White paper
Cisco public

The bridge to possible

IT and OT Cybersecurity: United We Stand, Divided We Fall

Industrial environments are changing. Technological evolutions such as Industry 4.0 and the Internet of Things (IoT) are Altering Operational Technology (OT). These innovative technologies are far outpacing cybersecurity within industrial networks, and many organizations have already been struggling to retrofit aging environments that were insecure by design. OT and IT have become inextricably linked, and organizations must unify their efforts to better protect themselves.

IoT devices have started to play a major role in OT networks. IP cameras now monitor critical systems, and smart sensors in manufacturing environments transmit valuable data directly to the cloud. These developments have improved quality and made processes run more quickly than ever. However, these developments also carry risks that can leave industrial environments vulnerable.

Many assumptions regarding the best methods for securing industrial networks and critical industrial control systems are no longer valid. Traditional measures such as "security by obscurity," air gapping, or establishing an industrial demilitarized zone are no longer sufficient to protect industrial environments. Isolating industrial networks is not always effective, and air gaps make data inaccessible and prevent reconfigurations and patching. The truth is, many of these so-called air-gapped systems are rife with back doors. For example, just think of the vendors and third-party technicians who have set up their own remote access to update systems and devices in OT environments.

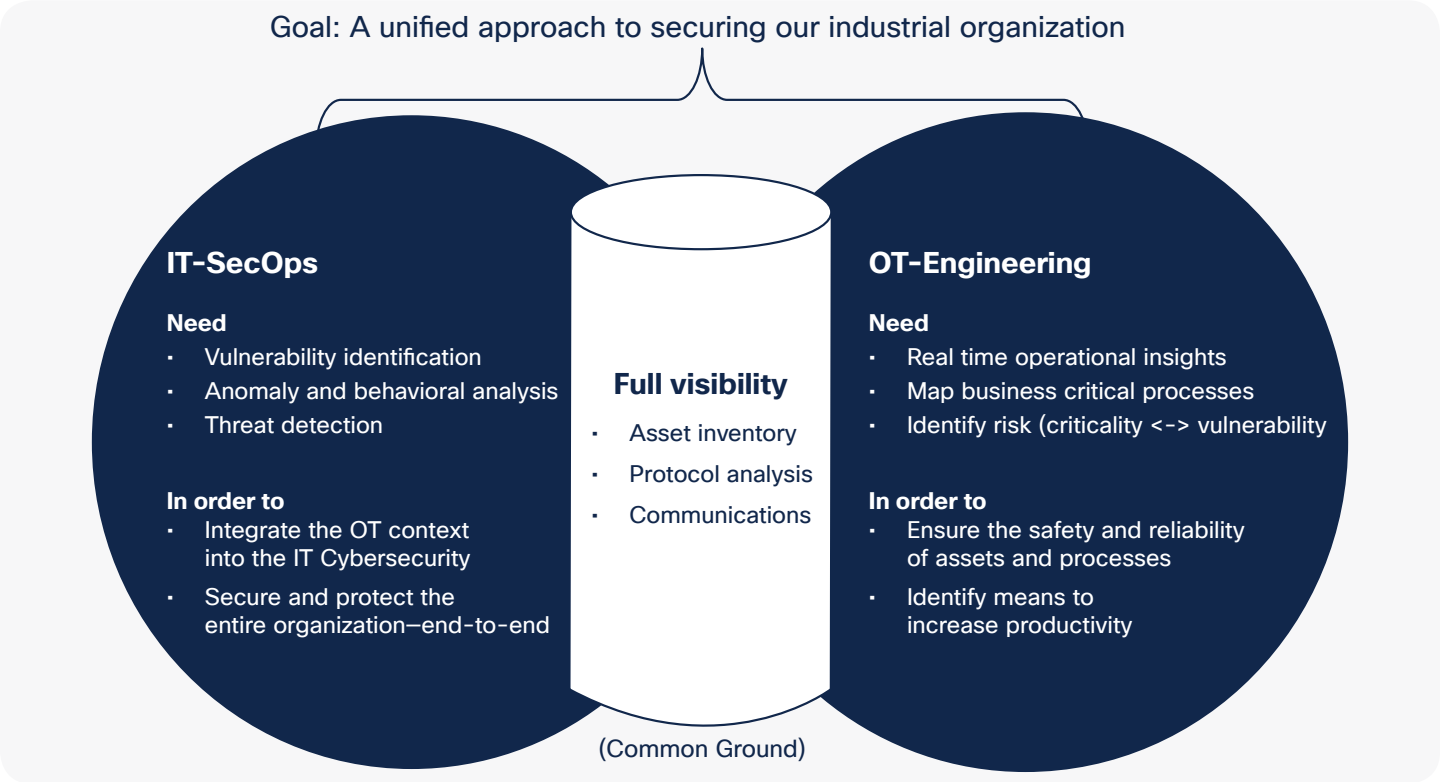
As cyber attacks on industrial environments increase in frequency and complexity, board members and government regulators are pressuring organizations to ensure that these risks are managed and that business-critical IoT/OT networks are adequately protected. Accomplishing this task requires a collaborative approach in which IT and OT have an equal footing.

