FORESCOUT

Monitoring Industrial Control Systems to Improve Operations and Security

An overview of the threats to industrial control systems and the technologies that protect them

Contents

The Need for Monitoring

Industrial control systems (ICS) sit at the core of every industrial process - from power generation to water treatment and manufacturing. The term ICS refers to the set of devices that govern the process to guarantee its safe and successful execution and include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control systems such as Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC). A malfunction in any of these systems or the network in which they operate might cause the entire industrial process to fail, with serious consequences in terms of economic loss and compromised public safety. For instance, an incorrect distribution of power in an electricity transmission network might affect availability to households, offices, hospitals, etc. Similarly, a faulty component that regulates the amount of chemical substances in a pharmaceutical production process might lead to entire batches of harmful compounds.

The need to monitor ICS networks is advocated in many venues and has been included in several recommendations, guidelines and standards, such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)[2], the NIS Directive from the European Union[3], and America's Water Infrastructure Act (AWIA)[4]. There are several reasons why monitoring should be an integral part of operations and may even be considered a competitive advantage. The marked increase of cyberattacks directed against ICS, as frequently reported by the ICS Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security, is only one of them. Stuxnet, WannaCry, TRITON, NotPetya, LockerGoga and Ryuk have seized the full attention of the media but represent only a small portion of the cyber threats targeting ICS.

Today, organizations rely heavily on third parties like contractors and vendors, to streamline their operations. Smaller organizations, such as local utilities, have consultants programming and maintaining their PLCs, while larger organizations have direct lines connecting their process control devices to vendors for 24/7 support and maintenance. In all cases, connectivity comes with gains in productivity but adds a totally new dimension of risks that make securing ICS networks absolutely critical. The shift in how industrial networks are operated and maintained makes it crucial for organizations to monitor their infrastructure not only against cyber attacks, but also against system misuse by third parties. Additionally, there is an ever-present threat coming from insiders, including disgruntled employees, human error and network and system misconfiguration, which could affect or lead to disruption of the production process. All these threats could impact the revenue of an organization and should receive daily attention from the boardroom.

Organizations can mitigate these threats by implementing a solid monitoring infrastructure for ICS and back-office networks. With an effective monitoring infrastructure in place, organizations are not only able to detect problems at an earlier stage, but can also mitigate consequences before any real damage is done and recover more quickly from an incident, no matter the nature.

> Continuous monitoring and early analysis of identified issues help organizations pinpoint root causes of a problem and enforce effective countermeasures and remediation actions.

Before implementing any monitoring infrastructure or even considering a specific solution, however, organizations should assess the exposure to risks and threats of their network and devices. Quite often, organizations overlook this phase of the security process and rush into picking a solution that does not match their needs or expectations. This document is not intended to provide details about risk assessment procedures. Nevertheless, it is important to understand its key concepts and identify the steps that lead to the selection of appropriate monitoring solutions.

Assessing the Risk

The process of securing an industrial environment is a never-ending cycle that aims to continuously improve the security posture of the organization. To prioritize the next steps, estimate effort and measure improvement (or regression) over time, security personnel need to assess the organization's current security status in a number of areas.

A typical risk management process consists of three phases: risk analysis, risk evaluation and risk mitigation. During the risk analysis phase, an organization must identify its key assets and their vulnerabilities, as well as the related threats and threat sources. Threat sources can be either external to an organization, such as foreign intelligence agencies, cyberterrorists and hacktivists, or internal, such as poorly trained or disgruntled employees, contractors and vendors. Each adversary has different characteristics in terms of funding and capability to exploit an organization's critical assets. Evaluation of insider threats should take into consideration not only system misuse, but also the chance of device failure, which is often the cause of industrial process disruptions.

To effectively analyze risk, it is important to carefully assess the impact and likelihood of each threat being exercised against an asset or the network. The best way to proceed is to take into consideration high-impact threats and determine the cost and effort needed to recover productivity. A good network monitoring tool can provide an automatic ranking of these threats based on overall likelihood and impact on the network.

