Radiflow

Case Studies 2020

Securing a Large-Scale Power Plant in Central Europe

OVERVIEW

When you think of critical infrastructure, the first thing that comes to mind is power generation, where a single cyber attack has the potential to disrupt all areas of civil life.

The precedent of the December 2015 attack on a Ukrainian power utility, as well as many other attacks on industrial facilities, have raised awareness among power utilities in the region and triggered local governments to issue regulations for national critical infrastructures.

The combination of these two factors led the operator, one of the largest energy utilities in Central Europe, to seek a cyber-security solution for its main power generation plant.

Typical production turbine used in large-scale powerplants. The project described called for each turbine to be secured individually.

SCOPE

The tender for the lucrative project specified securing and monitoring the production turbine operations in a 3,000-MW coal-based, multi-turbine power plant, where each turbine (as well as other industrial processes) was to be secured individually for intrusion detection as well as for control and maintenance operations.

CHALLENGES

The project's specifications called for a central IDS, installed at a Security Operations Center (SOC), for analysis of network traffic received from each operational unit as well as for network visibility.

This created the challenge of sending extremely large volumes of data without overloading the plant's local area network, as is the case with most data traffic collectors.

In addition, the tender called for a secure, rule-based user access authorization management system for each operational unit, that would provide full control over scheduled maintenance operations.

RADIFLOW'S PROPOSED SOLUTION

Radiflow's proposed solution entailed installing its iSID Industrial Threat/Intrusion Detection system at the operator's SOC.

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.

In addition to threat detection using multiple secuirty packages, iSID provides industrial operators full network visualization, as well as risk mitigation insights

To overcome the problem of network overload caused by sending network traffic from the power plant's operational units to iSID, Radiflow's solution included its iSAP Smart Collectors (20 in all) that compress the data packets sent to iSID using a unique, patented compression algorithm. iSAP further reduces the network load by sending only packet headers for IT traffic. This results in a reduction of up to 70% in bandwidth consumption.

Radiflow's solution also called for installing over fifty of the company's award-winning iSEG RF-3180 DPI firewall-equipped secure gateways, which upon detecting network anomalies are able to automatically generate alerts, block the abnormal activity and enforce network segmentation.

In addition, to facilitate compliance with local standards and regulations, the iSEG RF-3180 includes APA (Authentication Proxy Access) for authenticating and limiting users' access to predefined devices and functions, all fully logged.

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

THE TENDER AND SELECTION PROCESS

As expected in a project of this scope and criticality, practically every leading OT cyber-security vendor worldwide responded to the tender.

As part of the vendor selection process the operator compared the analysis results for the same snippet of data traffic.

DECIDING FACTORS

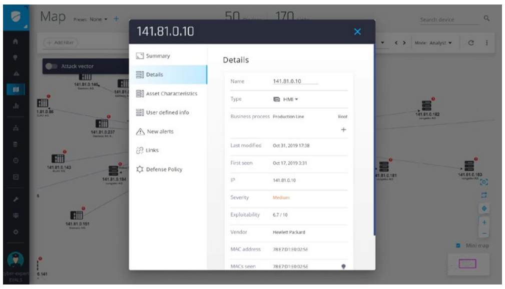
In the end, the main deciding factors for choosing Radiflow:

1. Radiflow's overall technological capabilities which met all of the customer's requirements.
2. Radiflow's iSAP Smart Collector was the only solution that was able to overcome the problem of network overloading resulting from sending large volumes of OT data traffic to the central IDS.
3. Radiflow was the only vendor in the tender to provide both an IDS (iSID) and a SCADA DPI firewall (iSEG), thus greatly simplifying both project management and execution.
4. The level of service and expertise displayed by Radiflow's local representative/distribution partner.

CURRENT STATUS

Once Radiflow's local partner (in collaboration with the customer) finished "cleaning up" the baseline network model and optimizing iSID's detection rules, the turbine security system was deemed fully operational. It has since provided the site operators with a much-improved tool and method for monitoring operations.

Currently, the customer and Radiflow are working on expanding the project to securing peripheral networks in this power plant as well as securing additional power plants operated by the same utility.



141.81.0.10

Details

Name 141.81.0.10
Type HMI
Business process Production Line Root
Last modified Oct 31, 2019 17:38
First seen Oct 17, 2019 3:31
IP 141.81.0.10
Severity Medium
Exploitability 6.7 / 10
Vendor Hewlett Packard
MAC address 78:E7:D1:E0:02:5E
MACs seen 78:E7:D1:E0:02:5E

Upon activation, iSID learns the network, including all assets, connections and protocols. The result is a detailed network topology visualization model, with drill-down to each assets full details.