In many organizations, the Chief Information Security Officer (CISO) and the IT team have the overall accountability for cybersecurity. They have the tools, expertise, and methodologies necessary to secure the enterprise, and they often control the budget. However, IT and SecOps personnel rarely have the required expertise or insight into operational and process control technology. This knowledge gap often leads IT and SecOps personnel to assume that the same approach they use to secure IT will work in the OT environment.

To forge ahead, IT teams need to work alongside OT engineers to ensure that they have a deep understanding and appreciation both of what needs to be protected and how to protect these assets without disrupting production. In order for IT/OT collaboration to be successful, both sides must have something to gain.

Addressing the needs of all

Figure 1. Unifying IT and OT to identify risks and ensure security



IT and OT personnel have different operating procedures and roles to play, and their worldview can differ considerably. However, their goals with respect to securing the company should be identical, and the path forward involves finding common ground.

OT engineers are tasked with building and maintaining IoT/OT networks and the devices connected to them. These systems must run consistently, often in oppressive environmental operating conditions. System and asset integrity are paramount, and failures or downtime can be costly and potentially catastrophic.

OT personnel are focused on safety, reliability, and productivity. Their role is to protect people, lives, the environment, the operation, and production.

Conversely, cybersecurity personnel are focused on maintaining the confidentiality of information and the integrity and availability of IT systems.

However, the goals of these entities do overlap. Both are committed to securing the organization, minimizing risk, maximizing uptime, and ensuring that the organization can continue to safely generate revenue.

The view that OT and IT are distinctly separate entities is antiquated. Failing to acknowledge the increasingly interconnected nature of OT and IT can have detrimental consequences for industrial organizations. A lack of trust, understanding, and collaboration between OT and IT departments can have a devastating impact on the security posture of an organization.

Typically, IT cybersecurity efforts are driven by the CISO, who is responsible for establishing and maintaining the enterprise's vision, strategy, and program to ensure that information, assets, and technologies are adequately protected.

Many industrial companies will also have a Chief Risk Officer (CRO), who is responsible for reducing business risks that endanger an organization's profitability and productivity. In particular, industrial entities operating critical infrastructure are all too familiar with the concept of risk.

However, regardless of title, those tasked with securing industrial environments must give equal weight to both the IT and OT sides of the organization. OT teams need visibility into assets and processes to keep production going and reduce downtime. Security teams don't need to monitor every single change in the network and should be focused on monitoring only major incidents.

Do you see what I see?

In most industrial organizations, IT cybersecurity and OT departments operate in silos. There is little visibility across the aisle and minimal understanding of how the opposite domain operates.

The lifecycle of OT systems (15 to 30 years or more) is much longer than that of IT systems (3 to 5 years). Since the devices and components are part of business-critical processes, there is very little downtime or often none at all. There is no such thing as "patch Tuesday" in OT environments. The processes that IT has been using safely in their environment for years are simply not applicable.

When IT security solutions are brought into the OT environment, they are often implemented without context. IT personnel often lack an understanding of and basic visibility into the OT environment and how it works, and cybersecurity decisions are often made without input from OT engineers. As a result, poor implementation can cause downtime and make OT engineers more resistant to further change.

To ensure that security measures are implemented successfully, IT and OT teams must work in harmony through each phase of the cybersecurity process. Collaboration early in the process is a key factor in success.

Building alignment and common ground

While the perspectives of OT and cybersecurity teams can and should be different, building a common language is critical. Alignment around a shared set of standards or a cybersecurity framework such as IEC 62443, ISO 27001, NIST, CPNI, or ENISA will go a long way toward improving each side's understanding of their roles and responsibility to the organization.

For example, some of the main differences in approach between IT and OT are demonstrated by the National Institute of Standards and Technology (NIST) SP 800-82 standard. Although in IT systems actions such as rebooting are tolerated, these are not acceptable in OT systems. Similarly, while downtime can often be tolerated in IT systems, in OT systems changes can take place only during scheduled maintenance periods, and outages must be planned and scheduled weeks or even months in advance. Patching in OT environments, for example, is a very different and significantly more arduous process than in IT. The lag from vulnerability identification to patch availability can often be extensive due to the supply chain and the exhaustive testing required because of the sensitive nature of the aging technology.

Developing an approach that takes the requirements of OT systems into account is paramount to building trust and acceptance.

