The bridge to possible

Extending Zero Trust for Workplace to Industrial IoT

Securing the workplace in industrial networks

July 2023

Extending Workplace Zero Trust to Industrial Settings

Endpoint Visibility

Endpoint Compliance

Network Segmentation

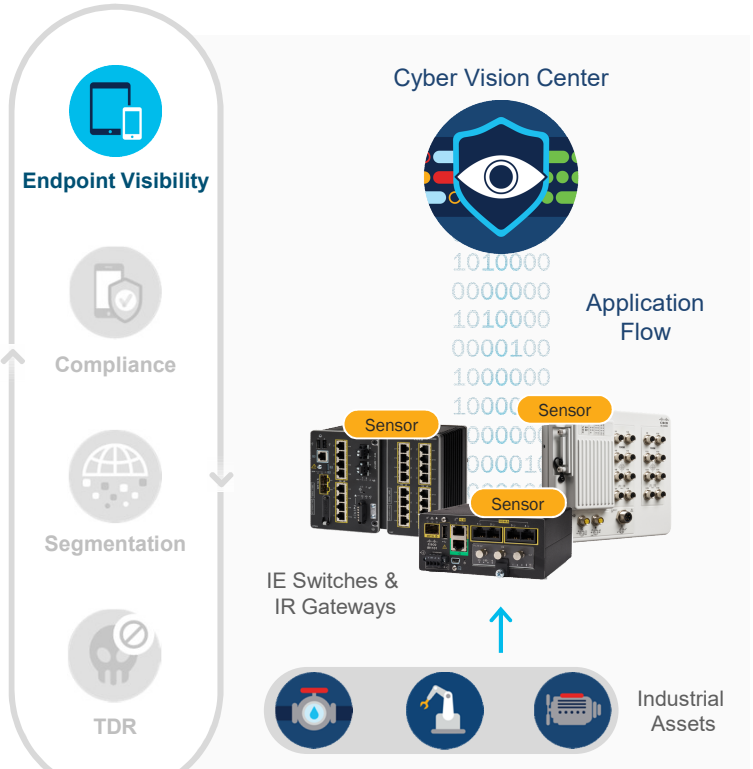
Threat Detection & Response

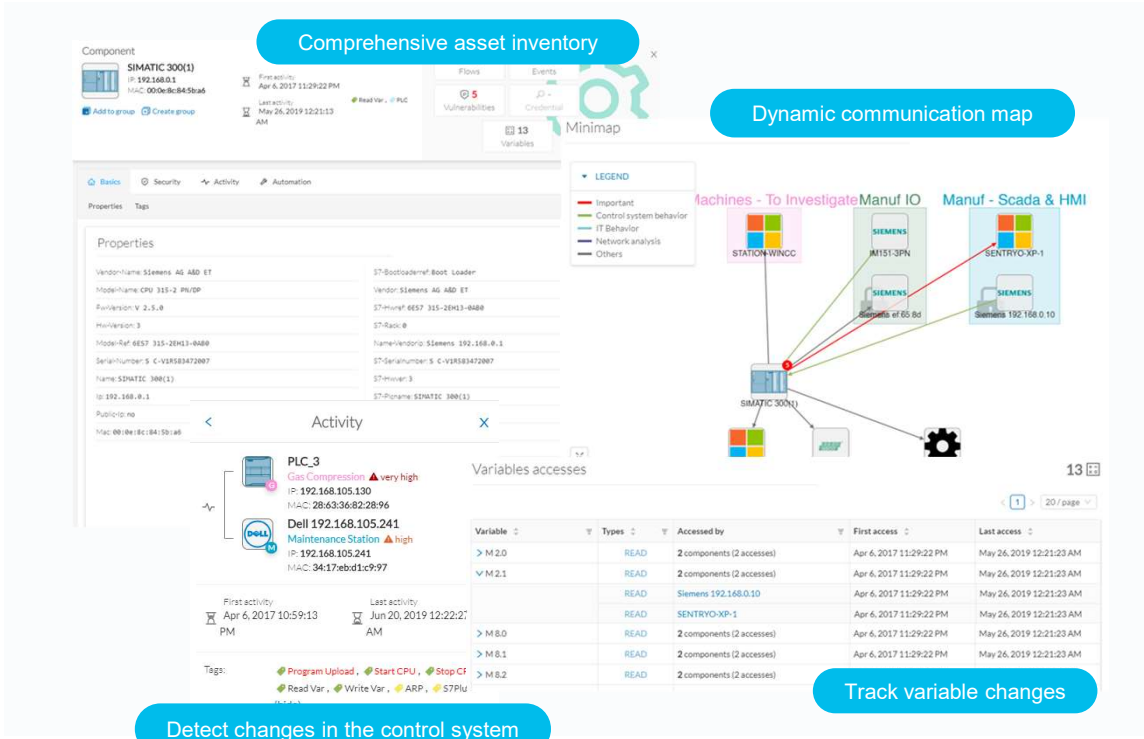
Cisco IoT

Industrial Endpoint Visibility

Industrial Control System device visibility based on application-level decoding of industrial protocol traffic and behavior modeling of industrial endpoints

