Cisco ISE and Cyber Vision Working Together

Driving dynamic network segmentation in industrial settings

Benefits

- **Reduce the OT attack surface** by limiting the network access of each device.
- **Improve operations performance** by reducing unnecessary OT network traffic.
- **Enable collaboration** between IT and OT teams to build the right security policies.
- **Drive compliance** with IEC62443-3-3 by implementing industrial zones and conduits.
- **Extend zero-trust security** to your industrial settings by granting access based on least privilege.

How it works

- Cisco Cyber Vision inventories all industrial assets and maps their communication activities.
- Operations managers leverage the Cyber Vision maps to group devices into industrial zones.
- Cisco ISE is enriched with OT asset profiles and zone information from Cyber Vision using pxGrid.
- IT and OT managers work together to define policies to be applied between zones.
- Policies defined in ISE are enforced through dynamic assignment of VLANs, dACLs, or SGTs/Cisco TrustSec® to network equipment.
- Policies are automatically applied to devices when added or moved to a group in the Cyber Vision UI.

Overview

Many industrial networks have grown over the years to become large, flat, Layer 2 networks. The priority was to connect OT devices to accelerate industry digitization and enable more industrial automation. But more devices are being connected to industrial networks every day, many of which now need access to IT and cloud domains. It is becoming critical to segment industrial networks to reduce cyber risks and improve performance.

Together, Cisco® Identity Services Engine (ISE) and Cisco Cyber Vision offer an ideal solution for operations and IT teams to work together in implementing policies that will limit communications between industrial assets without having to modify network setups or impacting production. Malicious traffic and cyberattacks can now be contained, and network resources are optimized to improve production efficiency.

Cisco Cyber Vision

Cisco Cyber Vision is designed to help industrial organizations and critical infrastructures improve operational resilience by gaining comprehensive visibility into their industrial control networks and their OT security posture. It automatically builds a detailed inventory of all industrial assets and maps their communication patterns to provide insights into device vulnerabilities, network issues, malicious traffic, abnormal behaviors, and more.

Operations managers and control engineers can leverage the Cyber Vision map to group devices according to their role in the industrial process, creating logical zones within which communications are allowed. By doing so, they are documenting how the industrial network should be segmented and are building the foundation to drive compliance with the IEC62443-3-3 industrial security standard.

Cisco Identity Services Engine

Cisco ISE automates security policy enforcement by enabling visibility-driven network access control and segmentation. With ISE you can extend zero trust across the distributed network by gaining pervasive visibility into everything connecting to it, enforcing endpoint compliance, and enabling policy-based access to contain and prevent the lateral movement of threats.

With Cyber Vision, ISE gets detailed profiles of industrial devices. Cyber Vision operators understand the industrial processes and will create groups of devices that network managers can leverage to define zones of trust and build policies accordingly. Network equipment will then enforce these policies, effectively segmenting the network without modifying its physical setup. Different policies are automatically applied when devices are moved to a different group in Cyber Vision, making operations teams self-sufficient while maintaining compliance with security policies.

How it works

Profiling industrial assets in Cisco ISE

Cyber Vision leverages passive and active discovery to identify industrial assets. Discovery is performed by network switches and routers, so inquiries are not blocked by firewalls or NAT boundaries, resulting in 100% visibility. Using Deep Packet Inspection (DPI) of industrial protocols, it creates detailed asset profiles and maps that operation teams can easily correlate to their industrial processes. They can group assets into production zones, defining the segmentation logic that Cyber Vision shares with Cisco ISE using pxGrid.

