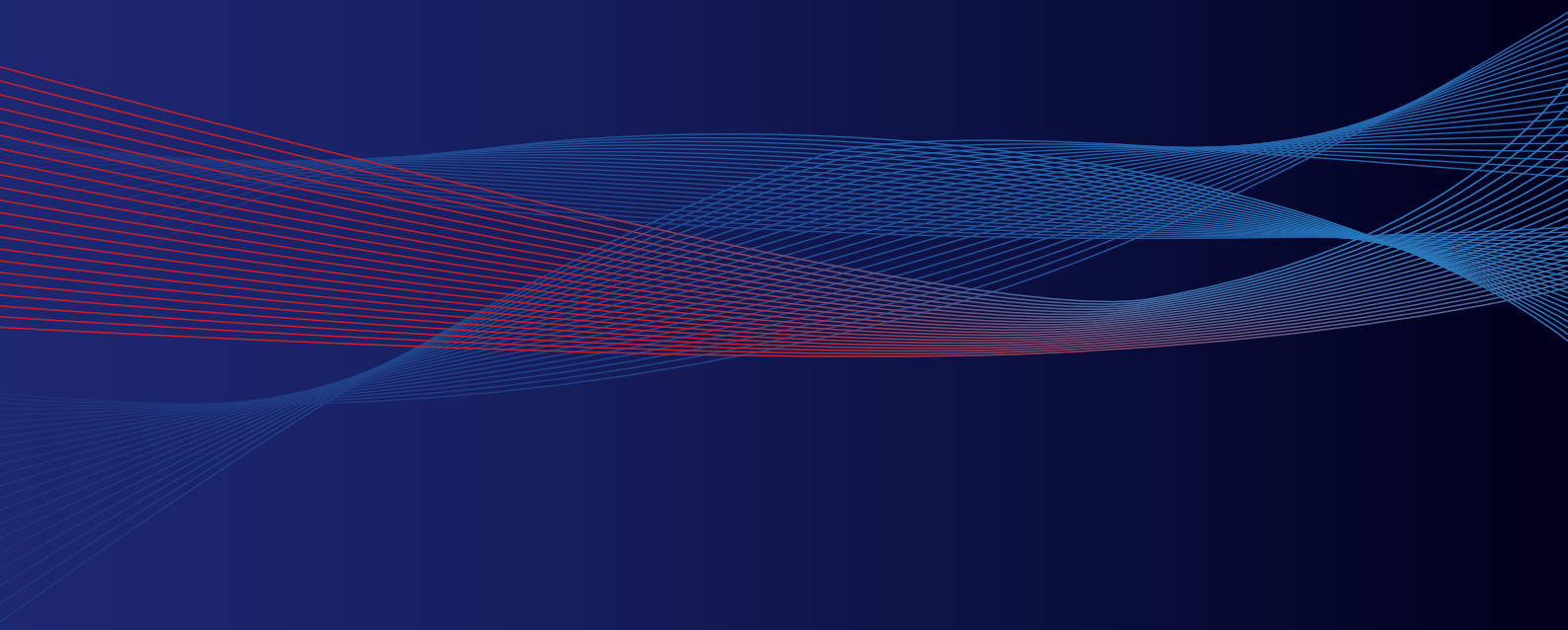
SCADAfence

The SCADAfence Governance Portal

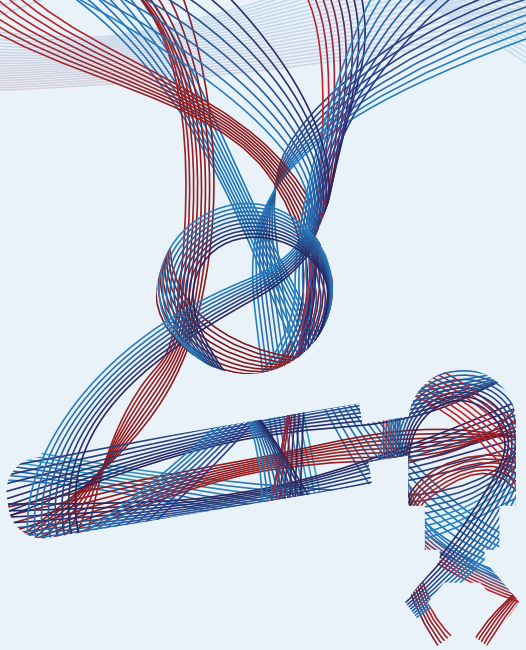
NIST Cyber Security Framework Compliance



