ARC WHITE PAPER

FEBRUARY, 2021

Cisco Cyber Vision Enables Active Defense of Industrial Operations

By Sid Snitkin

Summary

The need for better industrial cybersecurity has never been more apparent and urgent. Ransomware is disrupting industrial operations around the world. Sophisticated attacks on operational technology (OT) systems are threatening the safety and reliability of critical infrastructure. Expanded access for remote workers and developments like cloud apps, edge computing, and digital transformation are expanding an already challenging attack surface.

CISOs in industrial organizations are under extreme pressure to ensure the security of IT and OT systems. To do this, they need complete, accurate information about the security status of every corporate cyber asset. They also need a team of experienced defenders with technology that enables rapid detection and response to new threats. While IT cybersecurity programs generally support these requirements, few OT programs have reached this maturity level.

Industrial companies need to protect facilities from sophisticated attacks and security gaps introduced by digital transformation. Cisco Cyber Vision can provide the visibility and access that defenders need to rapidly detect and deal with these threats. It's architecture also facilitates IT-OT cybersecurity convergence efforts.

OT systems are inherently difficult to secure. Legacy assets, like PLCs and DCS systems, can't be upgraded or protected with conventional security products. Many industrial applications require old, unsupported operating systems. Industrial networks lack basic security capabilities. Even where security solutions are deployed, operating constraints prevent timely updates and patches.

Anomaly and breach detection has emerged as a panacea for these OT security challenges. But adding this technology to an insecure system won't help unless there are experienced defenders to monitor alerts and deal rapidly with suspicious behaviors. Smart companies recognize that anomaly

detection investments need to be part of a broader program that integrates IT and OT cybersecurity people, processes, and technologies.

This report discusses the role of anomaly detection in OT system cybersecurity and what is needed to realize true security benefits. It also highlights the challenges companies need to consider to deploy this technology effectively.

An analysis of Cisco Cyber Vision and the broader Cisco cybersecurity portfolio reveals Cisco's deep understanding of OT cybersecurity and the company's commitment to helping industrial companies establish better security across their complex operations.

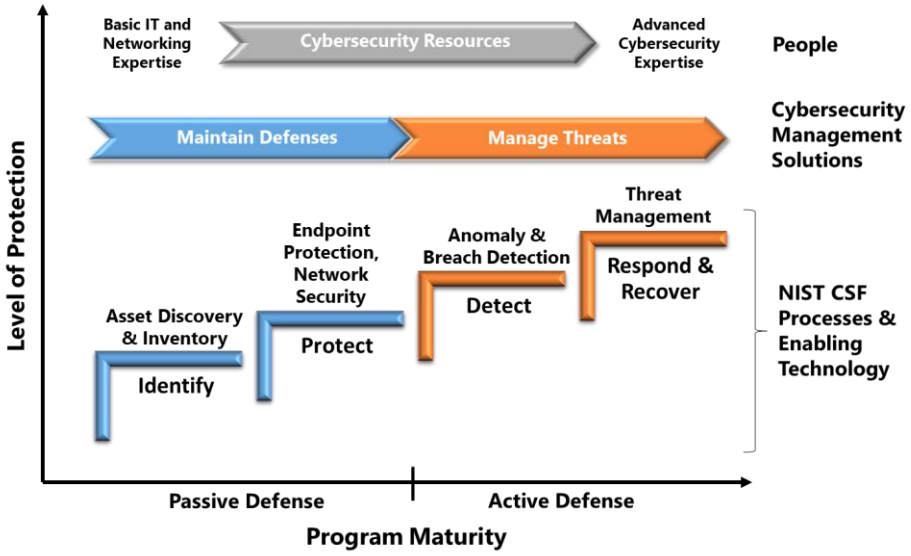
Growing Threats Demand Active OT Cybersecurity

OT cybersecurity is not a new issue. Industry and governmental groups already provide guidance and standards to help companies defend critical plant systems. While many companies have made the necessary investments to meet the basic requirements, few have invested in the people and processes needed to maintain defenses and manage threats. Isolation has been the primary focus, with the hope that this is enough to overcome inherent security weaknesses and resource constraints.

