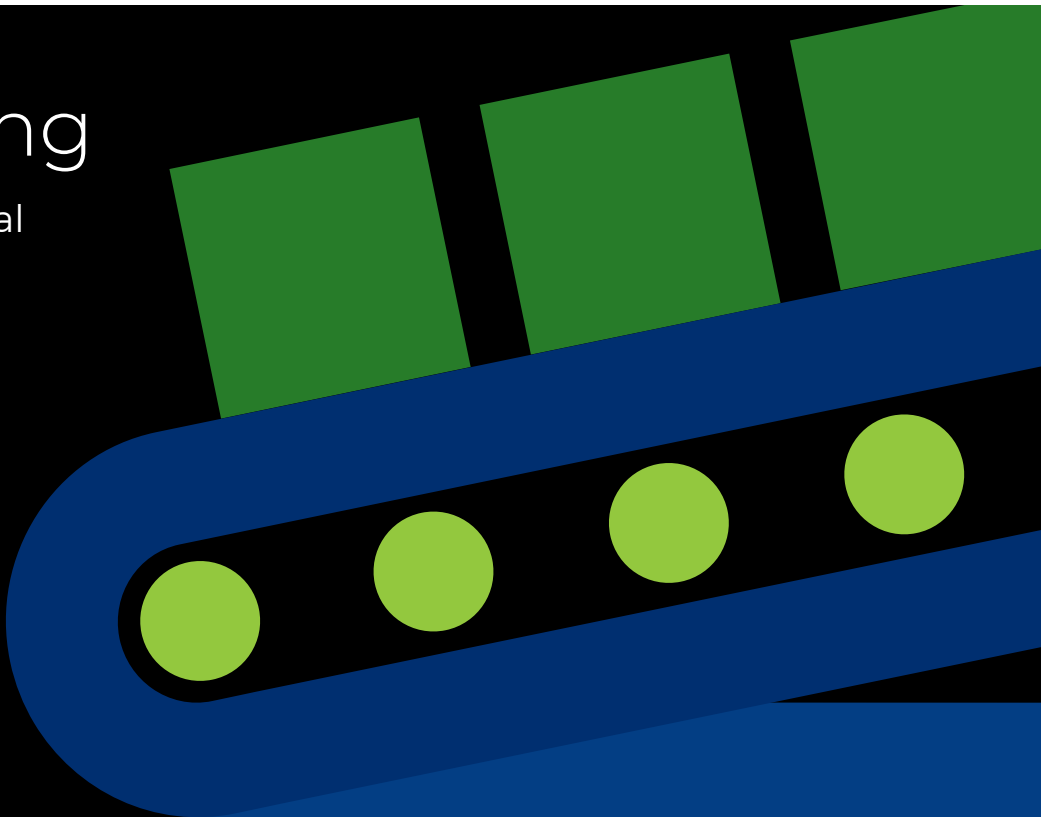
ICS Monitoring

How to improve operational resilience and security



An overview of threats to industrial control systems (ICS) and strategies to mitigate risk

Threats from inside and outside your network can compromise the performance, reliability and profitability of the power stations, water treatment plants and manufacturing facilities upon which communities and corporations depend. The industrial control systems (ICS) running those facilities constantly face risks within plant-level operations technology (OT), as well as enterprise-level information technology (IT) networks. This white paper describes risks, outlines common threat scenarios and provides pros and cons of five different mitigation strategies. Forescout's solution of comprehensive device visibility and automated mitigation across your Enterprise of Things can play a key role in containing those cyber and operational risks.

MONITOR FOR:

- Standards compliance
- Insider risks
- Outside attacks
- Third party threats

CONTENTS

3 The Need for Monitoring

4 Assess the Risk

6 ICS Threat Landscape

6 Threat Sources

7 The Weak Spots

11 Threats

13 Mitigation Solutions

14 Signature-Based Solutions

15 Rule-Based Solutions

16 Anomaly-Based Solutions

17 Sandboxing Solutions

18 Solution Comparison

19 Conclusion

21 Acknowledgments

21 Want More Information?



The Need for Monitoring

Industrial control systems 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 and hospitals, among others. Similarly, a faulty component that regulates the amount of chemical substances in a pharmaceutical production process might lead to entire batches of harmful compounds.