The value of a shared vision

To help reduce cyber risks to critical infrastructure, NIST has developed a cybersecurity framework (Framework for Improving Critical Infrastructure Cybersecurity). It leverages standards, guidelines, and best practices to help industrial organizations get their OT security projects started.

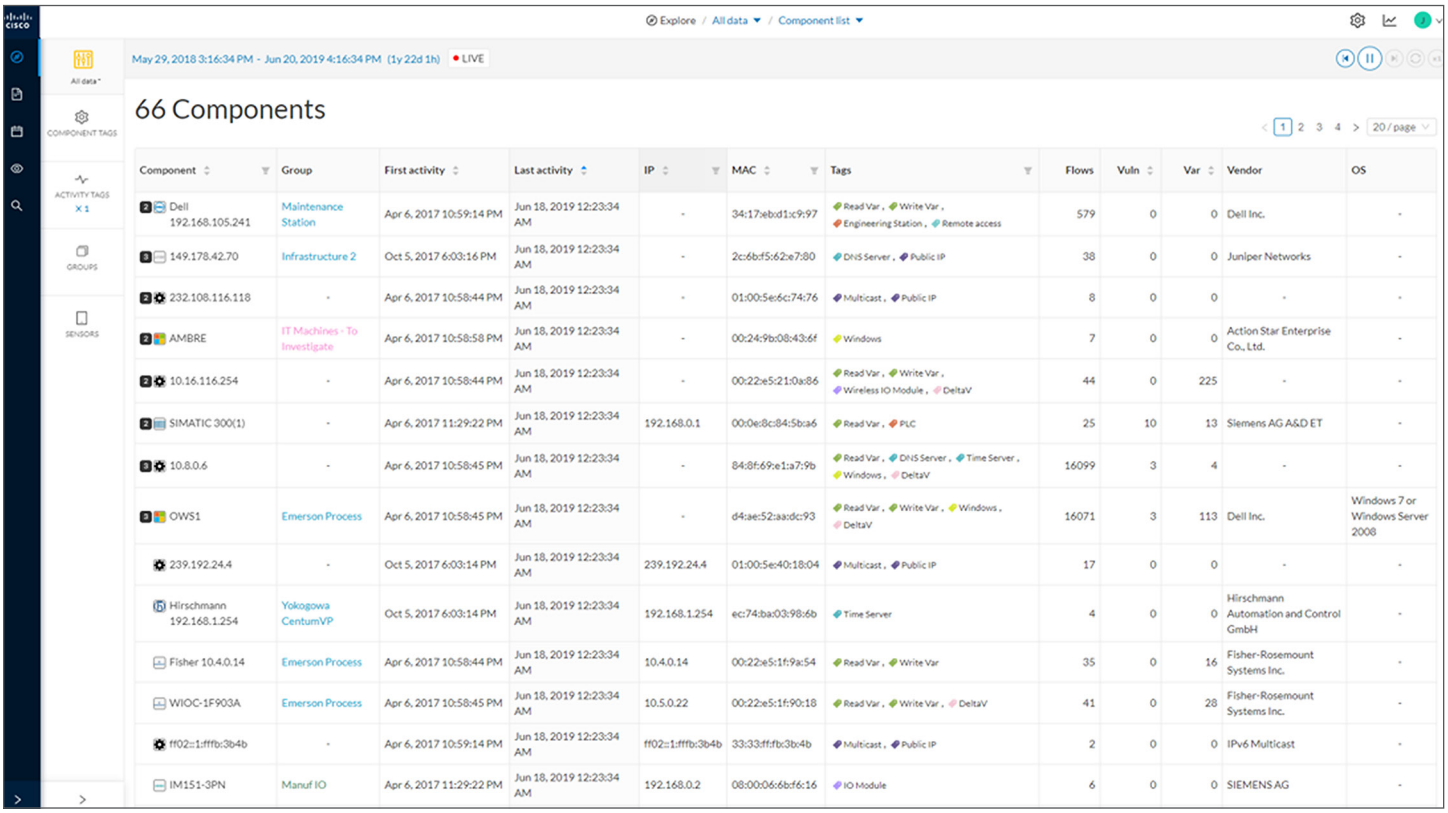
Step 1: Identify

The first function of the NIST cybersecurity framework is the Identify function. This function involves identifying not only the physical assets but also the data, personnel, devices, systems, capabilities, and facilities that make up an organization. Developing a complete risk management strategy means having a full understanding of both the resources that support critical functions and the related cybersecurity risks. In short, context is everything.

Securing industrial environments requires continuous visibility into every device within the environment at every stage, from the moment it enters the environment to the time that it is removed. This helps organizations keep track of vulnerabilities, remote access for vendors, and decommissioned assets.

