SCADAfence

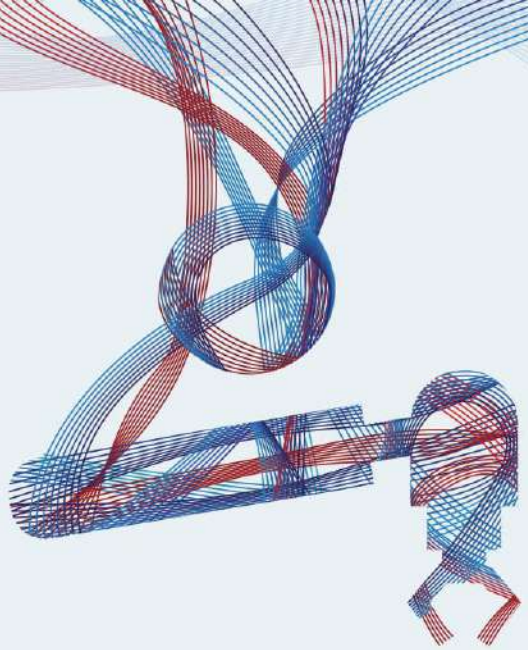
Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

OT & IoT Cybersecurity For The Mining Sector

Securing The Mining Sector With Precision & Fidelity

Table of Contents



The Challenge

In recent years, there has been a growing demand for standards and guidelines to manage the risk exposure of OT infrastructure.

This includes industrial facilities, distribution centers, automated warehouses, building management systems, data center infrastructure, and other similar networks which are now required to comply with standards and frameworks such as IEC-62443, NIST, NERC CIP and others.

IT and OT departments, who typically manage cyber security standard compliance across the organization, are now also required to monitor the compliance of these standards in remote OT locations. These locations are managed by OT organizations who run sensitive, revenue-generating systems, in which downtime translates to immediate financial losses.

Therefore, system availability is a top priority. Furthermore, remote OT operations are typically distributed geographically over many locations in which the OT infrastructure resides, while their cyber security standards are managed centrally by the IT departments.

The SCADAfence Governance Portal

To address the aforementioned needs, the SCADAfence Governance Portal was created. Its main purpose is to provide a governance solution portal that enables the IT and OT departments to centrally define and monitor the organizational adherence to OT-related regulations and to organizational security policies.

The SCADAfence Governance Portal offers the ability to define compliance enforcement policies and continuously monitor compliance enforcement status for various ICS standards, frameworks and regulations. It measures compliance progress made over time across all sites and identifies all of the gaps and bottlenecks.

The SCADAfence Governance Portal is compared with self-reporting and sending auditing teams on-site.

1. **Fully Automated** – Doesn't require any manual labor in reporting.
2. **Accurate** – An automated solution doesn't suffer from human errors and misunderstandings.
3. **Up-To-Date** – The reports are based on real-time information coming from the remote sites. No need to wait for the next quarter or year to get results.

The SCADAfence Governance Portal has built-in, site-specific compliance reports which enable users to generate systematic strategies and improve organizational security at scale.

Features Overview

- Multi-Site regulatory and policy compliance framework.
- Compliance policy manager – define required compliance standard.
- Organizational policies compliance management.
- Compliance dashboards – automatically created, and available at all times for compliance visibility.

Advantages with the SCADAfence Governance Portal

- Increase readiness and compliance for organizational policies and regulations.
- Accurate auditing based on real traffic data.
- Enable end-to-end management of the compliance process across the organization.
- Ready-to-use compliance dashboards and reports for managerial and regulative use.
- Enable a gradual enforcement process - with flexible policy options.