Finally, an organization must decide what course of action to take with the identified risks and threats, like whether they can be avoided, should be accepted or could be reduced by means of adequate controls. In traditional risk management, there are several types of controls that can be applied to reduce a risk, including legal, deterrent, preventive, monitoring, detective, corrective, etc. The implementation of each of these controls might involve different elements of an organization, including:

- People implementing good practices and receiving proper training
- Controlling access to systems in the physical realm
- Putting proper procedures into place for things like change management and disaster recovery
- Applying technologies like antivirus and intrusion detection systems

The selection of the right combination of controls should aim at minimizing the likelihood and impact of the identified threats, to maximize the benefit for the organization.

In the rest of this whitepaper, we discuss the most prominent cyber threats to ICS networks and their possible impact on an organization. We also give an overview of the existing technologies that can be employed to mitigate them.

ICS Threat Landscape

A threat and vulnerability analysis is a mandatory step that should precede all security-related decisions, including decisions regarding which procedures to adopt and which detection and prevention solutions to employ. Unfortunately, more often than not, this step is skipped altogether.

In this section, we analyze the possible threats to ICS networks. The threat analysis is performed in three steps:

1. We discuss the major sources of threats to industrial organizations and their capabilities
2. We define ICS networks, pinpointing the key components, their weaknesses and their vulnerabilities
3. We present some threat scenarios and example methods that adversaries can use to disrupt or sabotage a victim's industrial process.

The identification and selection of the most prominent threats to an organization is instrumental in determining the most appropriate countermeasure to be employed for mitigation.

Threat Sources

Cyber threats to ICS networks can come from several sources, including hostile governments, terrorist groups, competitors, contractors and disgruntled employees. In addition to malicious actors, organizations must account for the inevitable threat of human error, malfunction and failure of digital assets and networks, which characterize the vast majority of disruptions to industrial processes. These threats and threat actors can be classified in many ways. For simplicity, here we consider the following two categories:

- **External:** Adversaries who are not associated with the organization and are acting from outside the perimeter
- **Insiders:** Adversaries who are already within the target organization's perimeter, as well as any other threat originating from inside the network

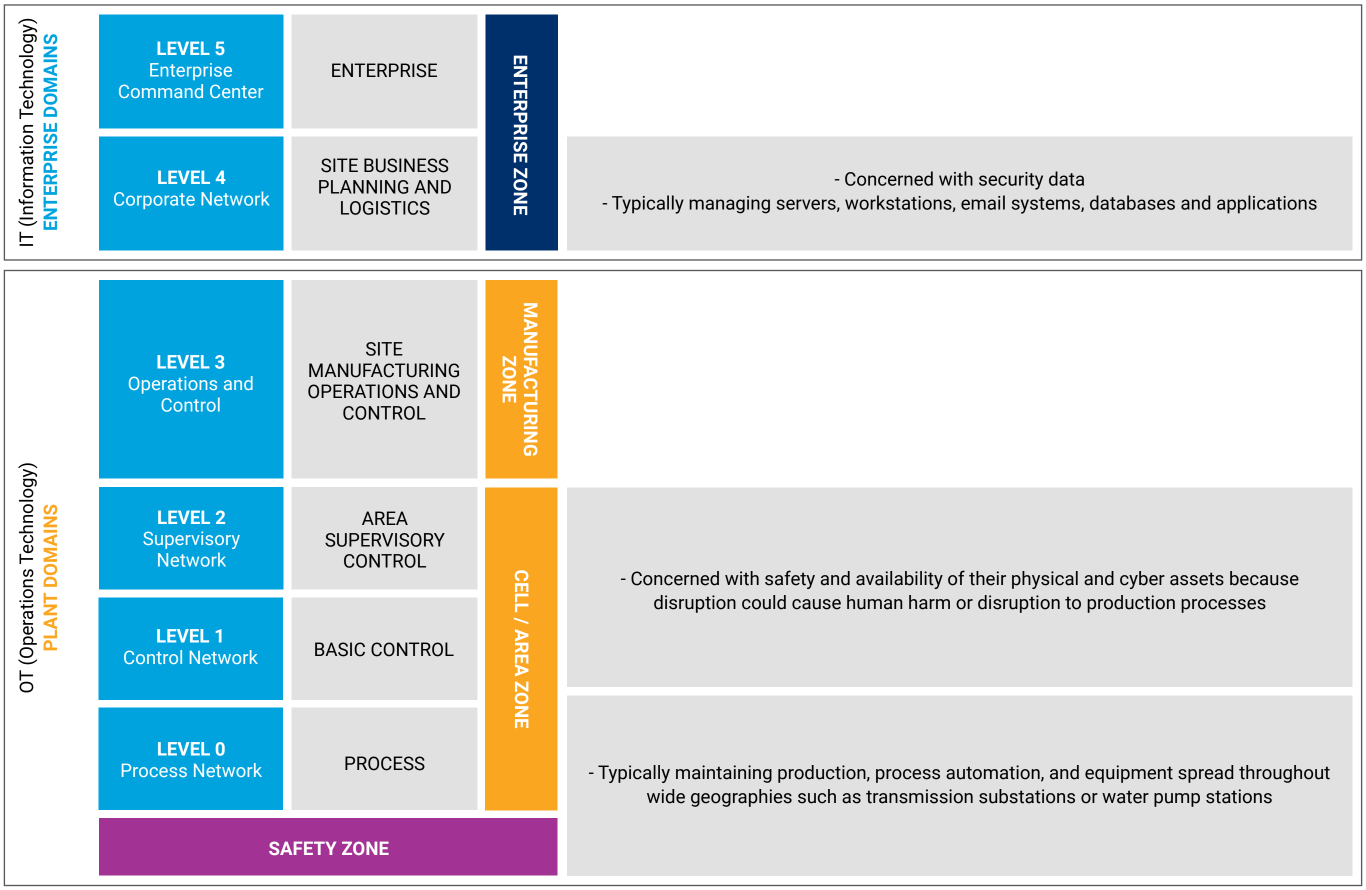
External threat actors include governments and foreign intelligence services, hackers and hacktivists, industrial spies, cyber terrorists and organized crime. These actors have varying degrees of knowledge and motives. They may perform attacks for information gathering, espionage activities or to disrupt or weaken the target's processes. They are usually motivated by political, monetary or reputational reasons.

