OTORIO

spOT™

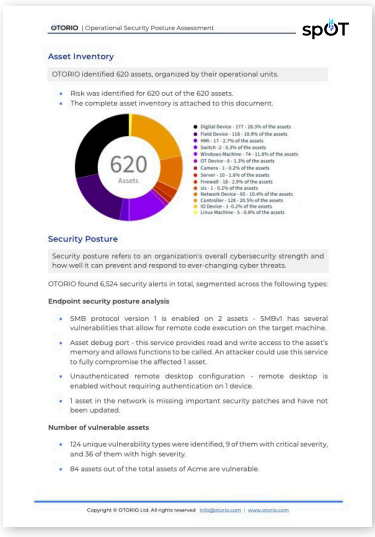
for Security and Compliance Assessment Services Enabling MSSPs, Auditors, Consultants, Engineering Companies and Integrators Deliver Faster, Superior-quality Assessments

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


Overview
COMPLIANCE
spOT
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 (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,
71%
Compliance
CIP-003-8: Security Management Controls 84%
Requirement | Question | Answer
Cyber Security - Security Management Controls
CIP-003-8-R1 | Do you have a cyber security policy in place? | No
CIP-003-8-R1 | CIP-003-8-R1 - Is the policy approved by management? | Partially
CIP-003-8-R1 | CIP-003-8-R1 - Is it reviewed once every 15 calendar months? | Yes
Cyber awareness
CIP-003-8-R2-1 | Do you reinforce cybersecurity practices through training once every 15 calendar months? | Yes
Electronic Access Control
CIP-003-8-R2-3.1 | Do you control network communications between systems that are part of the BES and "external" systems? (i.e. other systems/assets in the IT network) | Yes
CIP-003-8-R2-3.1 | Are the implemented controls continuously monitored? | Yes
CIP-003-8-R2-3.2 | Do you have security controls in place for authentication remote access connections? | Yes
Copyright OTORIO™ © 2021 All rights reserved
2 / 15


OTORIO | Operational Security Posture Assessment
spOT
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 and allows functions to be called. An attacker could use this service to fully compromise the affected 1 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 Acme are vulnerable.
Copyright © OTORIO Ltd. All rights reserved info@otorio.com | www.otorio.com

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.

spOT

Expedite the Assessment Process, Expand the Value

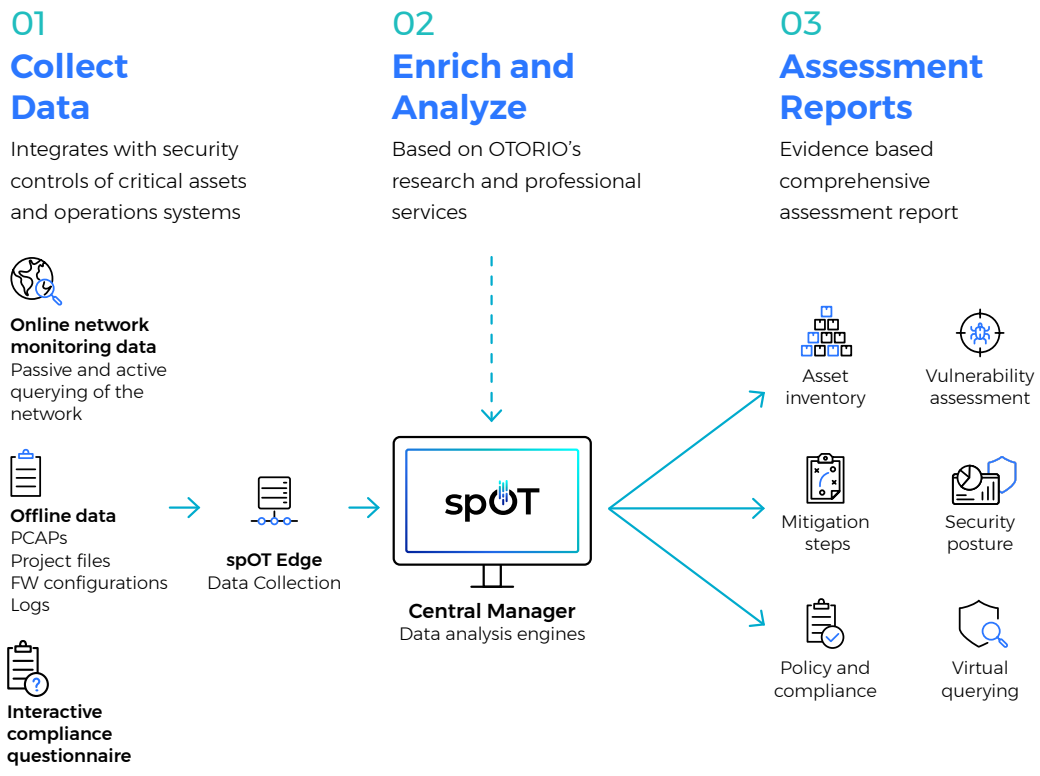
spOT is easy to set up and execute either on-site or remotely. Once connected to the network, spOT automatically builds the entire inventory of OT-IIoT-IT assets in the operational environment using industrial native and safe protocols and methods.This includes the discovery and identification of assets (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?