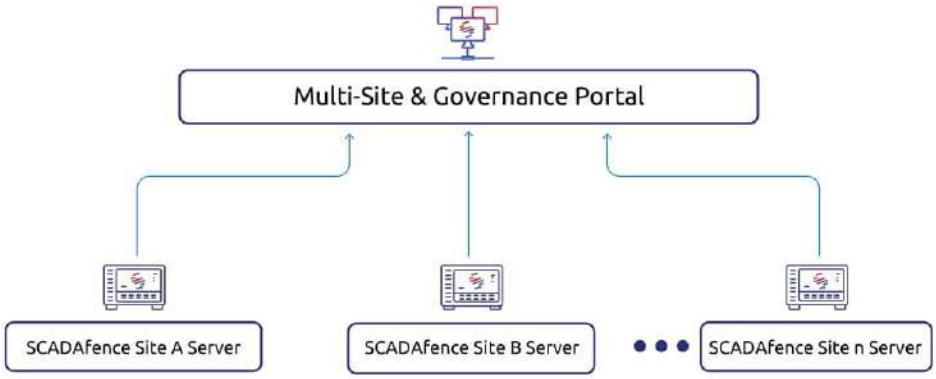
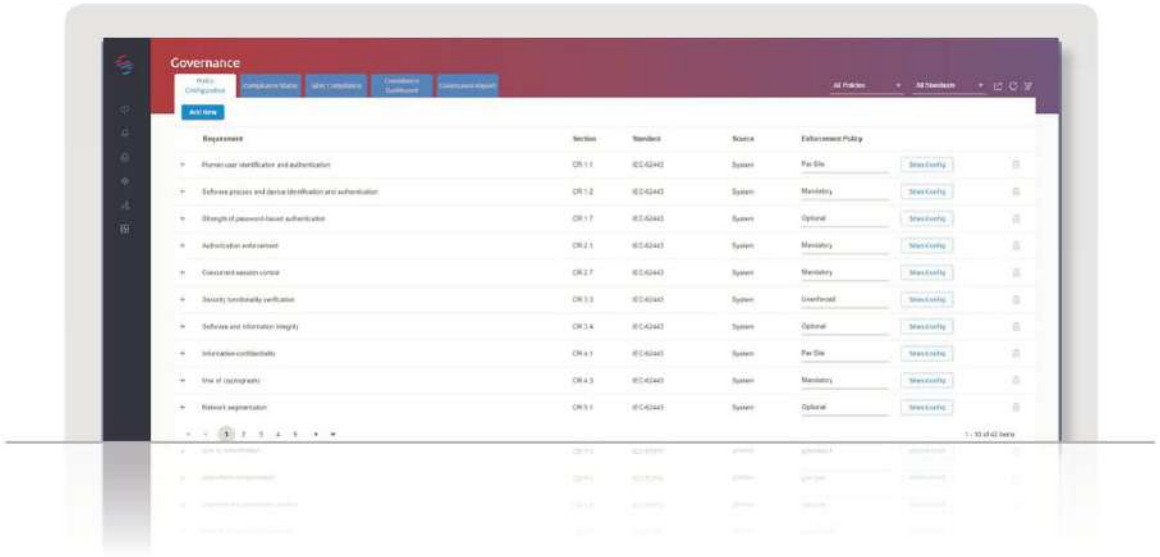
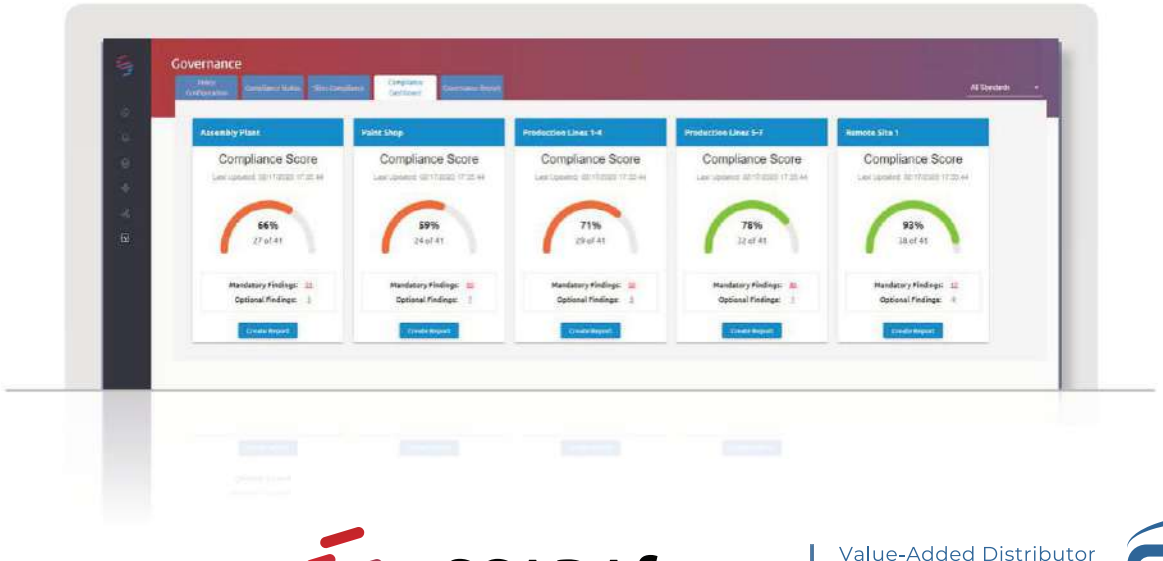


