The SCADAfence Governance Portal
NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

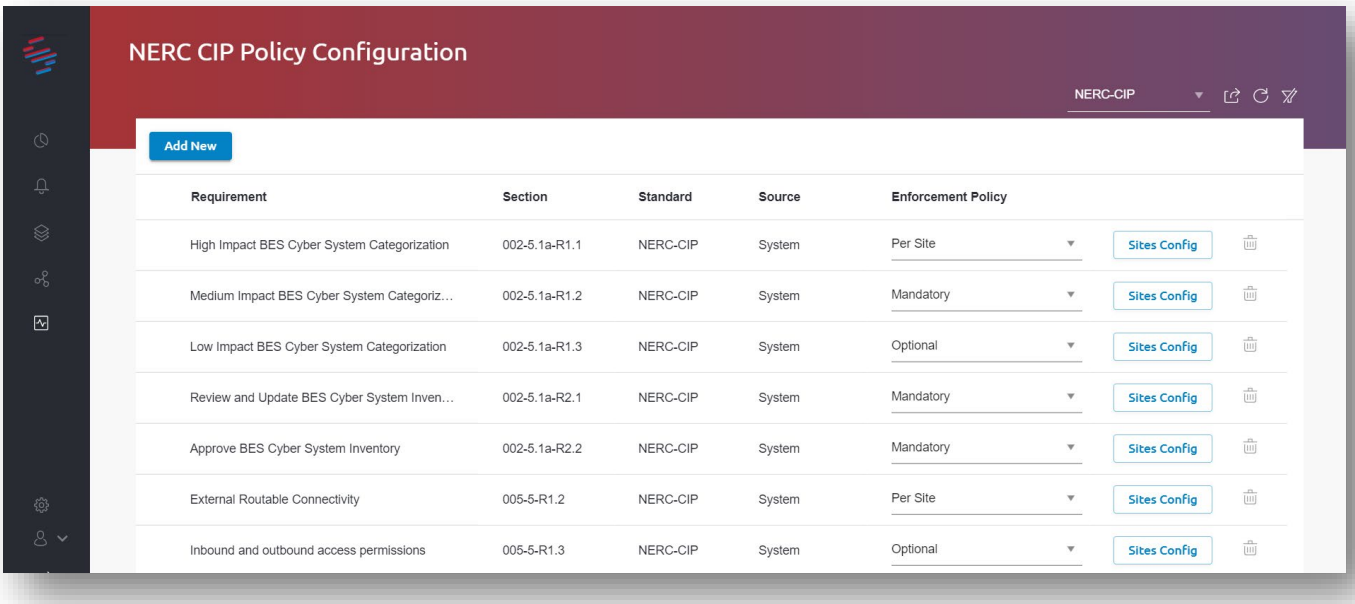
SCADAfence NERC CIP Compliance

The SCADAfence Platform for OT cybersecurity, combined with the SCADAfence Governance Portal, helps utility companies ensure that their Bulk Electric System (BES) is secure and reliable according to the North American Electric Reliability Corporation critical infrastructure protection (NERC CIP) standards.

The SCADAfence Governance Portal includes a built-in NERC CIP module which provides cross-organizational tracking and measurement of NERC CIP adherence.

The SCADAfence Governance Portal provides:

- Fully automated compliance dashboards and detailed compliance reports.
- Compliance status trends and comparisons over time.
- Accurate and up-to-date compliance status based on real network traffic data analytics.
- Tracking and measurement of regulations and organizational best practices which are solely based on questionnaires & documentation by using the Manual Questionnaire feature.



Our offices
Headquarters: Tel-Aviv
Regional: New York, Munich, Tokyo
www.scadafence.com

SCADAfence

The SCADAfence Governance Portal
NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

