sentryo

BUILD YOUR CYBER CONTROL ROOM

TO SECURE YOUR INDUSTRIAL AND OT SYSTEMS

www.sentryo.net

The Industrial Internet is relying on the convergence of Operational Technologies (OT) and Information Technologies (IT). The cyber threats which make headlines every day are now targeting OT networks. The difference is that they are impacting the real world in the form of production outage, environmental disaster or human safety.

Indeed, according to a 2016 report of the International Society of Automation (ISA), **nearly 750 actual OT related cyber incidents leading to deaths or severe outages (e.g the 2015 Ukrainian power grid) have been registered.** In addition, especially for critical infrastructure providers (CIP) or operators of essential services, **regulatory pressure is increasing globally** (e.g. NERC CIP, EU NIS Directive, French LPM…), which requires organizations to accelerate their readiness to detect and provide notification of severe cyber incidents and **be prepared for the worst.**

Chief security officers (CSO) and chief information security officers (CISO) are required by anxious executives to assess and manage industrial cyber risks in order to both answer to various regulatory bodies and to ensure the resilience of industrial operations. As a result, there is a sense of urgency that the CSO and CISO collaborate closely with OT staff (e.g. operators, control engineers) in order to **leverage cybersecurity best practices and experience** and to **incorporate cybersecurity into industrial processes through the establishment of a Cyber Control Room. A Cyber Control Room is an OT security operations center (SOC) using powerful threat intelligence, monitoring and detection capabilities** in order to effectively tackle the OT related cyber risks. With a Cyber Control Room, organizations are equipped to fully embrace and protect the Industrial Internet.

This paper is **intended for chief security officers (CSO) and chief information security officers (CISO)** and provides insights and best practices so that:

- they can address increasing OT cyber risks, raise awareness across their organization and drive in a progressive way the establishment of a Cyber Control Room in collaboration with OT staff (e.g. operators, control engineers);

- they can leverage the Sentryo ICS CyberVision platform to build and run Cyber Control Room capabilities.

Sentryo, a European company, headquartered in Lyon, France **is the pioneer and a leading vendor of Industrial Internet cybersecurity solutions.** Sentryo's mission is **to fight against digital attacks to the physical world,** addressing the convergence of the IT and OT worlds.

The **Sentryo ICS CyberVision platform allows organizations to build and run a Cyber Control Room and utilize its' capabilities** in order to protect against cyber-attacks targeting the Internet and industrial networks and to ensure their business operations continuity.

Through a pay as you go subscription model, it provides **unique full situation awareness, advanced anomaly detection, and incident response** core capabilities. Thanks to its leading edge **OT monitoring technology and machine learning techniques,** CyberVision is able to **detect early the "unknown unknowns"** before any intrusions have caused any severe damage. ICS CyberVision (**a hardware and software platform**) **is a fully passive and scalable solution which supports multiple OT vendor's protocols**.

THE INDUSTRIAL INTERNET

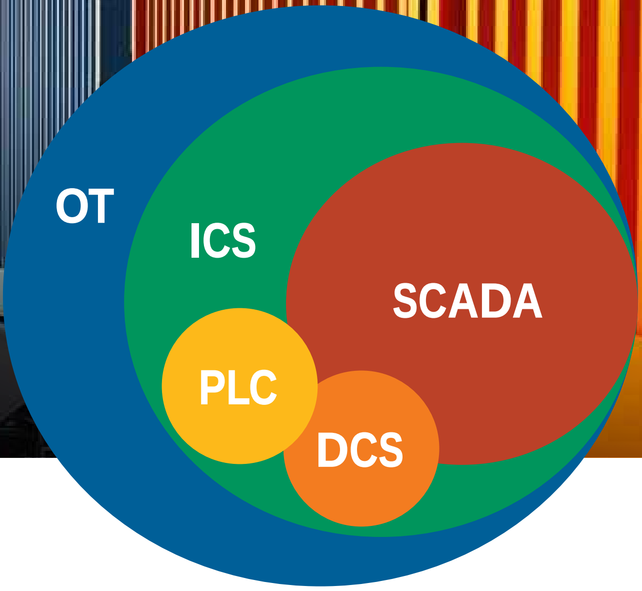


Figure 1: Overview of OT, ICS and SCADA (source KuppingerCole)

What do the phrases "Industry 4.0" or "Smart Cities" or "Smart Grids" mean to you? These phrases refer to major technological changes involving the Industrial Internet. Physical objects such as sensors, actuators and other types of machinery multiply exponentially and acquire a "digital skin" to create a pervasive digital presence across industry, business and society. **This is the Industrial Internet. The Industrial Internet is made of technologies such as machine-to-machine (M2M) communications and operational technology (OT).**

OT has been a critical part of operating, monitoring and maintaining physical infrastructure for decades, and is central to industrials processes. However, as OT has become digital, IT has been an increasing part of that evolution providing platforms, software and networks to enhance control and functionality. The Industrial Internet stretches from operational technology (OT) to the upcoming Internet of Things (IoT[1]) whose "nervous system" is digital and software based.

Though much has been written about OT, **what are the differences between OT and IT systems?** Unlike information technology (IT), the core deliverable of operational technology (OT)[2] is not information. Instead, the core deliverable of OT is a change of state, primarily in physical infrastructures. State changes take many forms (e.g. if a valve needs to be opened or closed, OT can open or close it; if a gas pipeline experiences pressure beyond its operating parameters, OT can bring it back within tolerance levels).

OT is often specific to an industry, a system or a process. OT is used in many different industrial sectors and critical infrastructures including:

- **Process-based manufacturing (continuous or batch):** oil & gas, chemicals, power generation, pharmaceuticals food…
- **Discrete-based manufacturing:** electronic, automotive, aerospace…
- **Distribution:** water distribution and wastewater collection systems, agricultural irrigation systems, oil and natural gas pipelines, electrical power grids...
- **Transportation:** postal service mail handling, railway transportation systems, airports, harbors, road transportation…

Typical OT systems include industrial control systems (ICS), distributed control systems (DCS) widely used in process industries, programmable logic controllers (PLC), Supervisory Control data acquisition systems (SCADA) and manufacturing execution systems (MES) which are increasingly supplemented with smart devices.

[1] The Internet of Things (IoT) is defined as "the network of physical objects that contains embedded technology to communicate and sense or interact with the object's internal state or the external environment."

[2] Gartner defines OT as "hardware and software that detects or causes a change of state, through the direct monitoring and/or control of physical devices, processes and events in the enterprise."

THE OPERATIONAL TECHNOLOGIES CYBERSECURITY PARADIGM

OT-RELATED CYBER RISKS HAVE REACHED A CRITICAL THRESHOLD

By design, **OT systems rely on purpose-built devices and networks** and interact with the physical world. They collect input data via sensors and directly drive the physical process via actuators.

The nature of the risks is very different between IT & OT worlds:

- business risks are mainly related to the **confidentiality and integrity of the data processed and hosted by the IT systems** which **leads to intangible consequences** such as loss of know-how, loss of reputation…

- for OT systems, business risks are related to the **availability, integrity, reliability and safety of the command & control system itself** which **leads to various operational consequences in the physical world** such as production shutdown and financial losses, derailed trains and the impossibility to control the process and to obtain accurate information about its state…

Previous beliefs that OT environments were somewhat impervious to outsider threats are now false. Industrial corporations, with widely available and low-cost Internet Protocol (IP) devices, are increasingly connected with each other to improve efficiencies and they are starting to resemble IT systems in some areas. To take advantage of the enhanced supply chain benefits, they may also allow suppliers, such as vendors, to connect to their automation systems for maintenance and asset management services. This integration provides significantly less isolation for OT from the outside world, creating a greater need to secure these systems. According to Frost & Sullivan[3], the supply chain introduces extra weaknesses allowing threats and entry point access to critical infrastructures **which requires thinking of the value chain as a whole.**

OT environments are also vulnerable and more exposed to cyber-attacks. Persistent design vulnerabilities (PDVs) are inherent in the design of OT systems as part of its function[4]. As stated by the ISA, "OT systems are not designed to ensure resilience against concerted attacks that intend to place components in dangerous operating states. This is expected to be a growing area of cyber-attack and engineering research." As OT environments increasingly incorporate poorly managed IT technologies, additional IT-related weaknesses are introduced. Because of the OT lifecycle (10-15 years) in terms of acquisition and maintenance combined with rare software changes, widely dispersed and old systems cannot be patched or upgraded in typical IT security fashion. As a result, OT environments will remain highly vulnerable for long time periods.