Diagram 1:The SCADAfence Governance Portal

The SCADAfence Governance Portal can be deployed within a few hours per site, it is not intrusive and it does not jeopardize the process availability in any of the OT sites. The solution is configured and managed from a central location, without bothering or burdening the remote OT teams with additional work.





IEC-62443

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).
IEC 62443 provides guidelines for the evaluation of existing and potential vulnerabilities within ICS and aids to reduce the risk of threats and failures within ICS networks. The standard provides recommendations on mitigating actions that needs to be applied for compliance with the standard.
The following pages list some of the significant IEC 62443 requirements and detail how the SCADAfence Governance Portal helps to comply with them.

FR 1 - Identification and Authentication Control

Asset owners will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of IAC protection. The goal of IAC is to protect the control system by verifying the identity of any user requesting access to the control system before activating the communication. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some control system components require strong IAC, such as strong authentication mechanisms, and others do not.

Human User Identification and Authentication

IEC 62443-3-3

SR 1.1 The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

IEC 62443-4-2

CR 1.1 Components shall provide the capability to identify and authenticate all human users according to ISA-62443-3-3 [11] SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.

The SCADAfence Platform

Provides network access and continuous authentication monitoring for both OT & IT protocols such as HTTP, HTTPS, FTP, SFTP, SMB and Telnet. The SCADAfence Platform alerts in real-time on excessive failed login attempts, brute-force attempts and in cases where authentication is performed using insecure protocols, default credentials or weak passwords.

Software Process and Device Identification and Authentication

IEC 62443-3-3

SR 1.2 The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.

IEC 62443-4-2

CR 1.2 Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA-62443-3-3 [11] SR1.2.
If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to ISA-62443-3-3 [11] SR1.1 may be part of the component identification and authentication process towards the other components.

The SCADAfence Platform

Serves as a compensating control and provides real-time alerts concerning the use of insecure methods such as plain-text protocols, default passwords, weak passwords and insecure protocols. This real-time detection helps users to easily address such cases and effectively enforce the identification and authentication requirements.

Strength of Password-Based Authentication

IEC 62443-3-3

SR 1.7 For control systems utilizing password-basedauthentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

IEC 62443-4-2

CR 1.7 For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines

The SCADAfence Platform

Serves as a compensating control and automatically alerts in real-time on the use of weak or default credentials as well as use of insecure protocols that do not enforce encryption.

Unsuccessful Login Attempts

IEC 62443-3-3

SR 1.11 The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.

For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.

IEC 62443-4-2

CR 1.11 When a component provides an authentication capability the component shall provide the capability to:

a) Enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period.

b) Deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.

The SCADAfence Platform

Provides visibility and real-time alerts on failed login attempts.
This functionality helps reduce the risk and make sure that proper policies are configured and enforced throughout the network.
By doing so, the SCADAfence Platform enables threat exposure mitigation and helps ensuring critical assets and services confidentiality.
By integrating the SCADAfence Platform with existing network infrastructure products, the system can provide the capability to deny access to a resource.

FR 2 – Use Control

Once the user is identified and authenticated, the control system has to restrict the allowed actions to the authorized use of the control system. Asset owners and system integrators will have to assign, to each user (human, software process or device), group, role, etc. the privileges defining the authorized use of the IACS. The goal of use control is to protect against unauthorized actions on the control system resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions.