The discovery process includes building an automated asset inventory that identifies the makes and models of devices, firmware, antivirus software, and other system factors to assess asset vulnerability. This step also includes a network discovery process to build a real-time view of the network.

Figure 2. Cisco Cyber Vision displaying a detailed asset inventory



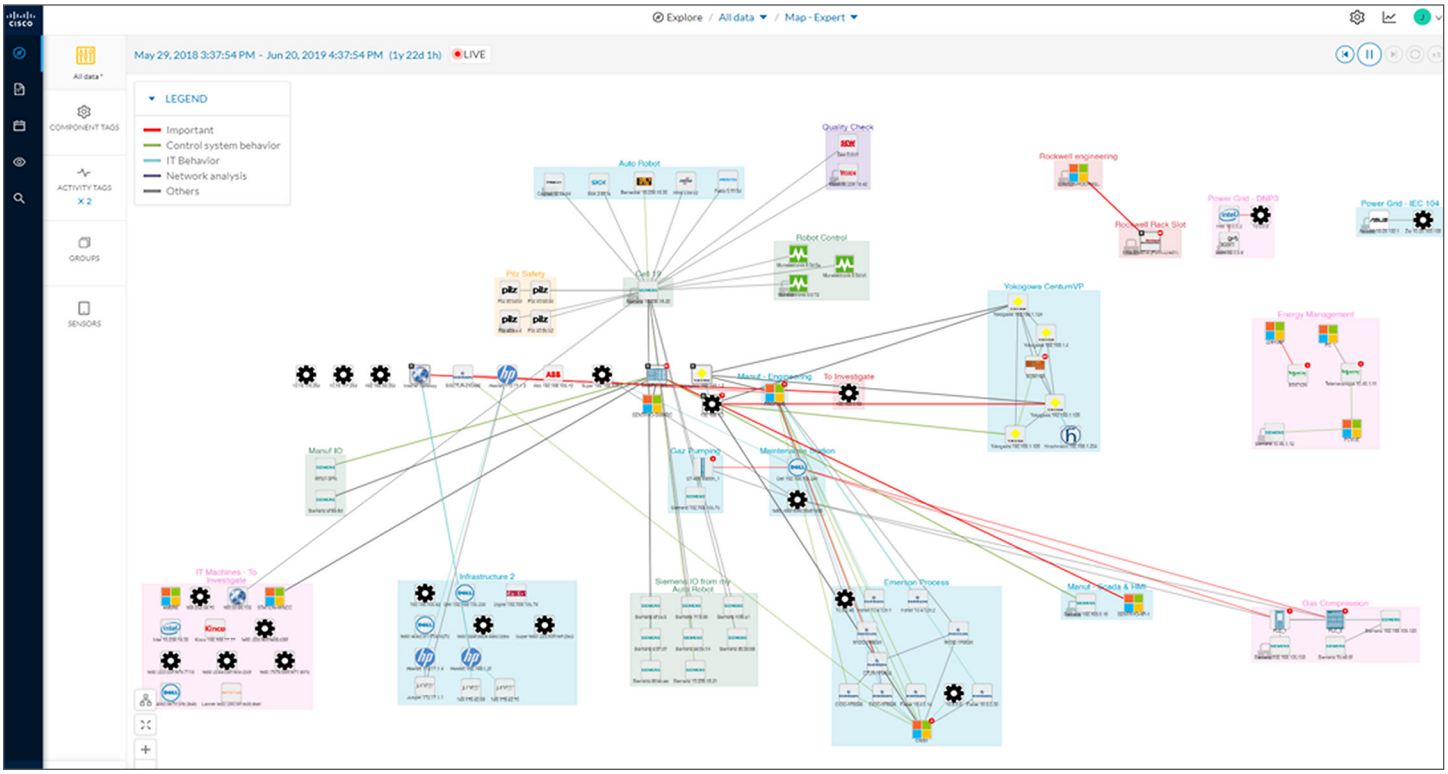
Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var	Vendor	OS
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var, Write Var, Engineering Station, Remote access	579	0	0	Dell Inc.	-
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server, Public IP	38	0	0	Juniper Networks	-
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast, Public IP	8	0	0	-	-
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7	0	0	Action Star Enterprise Co., Ltd.	-
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var, Write Var, Wireless IO Module, DeltaV	44	0	225	-	-
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var, PLC	25	10	13	Siemens AG A&D ET	-
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var, DNS Server, Time Server, Windows, DeltaV	16099	3	4	-	-
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var, Write Var, Windows, DeltaV	16071	3	113	Dell Inc.	Windows 7 or Windows Server 2008
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast, Public IP	17	0	0	-	-
Hirschmann 192.168.1.254	Yokogowa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server	4	0	0	Hirschmann Automation and Control GmbH	-
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var, Write Var	35	0	16	Fisher-Rosemount Systems Inc.	-
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var, Write Var, DeltaV	41	0	28	Fisher-Rosemount Systems Inc.	-
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast, Public IP	2	0	0	IPv6 Multicast	-
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module	6	0	0	SIEMENS AG	-

The key output of this phase is an analysis of the risk to business processes. Working together, IT/SecOps and OT teams can place assets into groups that represent key processes, define how those groups should communicate with each other, and define their criticality to the organization. Doing so enables event alerts for each group to be prioritized accordingly.