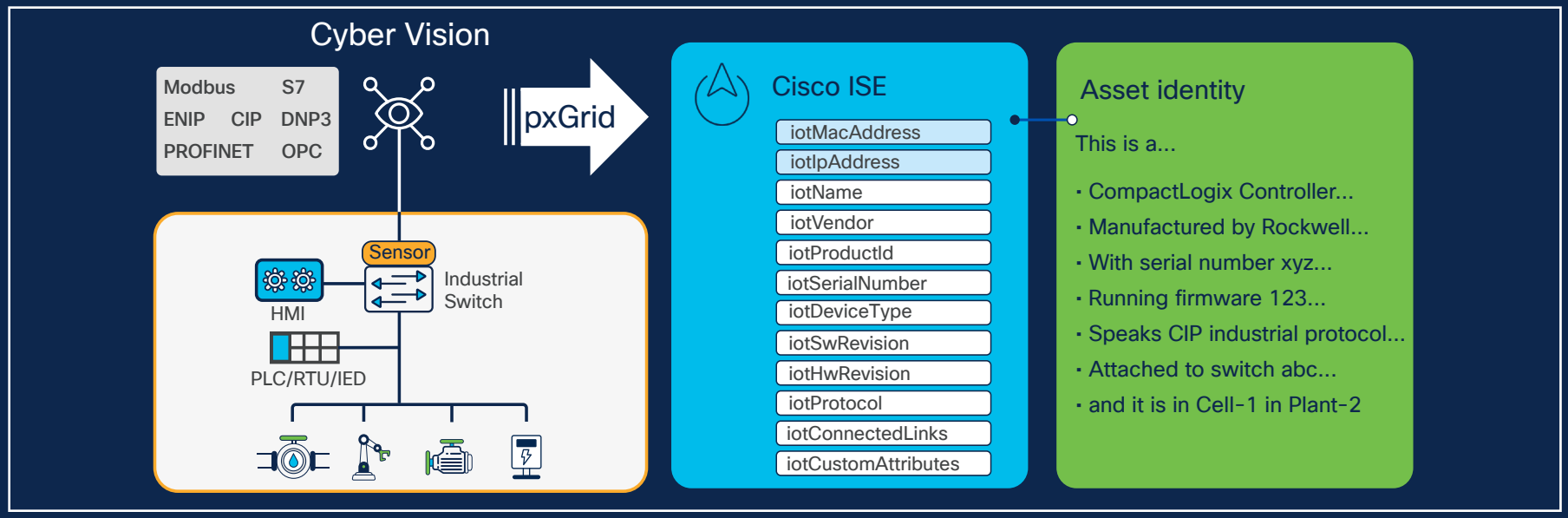

Figure 1. Cyber Vision enables ISE users to work with detailed asset profiles rather than just IP addresses

Enforcing IEC62443-3 zones and conduits with Cyber Vision

Instead of managing network access by IP address, Cisco ISE pushes security policies to the network infrastructure such as Cisco Industrial Ethernet switches. Each OT device automatically gets assigned a Security Group Tag (SGT) that defines its access policy, which all network equipment will now enforce. This allows teams to map and maintain policies much more efficiently and also to adapt them based on threat detection or the need to move a device to a different industrial process. The network becomes easier to scale, manage, and control.

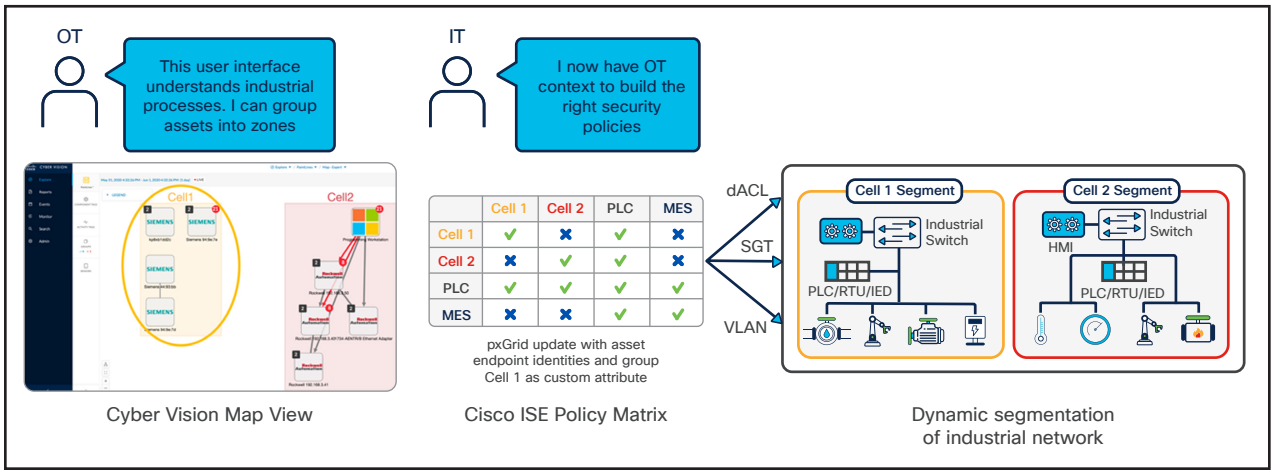

Figure 2. Visibility into OT assets and processes drives network segmentation

Start segmenting your industrial network today

Talk to a Cisco sales representative or channel partner and visit cisco.com/go/cybervision or cisco.com/go/ise to learn more.

The Cisco advantage

For more than 15 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.

C22-3350014-01 08/24