Authorization Enforcement

IEC 62443-3-3

SR 2.1 On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

IEC 62443-4-2

CR 2.1 Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities

The SCADAfence Platform

Monitors and provides alerts on ICS devices for various events such as programming changes, configuration changes, state changes (e.g. start/stop PLC) and allows users to examine such activities. Events can be correlated with source device and source user name, enabling accountability and policy enforcement using integration with network infrastructure products.
Events can be approved or disapproved by an authenticated SCADAfence system user, enabling further accountability.

Concurrent Session Control

IEC 62443-3-3

SR 2.7 The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.

IEC 62443-4-2

CR 2.7 Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

The SCADAfence Platform

Provides real-time alerts on packet floods and DoS attacks.
The SCADAfence Platform's wide integration with 3rd party security applications such as NACs and Firewalls, offer the ability to automatically limit or block network traffic based on those alerts.

Auditable Events

IEC 62443-3-3

SR 2.8 The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

IEC 62443-4-2

CR 2.8 Components shall provide the capability to generate audit records relevant to security for the following categories:

a) Access control
b) Request errors
c) Control system events
d) Backup and restore event
e) Configuration change
f) Audit log events

Individual audit records shall include:

a) Timestamp
b) Source (originating device, software process or human user account)
c) Category
d) Type
e) Event ID
f) Event result

The SCADAfence Platform

Alerts and logs real-time network and security events such as network scanning and reconnaissance activities, login attempts, malfunction indicators from devices & services and ICS device configuration & system changes (e.g. programming and state changes).
The SCADAfence Platform provides detailed information required for event analysis and response, such as timestamps, source and destination information, device details, potential causes, impact and remediation recommendations.

Response to Audit Processing Failures

IEC 62443-3-3

SR 2.10 The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations

IEC 62443-4-2

CR 2.10 Components shall:

a) Provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure

b) Provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

The SCADAfence Platform

Collects and audits network related security events inside the SCADAfence Platform, and serves as a completing control to network and as an ICS device audit trail.
The SCADAfence Platform can be used as an alternate source for an audit trail in cases of processing failures and provides additional network traffic audit capabilities.

Timestamps

IEC 62443-3-3

SR 2.11 The control system shall provide timestamps for use in audit record generation.

IEC 62443-4-2

CR 2.10 Components shall provide the capability to create timestamps (including date and time) for use in audit records.

The SCADAfence Platform

Has completing audit capabilities that include exact and accurate timestamps for all collected network and security events.
In cases where timestamps are not recorded by other components audit trail, users can refer to the SCADAfence Platform for detailed information with exact date and time records.

FR 3 – System Integrity

IACS often go through multiple testing cycles (unit testing, factory acceptance testing (FAT), site acceptance testing (SAT), certification, commissioning, etc.) to establish that the systems will perform as intended before they even begin production. Once operational, asset owners are responsible for maintaining the integrity of the IACS. Using their risk assessment methodology, asset owners may assign different levels of integrity protection to different systems, communication channels and information in their IACS. The integrity of physical assets should be maintained in both operational and non-operational states, such as during production, when in storage or during a maintenance shutdown. The integrity of logical assets should be maintained while in transit and at rest, such as being transmitted over a network or when residing in a data repository.

Security Functionality Verification

IEC 62443-3-3

SR 3.3 The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

IEC 62443-4-2

CR 3.3 Components shall provide the capability to support verification of the intended operation of security functions according to ISA-62443-3-3 [11] SR3.3.

The SCADAfence Platform

Provides a holistic security solution and an accurate up-to-date view of the current security status throughout the network.
The SCADAfence Platform is monitoring communications in and out of band fashion, and cannot be manipulated by attackers in the same way that endpoint security agents can. This creates a verified source of other security functions.
Additionally, the SCADAfence Platform's ability to detect vulnerabilities, malware and exploits in addition to monitoring all the network traffic, helps users ensure that other security controls such as antivirus applications, firewalls and NACs, are configured properly and serve their purpose in securing the estate.

