Radiflow

iSID Threat Detection for OT Environments

Non-intrusive monitoring of critical infrastructure and industrial networks for anomalies in topology and behavior, and prompt detection of cyber threats

HIGHLIGHTS

- Automatic learning of OT network topology and operational behavior, creating a visual network model
- Local and centralized deployments
- Easy onboarding for quick time to value
- Adapts to network segmentation of any degree
- Monitors and understands a wide variety of modern and legacy assets and protocols
- Eliminates irrelevant alert noise

Digital transformation to Cyber Physical Systems (CPS) continues unabated. The wide variety of vendor equipment and processes and the dynamic threat landscape make OT security highly complex.

iSID boosts operational resilience against cybersecurity threats and risks across industrial operations and critical infrastructure. Consolidating the visibility across the entire OT environment, **iSID** bolsters security posture and compliance with emerging cyber regulations and directives, delivering significant business value.

CONTINUOUS OT SECURITY POSTURE MONITORING AND PROTECTION

iSID learns ICS network activity and generates the baseline topology and a behavior model including all devices, ports, and connections. Passively monitoring network traffic, it determines deviations from proper behavior, detecting anomalies which may be indicators of compromise.

Radiflow

BUILT IN INDUSTRY-AWARENESS

iSID is loaded with Radiflow's vast experience in CPS across industries and critical infrastructure deployments, adding valuable operational and cyber knowledge to utility, power plant, and water operations, building automation, chemicals, food and beverage, manufacturing, maritime, oil and gas, paper and packaging, pharmaceuticals, transportation and logistics, and other industries. **iSID** safeguards OT networks, assets, systems, and processes from cyberattack and helps organizations comply with international, national, and industry regulatory requirements and security frameworks.

SMART, SAFE DATA COLLECTION

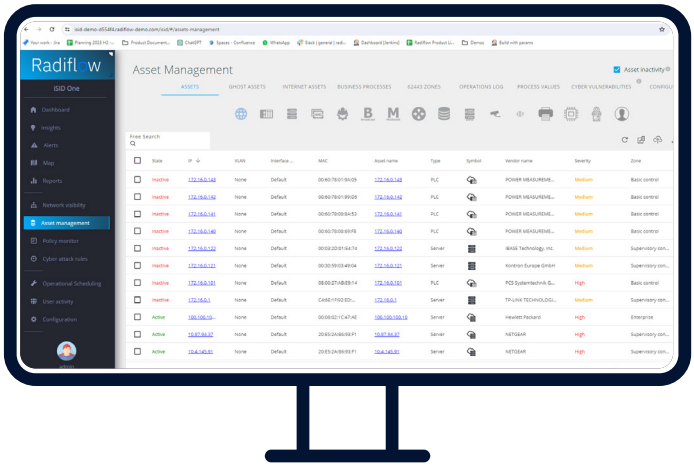
Through port mirroring, **iSID** passively inspects network packets. Patented data compression (100:1) enables it to keep up with traffic without putting a load on the network. Designed for industrial environments, **iSID** functions reliably in the harsh conditions of remote production sites and substations.

CLEAR NETWORK VISIBILITY FOR QUICK UNDERSTANDING

iSID creates a visual network model of all devices, protocols, and links. Map View displays graphical representations of all network devices in multiple, helpful display modes like Purdue, Flow, Analyst, and Custom. Maps are zoomable and elements can be dragged to any location on the screen.

COMPREHENSIVE ASSET INVENTORY MANAGEMENT

iSID automatically discovers assets and builds an accurate asset inventory that includes roles and their impact on the OT environment. Operating in numerous OT settings over many years, **iSID** monitors generations of legacy and modern asset types as well as their communication protocols. For convenient management, it separates out illegitimate assets and reduces alerts on them. In mixed IT/OT environments, **iSID** automatically groups internet-facing assets and manages them separately.



LATEST THREAT INTELLIGENCE AND CUSTOMIZED POLICIES

iSID keeps up with the latest threat intelligence as well as SNORT-based signatures, common attack signatures, and vulnerabilities, enabling it to quickly detect anomalies before they can cause damage.

EFFICIENT ALERT MANAGEMENT AND RAPID INCIDENT RESPONSE

iSID classifies assets in the operational environment, eliminating alert noise. It helps security practitioners respond effectively by displaying alerts by type and severity class for identification and efficient handling of the most important alerts, including:

- **Cyber Attack** for suspicious network behavior
- **Policy Monitor** for communication policy violations
- **System Alerts** for anomalous topology changes and behavior
- **Asset Management** for new CVEs or device control alerts
- **Network Visibility** for networking alerts

Automated notifications are sent to relevant personnel according to operational process and severity. Clear, practical, step-by-step risk-mitigation playbooks, tailored for operational environments, enable prompt and effective incident response.

Radiflow

POLICY MONITORING

Based on its automatic learning, **iSID** creates relevant policy suggestions that can be adjusted and approved for precise implementation. Users may define and modify policies for validating specific commands ("write to controller") and operational ranges ("do not set turbine above 800 rpm"). Internet-facing assets are highlighted. Continuous supervision of configuration changes in PLCs and other network devices prevents unauthorized and inadvertent disturbances to smooth operation.

UP-TO-DATE VULNERABILITY MANAGEMENT

Accurate identification and mapping of publicly known vulnerabilities (CVEs) keep industrial sites free of cyber threats. **iSID**'s CVE database is regularly updated. For maximum efficiency, CVEs may be organized per asset and assets may be organized per CVE. Asset Patch Management helps security personnel keep up with necessary and important updates.

INTEGRATIONS

iSID enriches the operational data it collects and makes it available to external systems such as:

- **Asset management**
  - servicenow
- **Dedicated industrial cybersecurity systems**
  - cervello
  - SIGA
- **Firewalls**
  - paloalto NETWORKS
  - FORTINET
- **SIEMs**
  - splunk>
  - Radar
- **IAM**
  - RSA SecurID
  - Microsoft Active Directory

HELPFUL DISPLAYS AND DASHBOARDS

Easy-to-understand dashboards and reports display comprehensive security posture assessments and governance. **iSID** creates rich, granular reports of comprehensive security posture analyses and compliance with standards like IEC 62443. Customizable reports on vulnerabilities, compliance auditing, and more are furnished upon demand. Users may define and execute queries on any part of the **iSID** database for ad hoc and regular monitoring and reporting.

DATA-DRIVEN, AUTOMATED RISK MANAGEMENT

iSID also feeds its enriched data to the Radiflow CIARA Risk Management platform that empowers CISOs and other stakeholders to optimize their OT-security expenditure and ensure the effectiveness of threat-mitigation controls in accordance with NIS2, IEC62443, and other requirements.

FLEXIBLE DEPLOYMENT

iSID can be deployed at a central location, locally at each remote site, or a combination of both. MSSPs may monitor and manage multiple customers centrally via the iCEN centralized management dashboard. Large enterprises with multiple sites may monitor and manage all their remote **iSID** installations centrally, eliminating the need for remote security staff.

Radiflow

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.

www.radiflow.com

info@radiflow.com