Insider threats include networking and operational problems, disgruntled employees and careless or poorly trained personnel, contractors and vendors. While external actors may have greater funds and resources, insider threats should not be underestimated by organizations, firstly because some of those threats are beyond an organization's direct control. Network and equipment misconfiguration, malfunction and failure may occur unexpectedly and account for more than 90% of the threats at our global customer base. Secondly, internal actors have very deep knowledge and extensive access to an organization's infrastructure.According to the 2019 SANS State of OT/ICS Cybersecurity Survey, almost 40% of respondents ranked insider threats as one of their top three concerns[4].

The Weak Spots

ICS networks include assets which are directly involved in the control of the production process, as well as assets which provide management or business analytics functionality. Adversaries aiming at disrupting an organization's production process will attempt to access, damage or improperly use its most critical assets by exploiting one of their vulnerabilities.

The Purdue reference model[5] below has five levels and includes specific assets, provides specialized functions and has characteristic response times.



IT (Information Technology)
ENTERPRISE DOMAINS

LEVEL 5 Enterprise Command Center — ENTERPRISE

LEVEL 4 Corporate Network — SITE BUSINESS PLANNING AND LOGISTICS

ENTERPRISE ZONE

- Concerned with security data
- Typically managing servers, workstations, email systems, databases and applications

OT (Operations Technology)
PLANT DOMAINS

LEVEL 3 Operations and Control — SITE MANUFACTURING OPERATIONS AND CONTROL

MANUFACTURING ZONE

LEVEL 2 Supervisory Network — AREA SUPERVISORY CONTROL

LEVEL 1 Control Network — BASIC CONTROL

LEVEL 0 Process Network — PROCESS

CELL / AREA ZONE

SAFETY ZONE

- Concerned with safety and availability of their physical and cyber assets because disruption could cause human harm or disruption to production processes

- Typically maintaining production, process automation, and equipment spread throughout wide geographies such as transmission substations or water pump stations

Industrial networks are typically segmented to reflect this classification. Activities on level 3 and 4 are carried out in “back-office” networks, while activities on level 1 and 2 are carried out in so-called supervisory and process control networks, respectively. A simplified example of an industrial network and its components is shown in Figure 2.1.

