughout the global deployment.
- Long-term price considerations – attractive pricing model for multi-site deployment over the span of years.

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cyber-security vendors. Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 3,000 critical facilities worldwide. More at www.radiflow.com.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

www.radiflow.com | info@radiflow.com