



CLAROTY
Clarity for OT Networks

White Paper

Claroty

A New Platform For OT
Cybersecurity





Contents

Summary	1
The Business Perspective	2
Situation	3
The Market	3
The Opportunity	4
Platform Description	5
Roles Supported	5
The Dashboard	6
Central Management	7
Work Process Support	7
Differentiating Features	10
Benefits	11

Summary

Ensuring the security of industrial control systems (ICS) and the prevention or detection of cyber-related attacks and events is of increasing importance to users of these systems. The use of "commercial off-the-shelf" (COTS) technology in the design and configuration of these systems has resulted in them displaying the same vulnerabilities as more general or business information systems. In addition, more connectivity and the use of networked systems means that asset owners may not have a good understanding of how their systems are configured, or an accurate record of the devices and systems in use.

Detailed information about the configuration and operation of a system is essential in order to detect anomalous or unusual behavior that could be an indication of an attack or possible compromise. Products and technology that provide these capabilities must be justified based on solid business- and operations-related criteria, and implemented in a manner that complements normal operation of these systems. This includes the identification of specific roles that would use such tools, and the benefits that would be gained.

Capable and appropriate tools can enable or even encourage collaboration between the various roles associated with the operation and support of complex control systems. The most essential element of this collaboration is having a common vision of the current

The most essential element of this collaboration is having a common vision of the current state, as well as the desired goals.

state, as well as the desired goals. The use of common tools and sources of information will bring together experts from a variety of organizations and functions.

The Claroty platform represents an innovative approach to addressing the specific challenges associated with

cybersecurity in the industrial environment. The primary driver and purpose of implementing tools and technology for ICS security is to maintain and improve the operational security of the industrial control environment. Additional potential benefits include:

- more accurate records of installed systems.
- improved collaboration between internal and external operations and support groups.
- and a more rigorous management of change and configuration control discipline.

The Claroty platform represents an innovative approach to addressing the specific challenges associated with cybersecurity in the industrial environment.

The Business Perspective

Ensuring the security of industrial control systems (ICS) and the prevention or detection of cyber-related attacks and events is of increasing importance to asset owners in light of rapidly evolving risks. While there may be a tendency to look for a quick fix in the form of a product or solution that will address cybersecurity-related issues and objectives, it is important to first understand the business requirements and constraints. Decisions as to what should be done are only possible after there is agreement on the question of why such measures may be necessary.

Depending on the nature of the business or industry in question, business drivers include external expectations or regulations. Even in cases where formal regulations may not exist, there is generally an expectation of safe and reliable operation.

Every company and industry must respond to the expectations of its shareholders, including customers, industry associations, regulatory bodies, and the general

public. One of the more fundamental expectations is that the facilities are operated reliably, profitably, and safely. In order to meet this expectation, it is necessary to have a good understanding of risk.

Traditional risks associated with operations are well-understood, and include factors such as equipment failure, poor product, or raw material quality and interruptions to portions of the supply chain. A more recent development is the emergence of cybersecurity-related threats to the efficiency, availability, safety, and integrity of the process. Regardless of whether the threat is physical in nature or related to intrusions into automated systems by cyber means, the consequences can be the same.

Risk is generally defined as a function of threat, vulnerability, and consequence. It is the consequence element that should be the primary focus of the asset owner. Only those familiar with the operation can adequately identify and assess the consequence of negative events.

It is important to understand that negative consequences can occur as a result of cybersecurity threats and vulnerabilities. This reality has led to increased acceptance of the imperative to have adequate cybersecurity-related protection for computers and networks used in various aspects of manufacturing and operations processes. Cybersecurity is added to physical security as an area that requires attention and suitable response.

Situation

Although the understanding of the expectations and risks is improving and more people are accepting the imperative of addressing ICS cybersecurity, significant challenges remain. The environment in which industrial control systems exist has several characteristics that can be impediments to success.

The first of these is the inherent complexity of such systems. A typical industrial control system is a "system of systems", composed of components and devices from a variety of suppliers. The diversity of technologies and products found in the typical industrial control system

means that multiple communications protocols may also be present. Even though there are communications standards such as MODBUS, it is also possible to have a variety of protocols present.