Sophisticated attacks, like Triton, show that basic defenses aren't enough to protect OT systems, especially when they aren't maintained. Efforts to enable remote workers, vendor access, and connectivity with cloud apps, mobile devices, and IoT sensors also undermine the effectiveness of isolation strategies. Today's OT systems face the same challenges as IT systems and merit equal cybersecurity sophistication. This includes experienced defenders equipped with tools that enable effectiveness and efficiency, diligent management of known vulnerabilities and threats, continuous monitoring of systems for suspicious behaviors, and, rapid isolation and remediation of compromised assets.

ARC's Industrial/OT Cybersecurity Maturity Model illustrates the changes required in existing OT cybersecurity strategies. The model uses the NIST Cybersecurity Framework to show how cyber risks are reduced incrementally as companies adopt certain practices. It also shows the people, processes, technology, and cybersecurity management solutions needed to accomplish the goals of each step. Program maturity is assessed according to how well the company maintains alignment across all these categories.

Technology investments only generate security benefits when they are maintained and leveraged by knowledgeable defenders.



ARC Industrial/OT Cybersecurity Model

Blue and orange colors distinguish passive and active defense elements. Passive elements focus on reducing the likelihood of a system compromise. Active elements focus on reducing the impact of an actual compromise.

While IT cybersecurity programs include passive and active defense, OT cybersecurity investments are generally limited to passive defense. Some companies recognize the need for active defense in OT systems, but too many assume that this only requires adding anomaly and breach detection technology. As the ARC model illustrates, anomaly and breach detection is only one part of an active defense program. Few security benefits accrue without investments in the other active defense elements.

Active defense can raise the security of OT systems to the same level as corporate IT systems, but only if all of the elements in ARC's model are implemented. As this requires investments in the same kinds of people, processes, and technologies used in IT, smart companies are using this as an impetus for converging IT and OT cybersecurity programs. Converged programs reduce costs, promote use of common solutions, and enable integration of information that improves security of both IT and OT systems.

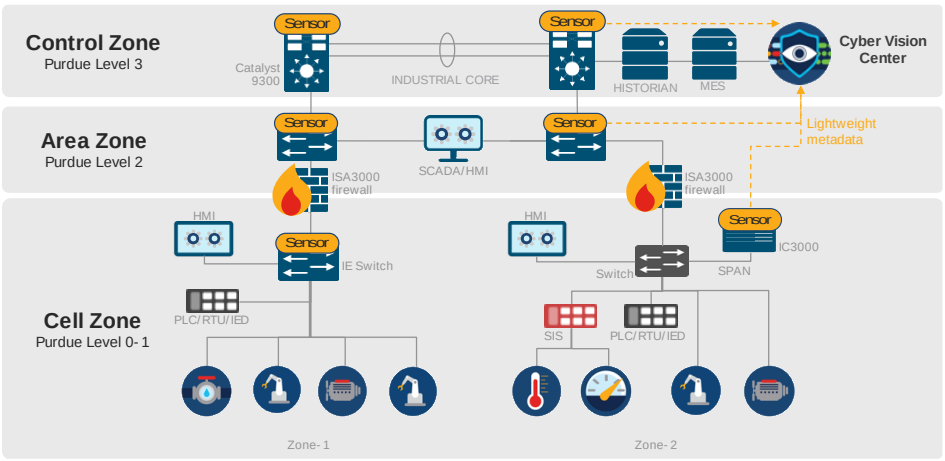
Cisco Meets the ARC Challenge

IT and OT people around the world know Cisco as a leading supplier of networking products for office and industrial environments. Security professionals know that Cisco is also a leading cybersecurity company with a broad portfolio of sophisticated IT, cloud, and mobile security solutions and services. Cisco Cyber Vision, a recent addition, extends the company's footprint to include OT anomaly and breach detection.