OT's role here is critical. They are charged with helping to overlay the business functions and identifying criticality. OT teams can use the real-time view of the OT network and assets to define industrial impact to assets, hence prioritizing events based on each asset criticality level. This step is necessary for building an effective detection strategy and avoiding event fatigue in the Security Operations Center (SOC).

IT/SecOps and OT teams need a comprehensive, contextual picture of the industrial environment. A complete and detailed asset inventory, an understanding of the communications between devices, and real-time insights into industrial processes are vital, particularly considering the changing environment.

Figure 3. Cisco Cyber Vision network map displaying assets, interactions, and business context (processes)



This picture allows OT engineers to get a clear view of how their OT network operates under different conditions, better plan for safety and production continuity, and work together with IT cybersecurity teams to document critical business processes with their associated devices. These measures also help IT/SecOps teams develop OT-friendly procedures and a blueprint to better protect and secure those processes. Bringing the OT context, understanding, and knowledge to IT/SecOps specialists and SOC analysts is fundamental to achieving the goal of organization-wide cybersecurity.

Step 2: Protect

Once they are clearly aligned around a single view of the networked devices, processes, and facilities, IT/SecOps and OT teams can work together to create a joint strategy for protecting the IoT/OT environment. This means developing and implementing appropriate safeguards to ensure that the industrial environment continues to operate smoothly and efficiently.

The Protect function of the NIST cybersecurity framework supports the ability to limit or contain the impact of a potential cybersecurity event. This requires designing a network architecture in which the different elements within an industrial network are separated into zones connected together via conduits, as described in the ISA99/IEC 62443 model.

A typical action to build such a network architecture includes network segmentation to secure devices involved in business-critical processes and to prevent any threats or malicious actors from moving unchallenged laterally through the network. Segmentation gives organizations the ability to isolate threats and focus threat detection efforts on those parts of the network that are most critical.

Segmenting with specialized industrial solutions such as the Cisco 3000 Series Industrial Security Appliances (ISA 3000) will enable IT and their OT partners to create local filtering rules to isolate manufacturing cells, industrial zones, or utility substations to help ensure that only authorized devices or connections have access, protecting the network from malicious or unwanted activities. In addition, these "OT-aware" firewalls will provide a layer of protection for vulnerable devices that simply cannot be patched.

Network segmentation can also be implemented using Network Access Controllers (NAC) such as the Cisco Identity Services Engine (ISE). While this solution does not offer the filtering or threat detection capabilities that next-generation firewalls would, it lets organizations easily implement security policies by allowing or denying assets the ability to communicate with each other based on their identity and profile. Network equipment is automatically configured to enforce these policies.

Because these NAC platforms are managed by IT, they cannot segment the industrial network without the help of OT. The profile of each of these industrial assets must be added to the platform so security policies can be configured. This can be done automatically by having products such as Cisco Cyber Vision continuously share asset information with the tool.

More importantly, OT engineering must define the policies to apply. They are the ones who know which communications should be forbidden and which ones are needed to avoid disrupting production. This collaborative effort between IT and OT can be achieved by sitting together and manually defining asset groups (zones) and communication policies (conduits). Or OT can use tools such Cisco Cyber Vision to set this logic and automatically share it with Cisco ISE so that IT has the required information to configure the appropriate security policies.

Step 3: Detect

The Detect function of the NIST cybersecurity framework involves the development and subsequent implementation of appropriate activities to identify the occurrence of a cybersecurity event.

As more and more IT building blocks are deployed in operational environments, detecting IT threats in industrial networks has become even more important. To this end, a combination of endpoint protection and intrusion detection and protection technologies is necessary.