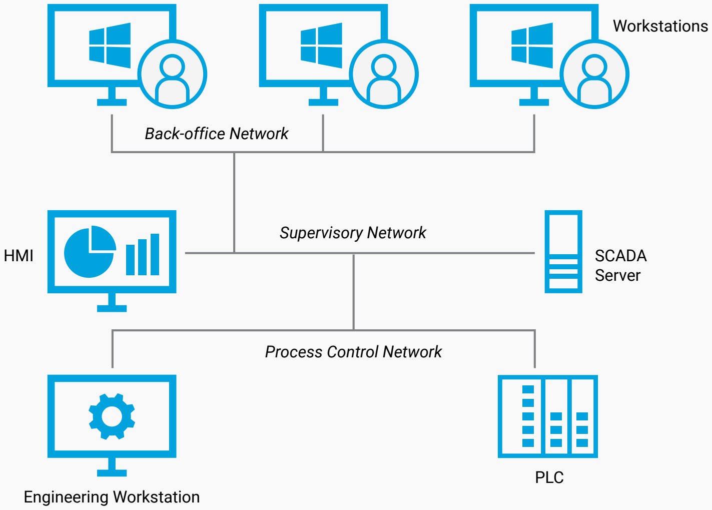


Figure 2.1 - Example of Industrial Network

The most critical assets for an organization operating industrial processes are those located in supervisory and process control networks (level 2 and below), since they provide full control of the organization's production process. Accordingly, organizations should direct most of their efforts towards protecting those networks and assets.

One of the biggest challenges in this respect is that ICS operators currently have little to no visibility into assets and network operations. This limits their ability to assess current vulnerabilities and threat exposure, in addition to existing operational problems and malfunctions, that altogether put the production process at risk. ICS networks have increased in complexity and connectivity, which makes the task of manually keeping an up-to-date network inventory almost impossible. Automated solutions are available to provide the missing visibility and situational awareness to ICS operators. This includes the ability to create an automatic asset and communication inventory, visualize a real-time map of the ICS network and highlight current vulnerabilities and threats (Figure 2.2).

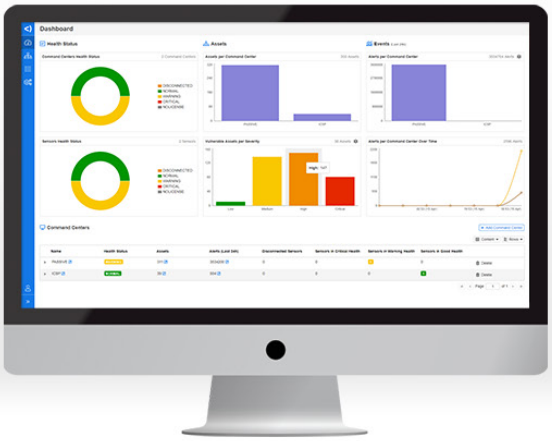


Figure 2.2 - Automated ICS Asset Inventory & Network Map

Example Threats

In this section, we present five example threat scenarios for the threat sources introduced in Section 2.1. In particular, we illustrate the possible effects on industrial networks of:

1. Malicious/careless operators
2. Uncontrolled configuration changes
3. Malfunctioning devices
4. A targeted attack exploiting an unknown vulnerability
5. Spread of malware

Malicious/Careless Operators

ICS operators and engineers have a thorough knowledge of all aspects of an industrial process, and are generally holders of "privileged access" to network resources. In the normal process of their jobs, they may modify a system's regular workflow, and they have access to sensitive information that could be passed on to third parties for any number of reasons. An employee may disrupt the production process by issuing unusual or incorrect commands, or by using parameter values that cause PLCs and other field devices to malfunction or crash. A trustworthy employee may become a threat due to financial gain or dissatisfaction, or simply a mistake. Whatever the motivation, the insider can cause catastrophic damage to an ICS network, as some have in the past.

Uncontrolled Configuration Changes

Threats to ICS networks do not necessarily originate from adversaries, but might arise during the normal course of operations. In fact, network and system configurations tend to change over time due to on site maintenance and hardware/software updates. Any organization dealing with critical processes tests the network and systems' configuration prior to deployment, and often stores a copy (a blueprint) for backup in case of disruption, so that restoring can be as quick as possible. It is fundamental to monitor and validate changes applied to the network to ensure their correct implementation, and to regularly update blueprints to reflect these changes. If, for any reason, blueprints are not kept up-to-date, restore procedures would not be effective and would cause additional delays and prolonged downtime if an incident occurs.