spOT Benefits

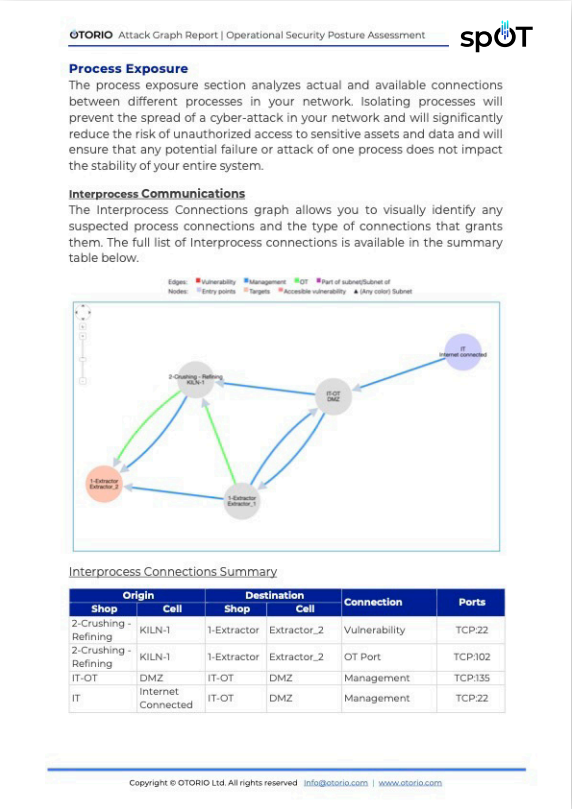
Save up to 75% of overall assessment time & Resources
Automated data collection, execution and reporting.

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



OTORIO Attack Graph Report | Operational Security Posture Assessment spOT

Process Exposure

The process exposure section analyzes actual and available connections between different processes in your network. Isolating processes will prevent the spread of a cyber-attack in your network and will significantly reduce the risk of unauthorized access to sensitive assets and data and will ensure that any potential failure or attack of one process does not impact the stability of your entire system.

Interprocess Communications

The Interprocess Connections graph allows you to visually identify any suspected process connections and the type of connections that grants them. The full list of Interprocess connections is available in the summary table below.

Interprocess Connections Summary

Origin		Destination		Connection	Ports
Shop	Cell	Shop	Cell		
2-Crushing - Refining	KILN-1	1-Extractor	Extractor_2	Vulnerability	TCP:22
2-Crushing - Refining	KILN-1	1-Extractor	Extractor_2	OT Port	TCP:102
IT-OT	DMZ	IT-OT	DMZ	Management	TCP:135
IT	Internet Connected	IT-OT	DMZ	Management	TCP:22