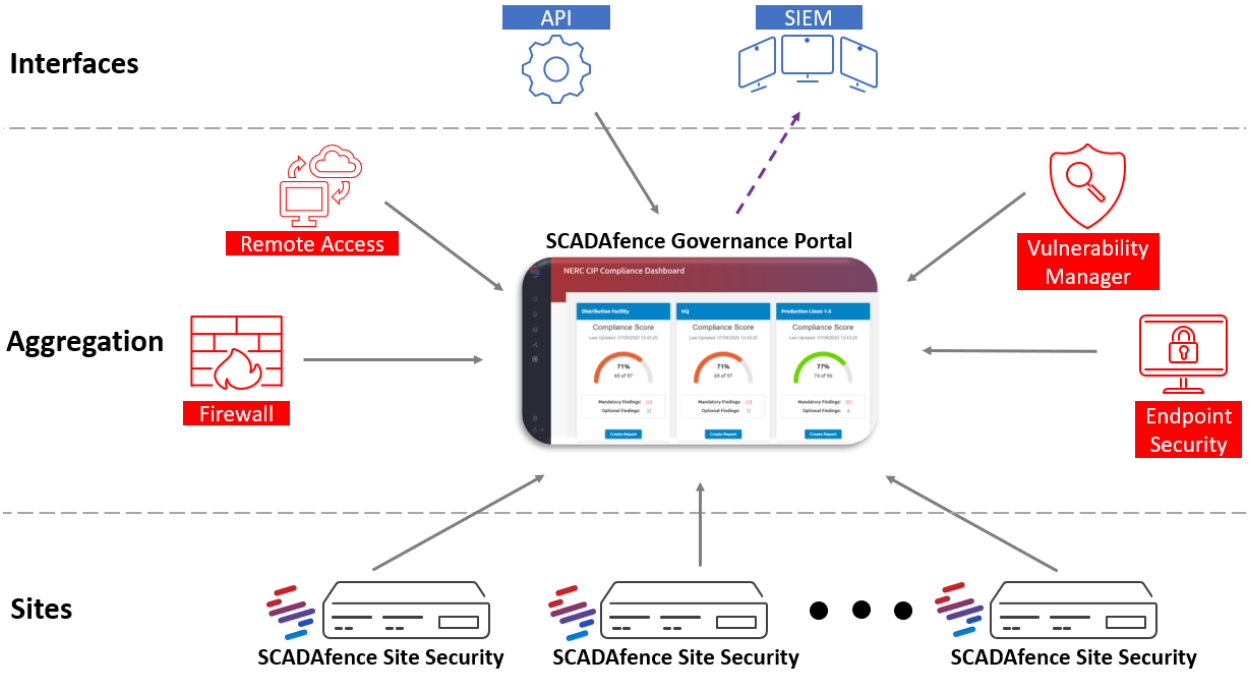
Organizational-Wide Compliance Management

The SCADAfence Governance Portal allows easy and simple integration with 3rd party security and orchestration controls (Firewalls, Endpoint Security, ticketing systems, etc.).

This provides the following advantages:

- **Maximum Coverage** – Addressing all types of regulatory and compliance requirements.
- **Single Pane of Glass** - Monitor compliance from a central system.

The generic integration mechanism opens the SCADAfence Governance Portal to any external source for enhanced compliance coverage and measurement based on accurate external inputs.



Our offices
Headquarters: Tel-Aviv
Regional: New York, Munich, Tokyo
www.scadafence.com

SCADAfence

The SCADAfence Governance Portal
NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

How SCADAfence Supports NERC CIP Requirements

NERC CIP-002:

BES CYBER SYSTEM IDENTIFICATION & CATEGORIZATION

The SCADAfence Platform:

- Automatically identifies all ICS devices in the network and creates a detailed asset inventory.
- Accurately categorizes assets by different attributes such as: device type, vendor, OS, etc.
- Defines and categorizes assets' criticality as low, medium or high impact BES cyber systems.
- Displays assets in various network maps that automatically shows all connections between assets.
- Automatically identifies and categories assets by subnets.
- Identifies and alerts on inventory changes.

NERC CIP-003:

SECURITY MANAGEMENT CONTROLS

The SCADAfence Platform & Governance Portal:

- Includes an exclusive Governance Portal which:
  - Offers built-in tracking & measurement of industry security standards and regulations.
  - Enables definition of organizational security controls that can be associated to real time security & operational alerts.
  - Delivers a significant advantage for security control implementation in critical dynamic OT networks challenges by automating the process and basing it on real network data.
- Provides the ability to set ownership on BES cyber systems as well as on related security alerts to establish accountability and responsibility as part of the protection process.
- Offers a comprehensive incident handling workflow for security personnel which corresponds with common security policies and processes.
- Integrates with existing organizational security controls via multiple interfaces.