Poorly managed changes can also present a challenge. Even if the number of different suppliers or protocols is small, these systems evolve over time as new technology becomes available and modifications or expansions are required. Unlike business systems that may be replaced on a relatively frequent basis, industrial control systems are more likely to be modified and expanded in place. In addition, it is common for changes to be made without careful attention to record keeping.

Effective security requires an accurate asset inventory. Staff in operations and security operations centers need better tools and processes to maintain this information, manage security updates, monitor policy compliance, and record anomalous events. These activities complement policy management.

Industrial control systems do not exist in a vacuum. Increased connectivity has led to a corresponding increase in risk, but even in cases where this connectivity does not exist, potential threats have evolved and increased as awareness of the systems and their importance has increased.

Perhaps the most important element of risk for the asset owner is the assessment of potential consequence. It has long been the practice to identify and assess consequences in areas such as process safety using tools such as process hazard analysis (PHA). The same techniques must also be applied in cybersecurity.

Finally, there is the challenge of sustaining such protections over time. It is not sufficient to conduct a risk assessment and implement the appropriate protections just once. There must be a sustainable program to repeat these steps as circumstances change, and to measure effectiveness.

The Market

The market for industrial cybersecurity products and solutions is large and diverse. Although the number of major suppliers and basic architectures is limited, these systems are installed in a wide variety of industries and process types. Each of these situations represents different priorities and business needs.

There are many ways to characterize the types of industries that employ industrial control systems. The most common is to assign specific plants or companies to any of several common industry sectors, such as chemical, mining, pharmaceuticals, etc. Considerable effort has also gone into the identification of a definitive set of critical infrastructure sectors. In the United States the scope and composition of the critical infrastructure is defined in the National Infrastructure Protection Plan. Other countries have similar plans and strategies. Taxonomies such as these are useful resources for characterizing companies, industries, and even individual facilities.

It is also important to be able to characterize ICS implementations in terms of the type of operation being controlled. The most common grouping includes continuous or batch processing, discrete manufacturing, and hybrid.

Examples of continuous process industries include chemicals, oil and gas drilling, petroleum refining and power generation and transmission, and paper making. Each of these can be characterized by its use of a continuously operating process to transform materials and create specific products. Batch processing is typically used in industries such as food and beverage or pharmaceuticals. Discrete manufacturing processes such as vehicle manufacturing and consumer electronics typically involve the assembly of products from parts and sub-assemblies.

Regardless the method used to group companies and industries, it is essential that security products and services are suitable for the broadest range of applications.

Although the technology and process elements are important, perhaps the most critical element is the people and the roles that they fill in the implementation,

operation, and support of industrial control systems. Since cybersecurity is a relatively new issue for operations, it is often unclear who is responsible for various aspects of the response. The resources and expertise required are typically not readily available at the plant level, and compliance with established policies may be overlooked.

Cybersecurity products and solutions must be carefully designed to meet the needs of the specific user roles. For efficiency, they also need integrated tools in plants and security operations centers to maintain accurate asset inventories, manage security updates, monitor policy compliance, and record anomalous events. If there is an incident, the investigation may involve roles from multiple organizations, both internal and external.

The Opportunity

All of the above elements (i.e., people, process and technology) must be addressed in a comprehensive cybersecurity management system. Such a system may be specific to the industrial control systems environment, or an extension of a broader corporate program. Regardless of the approach chosen, there must be a clear set of security policies that all service providers must follow, and a means to monitor compliance.

The unique needs and constraints associated with industrial systems must be respected. For example, remote access to industrial systems can be risky, particularly when multiple service providers are involved. However, a coordinated response for monitoring, maintenance, and incident response often requires a means of allowing such access, and standard procedures for authorization and privileges to manage the additional risks.

In order to address this opportunity, asset owners and support organizations need guidance, tools, and methods for the management and operation of complex industrial control systems and associated networks. This includes, but is not limited to: asset discovery, asset characterization, and anomaly detection.