March 2020

Technical White Paper

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, SCADAfence provides a governance portal that empowers 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. In comparison with those methods, the SCADAfence Governance Portal provides the following benefits:

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.
- Detailed reports – to drill down in each site and each improvement opportunity.

The SCADAfence Governance Portal Advantages

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

SCADAfence

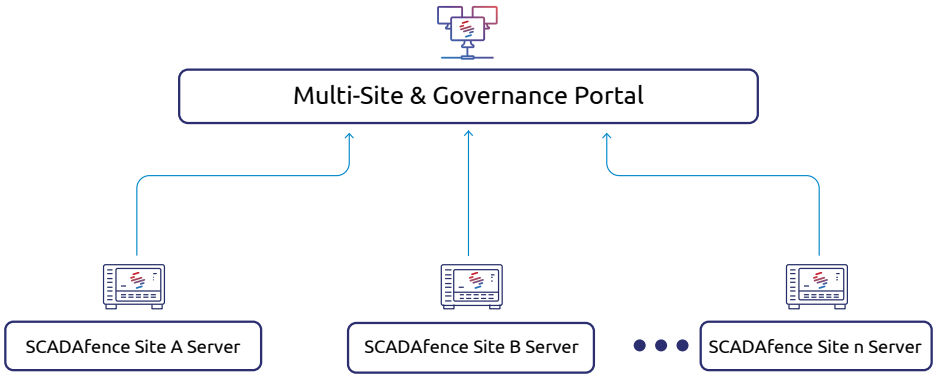
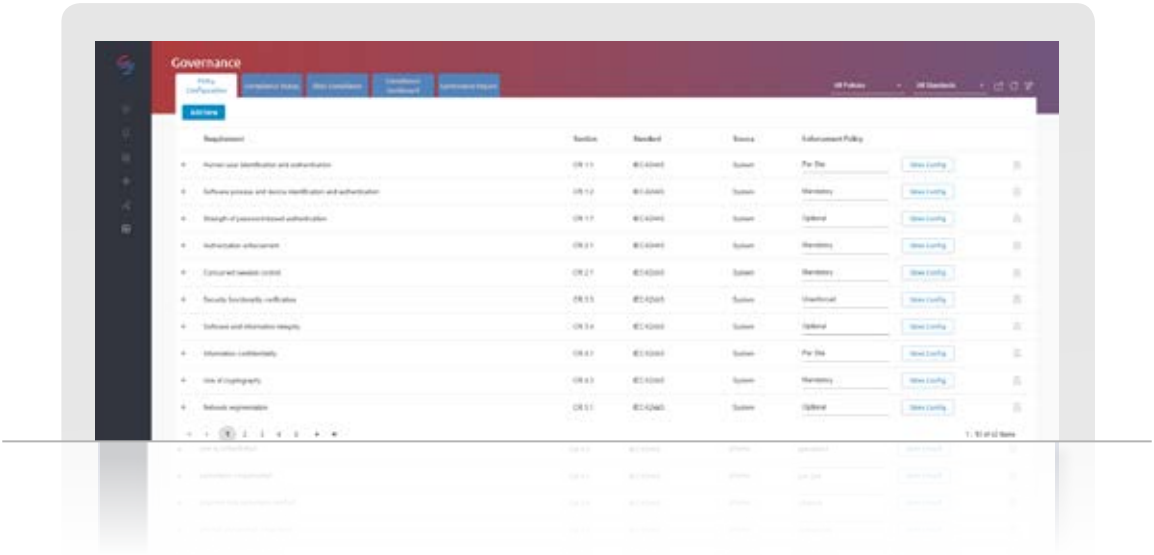
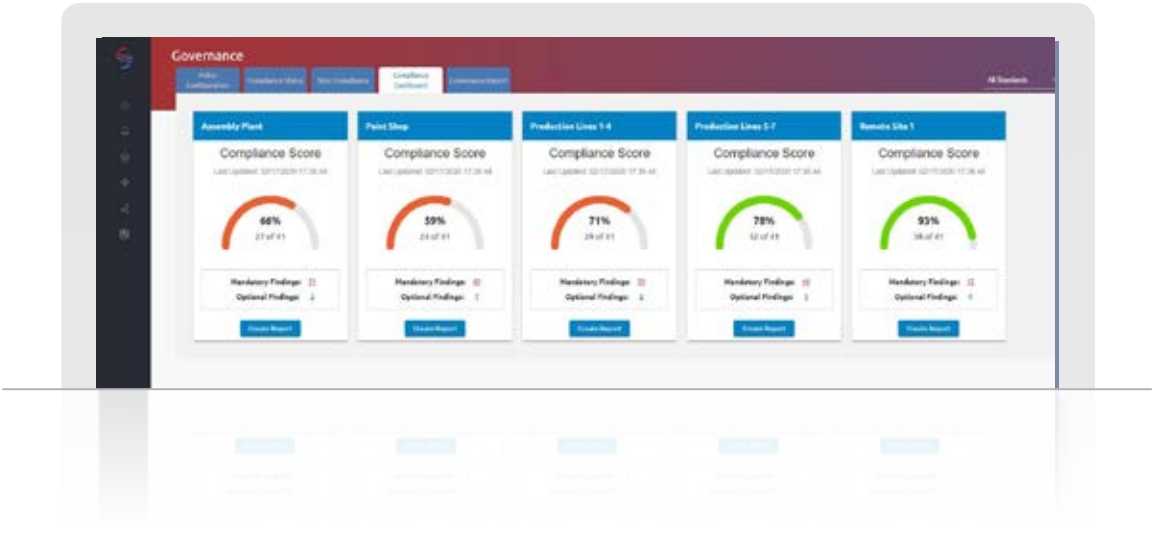