Industrial Endpoint Visibility with Cyber Vision



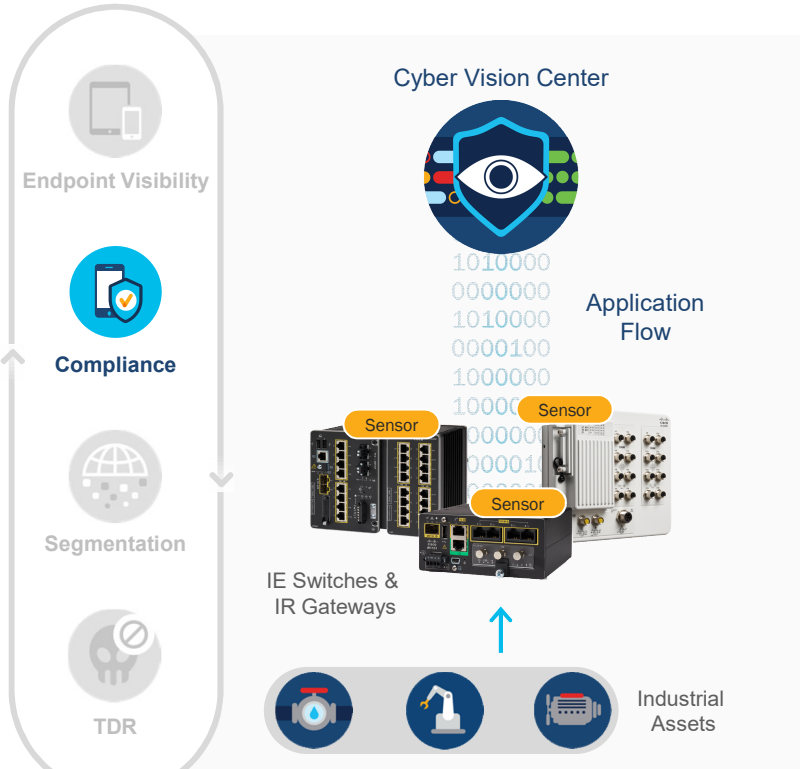


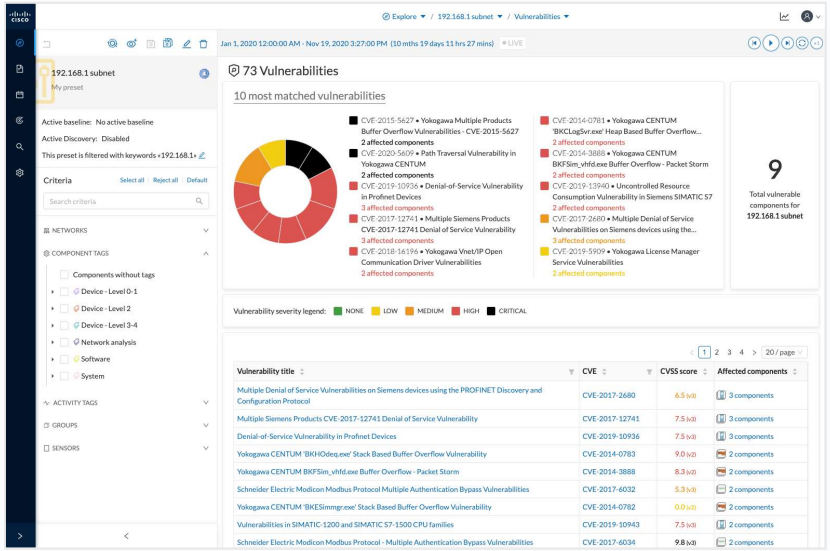
Cisco IoT

Endpoint Compliance for Industrial Endpoints

Common Vulnerabilities and Exposures (CVE) & **Risk Scores** for Industrial endpoints to identify and focus on the assets in the environment that need to be protected first.

