Radiflow

PRODUCT DATASHEET

Active Scanner

Active Asset Discovery & Data Enrichment for ICS Networks

Full asset discovery, using safe active OT scanning, made available to networks lacking port mirroring or passive monitoring, or for further enriching iSID passive discovery

Radiflow **Active Scanner** complements the existing passive listening functionality of the iSID industrial threat detection platform – with an active scanning component, which provides more comprehensive asset data than would otherwise be picked up in a normal operation cycle, such as modules, PLC version, project version and many others.

Developed specifically for OT networks, Active Scanner, in both standalone or hybrid mode (with iSID) uses safe active query methods – communicating with OT assets using their native protocols – to minimize the chance of service interruption (exhaustively tested in Radiflow labs).

Scan Methodology

Active Scanner operates as a standalone solution or within a hybrid solution with iSID, combining iSID's continuous passive network scanning with its active scanning results, which are further analyzed by iSID.

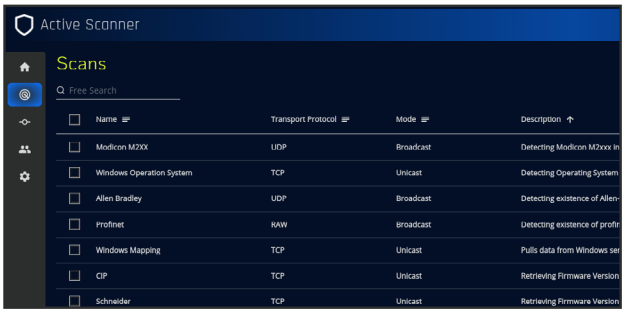
Using iSID-collected data, Active Scanner is able to perform targeted scans (rather than querying the entire network, typical to IT scanning solutions) for specific groups of industrial assets (e.g. PLCs), for different types of asset & asset data detections:

- Identification of silent devices: network device detection
- Identification of OT devices: industrial device detection
- Collection of additional information from existing devices

Active Scanner uses per-vendor and per-protocol queries, which are detected by iSID. By listening to assets' responses, iSID is able to correlate the sent data with its Asset Management database, for discovering assets which are silent on the network during normal operation.

Active Scanner does not require any network reconfiguration to allow a mirrored stream for passive scanning, making it suitable for ICS networks that don't allow mirrored streaming for IDS deployment.

The Active Scanner dashboard provides an at-a-glance view of the operator's scanning activity by type, activity and over time



Active Scanner's recent scans list

Furthermore, to minimize risk, Active Scanner never uses any brute force or exploit-based discovery methods on industrial assets.

Discoverable Vendors and Protocols in Use

Active Scanner offers targeted scans for discovery and fetching asset information for multiple vendors' devices, including:

Protocols:

- Modbus
- CIP
- Profinet
- SNMP
- IT ICMP
- NMAP
- DNP3
- WMI

Vendors:

- Schneider Electric
- Rockwell Automation
- Siemens
- Others

Operating Systems:

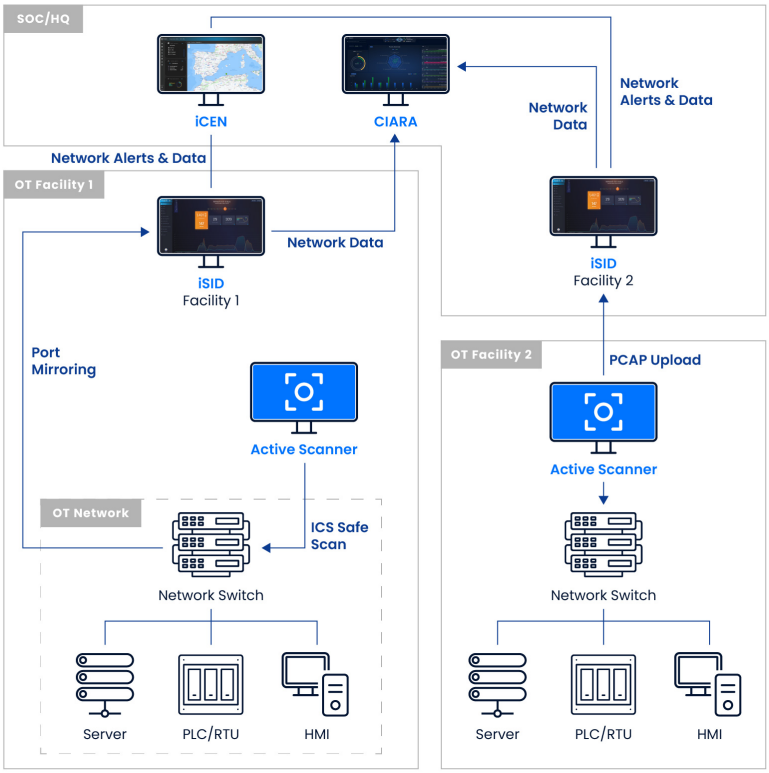
- Windows OS

Seamless Interoperability with iSID and the Radilfow Portfolio

Active Scanner allows for ad-hoc or scheduled scans, for discovering new assets and changing conditions on the OT network. In both cases the user is able to perform unicast scans of a defined IP range.

Scan results with scanned device parameters are saved to the Active Scanner, available for download in a particular format (PCAP, CSV or JSON), and transmitted to integrated Radiflow products such as iSID and CIARA for deeper analysis.

Scan PCAP files for all types of scans are also available for download and can be uploaded directly to iSID.



Active Scanner is deployed either standalone or within a hybrid configuration with iSID (shown; Active Scanner would still be required to run on a separate server)

About Radiflow

Radiflow develops OT-dedicated solutions that empower critical infrastructures and ICS organizations to monitor and analyze all ICS traffic toward preventing breach attempts, gainging full visibility into the network, and mitigating cyber risk. Radiflow operates a global network of certified local channel partners and maintains a top-tier technology partner ecosystem that allows cross-enriching legacy platforms with Radiflow's threat detection, asset management and risk assessment data. Founded in 2009, Radiflow protects over 8,000 sites worldwide in a wide range of industries.

Radiflow

(C) 2023 Radiflow LTD. All Rights Reserved. Radiflow reserves the right to change product specifications without prior notice.