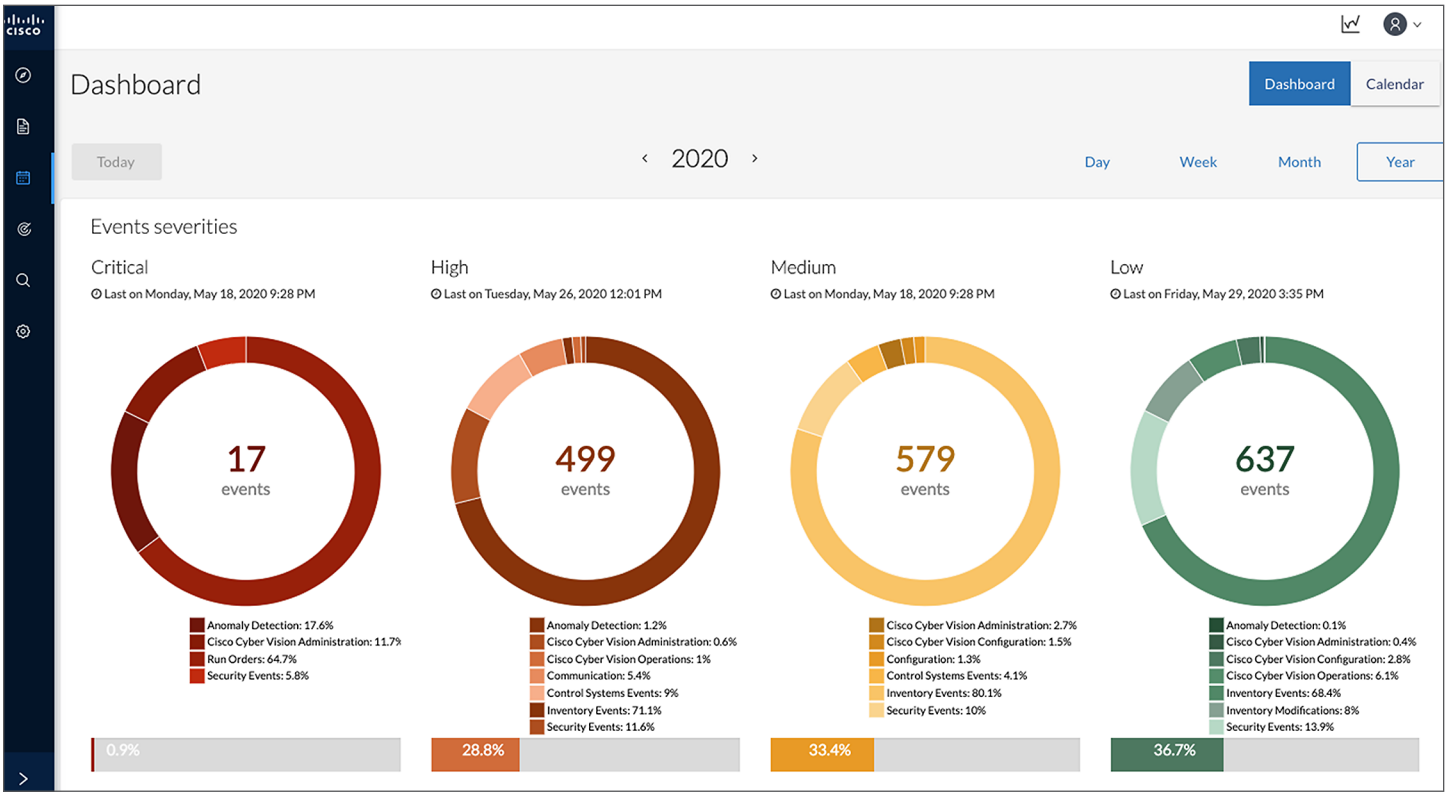
The security appliances deployed for network segmentation should include such capabilities so they can be leveraged for detecting malware and malicious traffic, for instance. However, while these next-generation firewalls are key, organizations need threat intelligence feeds such as Cisco Talos and Cisco AMP for Networks so that these firewalls can efficiently detect the broad array of known and emerging threats.

Organizations must also implement continuous security monitoring capabilities to monitor data integrity. While commonly associated with IT security, data integrity is also applicable to OT security when it comes to checking for process anomalies by decoding industrial network traffic and determining the integrity and legitimacy of the commands within such traffic. Organizations need a solution that understands the protocols used in these industrial environments and knows the OT processes, environment, assets, and correct use of protocols.

IT and OT personnel must work together to define what should be considered an anomaly. This includes defining what the normal industrial process should be, understanding the potential impact of an anomaly to set criticality levels, and enabling effective communications between IT and OT teams so that SecOps doesn't drown in false alarms during OT maintenance, for instance.