The control systems and network views must be integrated in a manner that allows information about the

total system performance to be presented to operations staff in a context that they can understand, without the requirement that they become “experts” in system and network management. Solutions must be able to be integrated into normal operations workflows.

In order to assess the suitability of specific products and technologies, it is important to have clear criteria. The first and most obvious criterion is the range of capability provided by the product or solution.

Because of the diversity and complexity of control systems, it is very important for the proposed product to be capable of understanding and communicating a wide variety of protocols. Finally, it is necessary to assess whether the solution has been conceived, designed, and applied in the context of industrial operations. Specifically, there must be an appropriate balance and blending of general and special-purpose technology and the potential for integration with other systems. Solutions originally developed for business IT environments may not be suitable.

*Solutions originally developed
for business IT environments
may not be suitable.*

The Claroty Platform

The Claroty platform represents an innovative approach to the pursuit of this opportunity, while addressing the specific challenges associated with the industrial environment. The following sections describe specific functionality and features of the platform that help with this mission.

Roles Supported

The Claroty platform includes the capability to be tailored to the needs of a variety of roles, and for use within several work processes. Potential stakeholders and associated roles include:

- Automation engineers, who typically have the responsibility for configuring the ICS to implement the desired control strategy.
- Plant or process operators, who have a view of the control system and controlled equipment on a 24/7 basis. They may not fully understand the security related behaviors and issues, but they do have a firm understanding of what is normal or abnormal in plant operation.
- There may also be a centralized security operations center (SOC) that has responsibility for monitoring activity and behavior on the network. However, they do not have a plant perspective.
- Maintenance and support staff, who have the responsibility of responding to problems and system or component failures and making the necessary corrections or repairs.

Each of these roles has its own perspective on the monitoring, management, and security of industrial control systems and associated networks. Automation engineers are concerned with the integrity of the control strategy, while operations staff focus on implications for the process under control. Those staffing security operations centers must be able to detect and respond to anomalous events that may be indicators of an attack or improper use of the system. Finally, maintenance staff must have a clear view of the system configuration in order to respond to the need for changes or updates to system components.

The relative prominence or even the existence of each of these roles will vary by situation. Therefore, it is important to present information in a form that allows interpretation without specialized expertise in subjects such as network support or cybersecurity.

The Claroty Platform

The Claroty dashboard provides a graphical view of the environment, identifying the functional components and the pathways between them. It also gives a summary of system status, which includes the number of current and newly discovered assets, any potential anomalies and a traffic trend.

Figure 1 is an example of the dashboard display.

The dashboard provides the general context for collaboration between the various roles involved in operating, monitoring, and maintaining the environment. This is essential, since maintaining the operational integrity of industrial systems requires skills and experience from several disciplines.