Third-Party and Insider Exposure

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 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 cyberattacks, 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, that could affect or lead to disruption of the production process. All these threats, whether or not of malicious intent, can potentially impact the revenue of an organization and are increasingly drawing attention from the boardroom.

MONITORING IS ESSENTIAL TO COMPLY WITH INDUSTRY STANDARDS

The importance of monitoring ICS networks has been well-documented and is included in several industry recommendations, guidelines and standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework[1] and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP),[2] both in the United States, the NIS Directive from the European Union,[3] and America's Water Infrastructure Act (AWIA).[4] Those standards are aimed at stopping or limiting damage from well-publicized breaches such as Stuxnet, WannaCry, TRITON, NotPetya, LockerGoga and Ryuk.

Mitigate Threats Through Comprehensive Monitoring

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

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. Organizations quite often do not give the necessary due diligence to this phase of the security process that leads to a solution implementation that is not optimized to 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 ICS detection and monitoring solutions.

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

ASSESS 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.

Analyze and Evaluate Before You Mitigate

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 ICS detection and monitoring tool can provide an automatic impact-based risk score of threats based on overall likelihood and impact on the network.

People, Process and Tools

Finally, an organization must decide what course of action to take with the identified risks and threats. For example, determine 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 and corrective, among others. 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 identified threats while maximizing the benefit for the organization.

In the remainder 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 risk from cyber and operational threats.

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

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

ICS THREATS COME FROM TWO SETS OF SOURCES:

External: Adversaries who are not associated with the organization and are acting from outside the perimeter.

Internal: Adversaries who are already within the organization's perimeter, as well as other threats originating from inside the network.

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.

External threat actors include governments and foreign intelligence services, hackers and hacktivists, industrial spies, cyberterrorists 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.

Internal 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 because some of those threats are beyond the organization's direct control. For example, network and equipment misconfiguration, malfunction and failure account for more than 90% of the threats across Forescout's global customer base. From a personnel perspective, internal threat actors, whether or not of malicious intent, often have very deep knowledge and extensive access to an organization's infrastructure.

THE WEAK SPOTS

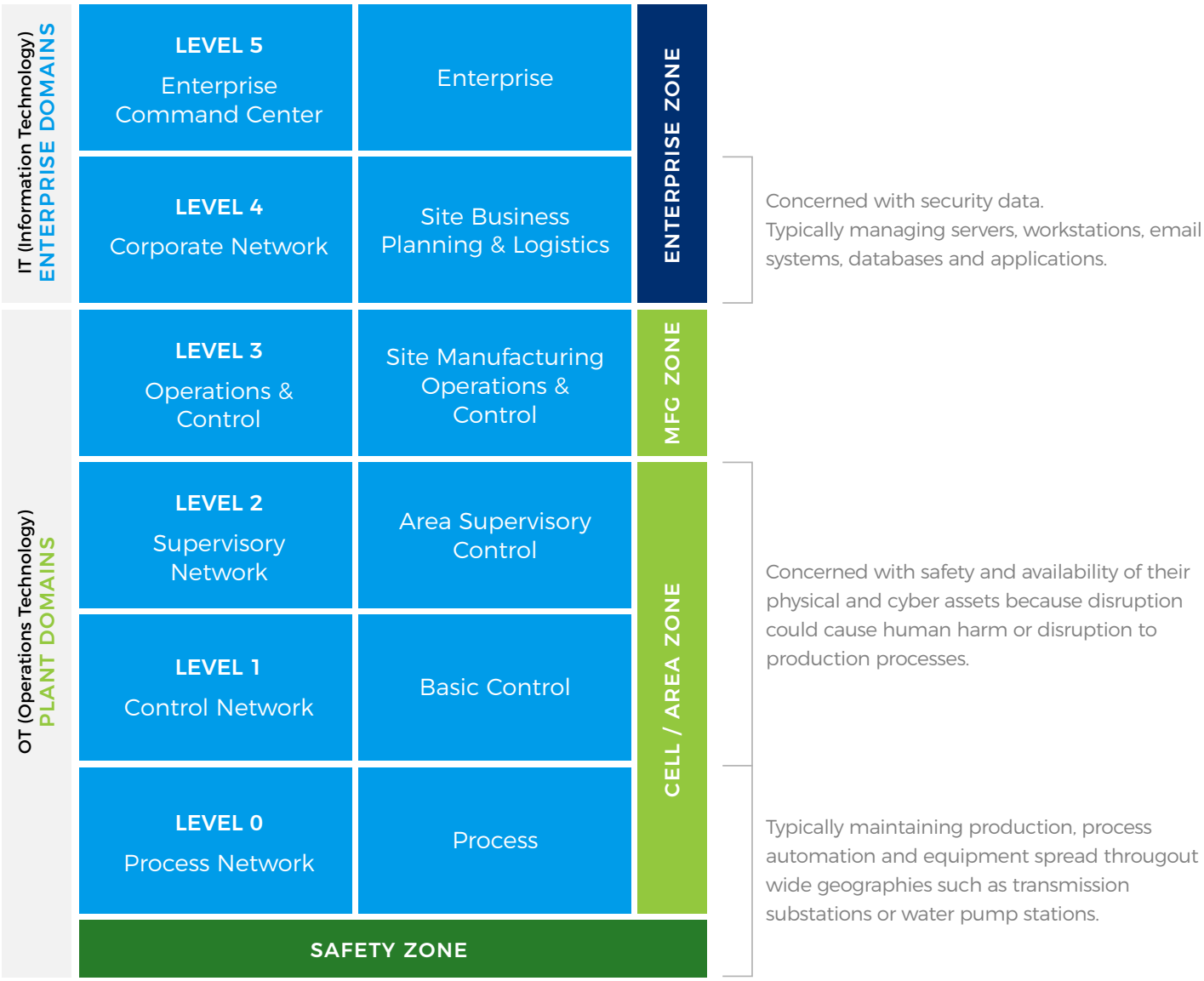
ICS networks include assets that are directly involved in the control of the production process, as well as assets that provide management or business analytics functionality. Adversaries aiming at disrupting an organization's production process will attempt to access, damage or improperly use its most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