Copyright © OTORIO Ltd. All rights reserved info@otorio.com | www.otorio.com

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

How spOT Assists with NERC CIP Requirements

Capability	NERC CIP Requirement	NIST CSF and SP-800-53
Asset Inventory management - using Active querying and by processing of offline data	• CIP5.1-002-a-R1.1-1 Identify each of the high impact BES Cyber Systems • CIP-5-005-R1.1-1 Cyber Assets shall reside within a defined ESP	• ID.AM1- Inventory of Authorized and Unauthorized Devices • ID.AM2- inventory of Authorized and Unauthorized Software • PR.DS3-, PR.DS6- Continuous Vulnerability Assessments and Remediation
Vulnerability management	• CIP-3-010-R3.1-3 Conduct a paper or active vulnerability assessment • CIP-3-010-R3.2-3 Perform an active vulnerability assessment in a production or test environment, and document results • CIP-3-010-R3.3-3 Perform an active vulnerability assessment of the new • Cyber Asset prior to connecting it to the production environment	• ID.RA1- Asset Vulnerability ID • ID.RA2- Vuln Threat Data from multiple sources • PR.IP12- Vulnerability Mgmt Plan • DE.CM8- Vulnerability Scanning • RS.MI3- ID of new vulnerabilities
/Identify vulnerable configurations of user accounts in Active Directory	• CIP-6-007-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-6-007-R5.3 Identify Individuals that have authorized access to shared accounts • CIP6-007- R5.4 Change known default passwords, per Cyber Asset capability • CIP -6-007-R5.6 Change passwords once every 15 months, where technically feasible	• PR.AC4- Access permissions are managed, incorporating the principles of least privilege and separation of duties. • PR.AC1- Identities and credentials are managed for authorized devices and users.
Configuration management - based on changes between scans (e.g. firmware change) with an option to extend spOT with continuous monitoring, or as a periodical check as a service	• CIP-3-010-R1.2-1 Authorize and document changes that deviate from the existing baseline configuration • CIP-3-010-R1.3-1 Update the baseline configuration for changes that deviate from the baseline • CIP-3-010-R2.1-1 Monitor for changes to the baseline configuration Document and investigate detected unauthorized changes	• PR.IP1- Baseline Configs • PR.AC5- Network Protection/ Segmentation • PR.PT4- Comms and Control Network protections • PR.IP1- Baseline Configs • PR.AC5- Network Protection/ Segmentation • PR.PT4- Comms and Control Network protections
A tool for FAT/SAT (Factory or Site acceptance tests).	• CIP2-010- R1.5-1 Document each change that deviates from the existing baseline configuration	• ID.AM1- Inventory of Authorized and Unauthorized Devices • ID.AM2- inventory of Authorized and Unauthorized Software • PR.DS3-, PR.DS6- Continuous Vulnerability Assessments and Remediation

SCM - Secure & Compliant Machinery

The SCM component collects security configuration information from Windows machines, and checks them for compliance with industry standards.

Security Control verified by spOT	NERC CIP Requirement	NIST CSF and SP-800-53
Host Firewall status	• CIP-6-005-R1.5-1 Detects known or suspected malicious communications	• PR.AC3- Remote Access Management • PR.AC5- Network Protection/ Segmentation • PR.MA2- Remote Maintenance • PR.PT4- Comms and Control Network Protections • DE.AE1- Baseline Network Ops and Data Flows
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	• CIP-6-005-R2.4-2 Determine active vendor remote access sessions • CIP-6-005-R2.5-2 Disable active vendor remote access	• PR.AC3- Remote Access Mgmt • PR.AC5- Network Protection/ Segmentation • PR.MA2- Remote Maintenance • PR.PT4- Comms and Control Network Protections • DE.AE1- Baseline Network Ops and Data Flows
Named Pipes and Shares 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	• CIP-6-007-R5.1-5 Authentication of Interactive User Access	• PR.AC3- Remote Access Mgmt • PR.AC5- Network Protection/ Segmentation • PR.MA2- Remote Maintenance • PR.PT4- Comms and Control Network Protections • DE.AE1- Baseline Network Ops and Data Flows
Audit Account Lockout Account Lockout Policy - Account lockout threshold Account Lockout Policy - Account lockout duration Account Lockout Policy - Reset account lockout counter after	• CIP-6-007-R5.7-5 Limits and logs the number of unsuccessful login attempts	• PR.AC1- Credential ID • PR.AC4- Network Protection/ Segmentation

Other security configurations from registry and group policy are checked for compliance with security best practices and vendor recommendations. Examples of these checks include:

- **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 shutdown the system**
- **and many more...**

Get Started

spOT can expedite any assessment and audit process, whether mock audit, pre audit, compliance or risk assessment.

spOT reduces the time and effort required, while significantly expanding the delivered value.

Start making your assessments more effective. Book your spOT value demonstration today and start leveraging the power of technology within a week: spot-assess@otorio.com

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.

www.otorio.com

CN 211216v1