Cisco Cyber Vision provides deep visibility into OT assets, industrial network flows, and anomalous behaviors in OT systems. The product also leverages Cisco Talos intelligence to detect vulnerabilities, intrusions, and malicious traffic. Deep integration with other Cisco security products delivers this OT security information to the company's IT security operations centers (SOCs) so defenders can quickly analyze and respond to OT system threats. Defenders can also use this OT data to strengthen IT system defenses and improve context in forensic efforts.

Cyber Vision Offers Flexible Deployment Options

Cisco Cyber Vision has a unique edge monitoring architecture that allows its use in a broad range of OT system environments. The way that processing is distributed between sensors and the Cyber Vision Center also reduces the need to install additional, out-of-band networks. Communication between sensors and Cyber Vision Center use lightweight metadata that can be sent on existing networks with minimal impact on bandwidth.



Cyber Vision Deployment Options

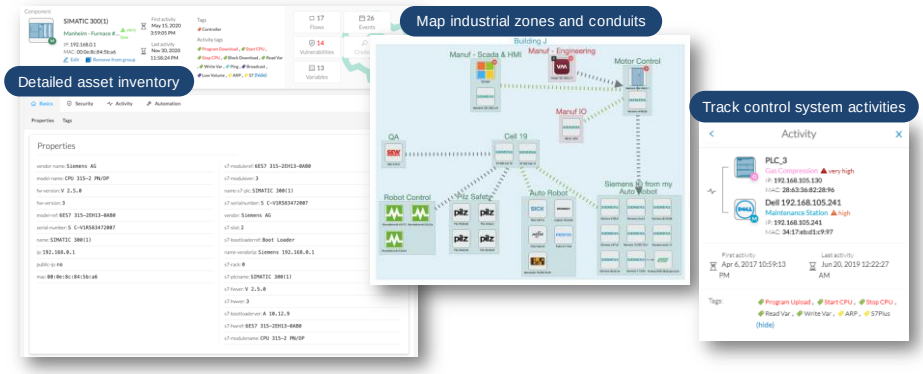
Cyber Vision sensors be embedded within certain Cisco industrial switches and routers like the IE3x00 and Catalyst 9300 switches or the IR1101 gateway. The reduced costs of this approach enables broad deployment and minimal NetOps support. This approach also provides comprehensive asset coverage by gaining visibility into each production cell without the need for dedicated security appliances or complex span collection networks.

Using the IC 3000 platform, Cyber Vision sensors can also be deployed as separate appliances that collect span data from existing network equipment. Cyber Vision Center can also embed sensor capabilities for cases where out-of-band span collection networks already exist. This enables easy upgrades of existing anomaly and breach detection systems.

Regardless of the deployment approach, Cyber Vision provides continuous parsing of messages for a variety of popular industrial networking protocols.

Cyber Vision Enables Better Asset Inventory Management

Cyber Vision Center uses the parsed information to develop and maintain accurate asset inventories and to detect anomalous OT system behavior that might indicate a cyber compromise or abnormal process conditions. Cyber Vision also supports active asset discovery. This is managed locally, within each sensor, to ensure maximum coverage of assets. Because sensors are embedded in network equipment, active discovery requests are sent below firewall and NAT boundaries, allowing Cyber Vision to see assets in sub-networks.



Cyber Vision Center

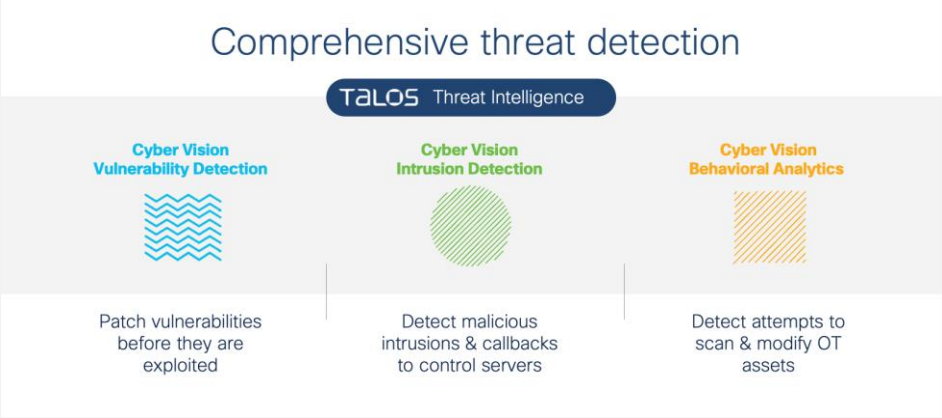
Cyber Vision Center was designed to have a friendly, comprehensive user interface for user access to asset information. It allows users to give assets