Meanwhile, in addition to the nature of OT environments, the knowledge and skills needed to attack OT networks are spreading rapidly in the wild, so that the OT-related cyber risks have reached a critical threshold - action must be taken now.

[3] Top Ten Cyber Trends Affecting the CNI Sector » (Frost & Sullivan 2014)

[4] The ISA refers to these not as "zero-day vulnerabilities" but as "infinite day vulnerabilities" because vulnerabilities are a combination of new and inherent vulnerabilities of the systems.

Gartner predicts that *"continuous cybersecurity breaches against critical infrastructure industries will result in environmental events exceeding $10 billion, catastrophic loss of life and new regulation, globally, by 2019"*.

OT CYBER-ATTACKS WITH HIGHLY VISIBLE IMPACTS IN THE PHYSICAL WORLD MAKE EXECUTIVES ANXIOUS

OT-related cyber risks are not only theoretical but real. **OT cyber incidents have started to be evidenced by headlines for over six years** even though many OT cybersecurity incidents stay undetected or unreported in this domain. For instance, various targeted or intentional intrusions leading to severe outages have been reported publicly starting in 2010 with the Iran nuclear plant (Stuxnet), then with the Norwegian oil industry massive attack[5] (August 2014) or the German steel mill facility (December 2014), to recently, in December 2015, with the Ukrainian power grid attack.

OT threats can impact various organizations or systems (e.g. heavy industrial companies, critical infrastructure providers, smart home technologies or smart building - HVAC, energy management, building automation…), and their negative effects can include significant danger to the health and safety of human lives, serious damage to the environment as well as significant financial issues such as production losses or negative impact to a nation's economy. Indeed, the fact that many of the industry sectors involved are part of what are considered national critical infrastructures means that, besides the potential damage inflicted on the companies directly involved, there is a secondary and magnified impact on the communities and countries that rely on key services provided by those targeted industries.

According to the ISA (International Society of Automation) in a 2016 report[6], **nearly 750 actual OT related cyber incidents have been registered** including more than 50 cases that resulted in more than 1,000 deaths combined, more than 10 major cyber-related electric outages and more than 60 nuclear plant cyber incidents with more than 15 resulting in reactor shutdowns. Gartner predicts that *"continuous cybersecurity breaches against critical infrastructure industries will result in environmental events exceeding $10 billion, catastrophic loss of life and new regulation, globally, by 2019"*.

[5] http://www.csoonline.com/article/2599258/cyber-attacks-espionage/50-norweigian-oil-companies-suffer-cyber-attack.html

[6] What Executives Need to Know About Industrial Control Systems Cybersecurity (International Society of Automation)

CHIEF SECURITY OFFICER (CSO) AND CHIEF INFORMATION SECURITY OFFICER (CISO) ARE ASKED TO ADDRESS OT-RELATED CYBERSECURITY AND REGULATORY RISKS

It is generally accepted that there is **a significant governance, knowledge, and experience gap between the IT and OT domains** of an industrial organization. OT staff have process engineering expertise but little or no cybersecurity training and understanding. Closing this cultural gap to make OT staff part of the cybersecurity chain is critical.

More broadly, on behalf of senior executives, chief security officers (CSO) and chief information security officers (CISO) are now requested to establish across all of their industrial organization a consistent cybersecurity operating model integrating the OT environments in order to address the following issues:

- **What are the major OT assets to protect?** Are they vulnerable? Where are they located? Are both external and internal threats considered? Does the organization understand the origin of threats (e.g. cyber criminals, competitors, governments, rogue employees, etc.)?

- **How shall OT cybersecurity be governed within the organization?** Is it well integrated into the corporate governance? Are the roles and accountabilities well defined among industrial site directors, IT, OT and cybersecurity stakeholders?

- **What are the major OT cyber risks the organization faces?** What are the risks of compromising the OT network to enter into the corporate IT network or vice versa? Is the organization able to detect abnormal events and weak signals of cyber-attacks?

- **How can we empower OT staff to make them aware of their role related to cybersecurity?** Did control engineers receive some basic cybersecurity awareness training?

- **In the event of a serious OT cyber incident, which incident response and crisis management process needs to be developed?**

Especially for critical infrastructure providers (CIP) or operators of essential services, **regulatory pressure is increasing with local specialties which will require the CSO and the CISO to accelerate the enforcement of cybersecurity best practices and the readiness to detect and provide notification of severe cyber incidents.**

The US NIST framework, the European NIS Directive and the French LPM law requires critical operators to conduct risk assessments exercises and to detect and provide notification of their severe cyber incidents to the national or federal information security agencies (to avoid potential systemic effects). They will also be required to source their detection and response capabilities through trusted and certified service providers. Therefore, the main current CSO and CISO challenge is to raise awareness at the industrial director's level and to increase their influence across the organization **in order to address in a holistic way increasing OT-related risks. For that, we recommend embracing five long-term tenets in order to guarantee continuity of business industrial operations** (for more details, see the Appendix).

OT ENVIRONMENTS FACE VARIOUS OPERATIONAL CYBERSECURITY CHALLENGES

OT cybersecurity derives many practices and technologies from IT security. However, changing the state of a system has unique safety, business continuity and security implications. This means that merely translating IT security practices and copying IT security technology to address OT security will not result in a secure OT environment.

In IT environments, technology is already there and security operations centers (SOC) have been set up to monitor and detect cyber-attacks although there have been many cases where IT cyber compromised systems have gone undetected for months.

In the OT world, **the use of active cybersecurity solutions** (e.g. firewalls, IDS, antivirus, vulnerability scanners…) has **limited value for several reasons:**

- For existing systems, implementing such security solutions is limited by the risks of false positive events which might create perturbation on mission critical OT networks.
- Such IT technologies are too intrusive for mission critical and low latency systems where false positives are not acceptable.
- Most OT components in the field today (PLC, Controllers, RTU, intelligent devices) do not support any third party IT security software.

The biggest challenge in OT environments remains to manage OT systems in order to reduce the attack surface and then to know when a cyber-attack occurs or has already started and respond rapidly so that corporations can ensure business resilience of their industrial operations.

As a consequence, a reasonable approach to protect an OT system is to implement both active cybersecurity solutions where possible (meaning where it will not disturb the system) and passive monitoring solutions without taking the risk of disputing the OT system by generating false positive events. Focus should be on **monitoring solutions that are tailored to the unique characteristics of OT environments** (i.e. mission critical, low latency, long lifecycle…).

HOW SENTRYO CAN HELP TO ESTABLISH A CYBER CONTROL ROOM

As a result, **if actions are not taken in the short term,** other serious safety accidents or disruption of critical infrastructures due to cyber-attacks will continue to occur. We strongly suggest that chief security officers (CSO) and chief information security officers (CISO) **adopt a more operational and pragmatic approach starting right now with the establishment of a sustainable Cyber Control Room**.

DEMYSTIFYING THE CYBER CONTROL ROOM

A **Cyber Control Room** is a Security Operations Center (SOC) dedicated to OT environments. We can simply define a **Cyber Control Room as a virtual facility for monitoring cybersecurity of OT networks and assets** (i.e. applications, software, controllers, devices, servers, networks…). Through sensors (i.e. the equivalent of cameras in the physical world) which can collect data from different OT environments, it can process and analyze data in order to monitor various systems (e.g. ICS, SCADA, security doors, building management, physical access management…). The value chain of such a Cyber Control Room is mainly composed of the primary and supporting activities as described in Figure 3.