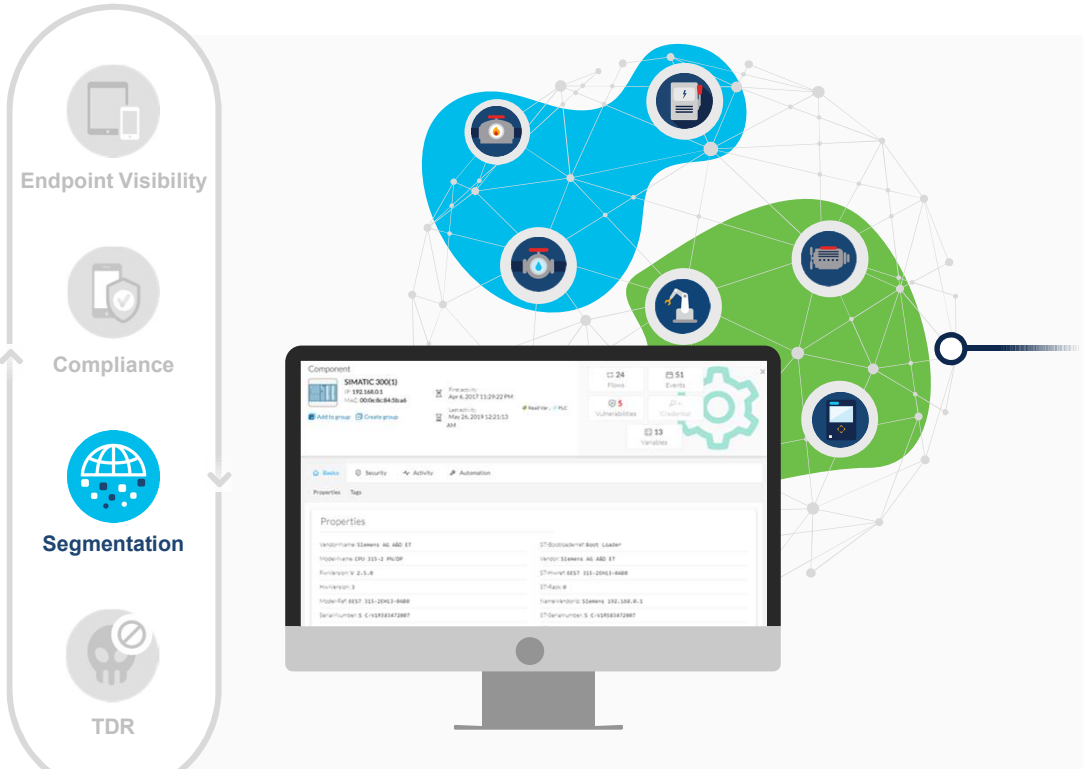
Industrial Device Vulnerability Detection





Cyber Vision matches device attributes against **built-in vulnerability database** curated by Cisco Security Teams to easily identify vulnerable components

Segmentation



View application relationships to **group endpoints into zones** and **identify conduits** in Cyber Vision

