Product Datasheet

iSID

Industrial Threat Detection

- Automatic learning of topology & operational behavior
- Central-location deployment (using Radiflow's iSAP Smart Probes) or local deployment at remote sites
- Network traffic analysis of SCADA protocols based on DPI technology
- 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

MULTIPLE SECURITY PACKAGES FOR COMPREHENSIVE THREAT DETECTION

iSID enables non-disruptive monitoring of distributed SCADA networks for changes in topology and behavior, using multiple 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.

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 over 5,900 critical facilities worldwide.
More at www.radiflow.com.

TYPICAL USE CASES

TECHNICIAN ON-SITE:

Automatic monitoring of maintenance activities during the predefined time window. Operations outside of the maintenance boundaries will trigger alerts.

UNAUTHORIZED PLC CONFIGURATION CHANGES:

Detection of 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.

PART OF RADIFLOW'S MULTI-TIER OT-SECURITY SOLUTION

iSID is part of Radiflow's multi-tier solution for threat detection & monitoring, policy enforcement and network analytics.

Radiflow's iSAP Smart Probes, installed at remote facilities, help prevent network overload due to the large volumes of data sent from remote sites to the central IDS by compressing and filtering the data, while maintaining the data integrity.

The iCEN management dashboard enables monitoring multiple on-site iSID deployments, including operational state, detection summary data, system health information and provisioning.

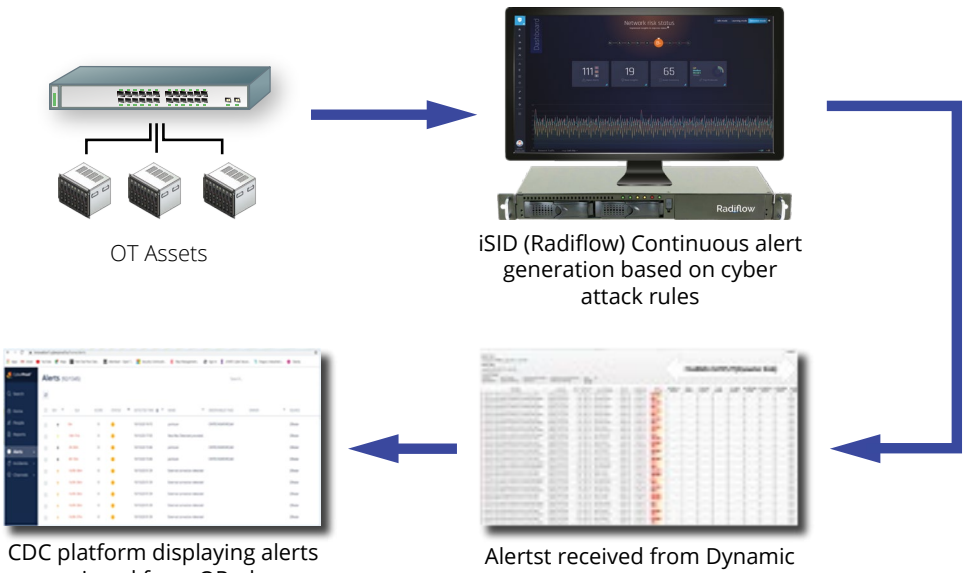
The CIARA risk assessment & management tool puts users in charge of their risk posture, with prioritized, plain-language mitigation recommendations aimed at optimizing OT-security expenditure.

The iSEG DPI-firewall gateway provides strict work order-based enforcement of identity and policies (for NERC CIP V6 compliance), as well as user activity logging and per-port validation of user activity using a DPI Firewall.

FLEXIBLE DEPLOYMENT (ON- AND OFF-SITE)

iSID can be deployed at a central location, locally at each remote site, or a combination of both (for larger facilities that require on-site threat monitoring).

Radiflow's solutions were designed for central monitoring and management by managed security service providers (MSSPs) using the iCEN central management dashboard for multiple instances of iSID. This provides smaller users with a viable replacement for an in-house cybersecurity department.



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