The biggest value expected in a Cyber Control Room comes from its early and accurate detection capability as well as its ability to streamline collaboration between OT staff, IT staff and cybersecurity experts. Its ease of integration with an IT SOC by correlating IT and OT events will enhance organizational detection capabilities as a whole.

Establishing a Cyber Control Room is a must have to win the OT cybersecurity battle but it represents a long journey for industrial corporations, particularly to be able to continuously monitor all the OT components in a 24/7 mode. Such a Cyber Control Room will entail positive side effects: deal with legacy OT equipment, move forward with IEC 624443, empower OT operators and staff, etc.. As represented below, industrial corporations **shall adopt a step by step pragmatic approach to avoid making the process so complex that the goals are never achieved.**

THE SENTRYO VALUE PROPOSITION:
ENABLE A SUSTAINABLE CYBER CONTROL ROOM

The **Sentryo ICS CyberVision platform allows organizations to build and run Cyber Control Room capabilities** in order to protect themselves against cyber-attacks targeting their industrial infrastructures and to ensure their business operations continuity.

ICS CyberVision **is a turn-key software/hardware platform.** Subscription model (based on the number of OT components to monitor), it provides **unique full situation awareness** (including asset discovery and classification, connection mapping and passive vulnerability management), **anomaly detection based on machine learning, and incident response** core capabilities. These capabilities are supported and enhanced by threat intelligence feeds (for more details, see the Appendix), data visualization and reporting.

The platform is composed of the ICS CyberVision **center** (appliance software/hardware or cloud) and a number of passive **sensors** (software agents or appliances) installed on OT networks in each industrial site which "understands" the machine to machine communications and extracts meaningful information.

The ICS CyberVision platform can be **delivered through the IT organization or the OT organization of the company, or through an external (managed) service**[7]. Depending on the communication flows security requirements and operational constraints, the CyberVision Center can be located on the industrial site or in a datacenter.

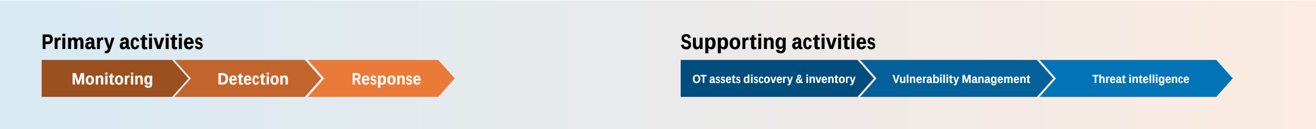


Figure 2: Main activities of a Cyber Control Room

[7] Companies also have the option that the ICS CyberVision platform be managed by Sentryo business partners' experts who can support them to identify suspicious and critical events, to close the gap between detection, response and remediation, and, as a result, provide a full Cyber Control Room capability dedicated to OT environments.

The ICS CyberVision platform provides a **single unified and comprehensive set of cybersecurity services and capabilities** dedicated to protect OT environments in order to **prevent, protect, detect and respond faster and better to cyber-attacks.**

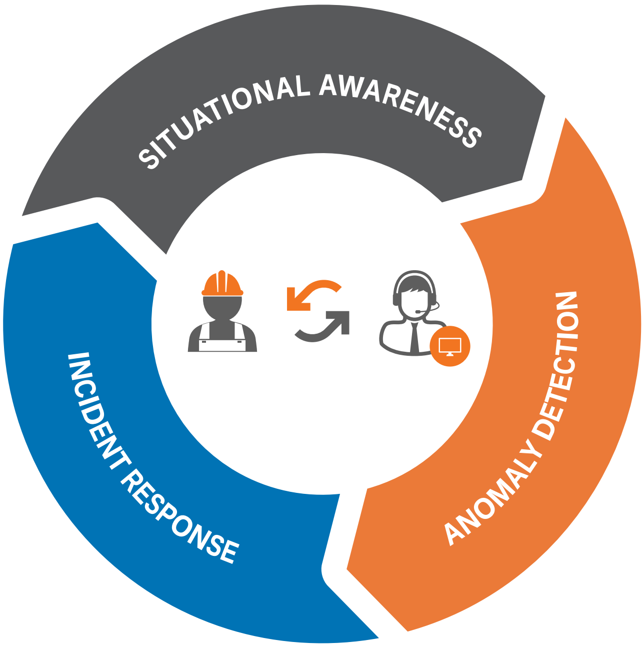


Figure 3: The CyberVision platform core capabilities

From an **end user perspective**, the ICS CyberVision platform **fosters collaboration** between different stakeholders **and gives:**

OT staff (e.g. operators, control engineers) the tools to:

- discover and inventory their assets, quickly spot OT vulnerabilities and efficiently implement their protection plans in order to reduce the attack surface.
- automatically detect in a continuous way abnormal events (new network flows from a machine, unauthorized changes…) which could be weak signals of advanced cyber-attacks, changes or potential compromise.
- rapidly pinpoint on their own (i.e. assess and characterize) the source of the problem without deep know how in cybersecurity.
- then, make first decisions appropriately and in a timely manner.

Cybersecurity experts the tools to:

- support OT staff in case of OT cyber attacks.
- carry out and accelerate their response and investigation after a critical event through all the gathered information and threat intelligence provided by the Sentryo research lab,

CSO and CISO the means to:

- document and provide reports for internal and regulatory compliance purposes (for more details, see the Appendix).

UNDERSTANDING
THE SENTRYO ICS CYBERVISION PLATFORM

With its **unique OT monitoring technology and machine learning techniques,** the CyberVision platform is able to detect early the “unknown unknowns” before any intrusions have caused any severe damage. For that, the CyberVision platform detects anomalies in a very different way from that of traditional IDS/IPS appliances or SIEM platforms. It does not use any signatures’ database or correlate any technical logs to detect breaches or malwares. It **leverages machine learning techniques** to improve the accuracy of detection (minimize false positives) and provides increasing value in terms of event’s assessment for OT staff. OT end users do not need to set and update rules that are complex and require a deep cybersecurity expertise.