THREAT DETECTION-BASED CYBERSECURITY

Threat Detection is a critical element in the protection of SCADA systems. By learning the network topology and creating a comprehensive normal network model, IDS systems enable detecting nuanced anomalies and handling highly complex cyber-attacks.

The iSID Industrial Threat Detection and Monitoring system provide operators a comprehensive view of the OT network for efficient network management.

As important is iSID's passive nature that makes it very easy to deploy, and do not interfere with the operational network traffic.

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.

In addition to threat detection using multiple secuirty packages, iSID provides industrial operators full network visualization, as well as risk mitigation insights

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.

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.

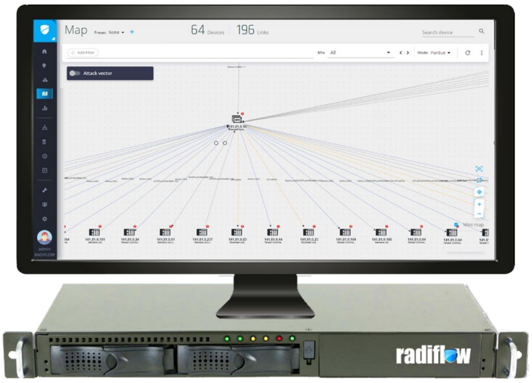
Securing a Global Chemicals Manufacturer (cont.)

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.

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.



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

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.

FLEXIBLE DEPLOYMENT FOR ORGANIZATIONS OF DIFFERENT TYPES AND SIZES

iSID can be deployed at a central location, to provide threat detection for multiple remote sites, or locally at each remote site (or a combination of both).

Central IDS deployments typically create a network overload problem, due to the large volumes of data sent from each local site to the central IDS. Radiflow's iSAP Smart Collectors solve this problem: installed at each site, they receive all LAN traffic from the local switch, using port mirroring, and filter the data, leaving intact the SCADA traffic (e.g. ModBus data).

To further prevent network overload, the filtered data is compressed and sent to the central iSID over VPN tunnels.

Monitoring/management of multiple iSID deployments at remote sites (typically larger remote sites) is performed using Radiflow's iCEN Central Monitoring System for iSID. iCEN provides a view of each iSID's operational state, ongoing detection summary data (e.g. network risk state, detected events) and system health information, and is used for remotely updating cyber-security threats and detection rules.

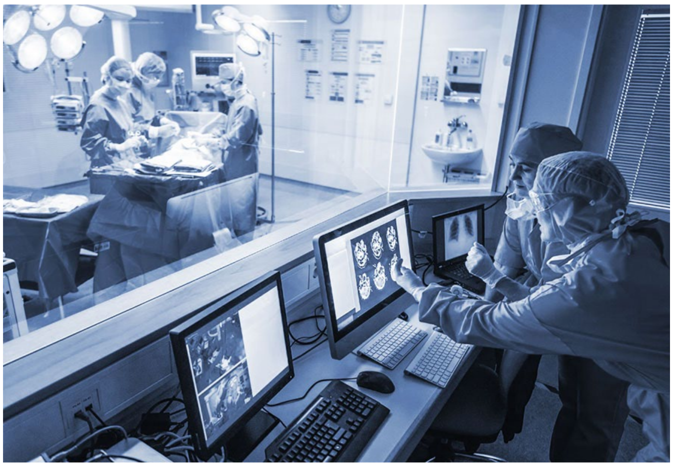
Securing a Large Hospital Campus

OVERVIEW

You'd be hard-pressed to think of a more complex environment to cyber-secure than a hospital campus, as was in the case of a major hospital campus in the EMEA region.

Beyond typical Building Management System functions, hospitals operate a myriad of interdependent critical systems, and are required to operate in preparedness mode, in case of a mega-event or epidemic, so OT-network uptime is crucial.

To make things worse, many hospital systems were not designed with cyber-security in mind.

