



OTORIO Titan Continuous NERC-CIP Compliance

Manage operational compliance with increased efficiency,
saving time and effort

Digitization expedited by rapidly transforming supply chains, exposes critical infrastructure and industrial organizations to an ever-growing number of cyber risks. Protecting complex multi-vendor, multi-generation ICS environment requires a comprehensive understanding of the operational technology (OT), security posture, and the operational context.

Conducting compliance and governance assessments are now a standards for critical infrastructure and industrial practitioners to ensure operational effectiveness and address the evolving threat landscape. Electric utilities are required to implement NERC CIP compliance programs to ensure the continuity of power supplies and the protection of community safety. However, as environments become more complex, manual assessments become a long, costly, and laborious efforts a spot in time.

Titan, OTORIO's Risk Management Platform, supports your OT security and compliance journey. OTORIO Titan ensures continuous compliance and policy fulfillment, with better efficiency and accuracy. It automates evidence collection and auditing which allows teams to focus on what matters. Most importantly, it improves your operational resilience and reduces the risk of non-compliance with regulations and policies.



Expedite the Compliance Assessment Process

OTORIO Titan empowers security practitioners to conduct security posture and compliance assessments from a single asset to the entire operational network. It offers out-of-the-box compliance assessment capabilities and supports your compliance with NERC CIP and other industrial security standards such as NIST 800-82, IEC 62443, NIS2 and more. OTORIO Titan provides overall compliance scores, as well as detailed information on any deviation, and the required remediation instructions. The platform shortens the time and effort required to generate all the necessary assessment



Comprehensive visibility

Complete and accurate asset inventory and vulnerability assessment across your entire OT/ICS environments (from site level down to level 0 assets). Accurate vulnerability management.



Out-of-the-box compliance

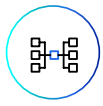


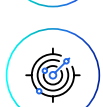
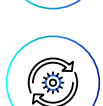
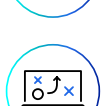

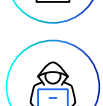
Quickly assess the security posture and compliance with industry security regulations and best practices. Automatically generate required documentation for compliance and security assessments.



Effective risk management

Impact-driven prioritization of the most critical risks with actionable prescriptive mitigation guidance tailored to the operational environment. Creating a common language between stakeholders for collaborative risk mitigation efforts.

OTORIO Titan Benefits

-  Automated accurate (down to level 0) asset inventory and vulnerabilities management
-  Automated evidence collection and risk assessment
-  Simplify audit and Governance with out-of-the-box compliance
-  Extended coverage from a single asset to site level
-  Compliance score Tracking and visibility for continuous improvement
-  Business-driven prioritization of mitigation actions
-  Actionable recommendations tailored to your operational environment
-  Ransomware-readiness assessments: host configuration gaps, FW rules and segmentation optimization, Security gaps identification

OTORIO Titan Deliverables

Extended Assets Inventory management

- Accurate asset discovery and identification
- Detailed asset attribution and inventory reports

Vulnerabilities management

- Automatic vulnerability identification
- Asset vulnerability reports
- Recommended patching and alternative mitigation actions

Contextualized security posture assessment

- Identifying security misconfigurations and security gaps in industrial systems and security controls
- Segmentation assessment
- Active directory (AD) misconfigurations and remote access monitoring

Attack graph analysis

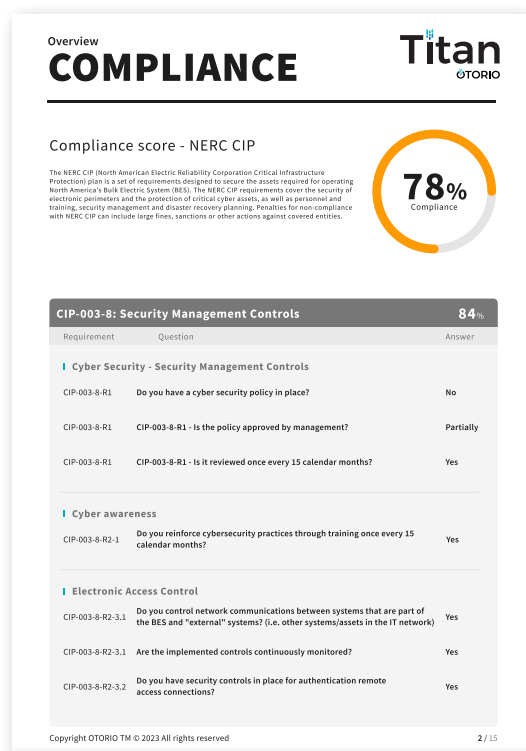
- Identifying critical exposures based on attack vectors analysis

Continuous Compliance and reports

- Comprehensive compliance assessment report
- Asset level & Site level compliance
- NERC CIP, NIST 800-82, IEC 62443 and more