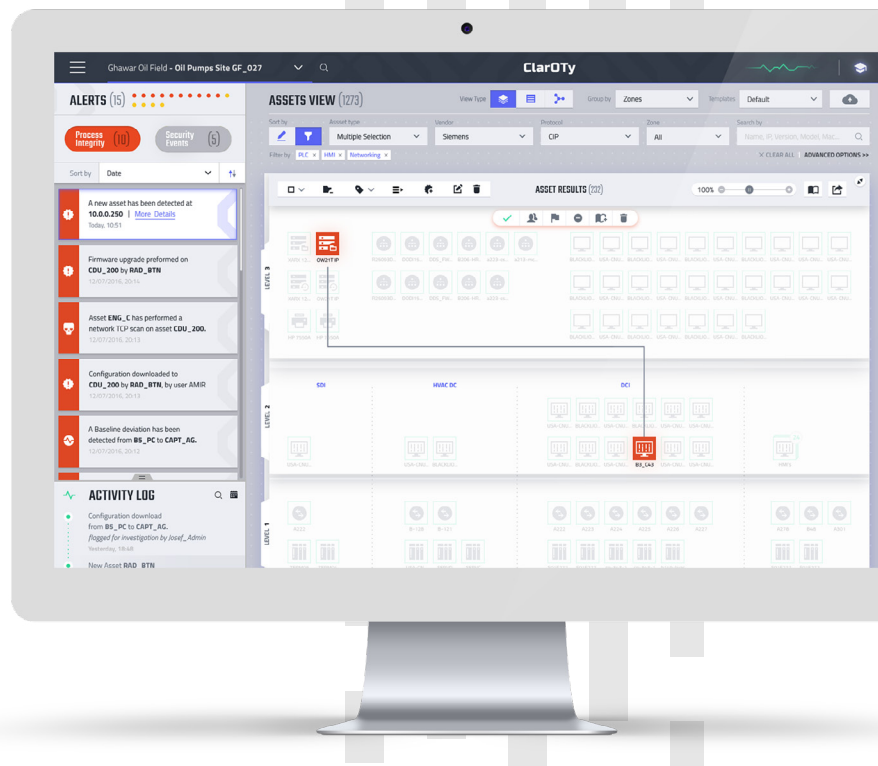


Figure 1 – Platform Dashboard

Central Management

Central management of multiple remote sites may be required to support business practices. An example of this would involve use of Claroty by staff in a security operations center. Such access must be provided in a manner that protects the integrity of the systems and assets being monitored. In such situations, a common requirement is to view multiple systems on a common display.

Figure 2 is an example of a display showing multiple remote systems.

In order to provide the information required to adequately monitor and control a typical industrial control systems environment, solutions used must support a wide range of