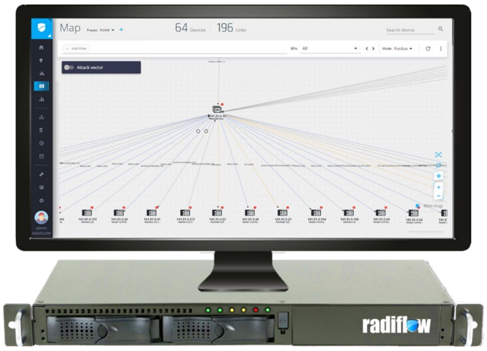


Hospitals are among the most complex industrial environments, operating a myriad of interdependent critical systems

OBJECTIVES AND CHALLENGES

The highest priority items (typical to hospital security projects) were:

- Protecting the high voltage power supply systems (securing the IEC61850 protocol)
- Securing critical BMS systems (using DPI for ModBus and BACnet protocols): HVAC, electrical, elevators and water/wastewater systems; monitoring the safe usage and storage of medical gases; and monitoring the temperature control systems in cold-storage appliances used for medicine, experiment specimens, organs and corpses.
- Monitoring various HazMat sensors



iSID's Map View graphically displays all assets, business processes and connections, and enables users to drill down to each asset's properties and threats

Most of the above challenges are due to the way hospital campuses and their data networks evolved over the years, as a patchwork of disparate systems and no segmentation between critical systems:

- OT and IT systems that share the same LAN, with only nominal firewall protection
- Lack of segmentation between buildings ,facilities and systems.
- Separate operational—but not security—monitoring interfaces for different systems
- No procedures in place for patching or hardening devices, leaving the hospital to rely on vendors for initiating per-device maintenance
- No system for securing and logging maintenance operations

SOLUTION AND PROCESS

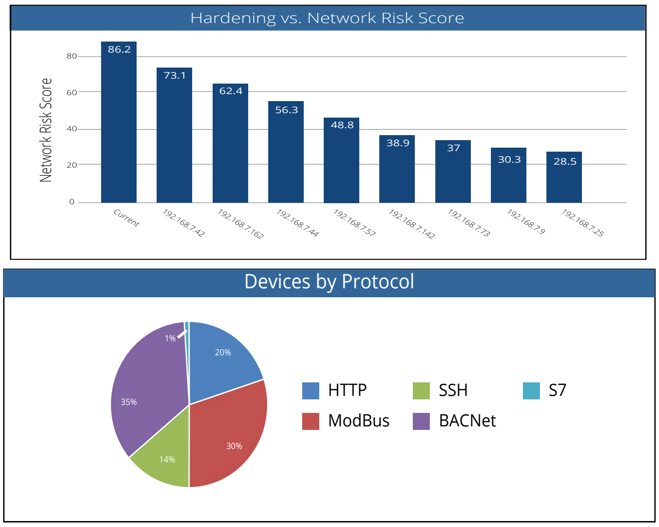
The first stage in the project was conducting a thorough OT-security assessment. This involved analyzing a few days' worth of operational data traffic by Radiflow's iSID Industrial Threat Detection system, operating in Learning Mode.

Once completed, iSID provided a detailed network model, including all assets, ports, open connections and protocols and vulnerabilities/risks associated with different assets.

As expected, the network model revealed a slew of vulnerabilities, from lack of segmentation between critical systems and networks to mundane configuration issues, such as use of default passwords or unpatched devices.

Securing a Large Hospital Campus (cont.)

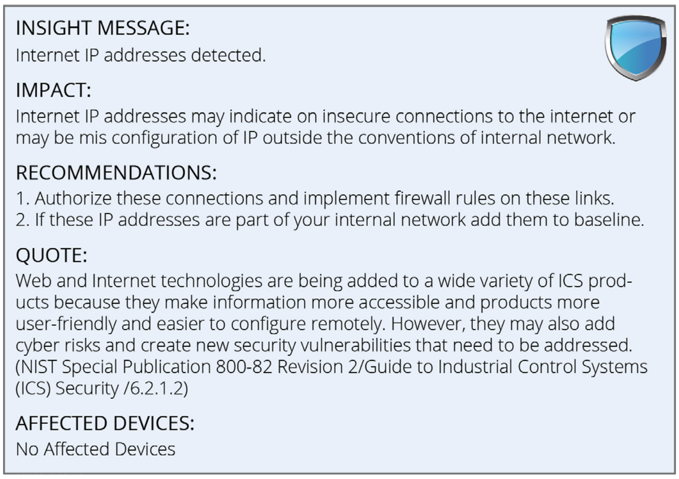
The results of the network analysis were processed by the Radiflow team members that had accompanied the project since inception, resulting in a comprehensive status report and mitigation plan.



