Case study: Incorporating Radiflow’s iSID in a managed OT SOC

SYNOPSIS:

By incorporating Radiflow’s solutions in a Managed SOC, ICS/SCADA-based organizations now have access to a highly professional, cost effective cybersecurity solution. At the core of the integrated solution is Radiflow’s iSID Intrusion Detection System, which protects OT networks and ICS/SCADA environments by alerting on breach attempts and cyberattacks into the OT network by flagging potential risks based on deep network learning and asset mapping.

An OT SOC Solution Designed for ICS/SCADA Installations

In recent months, Radiflow, a leading provider of industrial cybersecurity solutions for critical infrastructure, has launched a new program to enable its value-added partners to offer managed Security Operations Center (SOC) services for Operational Technology (OT) networks with industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems.

The need for a professional, cost effective integrated SOC solution has become eminent following the recent increase in cyberattacks on ICS/SCADA installations around the world.

At the core of Radiflow’s OT SOC tool-kit is the company’s iSID Industrial IDS (Intrusion Detection System).

iSID protects OT networks and ICS/SCADA environments by alerting on breach attempts and cyberattacks into the OT network by flagging potential risks based on deep network learning and asset mapping.

iSID offers six security packages, for Network Visibility, Cyberattack Detection, Policy Monitoring, Routine Management, Asset Management and Behavior Monitoring, to cover each and every operational situation and scenario.

For its OT SOC partners, Radiflow also provides its iSAP Smart Probe for collecting, efficiently and securely transferring OT network traffic from customer sites to the managed SOC. This solution provides the following benefits:

- Patented traffic compression, reaching ratios of 1:10 - drastically reducing the bandwidth requirements between remote sites and the central analysis location
- Complete preservation of original traffic information required for analysis, such as MAC address and TTL, which in some cases may be lost (e.g. during transit through a router)
- Secure and robust transport method, which overcomes practical ICS segregation, such as one-way-links
- Protection of customer information by whitening network traffic during inter-site flow

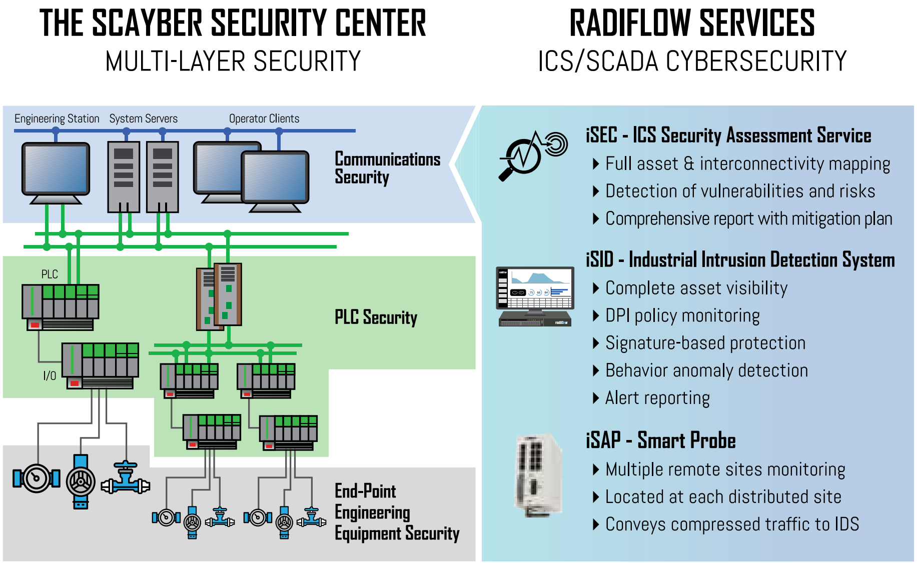
Continued...

Incorporating Radiflow's iSID in a managed OT SOC

The program was launched following an extensive implementation at a managed OT SOC operated by YANAI, a prominent Israeli electrical engineering company. YANAI's SOC, which is manned 24x7 by both cybersecurity and industry (electricity, water, etc.) experts, enables the quick detection and professional management of cyber events at customer sites. Furthermore, by sharing resources, customers are able to reduce OPEX and practically eliminate CAPEX, while utilizing equipment that would be outside the reach of individual operators.

The inclusion of iSID within YANAI's triple-tier SOC has allowed YANAI to broaden its target customer base, adding customers from the electricity, renewable energy, water, building management and other industries. By transitioning to a managed OT SOC, YANAI's customers were able to improve their cybersecurity operations and lower their operational and human resources costs.

Radiflow's OT SOC partner program is targeted at system integrators already working in the OT space that want to extend their service offering and provide their customers with ongoing managed security services.The OT SOC program can also serve as an entry point for IT managed security service providers (MSSPs) that want to enter the OT space. For these partners, Radiflow provides a powerful toolkit for analyzing events from multiple OT customers. Furthermore, the toolkit provides ongoing trend information so that Managed SOC operators can quickly detect emerging threats.



THE SCAYBER SECURITY CENTER
MULTI-LAYER SECURITY

RADIFLOW SERVICES
ICS/SCADA CYBERSECURITY

iSEC - ICS Security Assessment Service
- Full asset & interconnectivity mapping
- Detection of vulnerabilities and risks
- Comprehensive report with mitigation plan

iSID - Industrial Intrusion Detection System
- Complete asset visibility
- DPI policy monitoring
- Signature-based protection
- Behavior anomaly detection
- Alert reporting

iSAP - Smart Probe
- Multiple remote sites monitoring
- Located at each distributed site
- Conveys compressed traffic to IDS

Incorporation of Radiflow's solutions in YANAI's "SCAYBER" Security Center

Radiflow also provides its OT SOC partners with extensive knowledge transfer and support for conducting initial and ongoing security assessments of customer OT operations, including mapping of operational assets, analyzing revealed threats and vulnerabilities, and providing recommendations for a risk mitigation plan.

Radiflow is a leading provider of cybersecurity solutions for critical infrastructure's ICS/SCADA networks. Radiflow's security toolset validates the behavior of both M2M applications and H2M (Human to Machine) sessions in distributed operational networks. Radiflow's security solutions are available both as in-line gateways for remote sites and as a non-intrusive IDS (Intrusion Detection System) that can be deployed per-site or centrally.

Radiflow's solutions are sold either integrated within a global automation vendor's end-to-end solution, or by local channel partners, as a standalone security solution.

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 2461963
sales_UK@radiflow.com

Secure Your Assets