Mitigation Playbooks

- Actionable step-by-step mitigation recommendation



Supervisory/Administrative network

OS-Client1

Titan OTORIO

| ID | Type | Mac | IP | External ID | Vendor | Related Alerts | Vulnerabilities | Impact Level |
|-----|------------------------|-------------------|---------------|-------------|-----------|----------------|-----------------|--------------|
| 131 | Operator Station Cl... | 00:0c:29:42:db:32 | 192.168.70.85 | N/A | Microsoft | 6 | 0 | None |

Overview Additional info Compliance Networking Process details

Compliance score

| | |
|----------------------------------|--|
| IEC 62443 - based on standard | SL 1 = 59% (29/49), SL 2 = 55% (47/85), SL 3 = 56% (53/95) |
| IEC 62443 - based on mitigations | SL 1 = 59% (29/49), SL 2 = 55% (47/85), SL 3 = 56% (53/95) |
| NERC CIP - based on standard | 58% (14/24) |
| NERC CIP - based on mitigations | 58% (14/24) |

Not compliant

| | |
|---------------------------|---|
| Name | Restrict enumeration of SAM accounts and shares from anonymous connections |
| Description | This policy setting determines which additional permissions will be assigned for anonymous connections to the device. |
| Category | Authentication, Authorization and Auditability |
| IEC 62443 | SR 1.1 - Human user identification and authentication (SL 1) |
| NERC CIP | CIP-007-6 RS 5.1 Authentication of Interactive User Access |
| Recommended configuration | The policy should be enabled. |
| Current configuration | The policy is disabled or not applied |
| Path | Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/Network access: Do not allow anonymous enumeration of SAM accounts and shares |
| Show less | |
| Name | Account lockout threshold policy |

How OTORIO Titan Assists with NERC CIP Requirements

The table below maps NERC CIP requirements to OTORIO Titan's capabilities based on continuous monitoring of the network and OTORIO Titan's ability to integrate with multiple security and industrial systems within the operational

| OTORIO Titan's Capabilities and Value | NERC CIP Requirements |
|--|--|
| Continuous Asset Inventory management using Active querying, passive network monitoring, integrations and processing of offline data. | <ul style="list-style-type: none"> • CIP-002-5.1a-R1-1.1 Identify each of the high impact Bulk Electric System (BES) Cyber Systems • CIP-005-5-R1-1.1 Cyber Assets shall reside within a defined Electronic Security Perimeter (ESP) |
| Vulnerability management. Identify needed patches and suggest alternative mitigation actions when patching is not an option. | <ul style="list-style-type: none"> • CIP-010-3-R3.1 Conduct a paper or active vulnerability assessment • CIP-010-3-R3.2 Perform an active vulnerability assessment in a production or test environment, and document results • CIP-010-3-R3.3 Perform an active vulnerability assessment of the new Cyber Asset prior to connecting it to the production environment • CIP-007-6-R1-2.1 Security Patch Management • CIP-007-6-R4 Patch Management • CIP-010-3-R1-1.4 Cyber Security - Configuration Change Management and Vulnerability Assessments • CIP-010-3-R3-3.1 Conduct a paper or active vulnerability assessment |
| Identify vulnerable configurations of user accounts in Active Directory. | <ul style="list-style-type: none"> • CIP-007-6-R5.2 Identify and inventory all known enabled default or other generic account types, either by system, by group of systems, by locations, or by system type(s) • CIP-007-6-R5.3 Identify Individuals that have authorized access to shared accounts • CIP-007-6-R5.4 Change known default passwords, per Cyber Asset capability • CIP-007-6-R5.6 Change passwords once every 15 months- where technically feasible |
| Configuration management (e.g. firmware changes). | <ul style="list-style-type: none"> • CIP-010-3-R1-1.2 Authorize and document changes that deviate from the existing baseline configuration • CIP-010-3-R1-1.3 Update the baseline configuration for changes that deviate from the baseline • CIP-010-3-R1-2.1 Monitor for changes to the baseline configuration Document and investigate detected unauthorized changes |
| Continuous network monitoring and security control utilization Firewall (FW) rules optimization, Endpoint detection and response (EDR), default credentials, segmentation issues, and more), risk alerts, and mitigation recommendations. | <ul style="list-style-type: none"> • CIP-003-8-R1 Cyber Security - Security Management Controls |
| Define operational units and hierarchy and assign assets to related processes for operational context, compliance and risk assessment. | <ul style="list-style-type: none"> • CIP-005-6-R1-1.1 Cyber Assets shall reside within a defined ESP. |

