Radiflow

CASE STUDY

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 an advanced cyber-security solution for its main power generation plant.

Typical production turbine used in large-scale power-plants. 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.

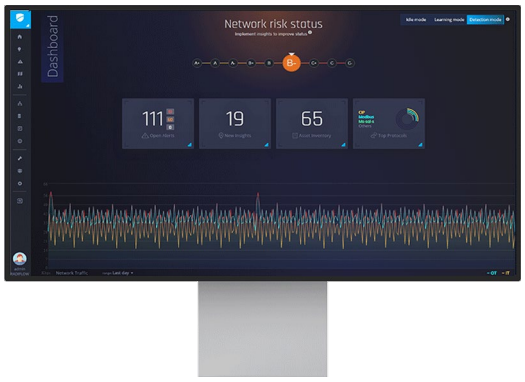
This created the challenge of sending extremely large volumes of data without overloading the plant's local area network, as is the case with most data traffic collectors.

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.

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

Radiflow's solution also called for installing over 50 of the company's award-winning iSEG-3180 DPI firewall-equipped secure gateways, which upon detecting anomalies are able to automatically generate alerts, block the abnormal activity and enforce network segmentation.

In addition, to facilitate compliance with local 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 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 selection process the operator compared the analysis results for the same snippet of data traffic.

DECIDING FACTORS

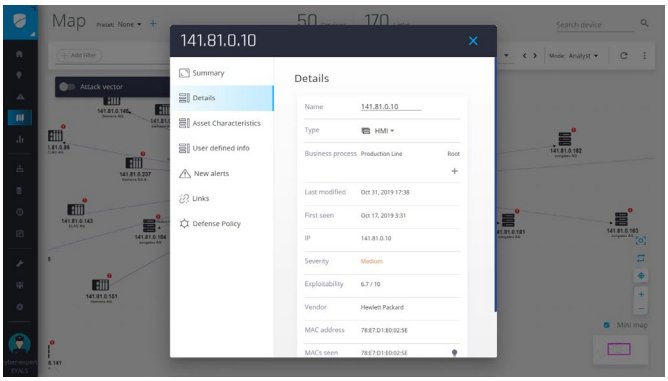
In the end, the main deciding factors for choosing Radiflow:

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 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.

Radiflow and the power plant operator are currently 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.



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.

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow