FORESCOUT

Case Study

European Gas Infrastructure Company Implements Network Monitoring to Benefit from Operational Visibility and Protection from Cyber Threats

Device Visibility and Control

With The company carried out the first ICS/SCADA network monitoring installation in 2012, making it an outstanding front-runner among critical infrastructure organizations worldwide.

The Objective

Implement a solution to achieve continuous situational awareness, validate network and operational changes, and detect known and unknown cyberattacks before they impact the national gas infrastructure.

The Challenge

The project involves both legacy OT systems and technology, and traditional IT networks and protocols. Therefore, the desired solution must:

- Identify ICS devices and understand proprietary ICS protocols, as well as custom extensions of standard ones.
- Analyze in full depth IT protocols to detect both known and zero-day attacks.
- Define a baseline of normal operations for both ICS networks and dynamic back office networks.
- Validate network and operational changes and alert in real-time for undesired network activity.

The Solution

SilentDefense detected the operational scenarios and cyber attacks simulated during the on-site proof of concept, and was chosen to monitor both the HMI network of gas storage sites and the gas distribution pipeline. Currently, SilentDefense monitors more than 400 IT systems and servers and thousands of RTUs scattered across the country.

The Results

Among the daily operational insights provided by SilentDefense to the company's operators, it identified two critical network and device misconfigurations which had a direct impact on the process and the company's disaster recovery procedures:

- Inconsistencies between production and acceptance network blueprints. Seeing as the acceptance network blueprint was to be used for recovery in the case of network failures, the result would have been an incorrect and possibly unpredictable operation of the gas infrastructure.
- RTUs not configured correctly by the vendor and reporting invalid values for customized fields of a standard SCADA protocol. As a result of the invalid values, the SCADA server could not guarantee accurate calculations and forecasting.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com