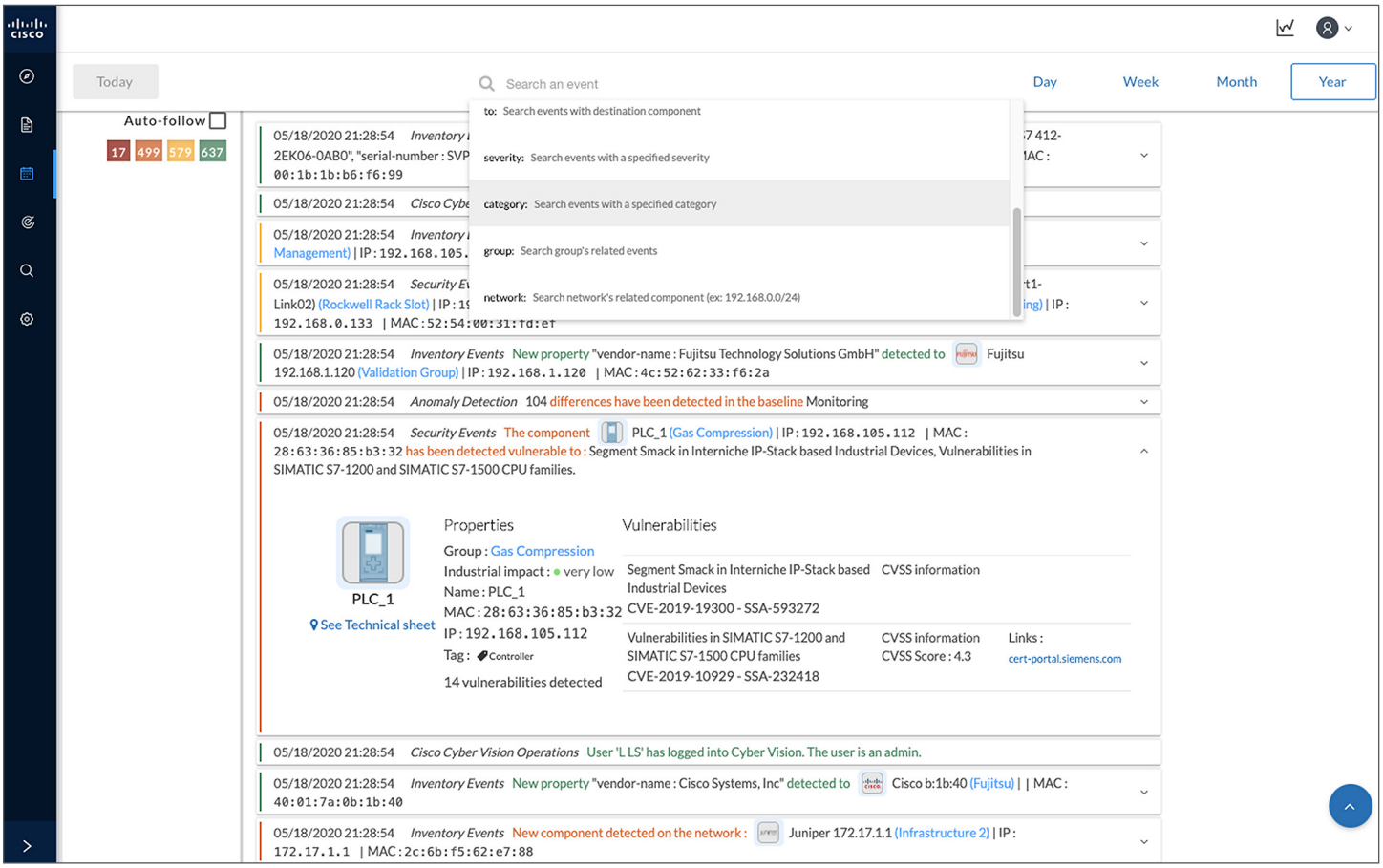
During their day-to-day activities, each side of the organization will need different kinds of data and insight to assess, investigate, and respond to OT security events. OT teams will be monitoring for process modifications and changes to devices. IT/SecOps teams will be monitoring vulnerabilities and IDS events. And SOC managers will need detailed asset information to simplify the investigation process and policy configurations.

Figure 4. Cisco Cyber Vision event dashboard enables both OT and IT to track all events in industrial networks



An IT/OT SOC analyst will need a complete view of the cyber kill chain – one that encompasses both the enterprise IT network and the IoT/OT process network. The OT context and the ability to tightly integrate the IoT/OT into existing IT/SecOps and SOC tools will allow these teams to achieve the goal of minimizing cyber risk to the entire organization. In addition, the same detailed information is often required for compliance and regulations, depending on the industry.

Figure 5. Cisco Cyber Vision adds OT context to events so they can be understood and interpreted by OT/IT SOC analysts



Weave shared vision into your security architecture

Due to the size, complexity, and distribution of typical OT networks, IT NetOps teams will only approve a scalable solution that won't break the bank or the network.

While the first generation of dedicated OT cybersecurity platforms required standalone hardware-based sensors, the next generation of IoT/OT cybersecurity platforms has taken the more workable route of embedding the sensor capabilities – especially Deep Packet Inspection (DPI) – within network equipment. Embedding DPI features into the industrial network enables far greater distribution than with physical devices and in turn provides a superior source of information at a substantially lower Total Cost of Ownership (TCO). And less hardware is always a benefit.