The CyberVision workbench

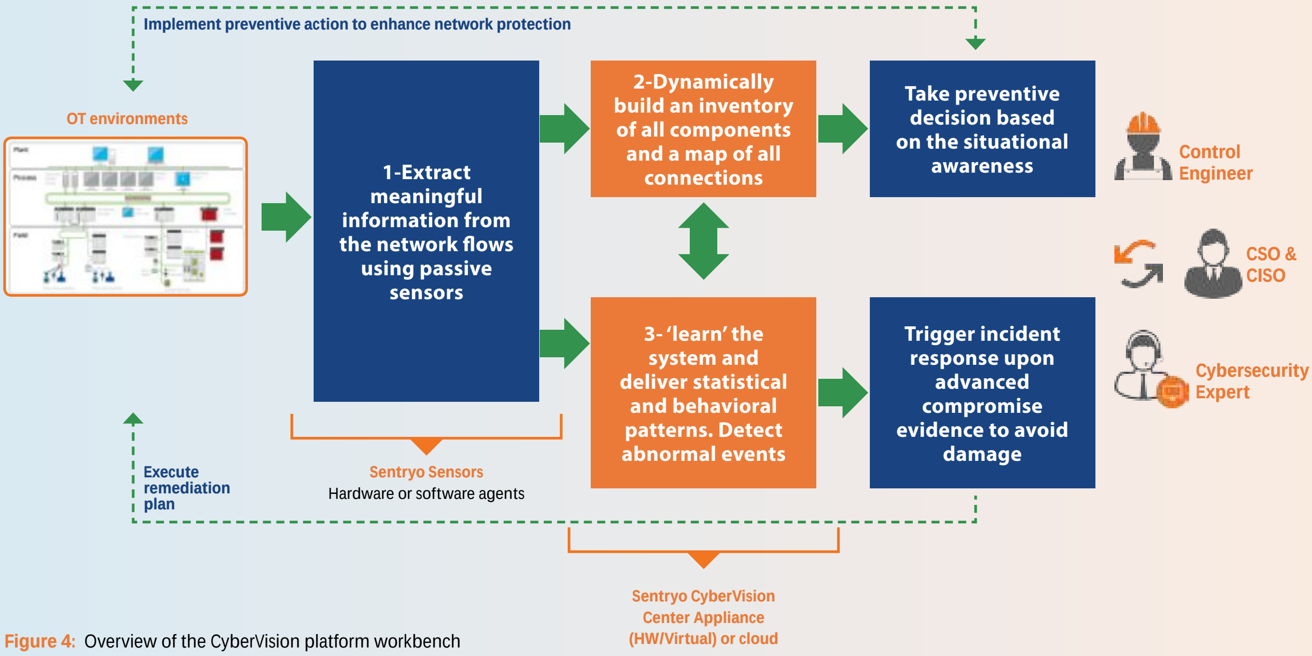

Implement preventive action to enhance network protection
OT environments
1-Extract meaningful information from the network flows using passive sensors
2-Dynamically build an inventory of all components and a map of all connections
Take preventive decision based on the situational awareness
Control Engineer
CSO & CISO
3- ‘learn’ the system and deliver statistical and behavioral patterns. Detect abnormal events
Trigger incident response upon advanced compromise evidence to avoid damage
Cybersecurity Expert
Execute remediation plan
Sentryo Sensors
Hardware or software agents
Sentryo CyberVision Center Appliance (HW/Virtual) or cloud

Figure 4: Overview of the CyberVision platform workbench

Extracting meaningful information from the OT network

The first challenge is to collect meaningful information on the OT networks while most components do not generate logs.

Relying on Sentryo Deep Packet Inspection technology, ICS CyberVision sensors analyze raw data from the network by understanding OT protocols and flows to extract certain information including:

- **Inventory information:** devices identification and devices properties (e.g: controller identification and firmware version),
- **Process control information:** messages exchanged between process control devices (e.g: download a block), program hash (watermarking the program), value of variable (e.g: pressure).
- **Network information:** messages exchanged between network devices (e.g: ARP messages between switches & routers)

All these information are accompanied by a set of metadata which characterized them and put them in context (time, source, destination, protocol, frequency etc……).

There are **dozens of industrial protocols supported by Sentryo** (for more details, see the Appendix) which address different industry segments, from those of large Distributed Control Systems in the process industries (e.g. Honeywell, Emerson, ABB, Yokogawa), through a mix of proprietary and standard protocols for manufacturing industries that rely on PLC and SCADA systems (e.g. Siemens, Schneider, Rockwell Automation), to those dedicated to smart buildings (e.g. Bacnet as a standard) or smart grid worlds (e.g. IEC 104 and IEC 61850 as new standards).

Providing full situational awareness

All the information collected by the sensors which are spread on the OT network are centralized and stored within the ICS CyberVision center database.

- Network information are complemented using Sentryo's own heuristic (e.g showing that an unknown IP address is routed on the Internet).
- Inventory information are correlated with internal and external feeds (knowledge database fueled by the Sentryo threat intelligence team, (see Appendix) to pinpoint software vulnerabilities on the OT network.
- Process control information are combined to create "normalized behaviors" which characterize the behavior of the OT network (e.g: SCADA station A is reading and writing variable value within the memory of PLC1 and the speed of variation of the value remain between 20% and 30% per minute)

ICS CyberVision data visualization engine dynamically builds a visual and real time representation of the OT network revealing each device (asset inventory) with its properties and known vulnerability as well as each logical connections between devices and all the behaviors observed on the OT network. This kind of "google map" of the OT network will allow the OT network manager to get a full situational awareness of the environment by zooming in and out.

This interactive **map** could be **directly enriched by control engineer's interactions adding business context and risk analysis information details.**

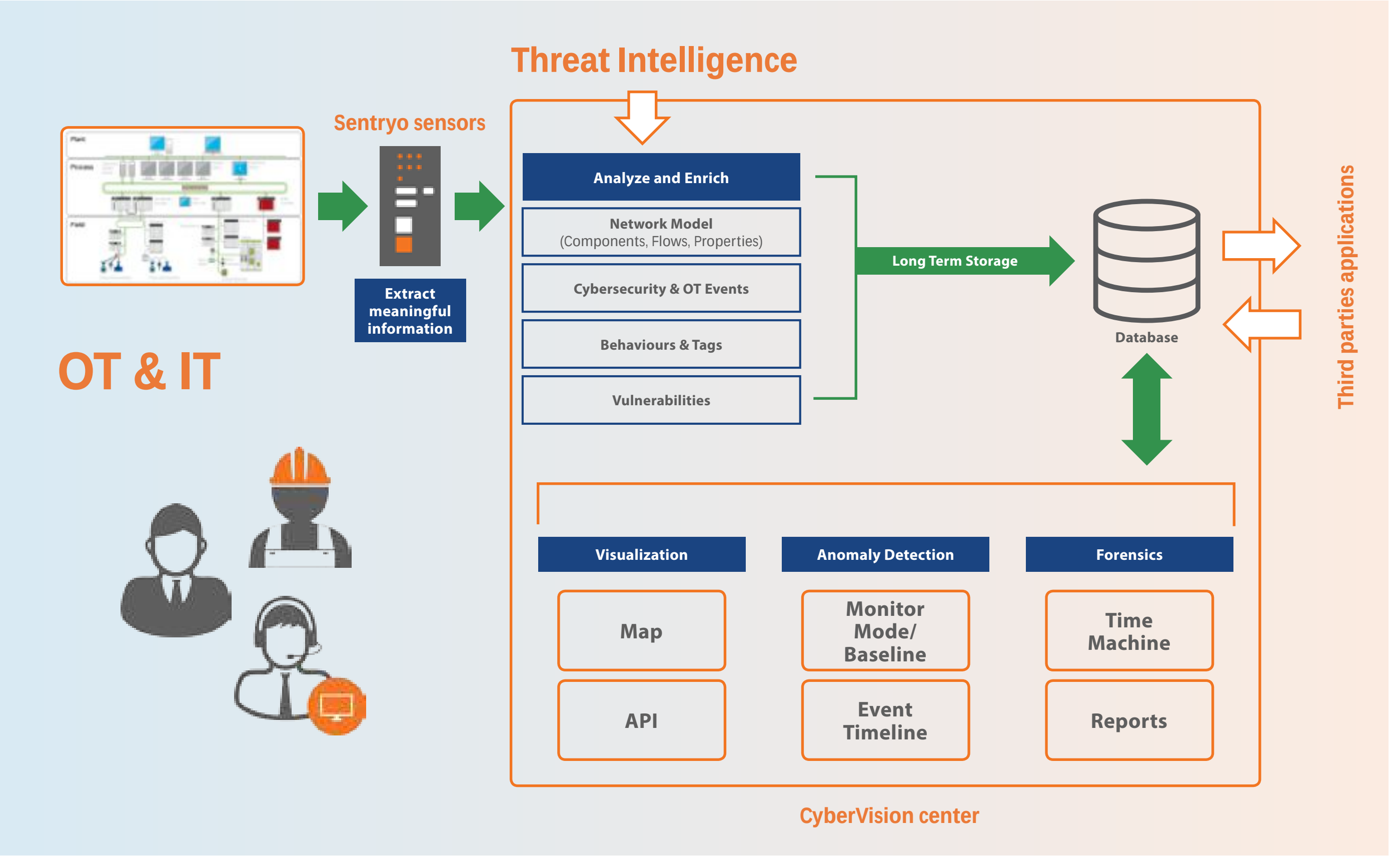


Figure 5: ICS CyberVision architecture

Detecting abnormal behaviors

Over time, all informations and behaviors stored within the ICS CyberVision center allows **the creation of “baselines”**. The baseline or reference point encompasses all the behaviors observed on the OT systems, and considered as legitimate, during a certain time window.