Diagram 1: The SCADAfence Governance Portal

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 SCADAfence Governance Portal is configured and managed from a central location, without bothering or burdening the remote OT teams with additional work.

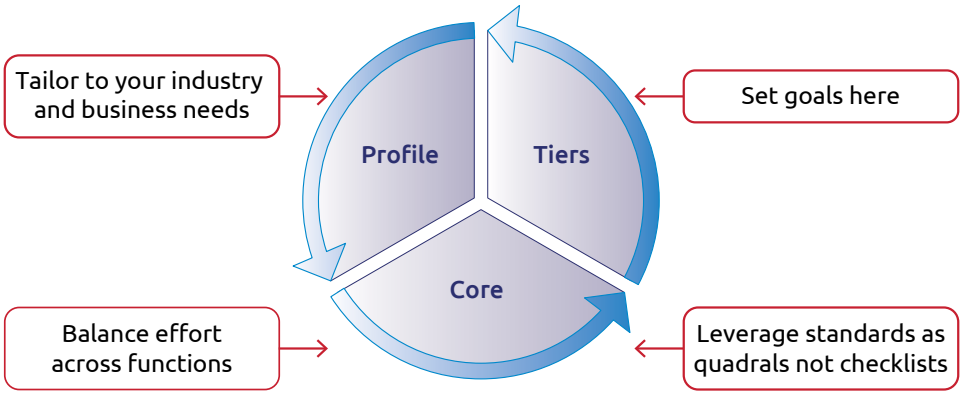




SCADAfence

NIST Cyber Security Framework

The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity risk and includes a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impact. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.
The following pages list some of the significant NIST CSF guidelines and detail how the SCADAfence Governance Portal enables organizations to comply with them.



