

On-demand OT cyber risk assessment

Evidence based risk and compliance assessment

Digitization processes, expedited by the rapidly transforming supply chains, are exposing operational environments and industrial control systems (ICS) to an ever-growing number of cyber risks. Protecting such complex multi-vendor, multi-generation IT-IoT-OT environments requires a comprehensive understanding of the operational technology (OT), the security posture, and the operational context. Risk assessment has become a de-facto standard for ensuring the resilience of critical infrastructure and industrial players. However, carrying out these assessments manually is a long, costly, and commercially challenging process with limited value.

OTORIO's spOT enables OT security practitioners to efficiently deliver high-quality, consistent, and standardized security and compliance assessments of operational environments at scale. spOT expedites the assessment processes by automatically collecting data from a variety of sources in the network, generating a consolidated asset inventory, identifying vulnerabilities, and analyzing the operational security posture. It shortens time to value and reduces required resources by up to 75%.

Delivers Assessors faster, superior-quality OT Assessments

COMPLIANCE

Compliance score - 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 America's Bulk Electric System. These assets include power generation, transmission, distribution, 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.

CIP-003-B: Security Management Controls 84%

Requirement	Question	Answer
I Cyber Security - Security Management Controls	Do you have a cyber security policy in place?	No
CIP-003-B-R1	CIP-003-B-R1 - Is the policy approved by management?	Partially
CIP-003-B-R1	CIP-003-B-R1 - Is it reviewed once every 15 calendar months?	Yes
I Cyber awareness	Do you reinforce cybersecurity practices through training once every 15 calendar months?	Yes
I Electronic Access Control	Do you restrict network communications between systems that are part of the BES and "external" systems? (i.e. other systems/assets in the IT network)	Yes
CIP-003-B-R2-3	CIP-003-B-R2-3 - Are the implemented controls continuously monitored?	Yes
CIP-003-B-R2-2	CIP-003-B-R2-2 - Do we have security controls in place for authenticating remote access connections?	Yes

Asset Inventory

OTORIO identified 620 assets, organized by their operational units:

- Risk was identified for 620 out of the 620 assets.
- The complete asset inventory is attached to this document.

620 Assets

Security Posture

Security posture refers to an organization's overall cybersecurity strength and how well it can prevent and respond to ever-changing cyber threats.

OTORIO found 6,524 security alerts in total, segmented across the following types:

Endpoint security posture analysis

- smb protocol version 1 is enabled on 2 assets - SMBv1 has several vulnerabilities that allow for remote code execution on the target machine.
- Asset debug port - this service provides read and write access to the asset's memory space. An attacker could use this service to fully compromise the affected I asset.
- Unauthenticated remote desktop configuration - remote desktop is enabled without requiring authentication on 1 device.
- 1 asset in the network is missing important security patches and have not been updated.

Number of vulnerable assets

- 124 unique vulnerability types were identified, 9 of them with critical severity, and 36 of them with high severity.
- 84 assets out of the total assets of 620 are vulnerable.



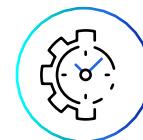
Deliver incomparable value

Consistent and standardized assessment across all OT/ICS environments (from site level down to level 0 assets). Actionable mitigation guidance prioritized by impact and risk.



Out-of-the-box compliance

Quickly assess the security posture and compliance with leading industry security regulations and best practices.



Reduce time to value

Simplify and improve the efficiency of the assessment process by up to 75%. Reduce spent resources for technical evidence collection, documentation and reporting.



Expedite the Assessment Process, Expand the Value

spOT is easy to set up and execute either on-site or remotely. Once connected to the network, spOT automatically builds the entire inventory of OT-IIoT-IT assets in the operational environment using industrial native and safe protocols and methods. This includes the discovery and identification of assets (down to level 0), machines, network segments, security configurations, accessibility, and actual connectivity between devices. The asset inventory is contextualized by asset role, relation to operational processes, and impact. Additionally, spOT maps publicly known vulnerabilities (CVEs) to the identified assets in the network.

spOT leverages OTORIO's cyber digital twin to analyze the security posture in a sandbox without interrupting operations. This includes analyzing asset configurations and security gaps, segmentation gaps due to misconfigurations of firewall rules, lacking endpoint protection, user access control, security configurations of industrial systems such as PLCs, DCS and SCADA, and more. It identifies critical attack vectors based not only on vulnerabilities but also on exposure to enable hardening against ransomware and potential

threats coming from the supply chain. For each risk, spOT provides prescriptive mitigation guidance with practical, step-by-step mitigation recommendations tailored to the operational environment. spOT provides a risk-based, impact-driven prioritization, so that operational security practitioners can focus on what matters most.

spOT also empowers assessors to conduct compliance assessments from the single asset to the entire operational network. It offers out-of-the-box compliance assessment capabilities for industrial security standards such as IEC 62443, NIST, and NERC CIP. spOT provides overall compliance scores, as well as clear and detailed information on any deviation and the required remediation instructions.

The solution shortens the time and effort required to generate all the necessary documentation needed for assessments, including information necessary for complying with global and local regulations. spOT is used for compliance assessment in a wide variety of segments, including Energy, Oil & Gas, Smart infrastructure, and Manufacturing.

How does it work?

01 Collect Data

Integrates with security controls of critical assets and operations systems



Online network monitoring data
Passive and active querying of the network



Offline data
PCAPs
Project files
FW configurations
Logs



Interactive compliance questionnaire

02 Enrich and Analyze

Based on OTORIO's research and professional services



spOT
Central Manager
Data analysis engines

03 Assessment Reports

Evidence based comprehensive assessment report



Asset inventory



Vulnerability assessment



Mitigation steps



Security posture



Policy and compliance



Virtual querying

spOT Edge
Data Collection

spOT Benefits



Save up to 75% of overall assessment time & Resources

Automated data collection, execution and reporting.



Superior assessment quality

In-depth rich inventory down to level 0. Contextualized evidence-based security posture assessment.



Actionable risk mitigation guidance

Step-by-step mitigation recommendations, with risk based prioritization.



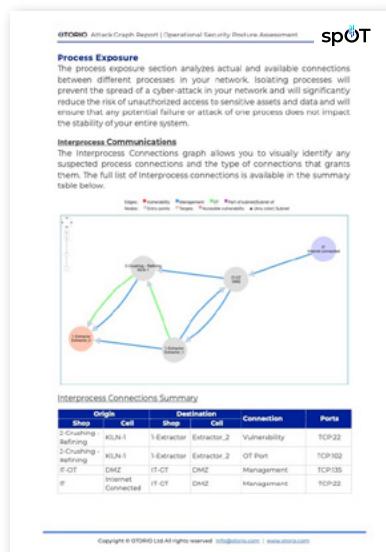
Out-of-the-box compliance

Asset and site-level compliance (IEC 62443, NERC CIP, NIST and more) and organizational policies.



Ransomware ready assessments

Identifying critical assets and network configuration for hardening against ransomware



spOT Deliverables

Extended Assets Inventory

- Detailed asset Inventory report
- Machine fingerprinting

Vulnerabilities & Contextualized security posture

- Comprehensive spOT security risk and compliance Assessment report
- Asset vulnerabilities reports
 - Asset & Vulnerability Orientation
- Segmentation assessment
- Attack graph analysis report

Compliance reports

- Asset level (IEC 62443-3, NERC CIP)
- Site level (IEC 62443-3, NERC CIP, NIST 800-82)

Mitigation

- Actionable mitigation recommendation

Other

- Option to retain the collected data and provide a periodic change management and virtual assessment
- Ready to use charts and content for upgrading your own assessment reports

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.