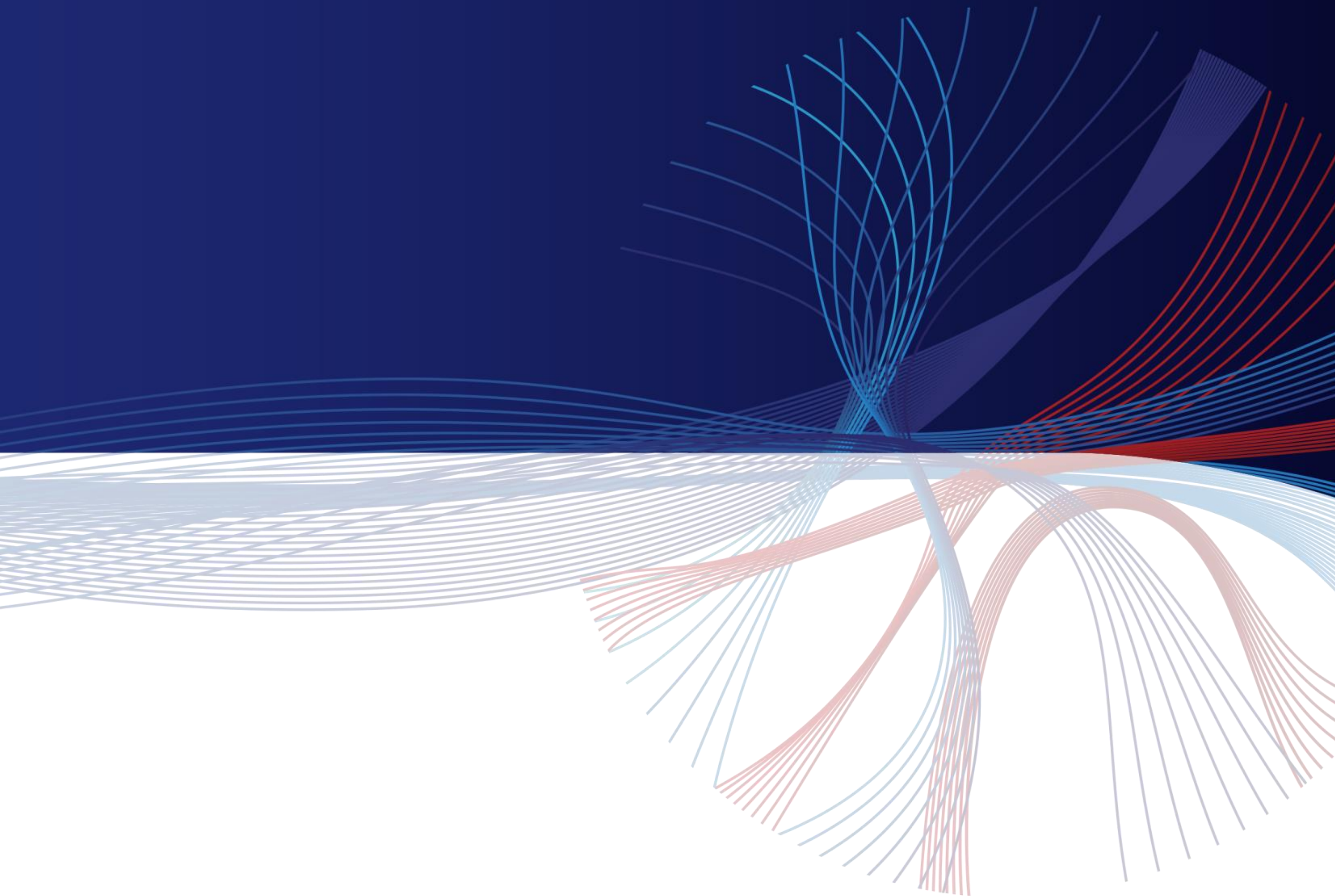
SCADAfence

Solution Brief

SCADAfence IT / OT Governance Portal



March 2020

Challenge

In recent years, there has been a growing demand for standards and guidelines to manage the risk exposure of OT infrastructures. IT and OT departments, who typically manage the cyber security standards across the organization, are now required to monitor the compliance of these standards across the various OT locations, central and remote. This includes industrial plants, distribution centers, automated warehouses, building management systems, datacenter infrastructures, and other critical networks.

On the other hand, the information provided today by the various IT and OT tools are dispersed, and are of a very technical nature. This makes the ability to translate them into risks and to prioritize actionable mitigations, very challenging and time-consuming.

The most common means of compliance tracking today, are manual questionnaires and periodical on-site visits. This results in outdated compliance information, as well as time and resource consuming compliance processes. When compared to the fast pace of advancements in attacker methods and tools, these processes are lacking the required agility to respond, and are inhibiting the effectiveness of countermeasures to the compliance findings.