Adapted From NIST Cybersecurity Framework, Version 1.1
Source: Garthner
ID: 464751

Diagram 2: Pragmatic Use of NIST CSF

> *According to Gartner's Security and Risk Management Survey in 2019: "73% of organizations around the world adopt the NIST Cybersecurity Framework (CSF). Although adoption levels are high, respondents report that risk management initiatives lack business participation and financial investment.*
> *Gartner inquiries indicate security and risk team exhaustion due to a control-focused CSF implementation leading to a checkbox exercise in informing senior management and the board about the organization's cybersecurity posture.*
>
> Gartner

SCADAfence

Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

NIST Subcategory	The SCADAfence Platform
ID.AM-1: Physical devices and systems within the organization are inventoried	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. SCADAfence's advanced technology provides continuous detection of devices plus 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.
ID.AM-2: Software platforms and applications within the organization are inventoried	For embedded devices such as PLCs and IEDs, the SCADAfence Platform identifies the model, vendor and firmware version. The SCADAfence Platform offers a built-in module which automatically lists all installed applications for Windows OS devices. The module also provides information on missing and installed Windows security updates.
ID.AM-3: Organizational communication and data flows are mapped	The SCADAfence Platform provides visibility capabilities for easy network traffic flow analysis. The built-in network map visualizes the entire network flows including all devices while the Exposure Analyzer provides the ability to define logical groups and segments for specific tracking and monitoring of communication. In addition, the SCADAfence Platform includes a layered map that allows users to view the network as Purdue model map.
ID.AM-4: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	The SCADAfence Platform includes a Threat Assessment module which enables users to easily classify ICS assets by criticality, centrality to operation and likelihood of it being attacked based on vulnerabilities and past incidents.

SCADAfence

Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

NIST Subcategory	The SCADAfence Governance Portal
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	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.
ID.GV-4: Governance and risk management processes address cybersecurity risks	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.

Risk Assessment (ID.RA)

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

NIST Subcategory	The SCADAfence Platform
ID.RA-1: Asset vulnerabilities are identified and documented.	The SCADAfence Platform proactively and passively gathers information about industrial and IT equipment, matches it with vulnerability data-bases and provides a vulnerability management system. In addition, the SCADAfence Platform provides tools for network architecture review and protocol security assessment. In addition, the built-in Exposure Analyzer provides the ability to monitor network segments and define alert rules for unauthorized communication between segments.
ID.RA-3: Threats, both internal and external, are identified and documented.	The SCADAfence Platform features a number of mechanisms for threat detection that are managed through the Alert Manager. These include: profile-based detection, micro-granular baseline, behavioral detection, threat intelligence, signatures, exploitation detection and others.
ID.RA-4: Potential business impacts and likelihoods are identified.	The SCADAfence Platform includes a Threat Assessment module which enables users to easily classify ICS assets by criticality, centrality to operation and likelihood of them being attacked based on vulnerabilities and past incidents.

Access Control (PR.AC)

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

NIST Subcategory	The SCADAfence Platform
PR.AC-1: Identities and credentials are managed for authorized devices and users.	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.
PR.AC-2: Physical access to assets is managed and protected.	The SCADAfence Platform offers continuous network monitoring and advanced baseline mechanism will detect and alert on pattern and behavioral changes that can originate in physical access to ICS devices. The system will automatically report in cases where devices and services malfunction and will also alert when ICS device state change notifications are reported. The SCADAfence Platform alerts on new assets and missing devices and can identify physical access based on network events. The SCADAfence Platform also provides active polling capabilities that allow detection of changes on assets, even if those changes originated from a physical source.
PR.AC-3: Remote access is managed.	The SCADAfence Platform identifies and alerts on both unauthorized inbound and outbound connections. The SCADAfence Platform's integration with various network infrastructure tools ensures that remote connections are routed through authorized tools only.

NIST Subcategory	The SCADAfence Platform
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	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. Events are correlated with source device, process and 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. By integrating the SCADAfence Platform with existing network infrastructure products, the system can provide the capability to deny access to a resource based on the source identification.
PR.AC-5: Network integrity is protected, incorporatin network segregation where appropriate.	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.