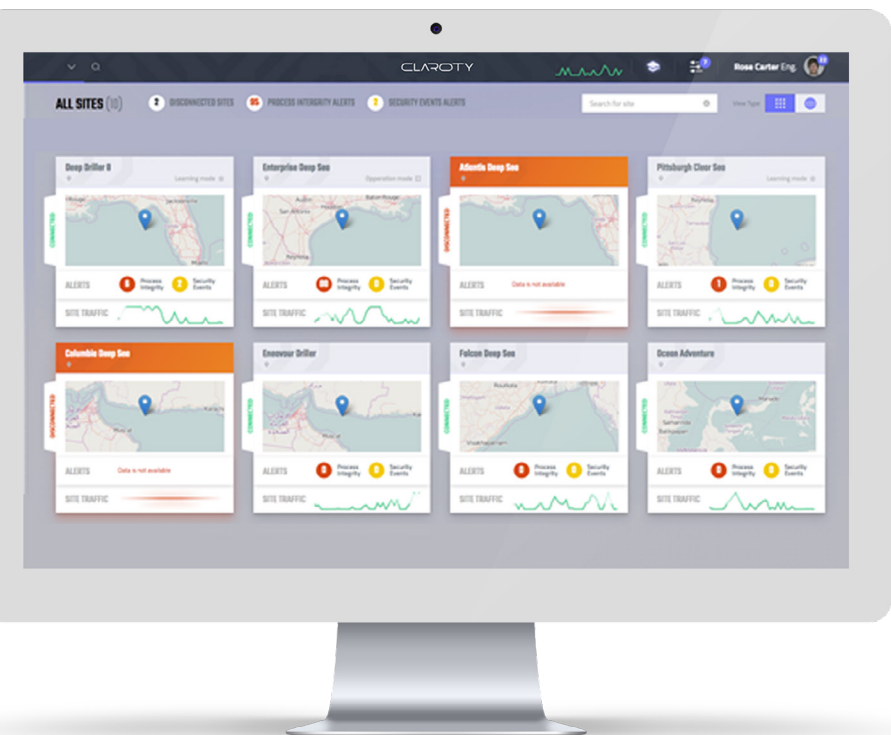


Figure 2 – Multi System Display

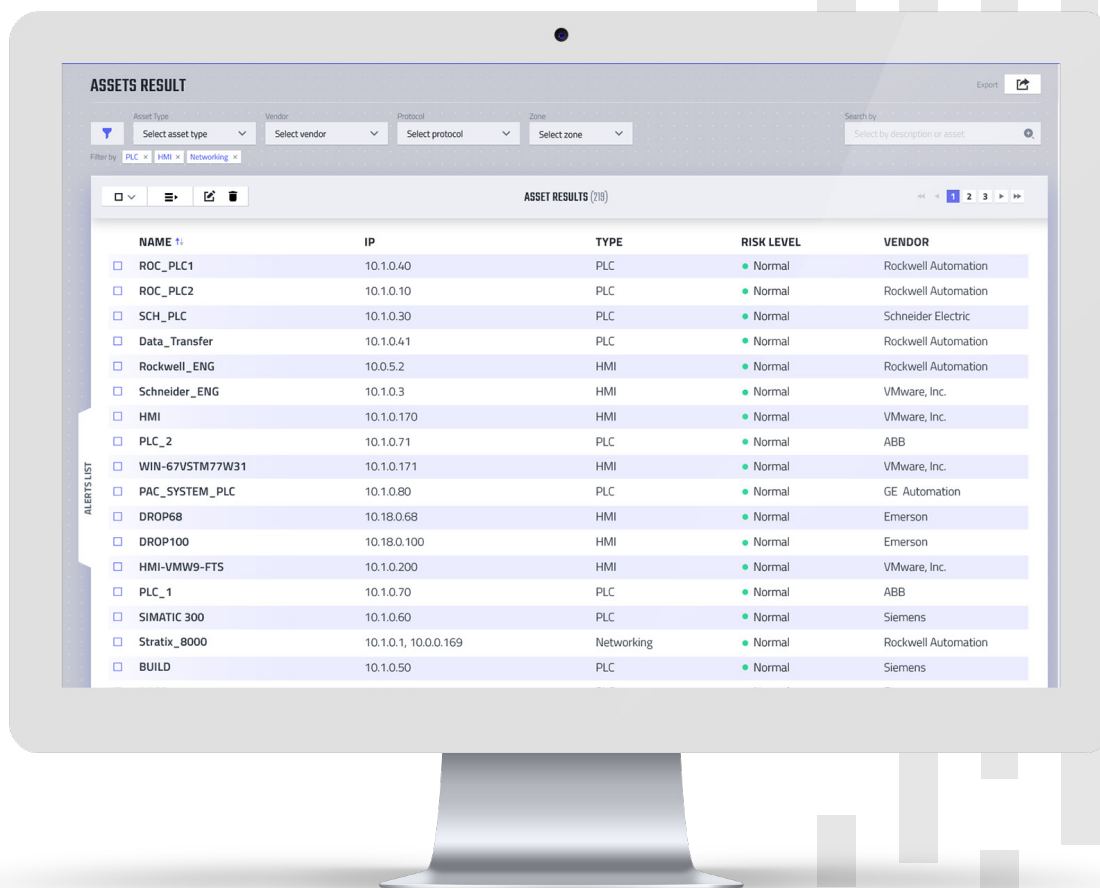


Figure 3 – Asset Discovery

functionality and technology. Typical control systems have been installed, enhanced, and expanded over a period of years or decades, using products and technologies from a variety of sources.

Detection and interpretation of the communications occurring between control system components provides the ability to generate and automatically update configuration and network diagrams, such as that shown as part of the dashboard in Figure 1.

Work Process Support

The Claroty platform collects and provides information that is essential in the context of several work processes, corresponding to the phases of the industrial systems life cycle. These include design, configuration, operation, maintenance, and incident response. While each of these

phases have specific needs, there are several functional capabilities that are of specific importance.

1. Inventory Management

At all phases it is essential to have an accurate and up to date inventory of assets. This inventory is can be assembled automatically, using the asset discovery capability of the platform. As new assets appear on the network, their presence is detected by Claroty and identified for confirmation. This capability is also useful in the detection of anomalous activities, such as the appearance of unauthorized or unexpected devices, as shown in Figure 3.

Detection of new devices or assets triggers an automatic alert.

Acknowledgement of such an alert will automatically add the asset to the current inventory. Asset discovery includes the collection of a considerable amount of information about their configuration. This information is added to the inventory when the discovery is confirmed.

2. Alert Monitoring and Reporting

Depending on the nature of the event or activity it is possible that several individual alerts may be generated. Claroty automatically groups related alerts for ease of analysis, as shown in Figure 4.