The Solution

To address the aforementioned needs, SCADAfence provides a governance solution that enables the IT and OT departments to centrally define and monitor the organizational adherence to organizational policies and to OT related regulations. The solution is easily deployed, is not intrusive, and does not jeopardize the process availability in any of the OT sites.

The solution is configured and managed from a central location, and aggregates compliance information from all sites in the organization. It also connects to other security systems, providing a cross-organizational, comprehensive compliance posture.

The SCADAfence Governance Portal measures compliance and monitors the progress made over time across all sites. It identifies all of the gaps and bottlenecks and allows users to generate systematic strategies to improve their organizational security at scale.

ISA NIST NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IEC

Solution Advantages

- Increase readiness and compliance to regulations and organizational policies.
- Accurate auditing based on real traffic data.
- Continuous risk and compliance assessment with dashboards and findings reports available 24/7.
- End-to-end management of the compliance process across the organization.
- Low TCO and significant process savings.

Deployment Architecture

The SCADAfence Governance Portal aggregates information from the organi

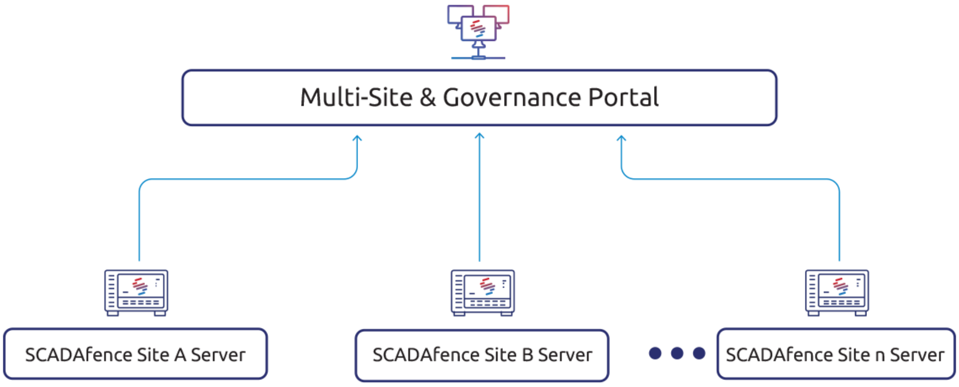


Diagram 1: The SCADAfence Governance Portal Architecture

<u>Deployment phases:</u>

1. Deploy one SCADAfence Platform agent per OT site and configure it to send telemetry to the SCADAfence Governance Portal. The local agent could be software or a small form factor appliance.
2. The central SCADAfence Governance Portal will aggregate the data from all the sites and compile an organizational-wide view of regulatory and policy compliance status. It will recommend best practices, and enable the risk manager to manage the compliance process via the system.
3. Connect any other security systems or other source of information to the portal and feed the portal with relevant information to get one, central compliance dashboard and compliance score.

Compliance Coverage

The SCADAfence Governance Portal manages organizational compliance for both industry standards and for organizational policies. It is customizable and can integrate with 3rd party tools to aggregate additional findings.

Standards Supported:

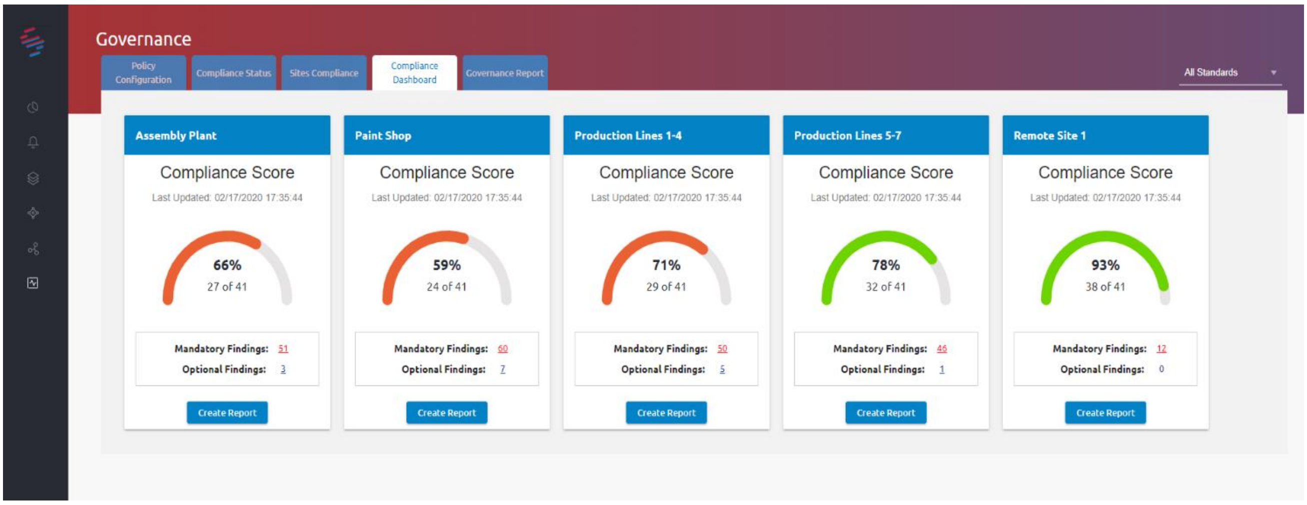
- IEC-62443
- NIST-CSF
- NERC-CIP
- EU NIS Directive
- and others

