CASE STUDY

Securing Petroleum Storage Tanks in Southeast Asia

OVERVIEW

The storage of petroleum products (crude and processed oil) is a complex industrial process. Oil storage tanks are tasked with maintaining precise environmental conditions (e.g. temperature, pressure and electromagnetic insulation), deviations from which may lead to horrendous environmental results.

When one of the largest petroleum distribution firms in Southeast Asia sought a solution for protecting one of its storage terminal facilities (and meet governmental cyber-security regulations), the project's specifications included, in addition to mere intrusion detection, also monitoring and management of multiple disparate intrusion detection systems, as well as tight control over access authorization management during maintenance operations.

Oil storage tanks include a host of security measures, both physical and cyber. Each tank houses multiple sensors and controllers that control the environmental conditions inside the tank.

SCOPE & PROPOSED SOLUTION

The oil storage terminal security project encompassed a large number of tanks, divided into three units. Each unit was to be connected to a Radiflow iSID intrusion detection system, for detecting anomalies, which may indicate an insider attack (e.g. installing malicious logic on a PLC or introducing an unauthorized device into the network).

iSID's multiple security engines offer capabilities pertaining to specific type of network activity: modeling and visibility of OT and IT devices, protocols and sessions; detection of threats and attacks; policy monitoring and validation of operational parameters; rules-based maintenance management; and networked device management.

The three instances of iSID were to be monitored and managed remotely from a central Security Operations Center (SOC).

Multiple instances of the iSID Industrial Threat Detection System were installed at the oil terminal, all managed remotely through the Radiflow iCEN Remote Management System.

To allow the remote management of multiple iSID systems, Radiflow's iCEN Central Monitoring System was used to display aggregated data from all iSID instances in an organization. This included full asset information, alerts (prioritized by severity and originating iSID detection engine) and network protocols used.

iCEN displays a status snapshot of all iSID instances across the organization, including their total risk and activity status, with easy drill-down and remote connection to each iSID instance.

Users are able to switch between geographical map and tabular display modes, both featuring color-coding for quick cross-site prioritization. iCEN provides a quick summary status, detailed properties and health monitoring status (CPU, RAM) for each monitored instance of iSID.

In addition, a number of Radiflow's iSEG 3180 DPI Firewall/Ruggedized Secure Gateways were installed at each tank. The iSEG gateway provides DPI firewall capabilities for analyzing SCADA traffic.

Upon detecting an anomaly the 3180 will automatically generate alerts, block the abnormal activity and isolate any affected sub-networks. To facilitate compliance

with local regulations, the iSEG RF-3180 includes an APA (Authentication Proxy Access) which allows remote access to authorized personal at predefined time slots.

To maximize efficiency, each RF-3180 Firewall/Gateway also hosted in its chassis an instance of Radiflow's iSAP Smart Collector.

The iSEG-3180 Ruggedized Secure Gateway provides DPI firewall capabilities, as well as an APA (Authentication Proxy Access) for rule-based user access managment

iSAP provides a cost effective, non-intrusive method for sending large volumes of data traffic from the gateways (using a mirrored stream) without over-taxing the local network (as is the case with typical data traffic collectors). This is done using Radiflow's proprietary compression and filtering (removal of IT protocol data) algorithm. The use of iSAP allowed installing only a handful of instances of iSID, thus reducing the overall cost of the project.

DECIDING FACTORS TO CHOOSE RADIFLOW

After weighing all vendors' proposals, the client chose Radiflow for the project based on a number of factors:

- Triple-layer IDS: Radiflow's holistic IDS solution can be adapted to OT networks' topology, size and modes of operation. This is done by incorporating, alongside iSID, the iSAP Smart Collector for sending data traffic from remote locations/subnetworks to a central instance of iSID; and the iCEN Central Management Solution for monitoring and management of multiple iSIDs in different locations. iCEN also allows MSSPs to effectively monitor multiple clients' iSID systems.
- Strong local partner: Radiflow's local partner's technical capabilities, excellent support and project accompaniment proved to be a key decision factor.
- Combined detection and prevention: going beyond merely detecting incoming threats, the Radiflow system provides operators with tools and insights for risk assessment and mitigation, for eliminating vulnerabilities and optimizing mitigation measures.
- Reputation as compliance enabler for critical OT organizations: Radiflow's solution was designed to meet all presiding local (governmental) and international standards and regulations.

Radiflow iCEN simplifies and streamlines the monitoring and management of multiple instances of Radiflow's iSID Industrial Threat Detection Systems.

CURRENT STATUS

At present, the Radiflow system is fully-functional, and has been regularly detecting anomalies and issuing recommendations for remediation since it began operations.

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

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com