OTORIO

spOT™ for Security and Compliance Assessment Services

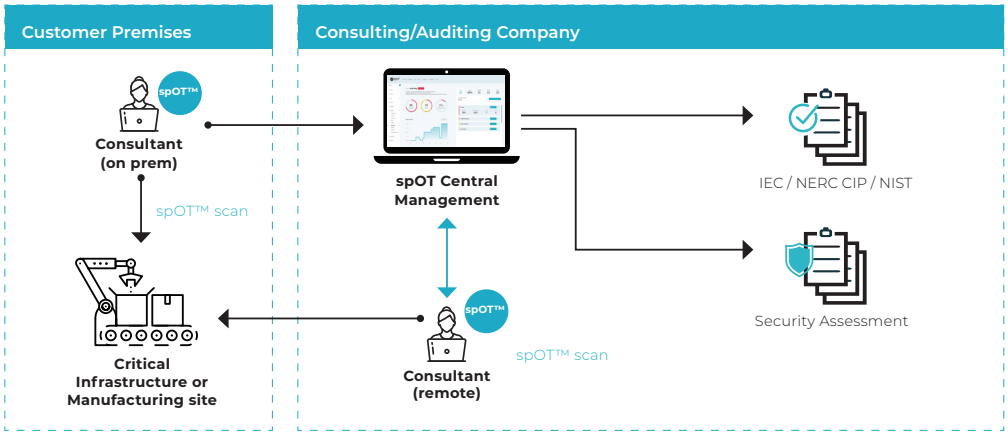
Enabling MSSPs, Auditors, Consultants, Engineering Companies and Integrators Deliver Faster, Superior-quality Assessments

Critical infrastructure and industrial environments can no longer be air gapped. Digitization processes, expedited by the global pandemic and rapidly transforming supply chains, expose the operational systems and production floors to an ever-growing variety of cyber and digital risks. Protecting such complex multi-vendor, multi generation IT-IoT-OT environments requires a comprehensive understanding of the operational structure, the technology, processes, data flows and the effectiveness of existing security controls.

Conducting periodical risk assessments is now a de-facto standard for critical infrastructure and industrial players. However, as environments get more complex, carrying out these assessments manually becomes a long, costly, and laborious effort.

OTORIO's spOT platform was developed to automate Security and Compliance Assessment processes. By pulling data from a variety of data sources, spOT automatically generates a Security Controls, Risk assessment, Compliance assessment and Governance assessment, shortening audit time and required resources by up to 75%.

Automated Security and Compliance Assessment



Benefits

- **Save up to 75% of overall assessment time & resources** preparation, execution, and reporting
- **Superior assessment quality** out of the box rich asset inventory, multiple risk vectors' assessment
- **Compliance and Governance assessments** based on regulatory standards and customer's policies
- **Value over time & ongoing support** historical comparisons and risk trends as well as ability to provide ongoing alerting as a service
- **Customized playbooks** customer tailored, out of the box extended recommendations and step-by-step mitigations
- **Ransomware-readiness Assessments**

spOT™ - Expedite the Audit Process, Expand the Value

spOT from OTORIO is a powerful software solution that is easy to set up and execute on-site or remotly. Once connected and configured, spOT automatically builds an enriched OT, IT and IIOT asset inventory, including components, assemblies, complete machines, network segments, firewall configurations, connectivity between devices, protocols and more. The inventory is automatically organized by operational processes and the enriched data is pushed to a central database for deep, automated analysis.

spOT then starts to automatically build the security assessment. First, gaps in the security posture are identified including: asset and SW vulnerabilities, segmentation issues, firewall policy-misconfigurations, zero-trust holes, and others. The risks are prioritized by their business impact according to the importance of the business process and its influence on other components or processes.