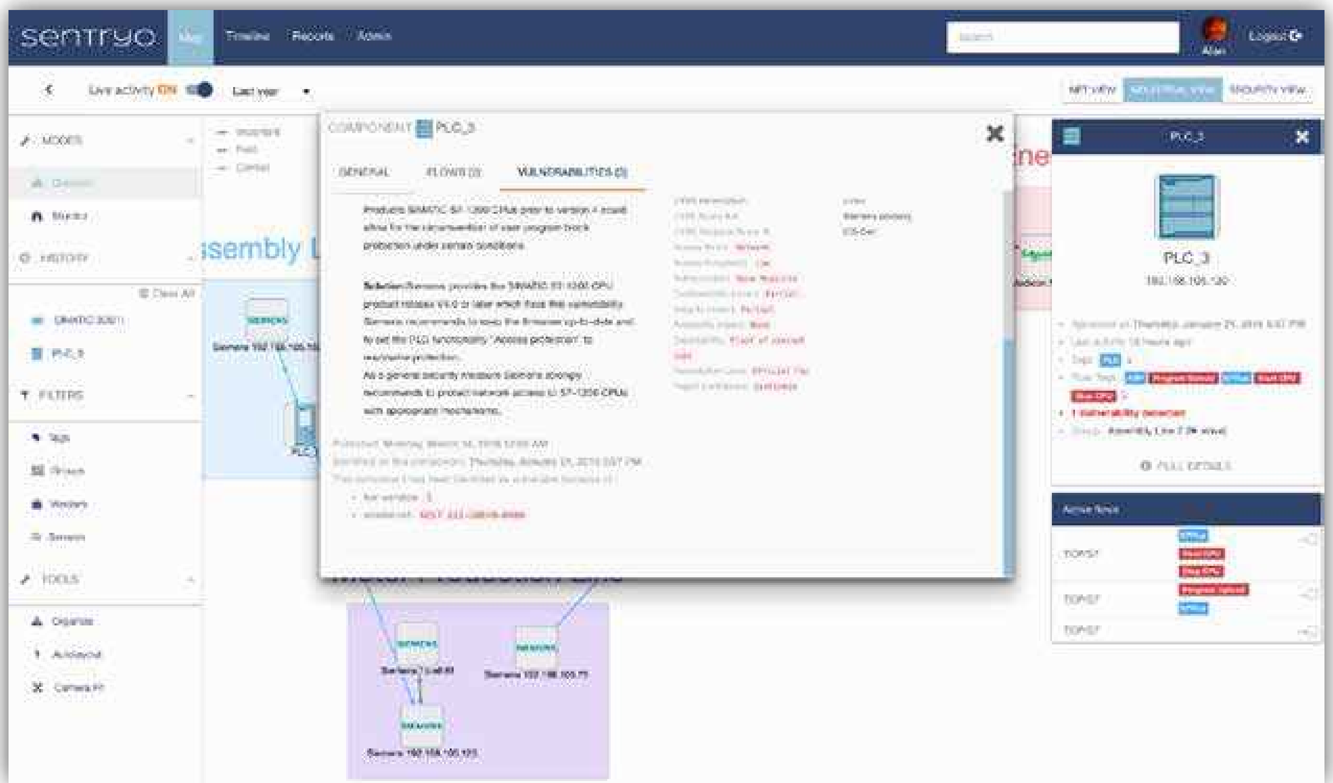
When a baseline is enforced, all new upcoming events not included in the baseline will be detected. They will trigger alerts and will be treated as such. Several baselines corresponding to different operating modes of the industrial process can be created.

Via easy to use API , OT staff can also implement their own “behaviors” tailored to their specific risk context in order to detect sequence of events which are known to be malicious . This will be the case for example for a PLC controlling a very sensitive part of the process for which the communication scheme will be predefined as a “normal behavior”.

By comparing a current or past situation on the OT Network to a ‘reference’ point, OT staff can quickly identify any aspects of the network that have changed and progress towards a desired cybersecurity policy

Anomalies are abnormal events such as new network flows coming from one machine, unauthorized changes in a timeslot, a rogue connection of a workstation to the Internet, a scan performed by the intruder to discover the network or an unusual communication pattern between the SCADA environment and the PLC.

Thanks to machine learning algorithms ICS CyberVision l earns the OT network as it operate improving its capacity to classify good and bad behavior and enhancing the relevance of the detection.



Products SIMATIC S7-1200 CPUs prior to version 4 could allow for the circumvention of user program block protection under certain conditions.

Solution: Siemens provides the SIMATIC S7-1200 CPU product release V4.0 or later which fixes this vulnerability. Siemens recommends to keep the firmware up-to-date and to set the PLC functionality "Access protection" to read/write protection.
As a general security measure Siemens strongly recommends to protect network access to S7-1200 CPUs with appropriate mechanisms.

Figure 11: Map of OT assets showing one vulnerability.

INTEGRATION OF THE ICS CYBERVISION PLATFORM WITHIN AN EXISTING SOC ORGANIZATION

In addition, regarding the **establishment of a Cyber Control Room,** the ICS CyberVision platform can support **several organizational contexts and bring flexibility:**

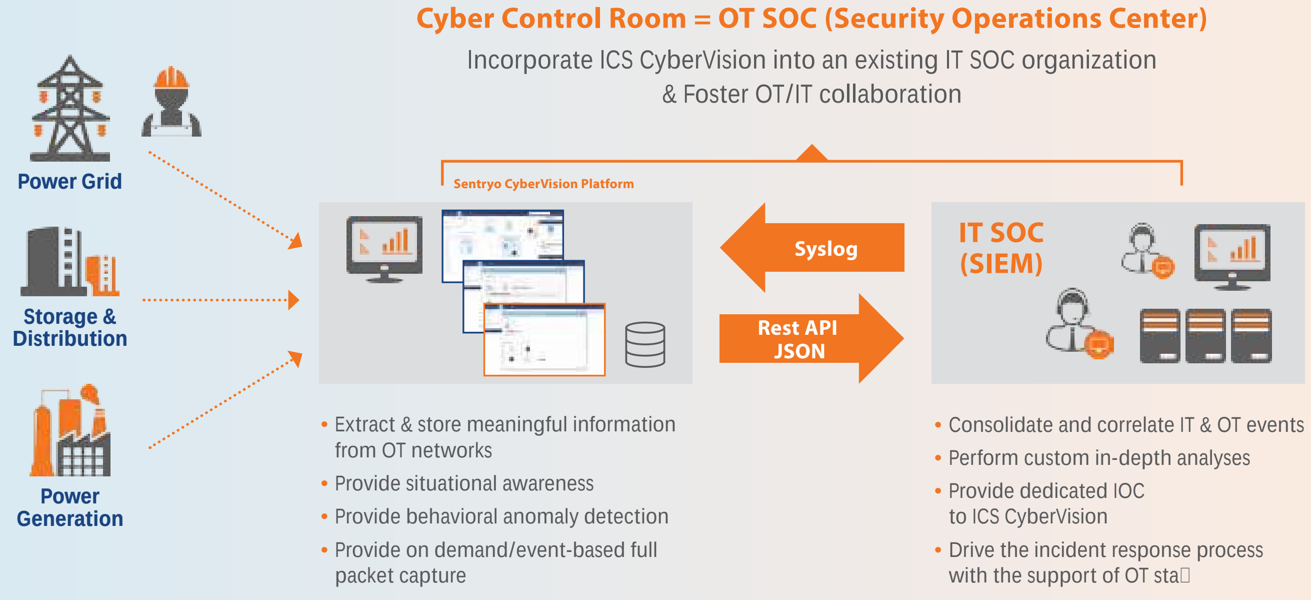
1. In a context where **a corporation does not yet have an IT SOC** including a security and information event management (SIEM) platform, it **can leverage the ICS CyberVision platform as an autonomous OT SOC with built-in capabilities** (e.g. asset discovery and inventory, passive vulnerability management, threat intelligence) **for OT environments and incorporate it into its existing industrial Control Room and processes.** Organizations do not need to invest in a heavy and costly SIEM platform with professional services to enforce rules. Anomaly detection is overseen by OT staff supported by internal or external cybersecurity experts in case of a critical abnormal event and for incident response. The abnormality of an event has to be considered from an industrial operation point of view and thus shall be validated by OT staff.