Two of the many items included in the network analysis report

Then, in collaboration with the client, the detected vulnerabilities were remedied, resulting in a "clean" baseline topology model which was used thereon for ongoing monitoring, threat detection and alarming also incorporated iSID, this time in Detection Mode.

In addition, using rule-based alerts for specific devices, iSID created a central monitoring point for critical systems, with alerts for exceeding different sensor or controller values, as well as changes to controller logic or adding devices to the network.



INSIGHT MESSAGE:
Internet IP addresses detected.

IMPACT:
Internet IP addresses may indicate on insecure connections to the internet or may be mis configuration of IP outside the conventions of internal network.

RECOMMENDATIONS:
1. Authorize these connections and implement firewall rules on these links.
2. If these IP addresses are part of your internal network add them to baseline.

QUOTE:
Web and Internet technologies are being added to a wide variety of ICS products because they make information more accessible and products more user-friendly and easier to configure remotely. However, they may also add cyber risks and create new security vulnerabilities that need to be addressed. (NIST Special Publication 800-82 Revision 2/Guide to Industrial Control Systems (ICS) Security /6.2.1.2)

AFFECTED DEVICES:
No Affected Devices

Insights produced by the Radiflow system provide simple, plain-language mitigation recommendations

CURRENT STATUS

At present, Radiflow's system is fully operational in one facility and has been greenlighted for installation throughout the entire hospital chain. The project will ultimately include an OT-SOC (Security Operations Center) outsourced to an MSSP, that will monitor all iSID systems installed at multiple hospitals.

ROI-BASED RISK MANAGEMENT

Radiflow offers ROI-based optimization of cybersecurity expenditure to ensure the effectiveness of threat-mitigation measures in relation to the adversaries and attack tactics relevant to the specific industrial network.

Radiflow's unique risk assessment algorithm combines the likelihood of attacks on networked assets (based on the industrial network's unique characteristics as well as a wide array of threat intelligence sources) with their quantitative real-world impact (e.g. monetary loss or non-compliance with governing regulations) to assess the risk introduced by different business processes.

Based on this analysis, the system provides the operator with a prioritized list of mitigation measures based on their contribution to reducing overall risk.

Securing an Offshore Oil-Drilling Rig in the North Sea

OVERVIEW

Sometimes the main challenge in landing a project to secure an industrial location is physically landing at the location.

Offshore oil drilling is one of the most lucrative segments in the energy sector, and is expected to increase its market share as new reserves are discovered and new technologies for deep-water drilling emerge (CAGR of 8.3% during the period 2019-2023, according to market researcher Technavio).

The Offshore Oil Drilling industry still operates under the shadow of the 2010 BP Deep Horizon oil spill and the subsequent ecological disaster, and has been subject to scrutiny over security concerns, both physical and cyber.

Needless to say, offshore oil drilling rigs are still very much associated with the infamous 2010 BP Deep Horizon leak and the subsequent ecological disaster that have generated great awareness and scrutiny over the entire industry. This scrutiny and the demand for stricter security measures (physical and cyber) were part of the incentive to harden the cyber-security of the rig.

The offshore drilling cluster of under a dozen rigs described herein is located about 150 km off-shore, and is accessible only by weather-permitted helicopter flight.

Communication with the mainland is limited to low-throughput satellite and RF communications.

The rig is regularly staffed by a few dozen employees.

WINNING THE PROJECT

Radiflow was introduced to, and eventually won the project through its local partner, based on previous successful Radiflow deployments in the energy sector.

The main incentives to install IDSs were preventing breaches into the OT network; gaining visibility into the network and all assets, including access to each asset's status and properties; and achieving compliance with the presiding standards and regulations.

Prior to installing the Radiflow system, cyber-defense of the rig relied solely on a firewall.

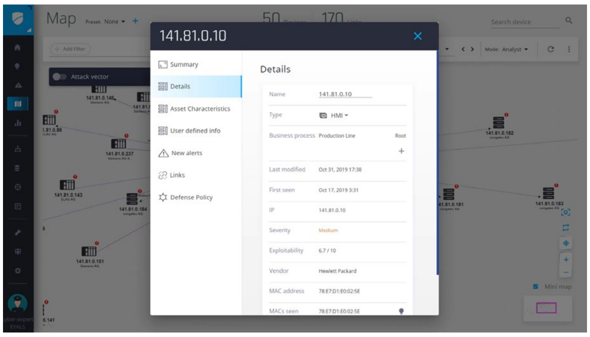
The iSID Industrial Threat Detection System installed at the oil rig goes beyond merely detecting breach attempts, with invaluable asset management features and insights for hardening the OT network.