Software and Information Integrity

IEC 62443-3-3

SR 3.4 The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.

IEC 62443-4-2

CR 3.4 Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.

The SCADAfence Platform

Ensures that configurations and programming changes performed on ICS devices are automatically monitored and logged by the SCADAfence Platform, which generates real-time alerts.
The detailed and comprehensive information collected by the SCADAfence Platform offers users the ability to investigate and to easily perform integrity checks on the ICS devices' software.

Input Validation

IEC 62443-3-3

SR 3.5 The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.

IEC 62443-4-2

CR 3.5 Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.

The SCADAfence Platform

Has advanced deep packet inspection (DPI) technology for industrial protocols provides the ability to analyze and validate process control messages.
In cases where verification fails, the SCADAfence Platform will trigger alerts in real-time providing comprehensive details required for analysis and forensics purposes.

Error Handling

IEC 62443-3-3

SR 3.7 The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.

IEC 62443-4-2

CR 3.7 The product supplier and/or system integrator should carefully consider the structure and content of error messages. Error messages generated by the component should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include well-known guidelines such as the OWASP Code Review Guide

The SCADAfence Platform

Provides continuous network monitoring that provides real-time indication of malfunctioning ICS devices and services and configuration and state changes that may result in production down-time. Providing this information in real-time, provides users with the ability to respond to errors immediately and, in many cases, prevent them beforehand.
The SCADAfence Platform also displays errors reported by industrial equipment such as PLCs.

Protection of Audit Information

IEC 62443-3-3

SR 3.9 The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.

IEC 62443-4-2

CR 3.9 Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.

The SCADAfence Platform

Organizes all of the collected information (including logs and packet capture files) and are kept securely on the SCADAfence Platform, which is accessible only by permitted users.
All stored information is "read-only" and cannot be edited nor tampered with.

FR 4 – Data Confidentiality

Some control system-generated information, whether at rest or in transit, is of a confidential or sensitive nature. This implies that some communication channels and data-stores require protection against eavesdropping and unauthorized access.

Information Confidentiality

IEC 62443-3-3

SR 4.1 The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

IEC 62443-4-2

CR 4.1 Components shall:

a) Provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported.

b) Support the protection of the confidentiality of information in transit as defined in ISA-62443-3-3 [11] SR 4.1.

The SCADAfence Platform

Automatically detects the use of insecure protocols and alerts in real-time with detailed information on network conversations which provides users with the ability to mitigate risks.
In addition, the SCADAfence Platform provides alerts on vulnerabilities that pose a threat to sensitive data and enables users to address them in a timely manner.
The SCADAfence Platform detects baseline violations that can indicate an asset being compromised by an attacker and its data at risk

Use of Cryptography

IEC 62443-3-3

SR 4.3 If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.

IEC 62443-4-2

CR 4.3 If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

The SCADAfence Platform

Performs network monitoring and alerts in real time when it detects the use of insecure protocols.

FR 5 – Restricted Data Flow

Using their risk assessment methodology, asset owners need to determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information. Derived prescriptive recommendations and guidelines should include mechanisms that range from disconnecting control system networks from business or public networks to using unidirectional gateways, stateful firewalls and DMZs to manage the flow of information.

Network Segmentation

IEC 62443-3-3

SR 5.1 The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

IEC 62443-4-2

CR 5.1 Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

The SCADAfence Platform

Provides visibility and enforcement capabilities for network segmentation.
The built-in Network map visualizes the entire network flows including all devices.
The Exposure Analyzer provides the ability to define logical groups and segments for specific tracking and monitoring of communication.
The Exposure Analyzer also provides the ability to define rules which alert in real-time on unauthorized communication between segments.
This allows to inspect communication between control segments, the DMZ and external networks, and detect site-to-site and site-to-corporate network connections.
Once an alert is triggered, automatic enforcement actions can take place using integration with 3rd party applications such as Firewalls and NACs to block traffic.
The SCADAfence Platform will alert on any new communication from the control segment to an external network and vice-versa.