2. In a context where a **corporation has already invested in a SIEM platform and built an IT SOC,** it makes sense to **integrate the ICS CyberVision platform with the SIEM platform that** is the cornerstone of the SOC. It allows the SOC organization **to extend its monitoring and detection scope to OT networks** by streaming all the data (e.g. situational awareness information, abnormal events, logs) collected and stored by the ICS CyberVision platform so that cybersecurity experts can correlate them with logs of IT systems and analyze further.

This integration could be done in two ways:

- **all the data stored in the ICS CyberVision center can be exported to the SIEM platform via a SYSLOG interface.** Such an integration will allow cybersecurity experts to correlate the data coming from OT systems with those collected on the IT systems in order to enhance detection capabilities. It will also allow cybersecurity experts to conduct in-depth analyses using their own tools. CyberVision/SIEM integration has been validated with leading edge SIEM vendors (e.g. Splunk, AlienVault, QRadar, …).

- The ICS CyberVision center provides a **standard interface (HTTPS REST)** which allows cybersecurity experts **to directly access all the data stored by the center.** Cybersecurity experts will be able to use the APIs in order to query the ICS CyberVision platform, in particular for forensics investigations. Following a cyber-attack, they will also be able to load into ICS CyberVision their organization-specific IoC files in order to "hunt" for a particular IoC (e.g. governmental agencies or CERTs share well-known IoCs).


Cyber Control Room = OT SOC (Security Operations Center)
Incorporate ICS CyberVision into an existing IT SOC organization
& Foster OT/IT collaboration
Power Grid
Storage & Distribution
Power Generation
Sentryo CyberVision Platform
Syslog
Rest API JSON
IT SOC (SIEM)

- Extract & store meaningful information from OT networks
- Provide situational awareness
- Provide behavioral anomaly detection
- Provide on demand/event-based full packet capture

- Consolidate and correlate IT & OT events
- Perform custom in-depth analyses
- Provide dedicated IOC to ICS CyberVision
- Drive the incident response process with the support of OT staff

Figure 7: How to incorporate the CyberVision platform into an existing IT SOC organization

THE RAMP-UP AND FIRST STEPS PHASES:
SET THE FOUNDATIONS OF YOUR CYBER CONTROL ROOM

Knowledge and understanding of your OT environments and related weaknesses **(full situational awareness)** is an essential first phase to tackle OT cybersecurity problems and start establishing a sustainable Cyber Control Room.

The ICS CyberVision platform allows OT staff to:

- **continuously monitor, capture, log and record** the OT network flows;
- **discover and inventory OT assets** and their related properties and **document them in a register;**
- **identify weaknesses:** vulnerabilities, remote access, Internet access, weak passwords, unknown workstations or IP addresses (IPv6), etc.

Understanding, logging, and recording activities are key capabilities for a Cyber Control Room to understand the current state of OT environments, validating that systems are operating as intended and that no policy violations or cyber incidents have hindered the operation of systems.

Industrial corporations **will set up an ICS CyberVision live pilot for a brief period (typically one or two months) to better know and understand their OT environments in one or two of their representative industrial sites.**

ICS CyberVision will provide, through a visual yet easy-to-use UI (User Interface), a dynamic inventory and map (e.g. all the running assets - PLC, Switches, IO Module). Using the map, OT staff will be able to build a prevention plan and fix critical vulnerabilities by discovering how many remaining vulnerabilities the OT environment has, enabling security officer risk assessments and planning the next patching campaigns.

The setup of a live pilot in one or two representative industrial sites will allow an organization to:

- start enforcing a collaboration scheme between OT and cybersecurity experts,
- establish the first Cyber Control Room capabilities with related processes (e.g. asset discovery and inventory, passive VM) and incorporate them into existing processes (e.g. control & monitoring, automation, maintenance).

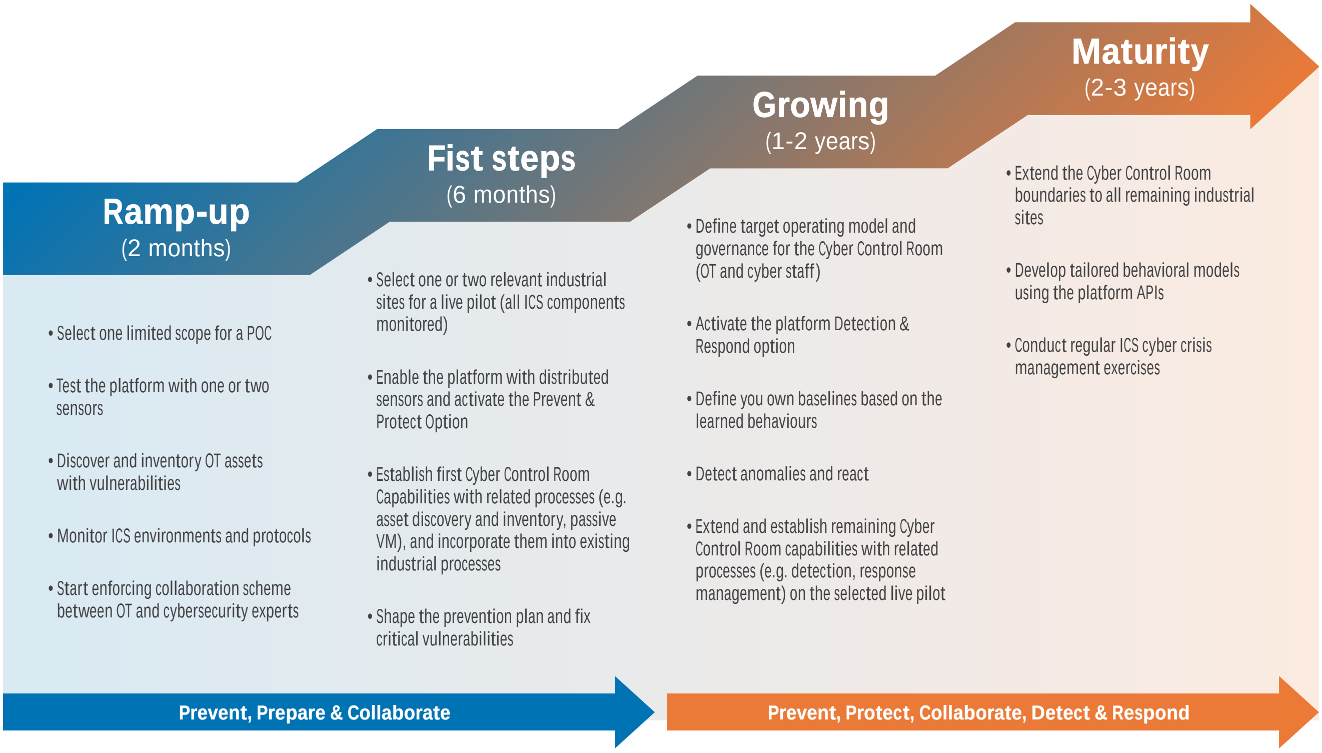

Ramp-up
(2 months)
• Select one limited scope for a POC
• Test the platform with one or two sensors
• Discover and inventory OT assets with vulnerabilities
• Monitor ICS environments and protocols
• Start enforcing collaboration scheme between OT and cybersecurity experts
Fist steps
(6 months)
• Select one or two relevant industrial sites for a live pilot (all ICS components monitored)
• Enable the platform with distributed sensors and activate the Prevent & Protect Option
• Establish first Cyber Control Room Capabilities with related processes (e.g. asset discovery and inventory, passive VM), and incorporate them into existing industrial processes
• Shape the prevention plan and fix critical vulnerabilities
Growing
(1-2 years)
• Define target operating model and governance for the Cyber Control Room (OT and cyber staff)
• Activate the platform Detection & Respond option
• Define you own baselines based on the learned behaviours
• Detect anomalies and react
• Extend and establish remaining Cyber Control Room capabilities with related processes (e.g. detection, response management) on the selected live pilot
Maturity
(2-3 years)
• Extend the Cyber Control Room boundaries to all remaining industrial sites
• Develop tailored behavioral models using the platform APIs
• Conduct regular ICS cyber crisis management exercises
Prevent, Prepare & Collaborate
Prevent, Protect, Collaborate, Detect & Respond

Figure 8: A long journey to establish a Cyber Control Room (example of a roadmap)

THE GROWING AND MATURITY PHASES: BUILD YOUR CYBER CONTROL ROOM CAPABILITIES

Situational awareness is a prerequisite but is not enough; industrial corporations must be able to detect anomalies or strange behaviors in their OT environments.