Organizational Policies:

User-defined policies and best practices

3rd Party Systems:

Firewalls, vulnerability managers, end-point security, and other 3rd party systems



Assembly Plant
Compliance Score
Last Updated: 02/17/2020 17:35:44
66%
27 of 41
Mandatory Findings: 51
Optional Findings: 3

Paint Shop
Compliance Score
Last Updated: 02/17/2020 17:35:44
59%
24 of 41
Mandatory Findings: 60
Optional Findings: 7

Production Lines 1-4
Compliance Score
Last Updated: 02/17/2020 17:35:44
71%
29 of 41
Mandatory Findings: 50
Optional Findings: 5

Production Lines 5-7
Compliance Score
Last Updated: 02/17/2020 17:35:44
78%
32 of 41
Mandatory Findings: 46
Optional Findings: 1

Remote Site 1
Compliance Score
Last Updated: 02/17/2020 17:35:44
93%
38 of 41
Mandatory Findings: 12
Optional Findings: 0

Screenshot 1: Control the Policy and Regulations Compliance Status

Benefits for IT Cyber Security Teams

Organizational Policies Compliance Management

IT cyber security teams can centrally define organizational policies, track network behavior, device behavior, software and network architecture vulnerabilities at the remote site. They can then check the adherence to the defined policies. For example, a policy can be defined regarding external access to the OT production lines. Then the compliance with this policy can be measured centrally across all of the remote sites.

Regulatory Compliance

The SCADAfence Governance Portal automatically correlates network events with industry regulations and provides a centralized report across all of the sites. For example, translating NIST-CSF, NERC-CIP or IEC 62443 requirements into OT network events and then providing compliance reports on related characteristics such as:

1. Network Segmentation and Segregation
2. Password Policy
3. Protocol Security
4. Incident Response
5. Open Vulnerabilities

The assessment is achieved from real traffic analysis, and not based on manual questionnaires, providing a real and accurate view of the security status.

Gradual and Process Oriented

Enterprise-wide compliance tools must maintain flexibility and time-sensitivity. Meaning, it’s not always possible to achieve 100% compliance from day one. Therefore, the solution enables users to define **Mandatory, Optional** and **Unenforced** requirements. As an organization’s cyber security program matures, requirements move from **Unenforced** to **Optional** and then to **Mandatory**.

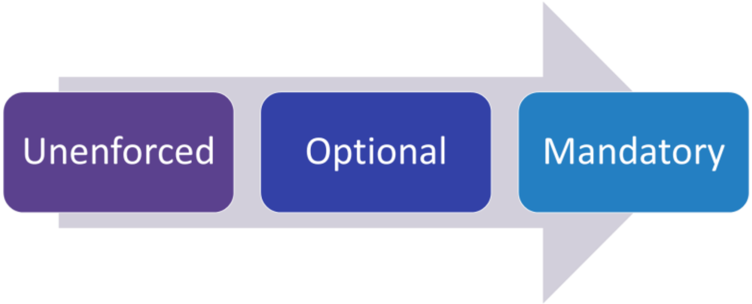


Diagram 2: Organize the compliance in 3 areas: Unenforced, Optional and Mandatory

Central Compliance Score and Compliance Management for Multiple Distributed Sites

The SCADAfence Platform provides a central view of multiple distributed sites. Risk levels are monitored for every site and simple-to-manage reports are generated for each site. Clear remediation guidelines are also presented for each finding. Progress can be tracked and presented over time, in order to track and measure improvements.

The SCADAfence Governance Portal can interface with the organization's existing security systems, mapping host security, or other network security events to regulations or organizational policies. This enables a wider range of coverage requirements and provides a comprehensive view of the security compliance.

Uniformity of Security Standards Across all Organizational Sites

All sites are measured by uniform and advanced metrics, both for industry regulations, best practices and internal policies. This will ensure uniformity in security practicing, while benefiting from best-practices across the various sites.

This has a significant security benefit, as risks from threat proliferation between sites will be greatly reduced.

Benefits for OT Cyber Security Teams

On top of the typical IT areas, the SCADAfence Platform knows how to correlate these requirements into OT specific events and characteristics. For example, it provides insights into industrial protocol usage, such as administrative access into production equipment. The SCADAfence Platform automatically derives the importance of findings according to the OT assets and network characteristics.

