The bridge to possible

Cisco XDR and Cyber Vision Working Together

Investigate and manage cyberthreats to your industrial operations.

Overview

Industrial networks and critical infrastructures have become the new playground for cybercriminals. As you are digitizing your industrial operations, you are enabling seamless communication between IT, cloud, and industrial networks, exposing both the enterprise network and the industrial environment to grave cyberthreats.

Cisco® XDR and Cisco Cyber Vision offer an ideal solution to investigate and remediate threats across both IT and industrial networks. Together, they leverage deep visibility into your Operational Technology (OT) and intelligence from your entire IT security stack, offering a unified view across domains, so you can better protect the global enterprise while drastically simplifying and accelerating critical security operations.

The bridge to possible

Benefits

- Understand your global threat surface – with a detailed dynamic inventory of industrial assets
- Simplify investigations – by aggregating and correlating global intelligence and local context across both your IT and OT infrastructures in one view
- Accelerate time to remediate – by leveraging out-of-the-box or custom orchestration workflows that empower your IT security tools to protect your industrial operations
- Enable better collaboration – between SecOps, NetOps, and OT teams by enabling information to flow seamlessly between tools designed for their specific roles

Cisco XDR

Cisco Extended Detection and Response (XDR) simplifies security operations, providing a streamlined approach to quickly detect, prioritize, and respond to sophisticated threats. It collects and correlates data and telemetry across multiple sources — network, cloud, endpoint, email, identity, and applications — to provide unified visibility and deep context into advanced threats while reducing time-consuming false positives. Built-in automation, orchestration, and customizable playbooks help defenders automate repetitive tasks and mitigate threats more effectively.

Together with Cyber Vision, Cisco XDR enables advanced OT threat detection, investigation, and remediation, by leveraging capabilities from your entire IT security stack. Investigations can be launched with a simple click, gathering insights from all connected security tools and threat intelligence sources. Remediation workflows can be triggered from within Cyber Vision, with tasks orchestrated across your security technologies.

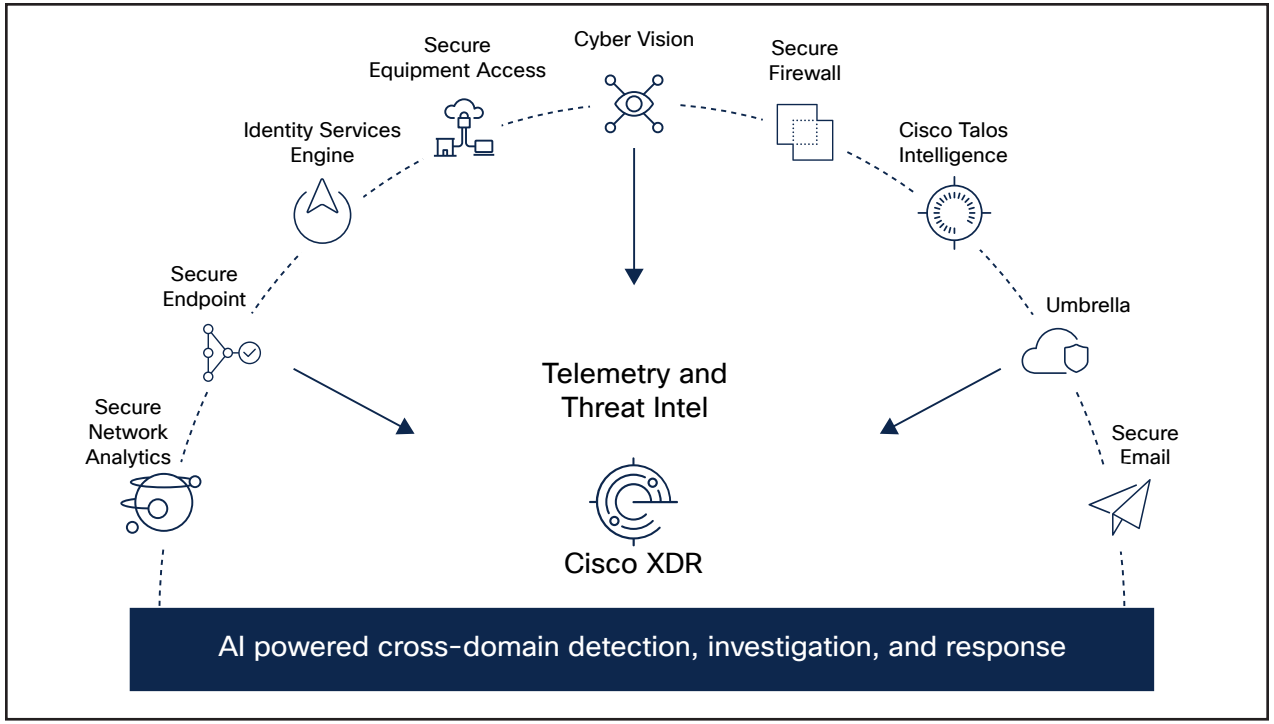

Figure 1. Manage threats using your entire security stack

The bridge to possible

Cisco Cyber Vision

Cyber Vision helps 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 connected industrial assets and maps their activities to provide insights into OT vulnerabilities, network issues, intrusions, malicious traffic, abnormal behaviors, and more.

Together with Cisco XDR, Cyber Vision extends your IT security tools and procedures to your industrial settings. It gives industrial operations teams the insights they need to maintain uptime while connecting them to your global cybersecurity strategy. Cyber Vision enables simple and effective ways to understand OT security events and protect the environment against unexpected modifications to the industrial control system, such as changes to a controller, communications with a public IP address, or remote access sessions, for instance.