Almost
40%
of respondents ranked insider threats as one of their top 3 concerns.[4]

2019 SANS State of OT/ICS Cybersecurity Survey

It can be helpful to take a step back and understand the context of an industrial organization's overall operational technology and information technology network. The often-used Purdue reference model[5] outlined below is comprised of five levels, each of which includes specific assets, provides specialized functions and has characteristic response times.

Purdue Reference Model:



Industrial networks are typically segmented in alignment with these classification. Activities on Levels 3 and 4 are carried out in "back-office" networks, while activities on Levels 1 and 2 are carried out in supervisory and process control networks, respectively. A simplified model of such an industrial network is shown in Figure 2.1.

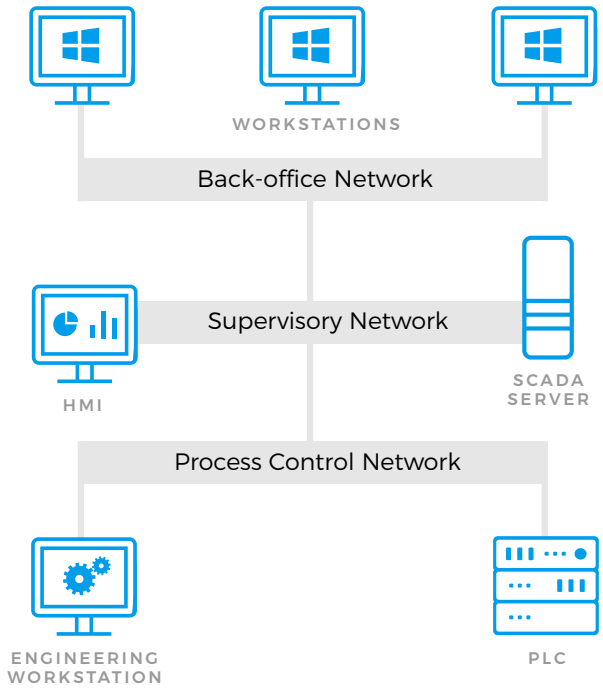


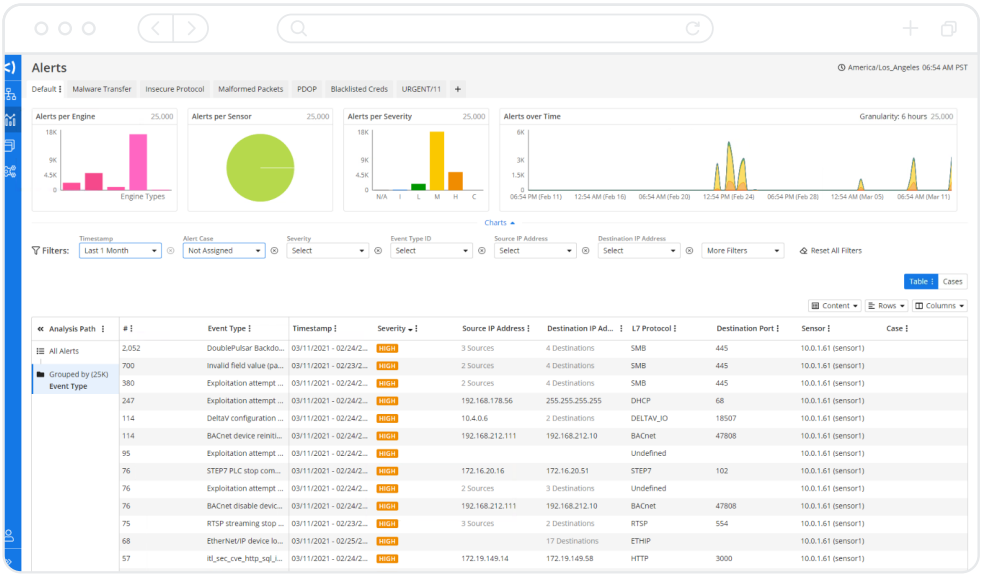
Figure 2.1 — Example of Industrial Network

Automated passive solutions are now available to provide the necessary visibility and situational awareness to ICS operators. This includes the ability to create an automatic asset and communication inventory, see a real-time map of the ICS network and a current list of vulnerabilities and threats based on risk score (Figure 2.2).

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 typically direct most of their efforts toward protecting those networks and assets.

One of the biggest challenges across industrial networks is that operators often have little-to-no visibility into their full device inventory and communication flows between assets. This limits the organization's ability to assess current vulnerabilities and threat exposure, in addition to potential operational problems and malfunctions, that altogether put the production process at risk. As ICS networks have increased in complexity and connectivity, the task of manually keeping an up-to-date network inventory has become almost impossible.

Monitor dashboards to identify and contain threats.



Map all networks in real time.