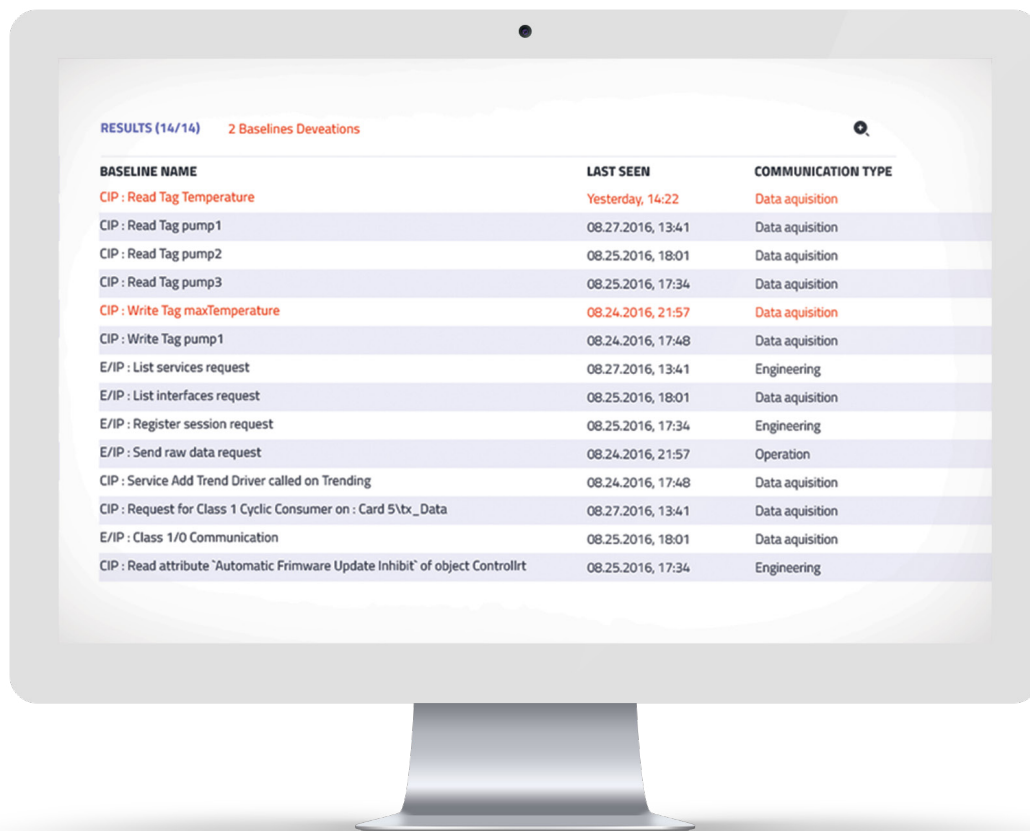
3. Management of Change

Claroty generates alerts on other types of activities, such as changes to the configuration of a particular asset. This can be very useful in detecting unexpected or unauthorized changes to control logic in controllers or other devices, which can indicate either human error, or malicious activity.

4. Behavioral Analysis

While it is important to be able to identify the devices on the network and detect when changes

are made, this is not enough. Claroty uses this capability to also monitor and interpret system behavior in order to establish a baseline for normal operation, and alert when deviations occur. This allows for the identification of and response to unusual behaviors, such as configuration or control commands coming from new or unusual sources. Evidence of communications between devices that have not traditionally exchanged information can be evidence of an attack. On top of that, Claroty utilizes its deep ICS knowledge to provide various off-the-shelf alerts on traffic patterns that reflect critical changes, that are either distinctively malicious (example: man-in-the-middle attack), or are important enough to be worth the attention of operator/security analyst (example: configuration download, or PLC mode change).



