Radiflow and Aperio

Combined methodologies for ICS cyber-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

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 secure gateways, Industrial IDS and many more.

- Multiple detection methodologies monitored and controlled through single pane of glass
- Aperio's Production Database (Historian) Value Analysis finger-prints the data produced by your production process to detect indicative inconsistencies
- All detection data and alerts visible through Radiflow's iSID ICS Analysis Platform
- Designed specifically for ICS systems
- Entire process is 100% non-intrusive

The Problem:

The key to successful detection of cyber-threats and attack attempts in ICS networks is utilizing multiple, parallel detection methodologies, each producing different values and insights.

This creates the challenge of correlating and presenting cyber context from different detection sources within a single network/production monitoring system.

The Solution:

Radiflow and Aperio's combined offering allows correlating both companies' detection methodologies—Radiflow's real-time network traffic analysis and detection, and Aperio's production database (Historian) value analysis—creating a powerful, comprehensive detection suite.

Radiflow's iSID ICS analysis platform combines the detection data, alerts and insights derived using both methodologies into a single pane of glass, along with actionable information for incident handling, mitigation and compliance:

- Non-Intrusive Network anomaly detection
- Behavioral analytics
- Asset discovery and change detection
- Signature base rules of ICS & IT
- Threat Intelligence
- *Aperio production data base analytics*

The Aperio Historian analysis engines non-intrusively learns your facility's monitoring systems by "fingerprinting" Sensor data. Upon detection of data manipulation such as injection of new synthetic data, replay of past data, or transformation of process data, Aoperio will send alerts in near real time to the Radiflow iSID platform. Aperio also pinpoints the physical location of equipment under attack, while reconstructing the true state of systems in real time.

radiflow Secure Your Assets APERIO

Use Cases

Use case #1 - Replay Attack

iSID detected a new asset in the network capable of accessing the OPC server and sending new function calls and values via the new network link. In addition an alert is triggered by Aperio Data Forgery engine indicating an attempt of a replay attack on Historian data. The objective of the exploitation attack is now in context, fraudulent data is erased from the data-base and the attack is mitigated.

Use case #2 - Inside User

An engineer with the appropriate privileges accesses the Historian, iSID detects that the login was made at an unusual time and alerts, Aperio Data Forgery Protection engines sends an alert of data manipulation. Correlating the two alerts, source and target of the exploit are identified.

Functional diagram of the combined solution

1. Aperio & Radiflow analyze different sources
2. Aperio sends alerts to Radiflow iSID
3. Radiflow iSID displays cyber alerts in a single pane
4. iSID sends alerts to SIEM or HMI

About Radiflow:

Radiflow is a leading provider of cyber security solutions for critical infrastructure networks. SCADA networks often extend across multiple remote sites, allowing automation devices to be controlled from the control center. Radiflow's security tool-set 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 was founded in 2009 as part of the RAD group, a family of ICT vendors with over $1Bn annual revenues.

Radiflow solutions were launched at the end of 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More information can be found at www.radiflow.com

About Aperio:

Aperio's solution ensures sensor data integrity for critical infrastructure & large scale Industrial facilities. Our Date Integrity engines authenticate the data provided by physical sensors in a plant and validates that it reflects the true state of the system. This translates to a very strong and unique value proposition for both cyber security, productivity, and safety. For cyber security in particular, Aperio are the only technology with a credible capability of preventing large scale, destructive cyber attacks against critical infrastructure – attacks which it is safe to assume will increase dramatically in the coming years.

Aperio's patented technology "learns" individual sensor signal characteristics, and using machine learning algorithms builds "fingerprints" of physical signals which allows plant operators to detect in real time issues related to sensor data regardless of whether this is malicious or if it relates to failures or misconfiguration.

Aperio software is installed around the world at major critical infrastructures such as power generation, transmission and oil & gas facilities. More at www.aperio-systems.com.

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