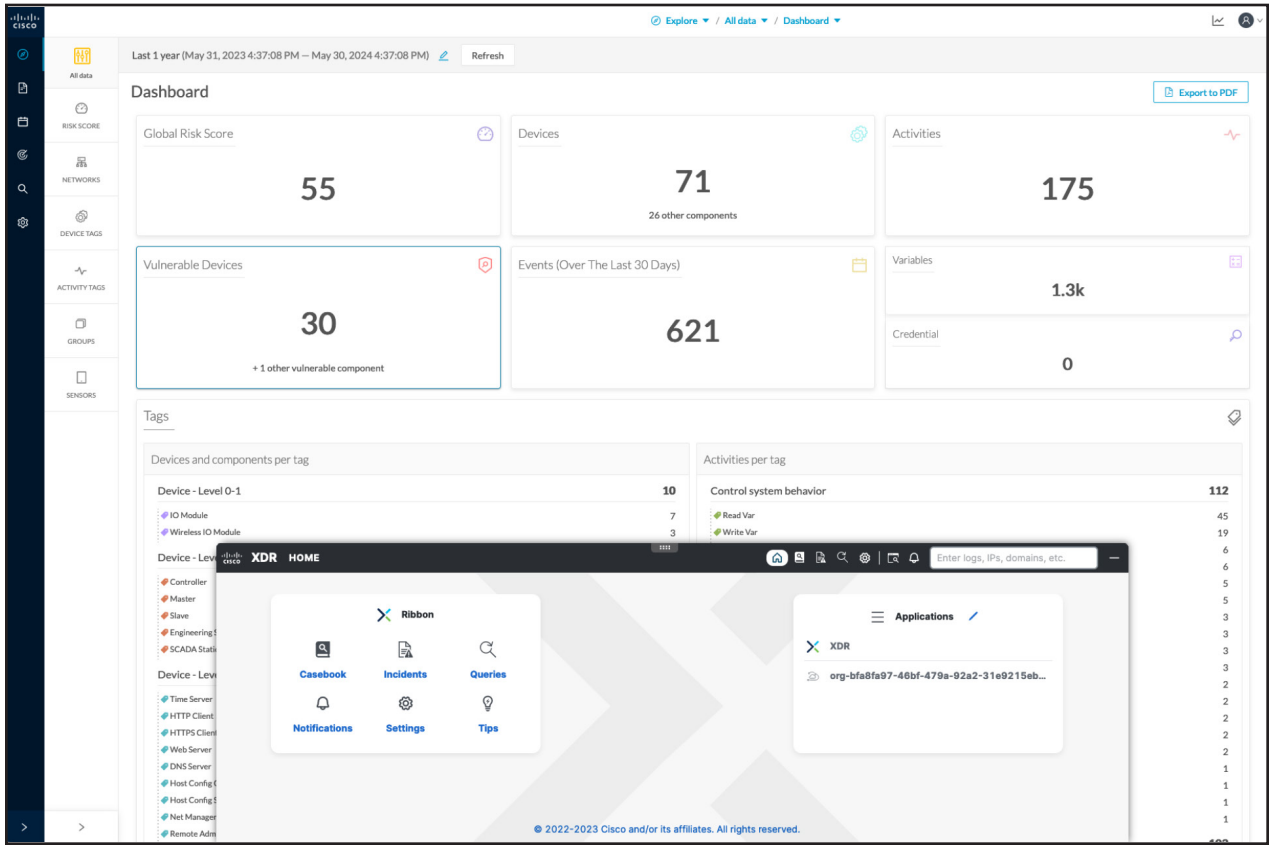

Figure 2. The XDR ribbon in Cyber Vision streamlines investigations and remediation orchestration.

The bridge to possible

How it works

Cyber Vision OT security insights

Cyber Vision combines protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis to help detect threats to your industrial operations. It lets you define what normal looks like by creating multiple baselines that focus on what is most critical to you. All events are shown in various lists, dashboards, and reports with additional context and criticality levels automatically applied to them. Events can be reported to Cisco XDR with a simple click to create cases and have security analysts run detailed investigations.

XDR ribbon

The Cisco XDR ribbon is a persistent bar in the lower portion of the Cyber Vision user interface, letting you search the current Cyber Vision page for any cyber observables, create and manage cases, trigger orchestration workflows, and more, so you don't have to navigate to multiple consoles to run the functions you need. With the XDR ribbon, you can also quickly pivot between Cyber Vision, XDR, and the console of any integrated product to perform advanced tasks with the appropriate context provided by Cyber Vision.

XDR investigations

Cisco XDR simplifies threat hunting and incident response by providing your security investigations with context and enrichment from your Cisco security solutions, Talos® threat intelligence, and third-party tools, all in a single console. It identifies whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious or malicious, and whether you have been affected by them. These investigations can be easily launched from Cyber Vision by selecting a suspicious component in the XDR ribbon.

XDR orchestration

Cisco XDR automates repetitive and critical security tasks such as threat hunting and remediation by leveraging prebuilt workflows and response capabilities. You can also create your own tasks with a no- or low-code, drag-and-drop canvas. XDR leverages Cisco Secure and third-party multidomain systems, applications, databases, and network devices in your environment to run these workflows. An example would be to assign a security group tag to an OT asset in Cisco ISE that would ultimately prevent this asset from communicating on the network.

The Cisco advantage

For more than 20 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.

Streamline OT threat investigation and remediation today

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

C22-3357334-01 06/24