The SCADAfence Governance Portal
NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

NERC CIP-004: TRAINING AND PERSONNEL SECURITY	**The SCADAfence Platform & Governance Portal:** - Increases security awareness by identifying vulnerabilities and exposures. - Helps improve training processes by providing remediation recommendations to detected incidents. - Tracks security awareness progress over time within the SCADAfence Governance Portal. - Automatically correlates known CVEs to assets in order to increase organizational security awareness.

NERC CIP-005: ELECTRONIC SECURITY PERIMETER	**The SCADAfence Platform:** - Provides a unique remote OT security module that correlates external connections with internal activities and assists in making sure only approved protocols and applications are used for remote access. - Enables users to create firewall like user-defined rules that alert in real-time when assets connect outside of the ESP (Electronic Security Perimeter). - Ensures that the network and the perimeter security controls are configured properly by alerting in real-time on unauthorized access. - Alerts automatically when outbound connections are initiated.

Our offices
Headquarters: Tel-Aviv
Regional: New York, Munich, Tokyo
www.scadafence.com

SCADAfence

The SCADAfence Governance Portal
NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

NERC CIP-006:

PHYSICAL SECURITY OF BES CYBER SYSTEMS

The SCADAfence Platform:

- Detects and alerts in real-time on ICS device state changes that come from physical access.
- Detects and alerts in real-time alerts on malwares and exploits originated in physical access to BES cyber systems.

NERC CIP-007:

SECURITY SYSTEMS MANAGEMENT

The SCADAfence Platform:

- Utilizes different threat detection engines to protect the OT network.
- Generates real-time alerts such as:
    - Detection of malwares and exploits.
    - Suspicious ICS commands.
    - Operational ICS commands (such as Stop PLC).
    - Reconnaissance attacks.
- Includes a built-in precise CVE management module which automatically identifies vulnerable assets and allows quick and efficient mitigation.
- Integrates with existing security controls and allows proactive mitigation measurements such as blocking traffic of infected or compromised assets.

Our offices
Headquarters: Tel-Aviv
Regional: New York, Munich, Tokyo
www.scadafence.com

SCADAfence

The SCADAfence Governance Portal

NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

NERC CIP-008:

INCIDENT REPORTING AND RESPONSE PLANNING

The SCADAfence Platform:

- Prioritizes and categorizes alerts for easy response planning based on severity and urgency.
- Helps in creating response plans by providing detailed explanations and remediation recommendations for each security incident.
- Supports collaboration with other security controls via various interfaces to enable centralized incident response.
- Provides forensics data for each alert including PCAP recording, traffic records and user activity log map.

NERC CIP-009:

RECOVERY PLANS FOR BES CYBER SYSTEMS

The SCADAfence Platform:

- Provides detailed audit-trail for all operations within the OT network, including:
  - Configuration changes.
  - Programming changes.
  - State change operations.
- Aids in planning recovery plans based on its built-in audit trail capabilities and offers reference to previous states in cases of actual recovery operations.
- Proactively collaborates with common ticketing and orchestration applications that manage recovery processes.

Our offices
Headquarters: Tel-Aviv
Regional: New York, Munich, Tokyo
www.scadafence.com

SCADAfence

The SCADAfence Governance Portal

NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

NERC CIP-010:

CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS

The SCADAfence Platform:

- Provides best-in-class detection of configuration changes and change management operations, such as firmware updates or programming changes.
- Includes a built-in Threat Assessment module that enables users to conduct prioritization of assets and exposures as part of the risk-based remediation approach

NERC CIP-011:

INFORMATION PROTECTION

The SCADAfence Platform:

- Protects the OT network by monitoring 100% of network traffic which enables the system to detect cybersecurity threats that can be missed in case of traffic filtering or sampling is used in isolation.
- Alerts in real-time on abnormal behavior that might indicate malicious activities and sensitive information extraction, by both malicious and careless insiders.

NERC CIP-014:

Physical Security

The SCADAfence Platform:

- Identifies missing ICS devices which are critical to transmission stations and substations' normal operation.
- Detects damaged and inoperable assets in real-time by alerting on service or device malfunction.
- Allows users to analyze device variable values that can indicate if a device is physically attacked.

Our offices
Headquarters: Tel-Aviv
Regional: New York, Munich, Tokyo
www.scadafence.com

SCADAfence

The SCADAfence Governance Portal

NERC CIP Cyber Security Framework Compliance

Technical Whitepaper

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner “Cool Vendor” in 2020, 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 critical infrastructure, manufacturing, and building management 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
www.scadafence.com

SCADAfence