SCOPE OF THE PROJECT

The first stage of the project called for installing Radiflow's iSID Intrusion Detection System at one of the rigs in the cluster, with the intention to do the same in the rest of the rigs (as the project grows with multiple instances of iSID, the client will be able to monitor and manage of the entire array of iSID systems through the Radiflow iCEN Central Management Solution.)

For this project, iSID was tasked with providing full visibility into the OT network, detection of attempted attacks and access violations, management of maintenance activities and monitoring of logic changes on controllers.

In addition, the Radiflow system provides operators with tools and insights for risk assessment and mitigation, for eliminating vulnerabilities and optimizing mitigation measures.



Details

Name 141.81.0.10

Type HMI

Business process Production Line Root

Last modified Oct 31, 2019 17:38

First seen Oct 17, 2019 3:31

IP 141.81.0.10

Severity Medium

Exploitability 6.7 / 10

Vendor Hewlett Packard

MAC address 78:E7:D1:E0:02:5E

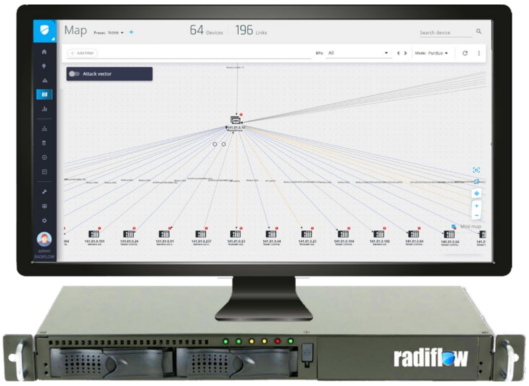
MACs seen 78:E7:D1:E0:02:5E

iSID enables drilling down to each assets properties, including logic version, alerts, defense policy and more.

Upon detecting anomalies, iSID would relay alerts to the company's SCADA system using Radiflow's OT protocols northbound interface. This enables the personnel at the operating room to be aware on any anomaly in their network or cyber and operation incidents through the SCADA system interface.

CHALLENGES

As mentioned, the main challenge of the project was physically accessing the site. This required Radiflow's local partner to diligently plan and stage the iSID system on terra firma prior to installation, and unsurprisingly, the installation took place smoothly. From then on, configurations were done remotely, in tight collaboration between the local partner, the Radiflow team, and the client.



iSID network visualization map provides operators a clear understanding of the logical placement of assets in the OT network

CURRENT STATUS

At present, iSID is fully operational at the oil rig. It has already detected vulnerabilities and misconfigured PLCs in the rig's OT network and has issued recommendations for remediation.

The operator's information security staff has been trained on operating iSID (at the operator's premises).

Following a few upgrades and adjustments to the system, it is expected that the next phase of installing iSID at additional rigs will be green-lighted soon.

NETWORK VISIBILITY AND ASSET MANAGEMENT

iSID's Map View displays a graphical representation of all network devices in multiple display modes (Perdue, Flow, Analyst & Custom). Maps are zoomable and elements can be dragged to any location on the screen. In addition, the Attack Vector analyzer can detect vulnerabilities within the interplay between different business processes.

To facilitate asset management, iSID's presents all system assets, categorized and filterable by type (e.g. PLC, Server, HMI, Engineering Station, Broadcast, etc.) or by any asset characteristic. Asset types are automatically detected by iSID; the user can change each asset's designation or add a custom asset type.

Additional asset management capabilities are available through integration with 3rd-party solutions.

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.

Securing Petroleum Storage Tanks in Southeast Asia (cont.)

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.

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.

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

THE ISEG RF-3180 SECURY GATEWAY

Once connected to the OT (SCADA/ICS) network, the iSEG RF-3180 starts gathering information from across the network (devices, behaviors, etc.) and suggest editable firewall rules.

The iSEG RF-3180 secures both M2M (Machine to Machine) and H2M (Human to Machine) traffic by incorporating DPI (Deep-Packet Inspection) capability for analyzing SCADA network traffic. Upon detecting an anomaly the 3180 will automatically generate alerts, block the abnormal activity and isolate any affected sub-networks.

To facilitate NERC CIP V6 compliance, the iSEG RF-3180 includes an APA (Authentication Proxy Access). It grants authenticated users access to predefined devices and functions, all fully logged.

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 6,000 critical facilities worldwide.

More at www.radiflow.com.

Radiflow | For more info: radiflow.com