Malfunctioning Devices

Another inherent threat to ICS networks comes from the failure or malfunction of critical devices. Critical devices such as PLCs, RTUs and I/O devices may function incorrectly for several reasons. These include:

1. An erroneous initial configuration from the vendor or system integrator, which may cause the device to not respond to certain requests as expected.
2. A device ending up in an error state due to an observed process parameter like an overflow of the device memory because of high fluctuation in measurements .
3. Devices becoming unreachable due to a network or internal misconfiguration.
4. Devices shutting down because of end of life.

If not detected in time, device malfunctions may lead to prolonged process disruptions and downtime.

A Targeted Attack Exploiting an Unknown Vulnerability

ICS networks are not generally targeted by what has come to be considered mainstream hackers. The ICS attacker is motivated, well-funded and possibly even state-sponsored, as research has shown of the latest successful ICS intrusions. Attacks to ICS are carefully planned and executed, employing specifically developed malware and zero-days, which circumvent standard security solutions by exploiting previously unknown vulnerabilities in target systems. The aim might be to steal financial or exploration data or to disrupt operation of the provided service. These attacks may be part of a larger cyber warfare campaign.

Spread of Malware

One of the main threats to ICS networks is malware that spreads from an IT network into an OT network. The harm resulting from malware infecting back-office networks can be huge, and it could become destructive if the infection manages to reach the supervisory or process control network. Despite strict network segmentation and corporate policies, supervisory and process control networks are rarely truly isolated from the external world. For instance, think about external consultants performing on-site maintenance with their laptops and support personnel with remote access to production systems, thwarting network segmentation and isolation policies. Once malware reaches a network, it can then spread easily, and often unnoticed, into sensitive, critical environments and force long periods of system downtime. An example of this scenario is represented by the ransomware attack that shut down a US natural gas pipeline for two days[6]. The threat actor used a spearphishing link to gain access to the IT network before pivoting into the OT network.

Mitigation Solutions

This section focuses on the various existing technologies that can be used to detect and mitigate ICS network risks and threats such as the ones presented in Section 2.3. There exist heterogeneous and complementary solutions to mitigate threats to ICS networks, each of which have pros and cons, and there is no silver bullet. Depending on the output of the risk assessment, an organization should select the set of solutions that best suits its needs.

Security monitoring solutions are divided into host- (or endpoint) and network-based. Most organizations employ "traditional" endpoint security solutions developed for IT environments, such as antivirus and application whitelisting, to protect their SCADA/DCS servers, HMIs and engineering workstations. These solutions, however, are inadequate when it comes to monitoring PLCs and RTUs, detecting insiders' misbehavior and identifying misconfigurations. Network-based solutions then become the only available choice for protecting some of the most critical assets for an industrial process. In the following paragraphs, we describe the existing network-based technologies, illustrating their advantages and disadvantages.

Signature-Based

Signature-based detection is the most common monitoring and detection method and is typically employed by anti-malware and intrusion prevention systems. The idea behind this approach is simple and straightforward. Knowledgeable people, like security analysts, make a list of known malicious and suspicious network messages and devise signatures to recognize them. Network traffic is then compared in real time against these signatures and, in the case of a successful match, the event is reported to the security operator.

Pros: The approach is simple, widely known and adopted among the IT security community, and very effective against mainstream threats, such as well-known malware and software exploits. Alert messages are clear, as they can leverage previous knowledge to describe the threat and possibly how to mitigate it. Usually, a signature-based solution can be deployed in a matter of hours. Some attention must be paid to the tuning phase, which is required to suppress false warnings that might be triggered by signatures that are too strict or even by the type of network traffic in a certain ICS network. An additional benefit of signature-based solutions is typically the option of turning prevention mode on, effectively blocking known misbehavior.