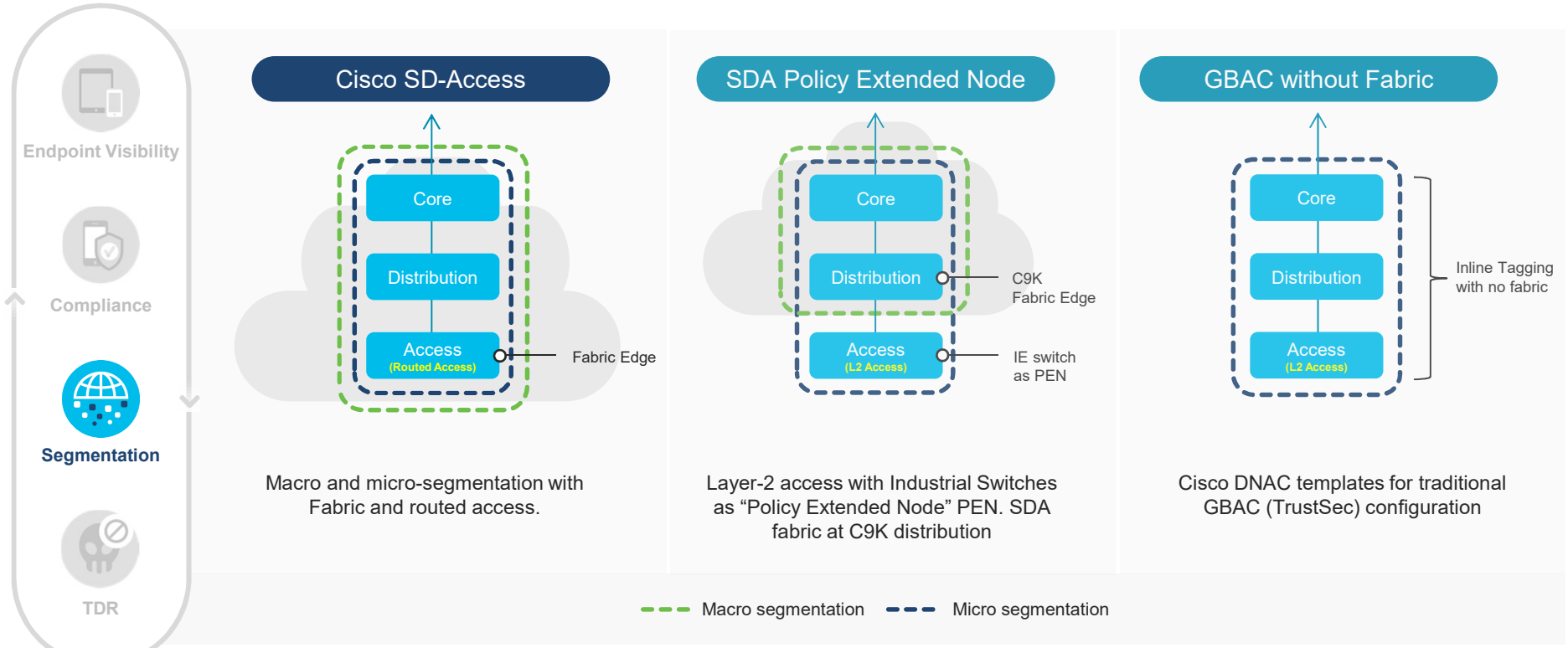
Enable OT users to **dynamically map zones to scalable group tags** of pre-defined TrustSec policies built by IT in ISE

Visualize **traffic activity between scalable groups** in DNAC policy analytics

Deploy group segmentation policy with confidence once you are comfortable with the observed network behavior using DNAC Day-n templates

