Radiflow

Active Scanner

Active Asset Discovery and Data Enrichment for ICS Networks

HIGHLIGHTS

- Safe, active scanning of OT devices for rich, useful asset data unavailable via passive monitoring
- Scans multiple sites, delivering a holistic network picture
- Requires no network reconfiguration and never loads the network
- Works with iSID or standalone

Active Scanner complements or replaces passive monitoring of industrial networks. Employing safe, targeted methods, Active Scanner directly queries assets to obtain deeper data such as modules, versions, and patch levels, improving threat detection, risk management, and other cybersecurity solutions with a finer level of accuracy in alert generation, asset management, risk assessment, and compliance.

SEEING MORE AND COLLECTING MORE

While continuous passive monitoring captures and examines communications from devices that communicate on the ICS network, active scanning directly queries devices, even silent and redundant ones, that passive monitoring may not notice. The rich data it collects is especially useful for asset inventories, vulnerability assessments, compliance audits, and risk assessments. Networks that lack SPANs, mirrors, or monitor ports may employ active scanning to collect asset and other information. Small water-management sites or substations, where ISID cannot be deployed due to unmanaged network infrastructure or budget limitations, can still monitor their assets via Active Scanner.

SAFE SCANNING OF LEGACY AND MODERN ASSETS

To minimize risk, Active Scanner never uses brute force or exploit-based discovery methods. Instead, it communicates with assets in their native protocols, making sure that the traffic it generates stays well below any threshold that would impact the network. Without requiring network reconfiguration, Active Scanner performs ad hoc or scheduled targeted scans (by type, e.g., PLCs, or by IP range), discovering new assets and changing conditions on the OT network (e.g., changes to PLC logic), raising alerts as necessary.

The result is a comprehensive security report, replete with rich asset data and communication history, as well as a PCAP file for each execution for playing back the underlying communication.

Based on Radiflow's decades of industry experience, Active Scanner performs targeted scans across generations of device types, vendors, and protocols.

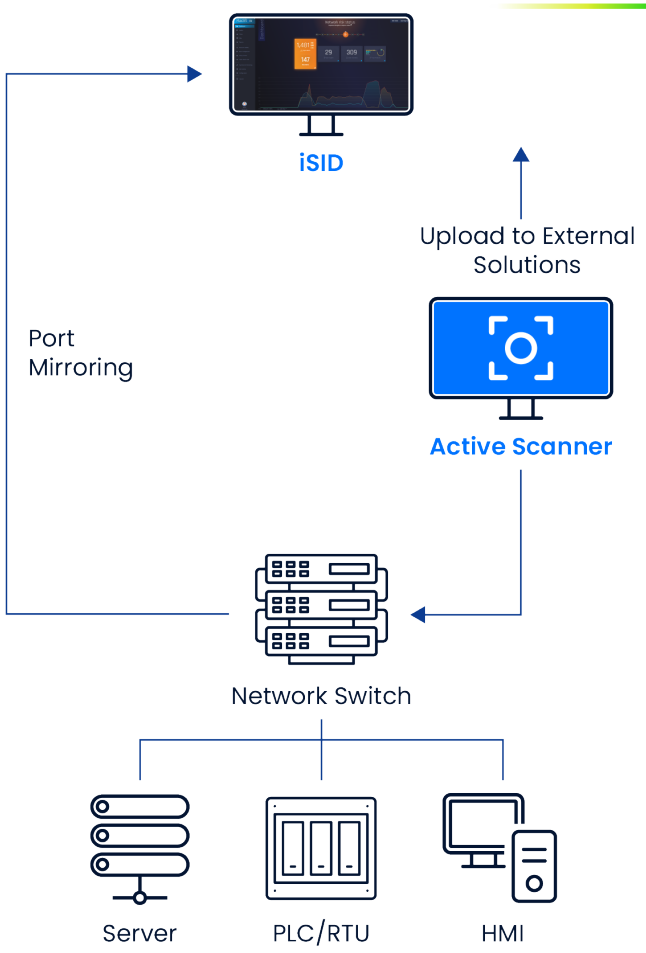
- **Modbus**
- **Profinet**
- **Windows**
- **SNMP**
- **BACnet**

HOLISTIC VIEW ACROSS SITES

Active Scanner delivers a holistic network visibility picture for multiple sites as it discovers assets, actively collects data, and organizes it for upload to asset management, risk management, and other external solutions. Scan results are available in convenient formats such as PCAP, CSV, or JSON.

ENRICHING iSID DATA AUTOMATICALLY

When working in tandem with Radiflow iSID, Active Scanner sends its proprietary broadcast messages and industrial protocol queries to devices on the network. Listening to their responses, iSID correlates the data with its own Asset Inventory.



Active Scanner working in tandem with iSID and/or generating files for upload

Radiflow

www.radiflow.com
info@radiflow.com

Radiflow is a leading, global provider of OT Security and Risk Management solutions and services for critical infrastructure and industrial automation. We enable operators to continuously safeguard their operations while they manage risk, optimize their security budget, and comply with standards, regulations, and industry best practices. Locally or centrally deployed, Radiflow solutions integrate with leading technology and partner platforms. Now part of the Sabanci Group, Radiflow protects over 8,000 sites worldwide.