Cons: This approach can only detect previously known misbehavior. Skilled attackers can easily circumvent detection, even by just morphing known attack payloads. Every time a new misbehavior or attack is discovered, a corresponding signature must be developed and distributed. It can take days before all monitoring systems are updated, especially in industrial environments. In the meantime, attack payloads that have not yet been analyzed and mapped to a signature can hit without notice. Stuxnet leveraged four unknown software vulnerabilities and went undetected for at least a year before being identified. Furthermore, some of the most common signatures developed by the community like YARA rules are designed for host-based detection and are ineffective for network-based analysis. Another limitation of signature-based detection is that non-malicious yet undesired activity, such as the device malfunction and uncontrolled configuration changes scenarios will also go unnoticed.

Rule-Based

Rule- or specification-based monitoring consists of identifying and detailing legitimate network activity using rules and blocking or alerting when non-matching behavior is observed. In other words, it consists of defining and enforcing network whitelists and blacklists.

The effectiveness and usability of rule-based solutions largely depend on how accurate the underlying analysis of ICS network traffic and protocols is. At one extreme, there are solutions with partial analysis capabilities like firewalls, ensuring that network traffic matches legitimate combinations of IP addresses, ports, protocols and possibly commands. At the other extreme, there are deep packet inspection solutions that analyze ICS traffic and protocols in full depth. Solutions featuring full-depth inspection are capable of tracking and monitoring industrial protocol parameters or even the use of field values, where threat indicators often hide.

The configuration of a rule-based solution is typically performed manually and involves expert personnel that are knowledgeable about the underlying processes. This is because rules are tailored to protect a specific environment, rather than a “general” infrastructure like signature-based solutions.

Pros: Rule-based solutions only allow network communications that have been explicitly whitelisted (or not blacklisted). As a result, they offer protection from a wide range of malicious events and behavior, including both known and unknown threats such as malware Command & Control communication and operator mistakes. Furthermore, rule-based solutions can be tailored to the needs of the organization and can be used to enforce company policies in addition to security restrictions.

Cons: This high level of accuracy, and thus effectiveness, comes at a cost. An important drawback of rule-based solutions is their potentially high configuration cost. The more accurate and fine-grained the desired level of analysis, the higher the setup cost. Whitelisting all message types and field values used in a production process is a daunting task that does not fit most budgets or time schedules, especially given the fact that configuration starts from limited knowledge and visibility into current communications. On the other hand, employing a coarse-grained configuration fails to take advantage of the full power of deep protocol inspection, resulting in a marked reduction in threat detection. Additional concerns and costs come from the fact that each time a network or system configuration is changed, the ruleset must likewise be updated.

Anomaly-Based

To enhance signature-based and ruled-based approaches, companies and researchers have developed automated techniques and algorithms to detect misbehavior without requiring previous knowledge of it. These approaches are usually called anomaly-based. Most anomaly-based solutions employ artificial intelligence algorithms, like neural networks, to first learn what the normal, legitimate “states” of an environment are and afterwards raise an alert when they observe anomalous network traffic. These algorithms have been successfully applied to other fields in the past. For instance, closed circuit television (CCTV) systems use artificial intelligence algorithms for recognizing a suspect among groups of people passing through border security.

When applied to network monitoring, anomaly-based solutions come in two inherent flavors, depending on whether they carry out quantitative (flow-based) or qualitative (content-based) analysis.

Quantitative analysis (flow-based): Quantitative solutions build a model of network flows by taking into consideration aggregate characteristics such as number of bytes exchanged between network devices, number of new connections, etc. over a time period. When subsequently observed flows differ from the model, the system raises an alert. The built model is typically automatically adjusted over time to incorporate changes in the network configuration.

Pros: The technology behind quantitative analysis is well established and has been revisited over time to deal with new attacks. Quantitative solutions are usually easy to tune and tweak for enhancing detection accuracy.

Cons: In practice, quantitative solutions can detect only a very small subset of threats, such as misbehavior that generates spikes in data volumes and network communications, denial of service, horizontal and vertical (port) scans and brute-force attacks. This represents a severe limitation, because some of the most common and dangerous threats, like malfunctions and misconfigurations, operational mistakes and advanced cyber attacks, would remain undetected, as they do not generate significant changes in network flows.