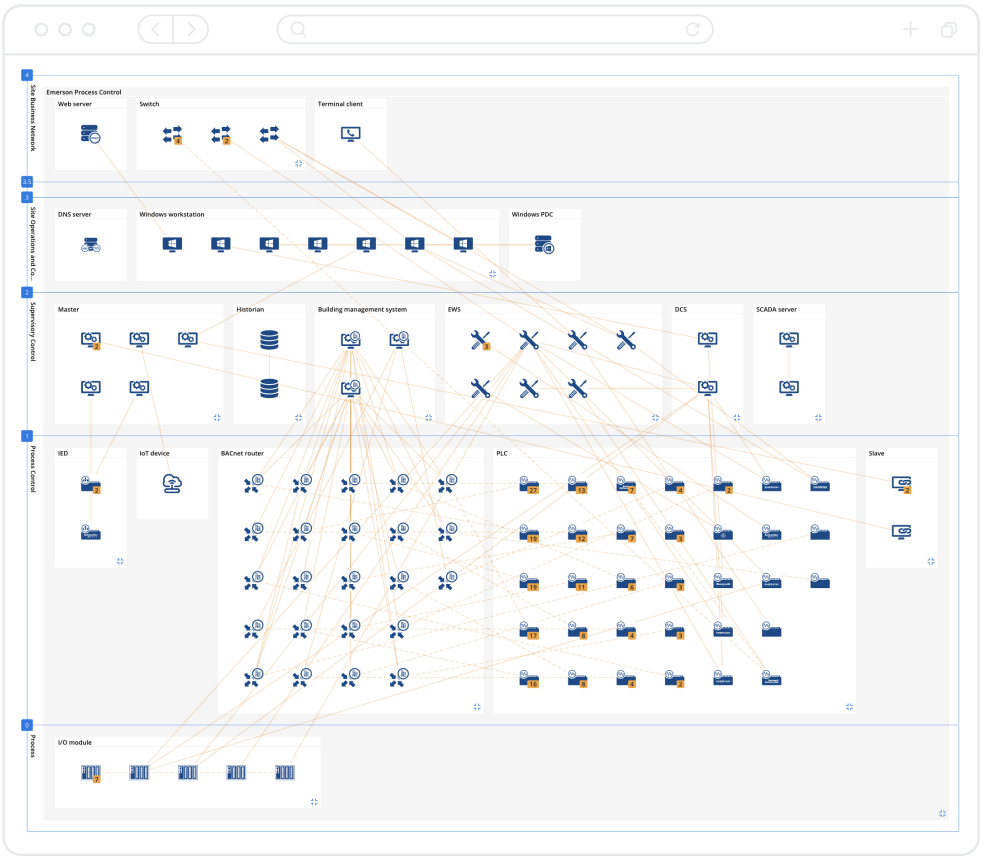


Figure 2.2 - Examples of Automated ICS Alerts and Network Maps

THREATS

In this section, we present five threat scenarios to illustrate the potential impacts on industrial networks from:

1. Careless/malicious operators
2. Uncontrolled configuration changes
3. Malfunctioning devices
4. Targeted attacks exploiting an unknown vulnerability
5. Spread of malware

Careless/Malicious 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 may 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 planned 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.

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.

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 unplanned 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 networks are carefully planned and executed, employing specifically developed malware and zero-day attacks, which circumvent standard security solutions by exploiting previously unknown vulnerabilities in targeted 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 on an entire industrial sector.

The ICS attacker is motivated, well-funded and possibly even state-sponsored, as research has shown of the latest successful ICS intrusions.

Spread of Malware

One of the main threats to ICS networks is malware that spreads from an IT network into an OT/ICS 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 because they are rarely truly isolated (air gapped) from the external world. For instance, consider the common example of 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 U.S. natural gas pipeline for two days[6]. The threat actor used a spear phishing link to gain access to the IT network before pivoting into the OT/ICS 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 because they are rarely truly isolated (air gapped) from the external world.

Mitigation Solutions

This section focuses on the various existing technologies that can be used to detect and mitigate ICS network risks and threats. There are multiple solutions to mitigate threats to ICS networks, each of which has pros and cons, and a defense-in-depth approach is critical as 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 categories. 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 for 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 section, we describe the existing network-based technologies, illustrating their advantages and disadvantages.

SIGNATURE-BASED SOLUTIONS

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.

ADVANTAGES

- A simple, widely known and adopted approach embraced by the IT security community.
- Very effective against mainstream threats, such as well-known malware and software exploits.
- Alert messages are clear, leveraging previous knowledge to describe the threat and how to mitigate it.
- Can typically be deployed in a matter of hours.
- Works well when attention is paid to the tuning phase 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.
- Some offer the option of turning on 'prevention mode' to block known misbehavior.

DISADVANTAGES

- Can only detect previously known misbehavior. Stuxnet, for example, leveraged four unknown software vulnerabilities and went undetected for at least a year before being identified.
- Skilled attackers can circumvent detection by 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, particularly in industrial environments. In the meantime, attack payloads that have not been analyzed and mapped to a signature can penetrate.
- 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.
- Non-malicious yet undesired activity, such as the device malfunction and uncontrolled configuration change scenarios, will go unnoticed.

RULE-BASED SOLUTIONS

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 who are knowledgeable about the underlying processes. This is because rules are tailored to protect a specific environment versus a 'general' infrastructure, like signature-based solutions.

The configuration of a rule-based solution is typically performed manually and involves expert personnel that are knowledgeable about the underlying processes.

ADVANTAGES

- Rule-based solutions only allow network communications that have been explicitly whitelisted (or not blacklisted).
- High levels of accuracy and effectiveness.
- Provide 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.
- Can be tailored to meet organization needs and enforce company policies in addition to enforcing security restrictions.

DISADVANTAGES

- An important drawback is their high configuration cost. The more accurate and fine-grained the desired level of analysis, the higher the setup cost.
- Configuration starts from limited knowledge and visibility into current communications.
- 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.
- 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.
- Each time a network or system configuration is changed, the ruleset must be updated.