meaningful names, group assets into IEC62443 zones, manage risk level by zone, gain insight on industrial processes, and alert people when an abnormal event is detected.

Asset information includes details like vendor references, firmware and hardware versions, serial numbers, rack slot configurations, etc. Asset relationships and communication patterns are also identified. All this information can be viewed in various types of maps, tables, and reports. Cyber Vision automatically applies tags to assets and communication flows so that anyone can easily understand a device role or a message content regardless of the protocol at play.

Cyber Vision Provides the Threat Visibility CISOs Need

Cyber Vision gives CISOs and security teams a full understanding of the security status of every OT asset and early warning when urgent action is needed. This is accomplished through a mix of asset vulnerability detection, intrusion detection, and anomalous behavior analytics.



Cyber Vision Threat Detection Capabilities

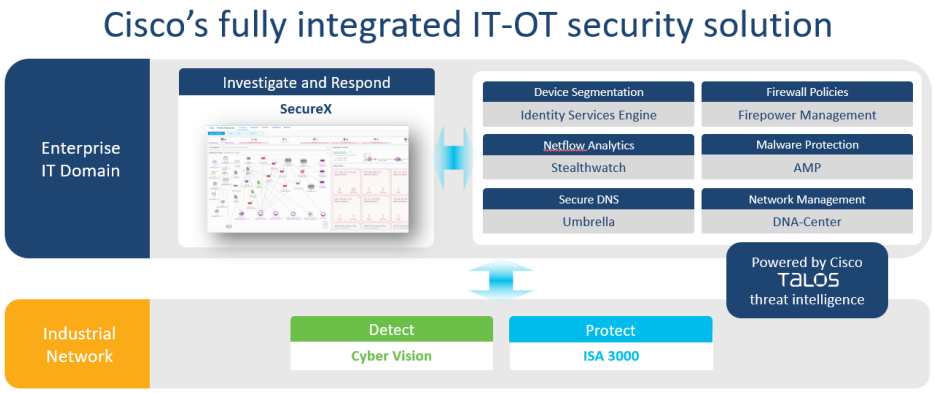
Cyber Vision's asset vulnerability detection keeps users abreast of known vulnerabilities in asset hardware, software, and configuration. The solution's intrusion detection leverages intelligence from Cisco Talos to detect any new threats that enter the system. Cyber Vision's threat knowledge base is updated several times per month to include the latest list of asset vulnerabilities and IDS signatures.

Cyber Vision's behavioral analytics engine automatically baselines industrial network communications and uses this to detect new or deleted assets,

unexpected activities, and changes to variables and device configurations. The analytics typically do not require a lengthy learning period and systems can have as many baselines as they need to focus detection on critical issues, specific assets, particular behaviors (like remote access), and minimize false positives during certain periods (like maintenance).

Deep Integration Enhances Cyber Vision Benefits

Cyber Vision's out-of-the-box integrations with Cisco's security portfolio and a broad set of third-party solutions enhance its value for CISOs and SOCs charged with defending OT systems.



Cyber Vision is Fully Integrated with Cisco's Security Portfolio

Integrations with Cisco SecureX and leading security information and event management (SIEM) solutions enable direct injection of OT events into security analyst workflows. This can accelerate investigations and reduce response times. SecureX enables defenders to quickly launch pre-populated searches of other Cisco products for related information and events. OT events can also be correlated with events occurring in other systems to speed root-cause identification.