Data Security (PR.DS)

Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

NIST Subcategory	The SCADAfence Platform
PR.DS-1: Data-at-rest is protected.	Configuration 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 enables users to validate the integrity of the ICS devices and prevent data leaks and data theft. The SCADAfence Platform features a number of mechanisms to detect and prevent theft and modification of data by malicious actors: These include: profile-based detection, micro-granular baseline, behavioral detection, threat intelligence, signatures, exploitation detection and others.
PR.DS-2: Data-in-transit is protected.	The SCADAfence Platform analyzes network traffic and ensures its integrity by making sure it is not modified. The SCADAfence Platform also alerts on "man in the middle" attacks and use of insecure protocols that expose data to risks. The SCADAfence Platform detects changes in traffic flows through its baseline mechanism that can indicate data leaks. The Exposure Analyzer and Alert Rules alerts when data leaves the segregated network against company policy.
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	The SCADAfence Platform automatically discovers and creates an accurate asset list of all ICS devices. The SCADAfence Platform alerts on any addition or removal of assets from the network, requiring an authenticated user to formally accept or deny the change, while providing an explanation that can be later audited periodically.

NIST Subcategory	The SCADAfence Platform
PR.DS-5: Protections against data leaks are implemented.	The SCADAfence Platform also alerts on “man in the middle” attacks and use of insecure protocols that expose data to risks. The SCADAfence Platform detects changes in traffic flows through its baseline mechanism that can indicate data leaks. The Exposure Analyzer and Alert Rules alerts when data leaves the segregated network against company policy.
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	The SCADAfence Platform detects modifications to important data such as configuration and programming changes performed on ICS devices. These modifications are automatically monitored for validity 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. Modifications to data that are done over the network are subject to logging, inspection and policy enforcement.

Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

NIST Subcategory	The SCADAfence Platform
PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained.	The SCADAfence Platform automatically creates and asset inventory and alerts on changes which deviate from the established baseline. The SCADAfence Platform monitors and alerts on abnormal configuration changes which are based on its unique granular baseline engine.
PR.IP-3: Configuration change control processes are in place.	The SCADAfence Platform detects and proactively gathers hundreds of events that indicate changes, requiring an authenticated user to formally accept or deny the change, while providing an explanation that can be later audited periodically. The current configuration status is displayed across the system, including historical data.

Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

NIST Subcategory	The SCADAfence Platform
PR.PT-1: Audit/ log records are determined, documented, implemented, and reviewed in accordance with policy.	The SCADAfence Platform issues alerts on 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 and system changes (e.g. programming and state changes). The SCADAfence Platform provides the detailed information required for event analysis and response, such as timestamps, source and destination information, device details, potential causes, impact and remediation recommendations.
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	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 usage). The SCADAfence Platform 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.
PR.PT-4: Communications and control networks are protected.	The SCADAfence Governance Portal, together with the SCADAfence Multi-site Management Portal provide organizations who rely on industrial infrastructure the ability to manage their cyber security posture. They allow alignment and measurement according to common standards such as NIST and IEC-62443, asset management capabilities, vulnerability management and threat detection. They also allow integration with network infrastructure tools to allow protection of the cyber assets.

Anomalies and Events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

NIST Subcategory	The SCADAfence Platform
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	The SCADAfence Platform's Exposure Analyzer module enables users to manage data flows by defining network segments. Users can also create alert rules and receive real-time alerts whenever a violation occurs. The SCADAfence Platform's granular baseline engine automatically detects abnormal network and operational behavior which result in real-time alerts.
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	The SCADAfence Platform provides comprehensive and detailed information for each alert triggered by the system and enables users to easily understand threats and respond accordingly. Alerts contain information (such as source and destination, used protocols, device details, etc.) as well as detailed explanation of the attack and remediation recommendations
DE.AE-4: Impact of events is determined.	Alerts that are triggered by the SCADAfence Platform are automatically prioritized and categorized. The SCADAfence Platform provides users with the ability to respond to incidents based on their severity and the affected asset's criticality so that risks are handled according to their proper priority. The SCADAfence Platform includes a Threat Assessment module which enables users to assess the impact of potential and current events based on KPIs such as device role, centrality, membership in Exposure groups and others.