Qualitative analysis (content-based): Qualitative analysis of network traffic is based on the assumption that malicious traffic will look different from regular and legitimate traffic. Solutions based on this approach observe network communications and protocol messages for a given amount of time (the learning phase), build network and protocol detection models to describe what is expected to be regular traffic and alert when the subsequently observed traffic is “different” from these models.

Pros: In theory, this approach can detect any threat to the network, including dangerous commands deviating the underlying process by sending offending parameters, to the most harmful and advanced attacks, such as those aimed at executing arbitrary binary code on targeted assets by exploiting unknown software vulnerabilities. Furthermore, anomaly-based solutions adjust to every network without any previous knowledge or configuration required.

Cons: The accuracy and usability of anomaly-based solutions varies a lot depending on the underlying algorithm employed. For instance, solutions based on machine learning are often cumbersome. They require large and comprehensive datasets of “clean” traffic in order to generate a model of “normal” traffic, and this model can be too complex to fine-tune to reflect the desired detection accuracy. In most cases, this results in many false and undesired alerts and a system that requires full reconfiguration every time a change is applied to the network.

Solutions bridging anomaly-based and rule-based detection build more comprehensible models of normal traffic that allow operators to spot and eliminate threats already present in the network and fine-tune the detection model to their needs, and are therefore more usable and beneficial.

Sandboxing

In this analysis, we also include sandbox solutions, although this technology combines host- and network-based analysis techniques. The idea behind sandboxing is to capture “interesting” data from network traffic, such as email attachments, binary files, PDFs and Office documents, and open or execute those files inside a controlled environment (the sandbox). By enforcing checks over sensitive process, data and configuration files like the Windows Registry it is possible to detect when a captured file could harm the targeted assets, for instance by dropping a botnet client.

Pros: Sandbox solutions are very effective when it comes to detecting advanced malware and threats spreading through files, even when exploiting new and unknown software vulnerabilities. They do not require signatures to work, although vendors typically include them to shorten detection time.

Cons: Sandbox analysis is strongly oriented to malware and malicious file detection. Hence, an attack carried out by using protocol commands and aimed at exploiting a vulnerability in a PLC would go unnoticed, and so would an erroneous command issued by an operator, because no malware or malicious file is involved in the process. Because of this, sandbox solutions are suitable for back-office and possibly supervisory networks, but not for process control networks.

Technology Comparison

Table 3.1 summarizes the detection capabilities of the different technologies available by showing which of the threats presented in section 2.3 they would be able to detect.

	Malicious/ careless operators	Uncontrolled configuration changes	Malfunctioning devices	A targeted attack exploiting an unknown vulnerability	Spread of malware
Signature-based	✖	✖	✖	✖	⚠
Rule-based	⚠	⚠	⚠	⚠	⚠
Anomaly-based (flow-based)	✖	✖	⚠	✖	⚠
Anomaly-based (content-based)	✔	✔	⚠	✔	✔
Sandboxing	✖	✖	✖	⚠	⚠

Table 3.1: Detection capabilities of the existing network monitoring technologies

✖ No detection ⚠ Partial detection ✔ Full detection

Within the table, “Partial detection” means that the solution might detect the threat depending on the way it is executed or the way the solution is configured. For example, signature-based solutions would detect malware spread if the malware was exploiting known vulnerabilities or a signature for the malware had already been devised. Similarly, a rule-based solution might detect malicious operator activity if rules to report that activity have been defined or if that activity was not whitelisted.

To combine the advantages and overcome the limitations of individual technologies, ICS network monitoring solution providers often integrate multiple detection methods within the same product or platform. This not only reports known threats in a clear and actionable way, but also identifies unknown threats and anomalies, providing a more comprehensive detection and response capability. When integrating different technologies, solution providers should keep in mind what makes sense for ICS network monitoring and what doesn’t.

In addition to constantly enhanced detection capabilities, ICS network monitoring platforms are constantly developing new features to enhance visibility and situational awareness for ICS operators. This helps organizations to better understand their environment and threat exposure throughout the entire security lifecycle, from design to implementation and daily operation of the network.

Conclusion

ICS networks sit at the core of every industrial process. Recommendations, standards and guidelines increasingly advocate the importance of implementing continuous monitoring of these networks, to protect them from the growing number and range of threats they face.

