iSID
Industrial Threat Detection

WHY RADIFLOW?

Radiflow is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures:

EXPERIENCE

Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure

UNIQUE METHODOLOGY

Radiflow offers a unique scan methodology to detect industrial attack vectors that can cause downtime.

EXPERTISE

Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

Radiflow offers a holistic portfolio of services and technologies, including SCADA gateways, routers and firewalls, industrial network IDS and many more.

- Automatic learning of topology & operational behavior
- Central-location deployment (using Radiflow's iSAP Smart Probes) or local deployment at remote sites
- Network traffic analysis based on DPI protocols for SCADA
- Supervision over configuration changes in PLCs
- Model-based anomaly detection analytics, signature-based detection of known vulnerabilities
- Non-intrusive network operation
- Low false-alarm rate
- Central management of multiple iSID instances using iCEN

Six Security Packages for Comprehensive Threat Detection

iSID enables non-disruptive monitoring of distributed SCADA networks for changes in topology and behavior, using six security packages, each offering a unique capability pertaining to a specific type of network activity:

1. NETWORK VISIBILITY

Using passive scanning of all OT network traffic, iSID creates a visual network model for all devices, protocols and sessions, with alerts upon detected topology changes (e.g. new devices or sessions.)

2. CYBER ATTACK

The Cyber Attack package handles known threats designed to the SCADA network, including PLCs, RTUs and industrial protocols, based on data from research labs as well as Radiflow's own research.

3. POLICY MONITORING

Define/modify policies for each network link, for validating specific commands (e.g. "write to controller") and operational ranges (e.g. "do not set turbine to above 800 rpm.")

4. MAINTENANCE MANAGEMENT

Limit network exposure during scheduled maintenance by creating work orders for specific devices during set time-windows. A log report of all maintenance activities is issued upon session completion.

5. ANOMALY DETECTION

The Anomaly Detection package creates a behavioral network model using multiple parameters, including device sequence sampling time, frequency of operational values and more, toward detecting behavioral anomalies.

6. OPERATIONAL BEHAVIOR

Monitor and audit the management of devices (PLC, RTU & IED) at remote sites, with alerts for firmware changes or configuration modifications (e.g. software updates or turning edge devices on or off) and activity logging.

Continued....

iSID - Typical Use Cases

TECHNICIAN ON-SITE:

iSID will automatically monitor maintenance activities during the predefined time window. Operations outside of the maintenance boundaries will trigger alerts.

UNAUTHORIZED PLC CONFIGURATION CHANGES:

iSID will detect known protocol commands which affect PLC configuration.

SCADA SERVER ATTACK:

iSID will detect and alert upon changes in the industrial model, including command sequence and timing anomalies in the commmand sequence and timing.

SPYWARE

iSID will detect attempts by spying malware to scan the network for SCADA devices such as PLCs and RTUs.

MAN-IN-THE-MIDDLE

iSID will detect and alert upon rogue devices in the network impersonating a valid server, workstation or SCADA controller, by means of Mac or IP address theft.

BLACK ENERGY (BE) MALWARE:

iSID will explicitly identify and alert upon BE and will detect unauthorized SCADA commands issues by BE SCADA plugins, as well as anomalies in the industrial process.

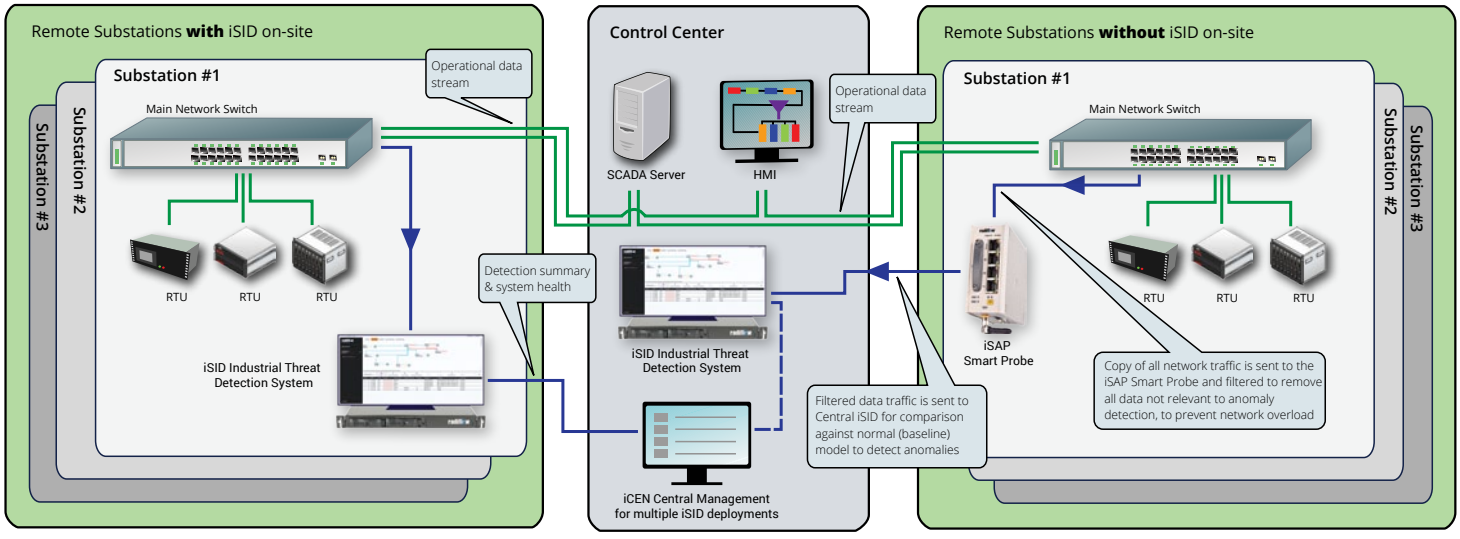
Central or Distributed iSID Deployment

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 Probes 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 remote software updating and maintenance.



iSID deployment model, combining central deployment at control center and on-site deployment at remote sites (using iSAP Smart Probes)

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

radiflow
Secure Your Assets