Physical sensor appliances connected to Switched Port Analyzer (SPAN) ports will still need extra network resources to collect data from industrial network equipment. The key is to have a minimal footprint and impact on the network so that IT NetOps can easily roll out and maintain the solution, thus helping ensure the success of the OT cyber projects. Failing to consider the solutions' ability to cost-effectively scale – both geographically and deep down into the process network – as a key success factor might lead to pushback from IT NetOps, leading to limited deployment or even a halt to the project.

Data visualization is also key to drive acceptance from various teams. The solution's ability to present meaningful data for individual roles in a usable way will help teams share a common understanding of the situation and get all stakeholders onboard.

The OT engineering teams need to be able to quickly zoom into part of their network, track their machines, group them into zones, and see variables or process anomalies to ensure production integrity, continuity, and safety. OT engineers may have responsibility for a particular site or facility, or they may be responsible for a particular process or a set of specific devices across multiple sites and geographies.

While these approaches differ between organizations, the important factor is to present the information to the OT engineers in terms of their role and tasks. They need an interface that is simple, flexible, and powerful so that they can use it when running operations and have an incentive to share OT context with IT/SecOps when an event occurs.

IT/SecOps and SOC teams need centralized views across all OT and IT sites so that they can leverage their existing IT security tools and procedures for investigation and remediation. To this end, the solution's integrations and interoperability (native or via API) are crucial. The first step is to integrate OT alerts and events into Security Information and Event Management (SIEM) tools, but the first generation of OT security platforms doesn't offer the ability to select events to be shared. Their behavioral analytics engine cannot be tuned to various production states, generating many false positives.

Next-generation OT security platforms prevent event fatigue by letting security analysts choose events they want to see in the SIEM tool and enabling OT engineering to easily create various baselines to tune behavioral analysis, depending on the part of the industrial process they want to monitor, the time period, or the state of the production.

IT is accountable for threat investigation across the organization, following the cyber kill chain wherever it may lead. Oftentimes, IT security is in the dark when it comes to the OT network and devices. At best they have MAC and IP addresses. Sharing OT asset information – such as device name, type and characteristics, business criticality, and more – with existing security tools enables effective investigation across both IT and OT domains.

However, the SOC can be overwhelmed with information and often lacks the ability to automatically cross-reference data to extract evidence. Investigating an abnormal behavior or a suspicious observable on the industrial network should be quick and easy. Platforms such as Cisco SecureX let you automatically search on a variety of observables detected by Cyber Vision or ISA 3000 with Cisco AMP, Umbrella, Stealthwatch, Firepower, and more. It aggregates all these sources so that security analysts can immediately see if the industrial asset has been compromised.

IT/SecOps also needs OT context in all their security tools to simplify policy configuration and remediation. Understanding the role of an asset in the industrial process, which production cell it belongs to, or the vulnerabilities that could not be patched makes it much easier to create the right security policies or build firewall rules, for instance.

For an effective and successful OT security strategy, all stakeholders must work hand in hand. The solution benefits all with industrial anomaly and threat detection that has a foothold in both worlds. OT threat detection requires an understanding of IT and OT. Threats may enter via the IT environment and proliferate into the OT environment. For security analysts to identify the cyber kill chain and prevent potential calamity, they need tools that will be capable of detecting threats in both environments and the relevant types of contextual insights for each environment.

The bridge to possible

United we stand, divided we fall

While the OT environment presents considerable challenges, the key to securing it is breaking down the departmental barriers between the silos. When IT and OT collaborate, they succeed. Instead of building new and disjointed OT security methodologies, it's vital for organizations to leverage existing tools and investments to better secure OT environments without disrupting production. Securing the industrial enterprise means extending the existing IT security tools (with existing skills, knowledge, and budget) into OT and bringing the OT information (devices, process, events, etc.) and OT engineer's knowledge into IT.

Making this happen requires IT/SecOps teams to work closely with OT teams, and so the chosen OT security solution must offer benefits to all stakeholders and their specific needs. It must be inherently designed to provide meaningful information to both teams so they share a common understanding of the situation and can start working together toward a common goal.

How Cisco can help?

Being the leader in both the cybersecurity and industrial networking markets, Cisco is making heavy investments to bridge the two and enable secure Industry 4.0 deployments.

The combination of Cisco Cyber Vision and Cisco industrial network equipment helps our customers gain this visibility and detect threats at scale throughout their industrial operations. Fully integrated with Cisco SecureX and the entire suite of Cisco security solutions, Cisco's solutions enable a truly unified IT/OT threat management strategy.

To learn more, visit cisco.com/go/iotsecurity or contact your local Cisco account representative here.

C11-744337-00 10/20