| OTORIO Titan's Capabilities and Value | NERC CIP Requirements |
|---|---|
| Analyzing network traffic and logs from remOT (OTORIO platform's secure remote access module). | <ul style="list-style-type: none"> • CIP-005-6-R1-1.2 External Routable Connectivity through an identified Extensible Authentication Protocol (EAP) • CIP-005-6-R1-1.3 Inbound and Outbound Access Permissions. |
| Provide assessment reports with top risks, unsecure protocols, misconfigurations and segmentation gaps. | <ul style="list-style-type: none"> • CIP-007-6-R1-1.1 logical port enablement |
| Integrate with security controls to provide consolidated data and identify suspicious behavior based on correlation of events from multiple sources. Alerting on security issues and risks. | <ul style="list-style-type: none"> • CIP-007-6-R3-3.1 Monitoring for Malicious Code • CIP-007-6-R4-4.2 Generate alerts for security events • CIP-008-5 Cyber Security - Incident Reporting and Response Planning |
| Vulnerability and security posture reports based on auditing of the operational network. | <ul style="list-style-type: none"> • CIP-010-3-R3-3.2 Perform an active vulnerability assessment in a production or test environment, and document results |
| On-demand querying and vulnerability assessment for machines prior to connecting to production. | <ul style="list-style-type: none"> • CIP-010-3-R3-3.3 Perform an active vulnerability assessment of the new Cyber Asset prior to connecting it to the production environment |

Titan

group

Dashboard
Factory
Investigate
Cases
Compliance
IEC 62443
NIST 800-82
NERC CIP
Integrations
Settings

NERC CIP

The NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) plan is a set of requirements designed to secure the assets required for operating North American Bulk Electric System (BES). The NERC CIP requirements cover the security of electronic perimeters and the protection of critical cyber assets, as well as personnel and training, security management and disaster recovery planning. Penalties for non-compliance with NERC CIP can include large fines, sanctions or other actions against covered entities.

78%

Compliance Score

Edit questionnaire
Reset compliance

CIP-003-8: Security Management Controls

CIP-005-6: Electronic Security Perimeter

CIP-007-6: Systems Security Management

CIP-010-3: Configuration Change Management and Vulnerability Assessments

Cyber Security Awareness

1. Do you reinforce cybersecurity practices on a continuous basis? How often does cybersecurity training occur?

☐ Yes
☐ No
☐ Partial
☐ Irrelevant

Add comment

2. Do you control physical access to assets? [How is such access controlled?]

☐ Yes
☐ No
☐ Partial
☐ Irrelevant

Add comment

Save and exit

BackNext

Asset level compliance audit

OTORIO Titan's capabilities support your compliance with NERC CIP. The platform also provides a site-level compliance questionnaire for trackability and transparency. OTORIO Titan provides out-of-the-box compliance auditing at the single asset level. It automates the collection of detailed security configuration information, maps the findings to the standards, and generates an overall compliance score. Each finding is delivered with actionable remediation guidance. The following table includes only a few examples of the configurations TORIO Titan collects and audits for compliance.

| Security Control verified by OTORIO Titan | NERC CIP Requirement |
|--|---|
| Host Firewall status | <ul style="list-style-type: none">• CIP-005-6-R1-1.5 Detects known or suspected malicious communications• CIP-005-6-R2-2.4 Determine active vendor remote access sessions• CIP-005-6-R2-2.5 Disable active vendor remote access |
| Remote Desktop Services | |
| Windows Remote Management (WinRM) Service | |
| Windows Remote Management (WinRM) Client | |
| Deny access to this computer from the network | |
| Remote Assistance | |
| Force shutdown from a remote system | |
| Named Pipes and Shares | <ul style="list-style-type: none">• CIP-007-6-R5-5.1 Authentication of Interactive User Access |
| Deny log on locally | |
| Disable Guest Account | |
| Enumeration of SAM accounts and shares | |
| Anonymous SID/Name translation | |
| Named Pipes | |
| Approval Mode for Built-in Admin account | |
| Disable Administrator Account | <ul style="list-style-type: none">• CIP-007-6-R5-5.4 Change known default passwords• CIP-007-6-R5-5.5 Password length and minimum complexity• CIP-00706-R5-5.6 Password change |
| Store password using reversible encryption | |
| Limit local accounts with blank passwords | |
| Password Policy - Password History | |
| Password Policy - Maximum password age | |
| Password Policy - Minimum password length | |
| Password Policy - Complexity requirements | |
| Audit Account Lockout | <ul style="list-style-type: none">• CIP-007-6-R5-5.7 Limits and logs the number of unsuccessful login attempts |
| Account Lockout Policy - Account lockout threshold | |
| Account Lockout Policy - Account lockout duration | |
| Account Lockout Policy - Reset account lockout counter after | |

In addition to the parameters mapped to NERC CIP requirements, OTORIO's platform checks asset configurations security best practices and vendor recommendations, promoting security hardening against ransomware. Several examples of these checks are:

- ✓ **Users are allowed to change system time**
- ✓ **Default AutoRun behavior**
- ✓ **Autoplay should be turned off**
- ✓ **Disallow Autoplay for non-volume devices**
- ✓ **Data Execution Prevention (DEP)**
- ✓ **More than one interface is connected**
- ✓ **Elevated privileges are used for installations**
- ✓ **Users are allowed to shut down the system**



About OTORIO

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IoT and OT environments for enhanced safety, productivity, compliance and resilience. Its flagship platform, OTORIO Titan, provides an all-encompassing suite of applications that brokers IIoT, OT, and CPS security controls into IT workflows, ensuring proactive protection and efficient risk management.

www.otorio.com