Once risks are fully assessed, mitigation insights are generated. Practical recommendations and step-by-step mitigation playbooks are compiled and bundled with the security report.

spOT generates Compliance reports, based on general and industrial-specific security standards and frameworks such as IEC 62443, NIST and NERC CIP. The reports provide an overall compliance score as well as a score per specific regulation/standard with a clear view of all open compliance issues. Similar process can be initiated to generate tailored Governance reports based on customer-specific policies and rules.

spOT™ - Deliver value over time

spOT's value increases over time. Reassessing the same environment, spOT will provide historical perspectives – what has improved, what has gotten worse and what is the trend.

spOT can also be used to provide risk-alerting services. Once scanned and assessed, an environment can be stored on the spOT database for monitoring. spOT will then continuously look at new risk information (e.g. new CVEs) and assess its impact on the environment. A risk-notification will be created if relevant information for an environment is discovered.

spOT Expedites the Audit Process

Sample Reports

spOT delivers automated compliance and security reports that can be presented to senior-level and technical clients as well as regulatory bodies and auditors. The rich reports assess risk by asset, assign compliance and security scores, and more with recommendations for improvement

Overview

COMPLIANCE

SPOT

Compliance score - NERC CIP

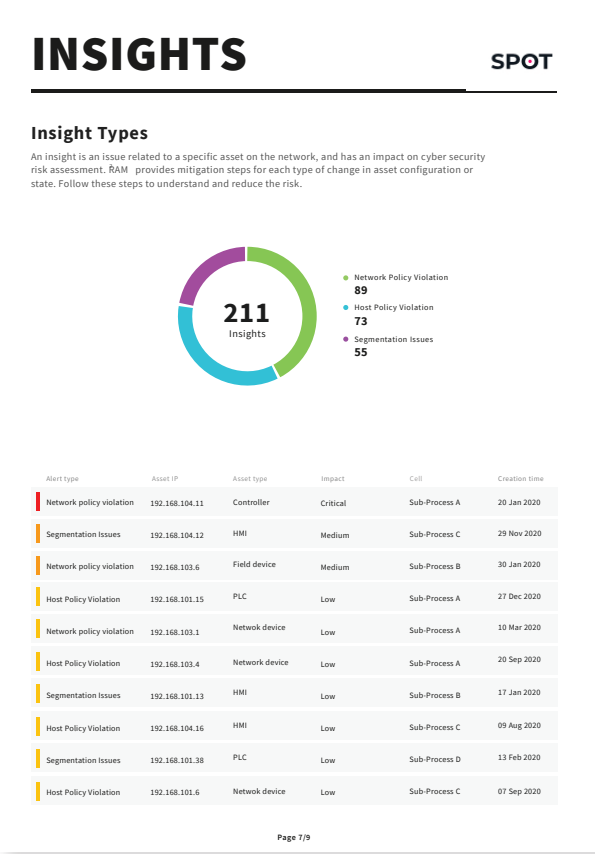
The NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) plan is a set of requirements designed to secure the assets required for operating North America's Bulk Electric System (BES). The NERC CIP requirements cover the security of electronic perimeters and the 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



INSIGHTS

SPOT

Insight Types

An insight is an issue related to a specific asset on the network, and has an impact on cyber security risk assessment. RAM provides mitigation steps for each type of change in asset configuration or state. Follow these steps to understand and reduce the risk.

211
Insights

- Network Policy Violation 89
- Host Policy Violation 73
- Segmentation Issues 55

Alert type	Asset IP	Asset type	Impact	Cell	Creation time
Network policy violation	192.168.104.11	Controller	Critical	Sub-Process A	20 Jan 2020
Segmentation Issues	192.168.104.12	HMI	Medium	Sub-Process C	29 Nov 2020
Network policy violation	192.168.103.6	Field device	Medium	Sub-Process B	30 Jan 2020
Host Policy Violation	192.168.101.15	PLC	Low	Sub-Process A	27 Dec 2020
Network policy violation	192.168.103.1	Netwok device	Low	Sub-Process A	10 Mar 2020
Host Policy Violation	192.168.103.4	Network device	Low	Sub-Process A	20 Sep 2020
Segmentation Issues	192.168.101.13	HMI	Low	Sub-Process B	17 Jan 2020
Host Policy Violation	192.168.104.16	HMI	Low	Sub-Process C	09 Aug 2020
Segmentation Issues	192.168.101.38	PLC	Low	Sub-Process D	13 Feb 2020
Host Policy Violation	192.168.101.6	Netwok device	Low	Sub-Process C	07 Sep 2020

Page 7/9

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 delivers next-generation OT security and digital risk management solutions that ensure reliable, safe and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial cybersecurity experts with cutting edge digital risk management technology to provide the highest level of protection to the critical infrastructure and manufacturing industry.