Cisco IoT

Segmentation Architectures



Identify Zones and Conduits

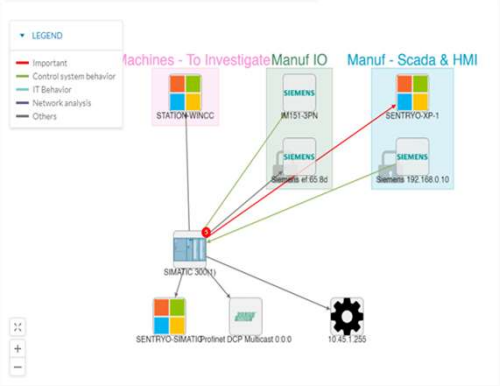
Endpoint Visibility

Compliance

Segmentation

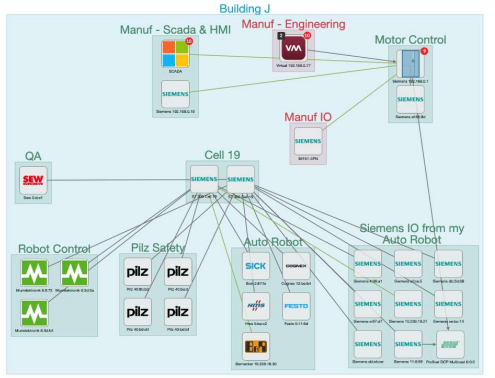
TDR

Identify Application Relationships



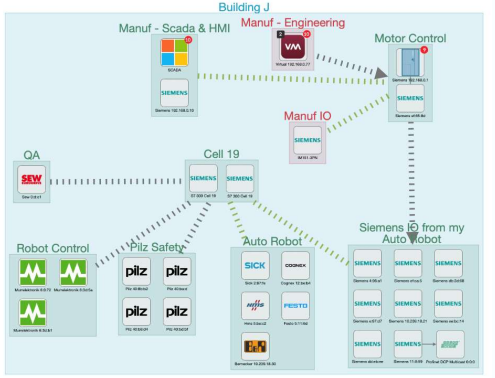
Cyber Vision maps traffic flows between endpoints and provides application-level details within the flows

Group endpoints into Zones



Users can leverage these application relations to group endpoints to match the industrial processes they represent

Visualize Conduits between Zones

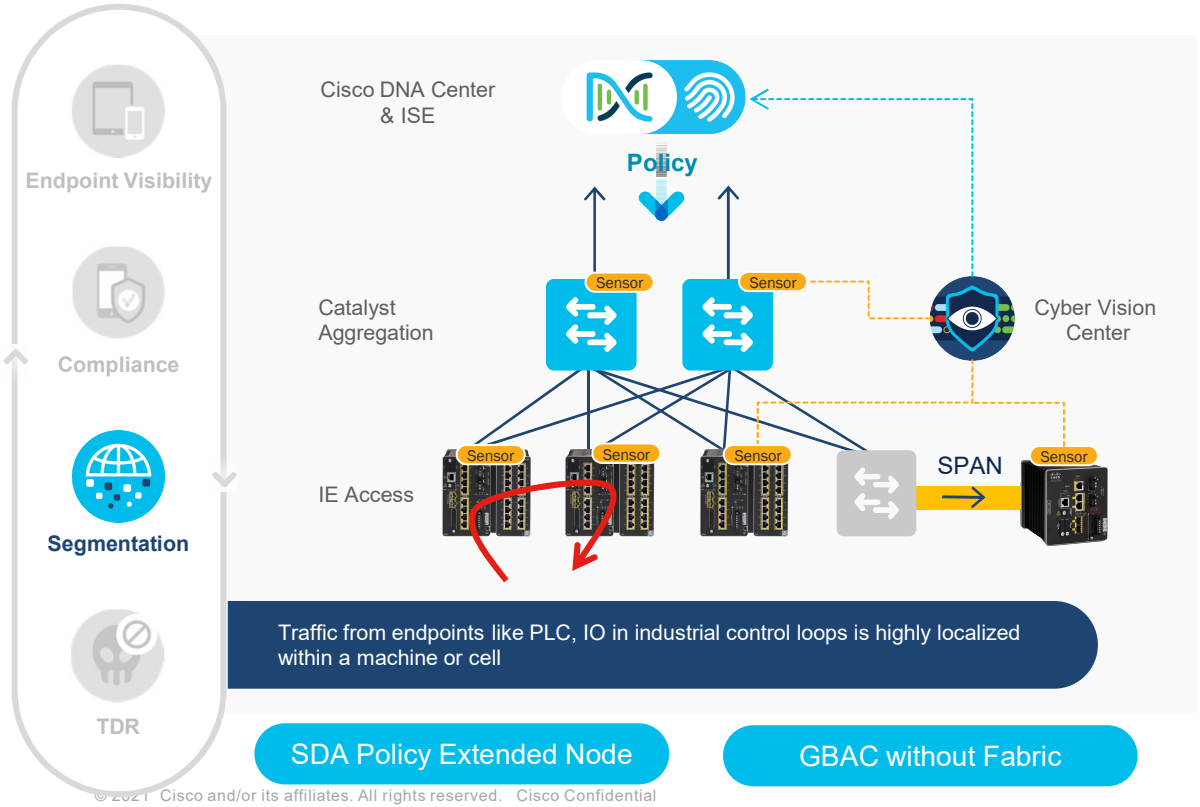


The traffic flows can be aggregated into conduits which can be used to inform segmentation policies