For that, they **shall extend the first Cyber Control Room capabilities to detection and incident response ones** starting with **the already selected one or two representative industrial sites** (within a 9 to 12 months' timeframe).

Based on learned behaviors, cybersecurity experts in cooperation with OT staff will then easily:

- agree on and define their own baselines,
- compare the current state with one of their defined baselines,
- use the ICS CyberVision platform to understand the frequency, danger, and impact of the observed anomalies.

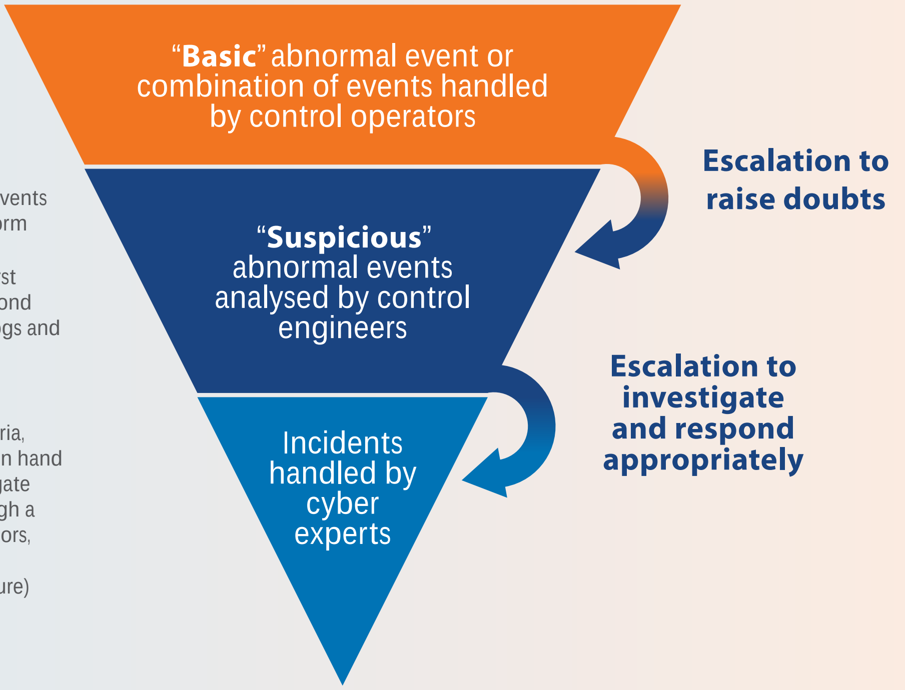
The ICS CyberVision platform also facilitates incident response by providing all of the collected information (e.g. baselines, inventory OT assets, map of all connexion, event logs, alerts) and available threat intelligence required by cybersecurity experts to investigate further and make appropriate decisions.

This phase is an opportunity to stress the incident response process in an OT environment. According to corporations' organization and culture, there exist various OT cyber incidents handling processes where OT staff and cybersecurity experts will be involved differently.

For example, in order to confirm or not the abnormality of an event regarding the process, anomalies could be handled by first level control operators, then further analyzed by second level control engineers to raise doubts and ultimately be investigated, if necessary, by cybersecurity experts.

The good news is that the Sentryo ICS CyberVision platform will facilitate the collaboration between OT staff and cybersecurity experts in order to jointly manage OT cyber incidents. Thus, cybersecurity will be progressively embedded in day to day industrial business operations.

- **Level 1:** first level control operators follow documented procedures for a basic abnormal event or a combination of events detected by the ICS CyberVision platform
- **Level 2:** the event appears to be suspicious. First level control operators escalate to second level control engineers who analyse logs and artefacts in order to raise doubts.
- **Level 3:** the event is considered to be a cyber incident according to predefined criteria, and cybersecurity experts work hand in hand with OT staff, support them to investigate further and respond to incident through a remediation plan (e.g. install new sensors, activate security policies, disconnect machines, redesign network architecture)



"**Basic**" abnormal event or combination of events handled by control operators

"**Suspicious**" abnormal events analysed by control engineers

Incidents handled by cyber experts

Escalation to raise doubts

Escalation to investigate and respond appropriately

Figure 9: One example of how OT staff and cybersecurity experts can jointly handle OT cyber incidents

MAIN CYBERVISION USE CASES

Let's illustrate three main ICS CyberVision use cases within a context of an industrial process which is automated and controlled using Siemens PLC and SCADA machines communicating with the S7 protocol (Sentryo supports multiple vendors and protocols – for more details, see the Appendix). S7 is widely used in many OT applications for manufacturing and distribution processes.

Use case 1:
the corporation does not know its industrial network.

They have installed ICS CyberVision sensors at multiple network points. Sensors extract meaningful information and sends them to the ICS CyberVision center. The center analyzes, creates the map and spots the vulnerabilities. OT staff are able to visualize OT assets and properties and to generate tailored reports for their management, the CSO and the CISO.

Use case 2:
a malware has infected a SCADA workstation and sent a new software version to one controller.

The ICS CyberVision platform has been deployed and OT Engineer have created a reference point related to the normal behavior of the OT Network. Within this reference point the behavior of the SCADA station is limited to read variable and write set points within certain memory register of one of the Siemens controller (PLC).

One attacker exploited a basic vulnerability (e.g. default password, lack of controls…) to penetrate into the OT network and end up to install a "stealth" malware on the Microsoft Windows SCADA workstation which has not been detected by the antivirus. Then the malware sent a rogue software version to the controller which pilot a critical machine. This has resulted in multiple orders in the S7 protocol (S7 download request block, download block, end download block, commit block, list block…) which have been extracted by ICS CyberVision sensors and send to the center.

The ICS CyberVision center analyses this information and combines them as a behavior which is compared in real time to the reference point.

Because this behavior is new it has triggered an alarm in the control room. Following the escalation procedure the control engineer warned by the operator is now in touch with the cybersecurity team to start the incident response process. They share information, using the map and all the information stored and timestamped within ICS CyberVision center.

Use case 3:
an attacker launched an APT attack against the corporation. The malware has initially infected a SCADA workstation then sent an order to open the emergency valve.

Use case 3 starts in the same way as use case 2. However, the attackers take aim at SCADA workstation, knowing that sending a new program would trigger a technical algorithm. So they decide to analyse deeply the SCADA program to extract the business logic. Once they found register IDs and value of the valve that could purge the circuit (ie emergency valve), they send at 3:00 am the "start purge" order. They are hoping to empty the tank before the next business day.

The OT engineer, using ICS CyberVision API has classified the message with the correct business logic (in that case "purge order") and categorized it as "high severity". Machine learning algorithms analyze it and detect that it is not legitimate in that "context". ICS CyberVision will raise an alert, showing to the OT staff that an abnormal sensitive message has been sent.

Using the same escalation procedure than in Use Case 2, the OT organization, will be able to react quickly and to stop the physical impact of the attack. Moreover, it will be able to provide all the needed forensic data to the cybersecurity expert team such as flow history including relevant properties.

BENEFITS

As OT cybersecurity budgets are quite low and attracting and retaining cybersecurity specialists is a challenge, few CSOs and CISOs have the means of constantly and consistently ensuring an appropriate level of security and compliance to keep up with changing cyber threats and regulatory compliance requirements. With Sentryo, organizations are able to use best of breed technologies while protecting OT environments against advanced threats at a fraction of the cost of traditional enterprise solutions that are less effective – removing the complexity of managing cybersecurity and compliance for their OT staff.