There are several existing technologies that can be employed to monitor and protect ICS networks. These technologies are complementary, as they are devised to detect different types of threats. Signature-based and sandbox solutions are designed to protect back-office networks and IT systems from known threats and unknown malware, respectively, and to prevent the spread of those threats to other network segments, but leave supervisory and process control networks mostly unprotected and susceptible to all the threats originating within those networks. Rule- and anomaly-based solutions, on the other hand, are the ideal choice to protect supervisory and process control networks, as they provide protection from any activity that is not explicitly denoted as legitimate and authorized.

To achieve the best defense-in-depth, ICS operators should implement a comprehensive monitoring infrastructure, as shown here in Figure 4.1. The infrastructure consists of:

1. A purely signature-based solution to stop known threats and malware originating in the back-office network
2. A sandbox solution to detect unknown malware and prevent it from spreading within the back-office network or to the supervisory and process control network
3. A solution combining ICS-specific signature-, rule- and anomaly-based detection to identify known problems and threats, as well as undesired configuration changes, unusual network activity and advanced cyber threats to ICS devices
4. A SIEM to integrate and correlate the input of all these solutions and provide monitoring personnel with a unified view of the current security status of an organization

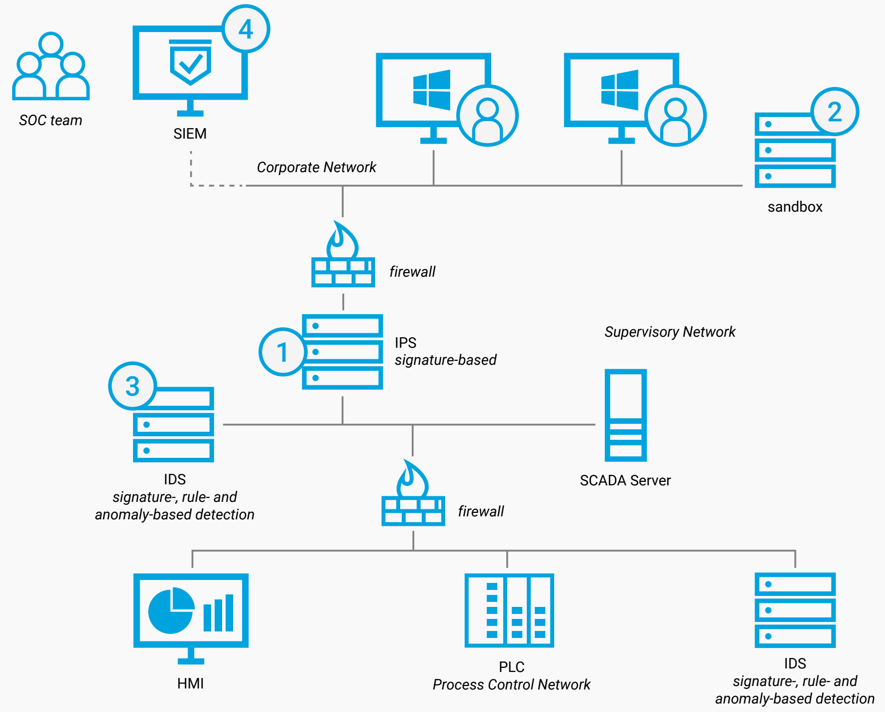


Figure 4.1 - A Comprehensive Industrial Network Monitoring Infrastructure

Acknowledgments

This work has been partially supported by the project “Cyber Security: A Fundamental Basis for Smart Grids” (reference no. TKISG02020). We thank Christina Hoefer and Fred Streefland for their useful insights.

See how our solution detects cyber and operational threats in an ICS network
EXPLORE VIDEO SERIES

Want More Information?

Click here to request a personalized demo.

References

1. https://www.nist.gov/cyberframework
2.https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
3. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
4. America’s Water Infrastructure Act (AWIA) of 2018, https://www.congress.gov/bill/115th-congress/senate-bill/3021/text
5. Theodore J. Williams (1994) “The Purdue enterprise reference architecture.” Computers in industry Vol 24 (2). p. 141-158.
6. https://www.forescout.com/company/blog/how-to-reduce-risk-of-disruptionware-attacks-for-oil-and-gas-producers/

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com