Cisco IoT

Bringing it all Together

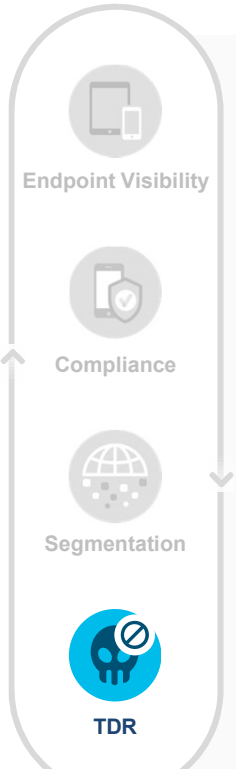
Segmenting with Visibility & Policy Analytics

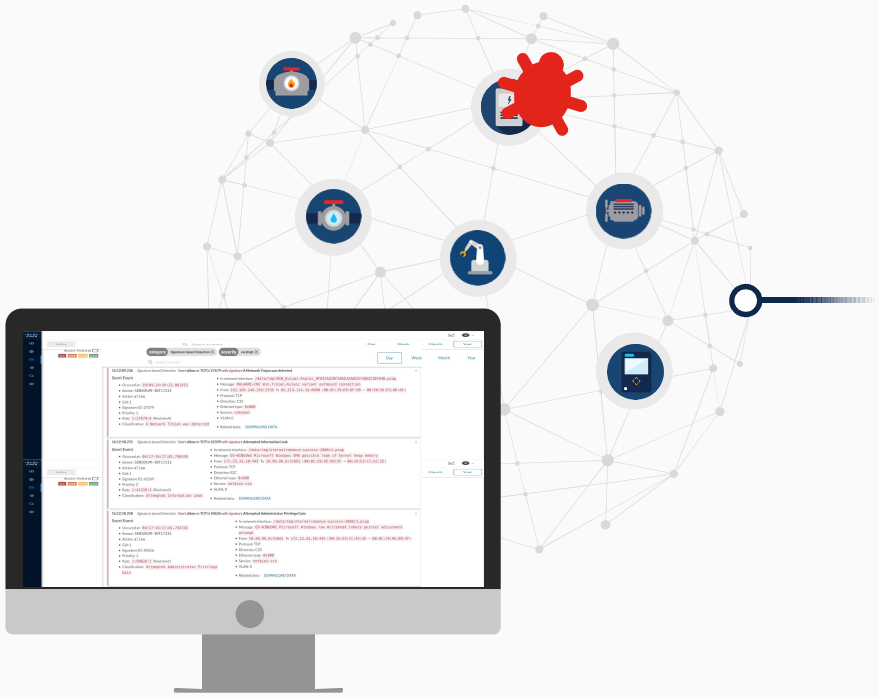


1. Discover endpoints and visualize application relationships in **Cyber Vision** to help inform creation of TrustSec group-based segmentation policies in **DNAC Access Control Application**
2. Endpoint grouping in Cyber Vision triggers pxGrid updates and results in dynamic assignment of SGTs in **ISE**
3. Visualize group-based network behavior using NetFlow traffic in **DNAC Policy Analytics**
4. Deploy segmentation policy with confidence using **DNAC Day-n templates** once you are comfortable with the observed network behavior

Cisco IoT

Threat Detection & Response





Detect Industrial **endpoint behavior anomalies and signature-based threat detection** in Cyber Vision

Stream **syslog events to SIEM** for SOC alerts

Promote incidents for investigations in SecureX

Integrate with ISE to **quarantine impacted endpoints** connected to IE switches

The bridge to possible