Security Continuous Monitoring (DE.CM)

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

NIST Subcategory	The SCADAfence Platform
DE.CM-1: The network is monitored to detect potential cybersecurity events.	The SCADAfence Platform features a number of mechanisms for threat detection that are managed through the Alert Manager. These include: profile-based detection, micro-granular baseline, behavioral detection, threat intelligence, signatures, exploitation detection and others.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	The SCADAfence Platform continuous network monitoring and advanced baseline mechanism will detect and alert on pattern and behavioral changes that can originate in physical access to ICS devices. The system will automatically report in cases where devices and services malfunction and will also alert when ICS device state change notifications are reported. The SCADAfence Platform also alerts on new assets and missing devices and can identify physical access based on network events. The SCADAfence Platform also provides active polling capabilities that allow detection of events on assets, even if those events originated from a physical source.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	The SCADAfence Platform detects and proactively gathers hundreds of events. Events are 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.
DE.CM-4: Malicious code is detected.	A wide variety of malware and exploits are automatically detected by the SCADAfence Platform's threat detection algorithms. Real-time alerts on such malicious tools and attacks helps in responding quickly and effectively to such threats.

NIST Subcategory	The SCADAfence Platform
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	The SCADAfence Platform detects unauthorized or suspicious user logon events, unauthorized connections and devices and malicious software. In case of suspicious or abnormal activities, the system will automatically trigger an alert so the incident can be addressed quickly.
DE.CM-8: Vulnerability scans are performed.	The SCADAfence Platform proactively and passively gathers information about industrial and IT equipment, matches it with vulnerability databases and provides a vulnerability management system. In addition, the SCADAfence Platform provides tools for network architecture review and protocol security assessment.

Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

NIST Subcategory	The SCADAfence Platform
DE.DP-4: Event detection information is communicated to appropriate parties.	The SCADAfence Platform provides enforcement mechanisms for prompt response to events including the ability to see which users have seen the alert and are handling it. The SCADAfence Platform offers the ability to share security alerts through various methods, such as syslog, advanced API for integration and email. In addition, the SCADAfence Platform and the SCADAfence Governance Portal, include a built-in security report that can be generated and exported at any given time.

Analysis (RS.AN)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

NIST Subcategory	The SCADAfence Platform
RS.AN-1: Notifications from detection systems are investigated.	The SCADAfence Platform's centric workflow UI provides various capabilities that ensure the ease of incidents management and investigation. The SCADAfence Platform provides all necessary information for an effective investigation and allows users to distribute alerts for investigation via syslog or email, add user comments to each alert and resolve them once the investigation is complete. The SCADAfence Platform provides an aggregated report about open and closed alerts, allowing supervision of the process.
RS.AN-2: The impact of the incident is understood.	Alerts that are triggered by the SCADAfence Platform are automatically prioritized and categorized. The SCADAfence platform provides users with the ability to respond to incidents based on their severity and the affected asset's criticality so that risks are handled according to their proper priority. The SCADAfence Platform includes a Threat Assessment module which enables users to assess the impact of potential and current events based on KPIs such as device role, centrality, membership in Exposure groups and thers.
RS.AN-3: Forensics are performed.	For each event produced by the SCADAfence Platform, it offers wide forensics data such as packet capture files, audit trails, conversation view including historical data and related events

Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

NIST Subcategory	The SCADAfence Platform
RS.MI-1: Incidents are contained.	Through integration with a wide collection of third-party applications such as Firewalls and NACs, the SCADAfence Platform provides the ability to automate response actions and contain security threats. The SCADAfence Platform allows human users to contain incidents utilizing the information provided by the system for each detected event.
RS.MI-2: Incidents are mitigated.	Through integration with a wide collection of third-party applications such as Firewalls and NACs, the SCADAfence Platform provides the ability to automate response actions and mitigate security threats. The SCADAfence Platform allows human users to mitigate incidents using remediation instructions provided within the system for each triggered alert.

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