They can **easily integrate the ICS CyberVision platform with their existing SIEM platform in their SOC organization, extending its scope to OT thus enhancing the cybersecurity value chain both in the IT and OT worlds, and leveraging their investments.**

Furthermore, roll out is also easy and rapid: customers can deploy the ICS CyberVision platform within hours rather than weeks or months and protect themselves better and faster, ensuring safe and reliable business operations.

Major benefits of the Sentryo ICS CyberVision platform are:

- **Fully passive solution:** no impact on the network, fully isolated sensors (data diode).
- **Powerful architecture:** enriched meaningful information with business logic and context.
- **Advanced threat detection,** with anomaly detection based on machine learning.
- **OT integrated within cybersecurity processes:** advanced data visualization to support decision making and OT adoption, near zero configuration, IT/OT collaboration.
- **Multi-vendor support:** ABB, Yokogawa, Forboro, Siemens, Schneider, Rockwell, Emerson and more…
- **Integration with leading SIEM vendors:** Splunk, AlienVault, QRadar…

APPENDIX

FIVE LONG-TERM TENETS TO GUARANTEE CONTINUITY OF BUSINESS INDUSTRIAL OPERATIONS

In order to ensure **overall business continuity and resilience,** industrial corporations **will need to incorporate cybersecurity into their business operations and will embrace progressively the following tenets:**

1. They will **rely on standards** such as the NIST Guide to Industrial Control Systems Security, the ISA/IEC 62443 standard, and on local guidance (e.g. the French ANSSI or the German BSI[8] agencies recommendations). These standards are moving targets which will require efforts in existing legacy OT systems and time to fully adopt them.

2. They will **heavily collect, analyze, evaluate and share threat intelligence** from and with multiple sources (e.g. governments, ICS CERT, CERTs, OT vendors…). Corporations will understand the process an adversary may take to achieve their goals - the so called "kill chain[9]" which derives from military terminology.

3. They will **integrate OT cyber risks into their risk management processes** with threat intelligence feeds and historical data of external OT cyber incidents in order to evaluate the likelihood of risk scenarios. Risk assessments will be a powerful tool to educate management about the increasing OT cyber risks.

4. They will **buy "security by design" products from trusted OT suppliers** and they will have confidence that selected products are robust against attacks and free from known vulnerabilities. Certifications will become the rule. However, it will not eliminate risks of product's misconfiguration and the need for monitoring OT networks.

5. Ultimately, **like safety, OT staff will enlarge their operational activities to handle cybersecurity tasks.** Cybersecurity events will be additional events to be monitored by OT staff. Therefore, in an industrial site, business operations will be traditionally managed as follows:

- **External experts:** Experts (often subcontractors) design, develop and install OT systems on behalf of the industrial organization. They will integrate "security by design" early in the OT systems development lifecycle because industrial corporations will have adopted ISA/IEC 62443 cybersecurity standards and will require it.

- **Maintenance operators:** Control or automation engineers conduct maintenance operations when necessary. In addition, they will install and change OT cybersecurity systems (e.g. firewalls, anti-malware, sensors…). They will also inventory OT assets and their weaknesses and update the CMDB using automated solutions.

- **Control operators:** they will receive relevant alarms related to cyber incidents categorized by priority level (e.g. abnormal behavior, rogue station connecting the network…). They will be able to react to high priority incidents by handling standardized procedures or handbooks.

[8] ANSSI - French Information Security Agency; BSI - (German Bundesamt für Sicherheit in der Informationstechnik)

[9] "The Industrial Control System Cyber Kill Chain" paper (SANS Institute)

ANSWERING TO STRINGENT **REGULATORY REQUIREMENTS**

In particular, for r**egulatory regimes** such as the French LPM or the upcoming EU NIS Directive, essential or critical **asset owners have to address the following requirements:**

- **Notify, document and report detected severe cyber incidents to their local authorities** (e.g. a French-based company which faces an incident in Germany will provide notification to the BSI in Germany…).
- Following the notification, **demonstrate to the authorities evidence that "effective, proportionate and dissuasive" cybersecurity measures have been put in place.**

Thus, all organizational, legal and operational security measures taken must be plotted, stored and documented in order to be provided in case of a severe cyber incident. **In case of lack of evidence and non-compliance, asset owners will pay heavy financial penalties (e.g. for the NIS Directive, sanctions of up to €10 million or 2% of revenues). In this regulatory regime context, industrial asset owners using the ICS CyberVision platform will be able to search and show authorities meaningful pieces of evidence such as: OT assets inventory, maps, fixed vulnerabilities, logs, prevention actions taken, recorded events or meta-data…**

VENDORS AND PROTOCOLS **SUPPORTED BY SENTRYO**

Sentryo supports and continuously integrates a wide variety of industrial protocols from the most popular vendors such as:

- **PLC control & field network communications: Siemens** - S7, S7 "Plus" for 1200/1500, Profinet; **Schneider Electric** - Modbus / XWAY / UNI-TE (PL7 Pro) / UMAS (M340 / M580 / TSX Premium); **Rockwell Automation** (Ethernet/IP, CIP) …
- **Standard protocols: Electrical engineering & Power system automation** - IEC 104 (IEC 61850 End of 2016); **SCADA / Data acquisition** - OPC-DA/UA; **IT Networks** - Ethernet, TCP/IP, DNS, ARP, FTP, HTTP…
- **Distributed Control System: Emerson** - Ovation, Delta V; **Heywell**[10] - Experion / Safety Manager; **Yokogawa**[11] - CENTUM VP / ProSafe RS / PRM…
- **IT Network protocols**

Sentryo regularly adds new protocols to meet the needs of its customers. For more information contact sentryo.

[10] Work in progress

[11] Work in progress

THE SENTRYO THREAT INTELLIGENCE CAPABILITY

One description of threat intelligence is the process of **moving topics from 'unknown unknowns' to 'known unknowns'** by discovering the existence of threats and **then shifting 'known unknowns' to 'known knowns' where the threat is well understood and mitigated.** For example, if we have discovered evidence that the CEO is going to be physically attacked outside our office, we find out who the attackers are and what weapons they're carrying. Then we inform the CEO so that travel plans can be changed or the attackers arrested before the incident takes place.

Threat intelligence is no longer an option for managers of OT networks. Because of this, Sentryo has established a world class cybersecurity research lab in order to provide accurate threat intelligence information to its customers and partners. By leveraging these feeds, partners and customers are able to discover intrusions before they have caused any severe damage.

Sentryo is very active and engaged in threat intelligence R&D projects. The Sentryo research lab mission is to model attacks, to look for attack vectors in protocols (vectors or method of attacks can be legitimate or malicious) and to develop tools for OT staff so that they can monitor and track OT environments (map, baseline, events).

The Sentryo cybersecurity research lab collects, analyzes and evaluates intelligence from multiples sources: ICS CERT, CERTs, OT vendors (Siemens, Schneider, Rockwell, Emerson…) bulletins, results of scanning tools (Nmap…), IoC, malware feeds, conferences, academia, technical blogs…

The Sentryo lab is able to provide threat intelligence **information related to vulnerabilities** (for passive detection purpose), **flow identification** (for packet inspection purpose), **hacker techniques & tactics and attack patterns** (for key behaviors and potential attack vectors purposes).

Threat intelligence information **fuels the Sentryo Knowledge Database (every week), the CyberVision platform (every two months) and early threat intelligence briefings (every month).** For early briefings (e.g. Ukrainian cyber-attacks against ICS), the Sentryo research lab analyses the various reports and information published by different organizations and grabs intelligence from technical blogs or social media. Based on its own research activities, the lab also provides in-depth insights and indicators of compromise.

Therefore, threat intelligence continuously enriches the value of CyberVision platform through increasing shared knowledge.

sentryo

e: contact@sentryo.net | w: www.sentryo.net

Sentryo HQ
66 Bd Niels Bohr CS 52132
69603 Lyon-Villeurbanne - France

Telephone
+33 (0) 970720876