Radiflow

JOINT SOLUTION REPORT

cisco Partner

Radiflow iSID & Cisco ISE pxGRID-Certified Integration

Enforcing an effective zero-trust policy, where personnel are granted only the least extent of access privilege to systems and networks needed for them to perform tasks, has become extremely challenging, with the increased use of cloud migration and mobility, and the proliferation of IoT-connected devices. Without complete and continuous visibility into all devices and other endpoints, zero-trust policies cannot be effectively enforced, thus exposing the entire network, and especially industrial operations, to cyber-breaches.

Cisco Identity Services Engine (ISE)® provides automated access policy enforcement for highly-secure networks, which can be safely extended to the ICS network with full contextual data related to OT devices and their full properties, provided by Radiflow's iSID industrial threat detection and management system.

iSID OT Data Enrichment for ISE

Contextual data on OT operations, including all OT devices, their properties, vulnerabilities, lifecycle status and zone affiliation, OT communication protocols used, ports, links and more, is crucial to ensure airtight, dynamic user authentication.

Radiflow iSID's integration with Cisco's Identity Services Engine (ISE) allows enriching the network's security enforcement capabilities with contextual data from OT operations, to provide ISE users with highly-secure network access to devices.

The ISE-iSID integration helps to gain visibility with a snapshot of OT network operations, which enables ISE users to enforce various security and access policies across the organizational network, including the OT network.

iSID's Deep Packet Inspection (DPI) engine is able to non-intrusively identify industrial assets, along with all their properties, on running industrial processes. Once identified, iSID is able to convey the OT contextual data to Cisco ISE using the pxGrid (Platform Exchange Grid) API, an open, scalable, and IETF standards-driven platform for sharing data among multiple security products across the organization, for better-informed security across all platforms and much improved threat containment.

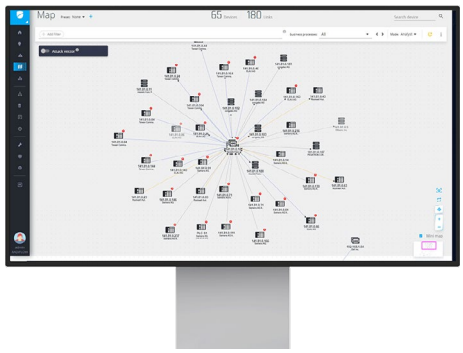
ISE is able to use iSID's detailed OT asset information to apply customer defined network access, for orchestrating appropriate levels of network access and security controls on a per-device basis.

Threat containment & prevention using ANC (Adaptive Network Control)

Devices can be "quarantined" based on alerts/anomalies detected by iSID. While it's extremely unlikely for a production OT asset to be intentionally quarantined from network access, OT security engineers or OT network administrators can activate iSID's ANC capability and apply a relevant quarantine policy to increase OT security.

This is done in iSID by restricting devices which were involved in security violation alerts, which is useful in cases of disabling remote access to devices and preventing new connections to and from devices, among other cases.

The iSID-ISE integrated solution allows extended OT asset visibility and OT environment-specific threat detection to manage and enforce customer-defined access policies in operational environments.

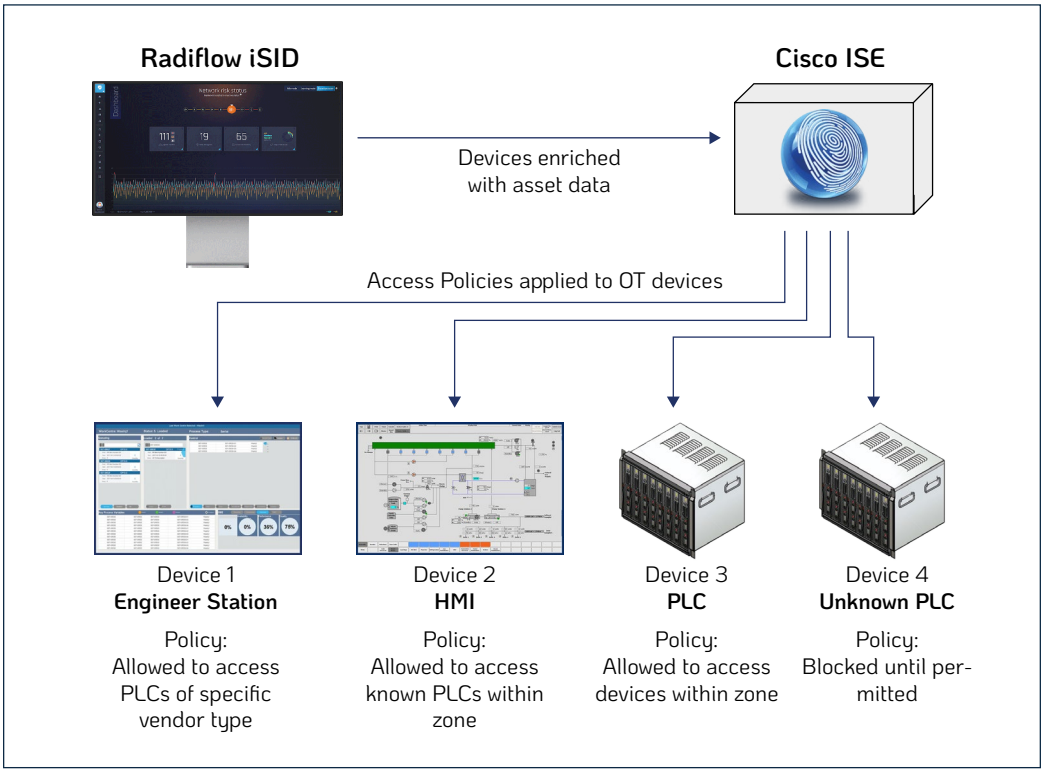


iSID provides visibility into all devices along with their full properties and connections

Solution Overview

The iSID-Cisco ISE integration combines the following capabilities and functionality to deliver powerful OT network detection and policy enforcement solution:

- OT asset information, communication patterns and network anomalies gathered and detected by iSID
- Detection of sensitive OT management commands by iSID
- ISE's policy engine allows network engineers to set up access policies according to specific cyber-security policies
- Authorization and authentication capabilities to control access to the network per device
- Utilization of Cisco's pxGrid framework for ISE integration, and ISE Adaptive Network Control capabilities to enforce quarantine policy for rogue endpoint



Schematic diagram of possible use cases for the Cisco ISE-Radiflow iSID joint solution

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

About Cisco

Cisco Systems Inc. is the worldwide leader in networking for the Internet. Founded in 1984, Cisco Systems shipped its first product in 1986 and is now a multi-national corporation, with over 35,000 employees in more than 115 countries. Today, Cisco solutions are the networking foundations for service providers, small to medium business and enterprise customers which includes corporations, government agencies, utilities and educational institutions.

Radiflow