ANOMALY-BASED SOLUTIONS

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 afterward raise an alert when they observe anomalous network traffic. These algorithms have been applied successfully 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 the number of bytes exchanged between network devices, the 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.

Quantitative solutions build a model of network flows by taking into consideration aggregate characteristics such as the number of bytes exchanged between network devices, the number of new connections etc., over a time period.

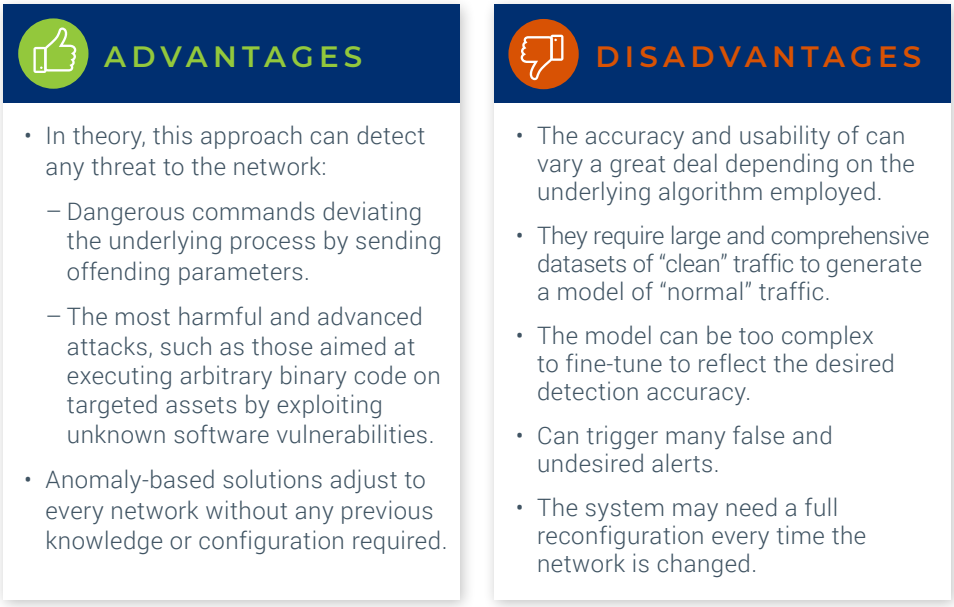
ADVANTAGES

- 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.

DISADVANTAGES

- Only detect a 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.
- Some of the most common and dangerous threats, like malfunctions and misconfigurations, operational mistakes and advanced cyberattacks, 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.



Qualitative analysis solutions observe network communications and protocol messages for a given amount of time, 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.

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, making them more usable and beneficial.

SANDBOXING SOLUTIONS

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.

ADVANTAGES

- Very effective for 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.
- Appropriate for back-office and supervisory networks.

DISADVANTAGES

- Sandbox analysis is strongly oriented to malware and malicious file detection.
- An attack carried out by using protocol commands and aimed at exploiting a vulnerability in a PLC will go unnoticed, as will an erroneous command issued by an operator, because no malware or malicious file is involved in the process.
- Not suitable for process control networks.

SOLUTION COMPARISON

Create a defense-in-depth approach across multiple solutions to mitigate the variety of risks threatening ICS networks.

SOLUTOIN TYPE	THREAT TYPE: Careless/ Malicious Operators	Uncontrolled Configuration Changes	Malfunctioning Devices	Targeted Attacks Exploiting an Unknown Vulnerability	Spread of Malware
Signature-based	✗	✗	✗	✗	⚠
Rule-based	⚠	⚠	⚠	⚠	⚠
Anomaly-based (flow-based)	✗	✗	⚠	✗	⚠
Anomaly-based (content-based)	✓	✓	⚠	✓	✓
Sandboxing	✗	✗	✗	⚠	⚠

✗ NO DETECTION ⚠ PARTIAL DETECTION ✓ FULL DETECTION

Table 3.1: Summary of strengths and weaknesses of detection and network monitoring approaches.

Within the table, “partial detection” means 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, arule-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, it also identifies unknown threats and anomalies, providing a more comprehensive detection and response capability.

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 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 technology-based solutions that can be employed to monitor and protect ICS networks. They 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. However, they leave supervisory and process control networks unprotected and susceptible to 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.