FR 6 – Timely Response to Events

Using their risk assessment methodology, asset owners should establish security policies and procedures and proper lines of communication and control needed to respond to security violations. Derived prescriptive recommendations and guidelines should include mechanisms that collect, report, preserve and automatically correlate the forensic evidence to ensure timely corrective action. The use of monitoring tools and techniques should not adversely affect the operational performance of the control system.

Audit Log Accessibility

IEC 62443-3-3

SR 6.1 The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

IEC 62443-4-2

CR 6.1 Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

The SCADAfence Platform

Serves as a completing control and logs significant network events as well as security events. The audit logs are secured within the SCADAfence Platform and can be only accessed by permitted users.
The audit logs are read-only, protected from deletion and cannot be tempered with

Continuous Monitoring

IEC 62443-3-3

SR 6.2 The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

IEC 62443-4-2

CR 6.2 Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

The SCADAfence Platform

Performs continuous network traffic monitoring and provides real-time accurate alerts based on profound domain-expertise and understanding of the ICS field.
The SCADAfence Platform leverages its granular anomaly detection mechanism to identify and alert on exposure to various threats and security risks.
Threats and risks include insecure methods of communication, network scanning attempts, data breaches, malwares & exploits as well as ICS device tampering.
Detected threats result in real-time alerts which are automatically prioritized and categorized to ensure easy and quick response by severity.

FR 7 – Resource Availability

The aim of this series of SRs is to ensure that the control system is resilient against various types of DoS events. This includes the partial or total unavailability of system functionality at various levels. In particular, security incidents in the control system should not affect SIS or other safety-related functions.

Denial of Service Protection

IEC 62443-3-3

SR 7.1 The control system shall provide the capability to operate in a degraded mode during a DoS event.

IEC 62443-4-2

CR 7.1 Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

The SCADAfence Platform

Provides real-time detection of various Denial of Service attacks such as packet flood enabling effective response and mitigation for critical assets.
The SCADAfence Platform's continuous monitoring assists users in identifying an increasing volume of network traffic that may result in a DoS attack and in taking automated prevention measures.

Resource Management

IEC 62443-3-3

SR 7.2 The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

IEC 62443-4-2

CR 7.2 Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

The SCADAfence Platform

Provides alerts on a wide variety of scanning tools used in the network, service latency & disruptions and excessive traffic usage. These can cause resource exhaustion, since automation equipment is normally limited in computing resources.
The real-time detection of such incidents allows users to either manually limit their use or automatically do so by integrating with 3rd party applications.

Least Functionality

IEC 62443-3-3

SR 7.7 The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

IEC 62443-4-2

CR 7.7 Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services

The SCADAfence Platform

Based on its unique anomaly detection baseline, the SCADAfence Platform identifies abnormal network behavior and alerts in real time on such anomalies (e.g. new port usageand feeds them into the SCADAfence Platform.
The SCADAfence Platform also provides industrial commands alerts and ICS configuration alerts that can automatically detect unauthorized & unnecessary actions.
In addition, the SCADAfence Platform displays all open ports for every asset and assists in making sure that no unnecessary ports are open.
The SCADAfence Platform alerts on default DHCP and DNS configurations that are vulnerable to attacks.

Control System Component Inventory

IEC 62443-3-3

SR 7.8 The control system shall provide the capability to report the current list of installed components and their associated properties.

IEC 62443-4-2

CR 7.8 Components shall provide the capability to support a control system component inventory according to ISA-62443-3-3 [11] SR 7.8

The SCADAfence Platform

Automatically discovers and creates an accurate asset list of all ICS devices.
The asset inventory provides an up-to-date inventory of devices such as: engineering workstations, HMIs, PLCs, RTUs and I/Os.
The SCADAfence Platform's advanced technology provides continuous detection of devices and provides detailed and updated information for each device, including firmware & hardware versions, OS, vendor, etc. Users can also manually add important information for easier and more effective management of their asset inventory.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives. SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in manufacturing, building management and critical infrastructure industries to operate securely, reliably and efficiently. To learn more, go to www.scadafence.com

Our offices

Regional: New York, Munich, Tokyo

Contact us: info@scadafence.com
www.scadafence.com

SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011