Get an Organization-Tailored Risk Assessment Posture at all Times

OT cyber security teams can understand their exposure levels and focus on the correct, most critical issues to address. This achieves an improved and optimized security level for their OT networks. The assessment is achieved from real traffic analysis, and not based on manual questionnaires, providing a real and accurate view of the security status.

Peace of Mind Regarding Regulatory Compliance

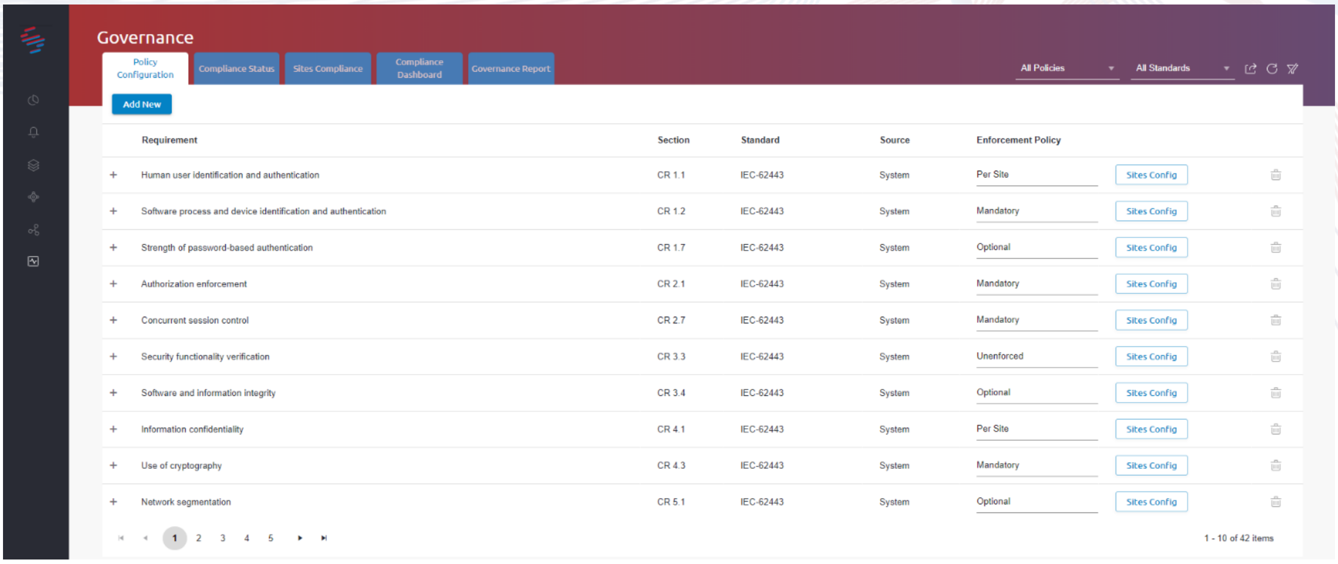
OT cybersecurity teams can measure their OT infrastructure's compliance with regulations, cyber security standards, and internal organizational policies.

Benefit from Knowledge and Best Practices from Other Organizational Units

As the system is deployed across various sites, each industrial plant can benefit from the others' experience. As mentioned, this also has significant security benefits, as risks from threat proliferation between sites is greatly reduced.

Increase Awareness and Cooperation on Security Topics

The cyclic process of tracking regulatory and policy compliance increases employee awareness and increases cooperation with other sites and headquarters. This has significant value in raising security levels and in quickly dealing with incidents if they occur.



	Requirement	Section	Standard	Source	Enforcement Policy	
+	Human user identification and authentication	CR 1.1	IEC-62443	System	Per Site	Sites Config
+	Software process and device identification and authentication	CR 1.2	IEC-62443	System	Mandatory	Sites Config
+	Strength of password-based authentication	CR 1.7	IEC-62443	System	Optional	Sites Config
+	Authorization enforcement	CR 2.1	IEC-62443	System	Mandatory	Sites Config
+	Concurrent session control	CR 2.7	IEC-62443	System	Mandatory	Sites Config
+	Security functionality verification	CR 3.3	IEC-62443	System	Unenforced	Sites Config
+	Software and information integrity	CR 3.4	IEC-62443	System	Optional	Sites Config
+	Information confidentiality	CR 4.1	IEC-62443	System	Per Site	Sites Config
+	Use of cryptography	CR 4.3	IEC-62443	System	Mandatory	Sites Config
+	Network segmentation	CR 5.1	IEC-62443	System	Optional	Sites Config

Screenshot 2: Set the Requirements for Every Site, with a Pre-Defined Knowledgebase

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
Headquarters: Tel Aviv
Regional: New York, Munich, Tokyo

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

SCADAfence