Applying mitigations across all IT and OT network layers:

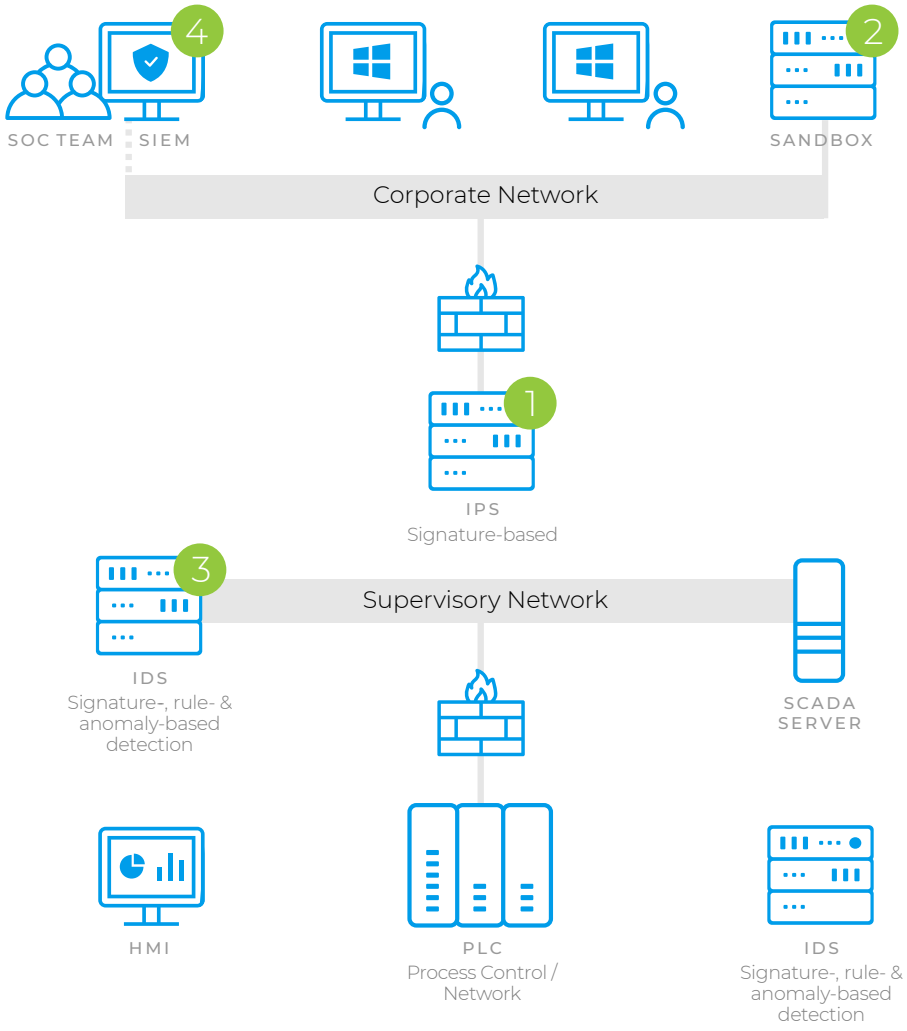


Figure 4.1 – A Comprehensive Industrial Network Monitoring Infrastructure

To achieve the best defense in depth, ICS operators should implement a comprehensive ICS detection and monitoring infrastructure. The infrastructure should consist 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 cyberthreats 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

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

This work has been partially supported by the project "Cyber Security: A Fundamental Basis for Smart Grids" (reference #TKISG02020). We thank Christina Hoefer for her insights.

WHY FORESCOUT?

Only Forescout can provide comprehensive OT/ICS visibility and automated mitigation to contain cyber and operational risks. Forescout is the first company to offer a multifunction IT/OT platform that helps you:

- **Gain complete visibility.** Automatically discover, classify and assess all OT devices and protocols.
- **Enforce compliance to limit blast radius.** Prioritize response to cyber and operational threats for faster and more effective mitigation.
- **Stop threats before incidents occur.** Detect and block risks cataloged in the world's largest library of industrial threats.
- **Ensure Zero Trust across IT and OT.** Apply policy-based segmentation and automated response for consistent access control.

Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

forescout.com/solutions/operational-technology salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

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

© 2021 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 03_21B