Cyber Vision's integration with Cisco ISE and Cisco Firepower extends software-based network segmentation and policy enforcement capabilities to industrial control networks. Cisco ISE leverages Cyber Vision's asset groups to automatically build secure zones and enable dynamic micro-segmentation of industrial networks. Cisco Firepower uses Cyber Vision's host information to provide additional context for firewall policies.

Cyber Vision is also integrated with Cisco Stealthwatch. This enhances its behavioral monitoring capabilities by adding context to the network flows it monitors, which speeds up incident response and forensics by pinpointing ICS assets on alarms.

Cyber Vision exposes functionality and data through a REST API. This enables integrations with third-party solutions (such as firewalls from Fortinet or Palo Alto Networks) and homegrown applications for activities like compliance and risk reporting, system and event monitoring, and dashboards. The solution's discovery and event data can also be output in syslog and common event format (CEF) for consumption by third-party applications like configuration management databases and security orchestration, automation, and response (SOAR) platforms.

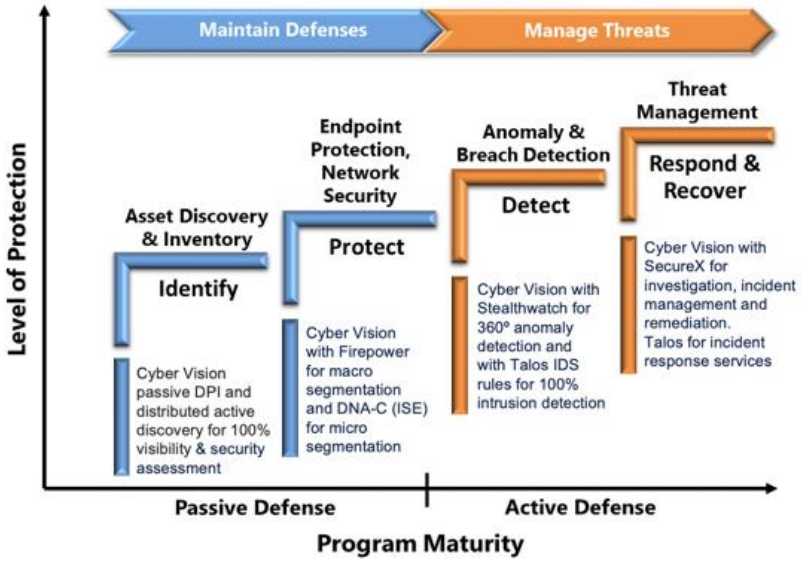
Cyber Vision Guidance and Support Services

Cisco's commitment to OT cybersecurity is clear from its investments in products like Cyber Vision and the ISA 3000 industrial firewall as well as its Talos team, which is dedicated to threat intelligence and incident response for ICS. These products and services reflect the company's deep experience in networking, security, and OT systems.

Cisco also backs its OT cybersecurity offerings with extensive investments in reference guides and support services to ease product deployment in industrial facilities. This includes pre-deployment (assessment services), during deployment (Cisco Validated Design reference architectures for manufacturing, utilities, and other industrial applications), and, post-deployment (Talos Incident Response services for investigation and remediation of cyber incidents).

Conclusion

This report discussed the importance of securing industrial OT systems and the inherent challenges that must be overcome. It highlights the need for active defense in OT cybersecurity strategies. While anomaly and breach detection is a necessary element, ARC's analysis showed why it isn't sufficient to ensure the health and safety of workers and operational continuity. These goals can only be achieved when the company has the people, processes, and supporting technology to rapidly respond to alerts and intrusions. Convergence of IT and OT efforts is recommended as the best way to achieve these capabilities.



Cisco's OT Security Portfolio Helps Organizations Protect Their Industrial Operations Along Each Phase of the ARC Cybersecurity Model

The review of Cisco Cyber Vision and the broader Cisco cybersecurity portfolio highlights the kinds of capabilities that CISOs need to ensure the security of OT systems. The urgency in implementing these capabilities can't be overstated. Sophisticated attacks continue to grow and digital transformation is rapidly eroding isolation barriers. Cisco offers one of the most comprehensive sets of solutions to help companies manage these critical risks.