BASLINE NAME	LAST SEEN	COMMUNICATION TYPE
CIP : Read Tag Temperature	Yesterday, 14:22	Data aquisition
CIP : Read Tag pump1	08.27.2016, 13:41	Data aquisition
CIP : Read Tag pump2	08.25.2016, 18:01	Data aquisition
CIP : Read Tag pump3	08.25.2016, 17:34	Data aquisition
CIP : Write Tag maxTemperature	08.24.2016, 21:57	Data aquisition
CIP : Write Tag pump1	08.24.2016, 17:48	Data aquisition
E/IP : List services request	08.27.2016, 13:41	Engineering
E/IP : List interfaces request	08.25.2016, 18:01	Data aquisition
E/IP : Register session request	08.25.2016, 17:34	Engineering
E/IP : Send raw data request	08.24.2016, 21:57	Operation
CIP : Service Add Trend Driver called on Trending	08.24.2016, 17:48	Data aquisition
CIP : Request for Class 1 Cyclic Consumer on : Card 5\tx_Data	08.27.2016, 13:41	Data aquisition
E/IP : Class 1/O Communication	08.25.2016, 18:01	Data aquisition
CIP : Read attribute "Automatic Firmware Update Inhibit" of object ControlIrt	08.25.2016, 17:34	Engineering

Figure 4 – Alert Grouping

Differentiating Features

In addition to specific functionality in the support of roles and work processes, the Claroty platform has several differentiating features, as described in the following paragraphs.

1. Totally Passive Operation

The IEC 62443-2-4 (Security for industrial automation and control systems – Security program requirements for IACS service providers) standard there is an enhancement to requirement SP.02.02 which states:

"The service provider shall have the capability to ensure the control system components used in the Automation Solution have the ability to maintain operation of essential control system functions in the presence of system and/or network scans during normal operation."

All of the network scanning (e.g., for asset discovery) performed by Claroty is entirely passive, based on observation and interpretation of network traffic. This approach ensures that such scanning will have no adverse impact on the normal operation of the control system, thus contributing to compliance with the above requirement.

2. Extensive Protocol Support

An equally important feature is the variety of protocols used for communications between system elements. Some are widely known and used (e.g., MODBUS), while others may be more obscure or proprietary.

Claroty fully supports the protocols used by virtually all leading control systems suppliers (e.g., Siemens, Rockwell, Honeywell, Emerson, ABB, Yokogawa, Schneider Electric, GE, and Mitsubishi), with the potential of others, depending on the demand or requirements. The extensive list of protocols is a clear distinguishing feature of the product.

All of the network scanning (e.g., for asset discovery) performed by Claroty is entirely passive, based on observation and interpretation of network traffic. This approach ensures that such scanning will have no adverse impact on the normal operation of the control system, thus contributing to compliance with the above requirement.

3. Configuration Detection

In addition to analyzing the communications streams and interpreting various protocols, there is a requirement for a solution to be capable of "looking into" various control-related devices on the network (e.g., controllers) and reporting on their configuration and the resident software. Claroty provides the capability to collect information not only on network configuration and inter-node communications, but also about the configuration of the individual elements.

Benefits

The primary driver and purpose of implementing tools and technology for ICS security is to maintain and improve the operational security of the industrial control environment. However, the use of such solutions provides a range of benefits, not all of which are directly related to security.

Capable and appropriate tools can enable or even encourage collaboration between the various roles associated with the operation and support of complex control systems. The most essential element of this

collaboration is having a common vision of the current state, as well as the desired goals. The use of common tools and sources of information will bring together experts from a variety of organizations and functions.

It is also essential to have an accurate view of the installed system and its normal behavior. Only with a detailed understanding of what is normal is it possible to identify and evaluate changes to configuration or behavior in order to detect potential security-related events.

Accurate asset inventories, coupled with strong management of changes, processes and procedures, are essential for long-term asset management. The ability to monitor the network and report on unanticipated changes or anomalous behavior is a fundamental capability in the successful application of such processes.

Successful implementation of automated security solutions and tools requires a detailed understanding of the roles involved in their operation, as well as the specific responsibilities and expectations. It is common for this level of understanding to be lacking before such implementations, so improved role definitions may be a side benefit.



About the Author

As the principal consultant at OIT Concepts LLC, Eric C. Cosman provides consulting and advisory services in the management of information technology solutions in operations and engineering. Eric is a pioneer in the ICS cyber industry and co-chair of the ISA99 Committee. With more than 35 years of experience in the process industries, he has held positions in process engineering, process systems software development, telecommunications, IT operations, automation architecture, and consulting.