



Simplifying CIS Benchmarks Compliance Measurement Through AGENTLESS Automation

Operational Technology (OT) Compliance for Major Fortune 50 Oil & Gas company

CHALLENGE: Assessing CIS security compliance levels for OT infrastructure to determine risk exposure

Operational Technology environments in the Energy sector are not like traditional IT systems. These systems run critical physical processes, so safety, uptime, and vendor requirements come first. Unlike IT environments, OT systems cannot be freely changed, automatically fixed, or standardized without careful review.

Because of this, compliance in OT is less about enforcing changes and more about understanding risk. Teams need a clear, accurate picture of how their systems align to security standards without disrupting operations. While OT and Process Control Network (PCN) assets do carry inherent risk, Energy organizations often protect them with multiple layers of cybersecurity controls. Any configuration changes must be carefully planned and coordinated with OT teams and equipment vendors to ensure safety and reliability are never compromised.

A leading Oil & Gas organization faced the challenge of understanding its cybersecurity risk exposure by assessing how closely its OT endpoints aligned with the Center for Internet Security (CIS) Benchmarks for system-level controls. The objective was not to remediate or harden systems, but to gain accurate, read-only visibility into current compliance levels and understand how those levels influence overall risk.

This challenge is highly relevant for Energy organizations that need to understand and communicate OT cybersecurity risk, assess compliance posture against CIS Benchmarks, and support informed decision-making.

SOLUTION: Only one tool met the criteria—SteelCloud's ConfigOS MPO.

Oil & Gas corporations have complex networks of critical OT/PCN sensors and detectors that monitor refinery, exploration, and pipeline infrastructures. These critical systems cannot be compromised, and their system software configurations cannot easily be altered without needing to be reaccredited by the corresponding OT/PCN vendor, a prohibitively time-consuming and expensive effort. The OT/PCN platforms are typically Windows Server/Workstation and Linux based systems with database and webserver software stacks together with the actual OT/PCN specific applications.

In order to scan these OT/PCN systems to determine their vulnerabilities and CIS compliance ratings, the scanning system must be able to operate without requiring an agent to be installed on the OT/PCN system. Since most vulnerability scanners—including Tenable Nessus—are all agent-based, the *only* agentless scanning solution fit for purpose is SteelCloud's ConfigOS MPO (Master Policy Object).

The initial implementation was deployed to support hundreds of OT/PCN and SCADA assets across a small number of business units. Scanning these assets and being able to capture the reporting in SIEM and ITSM platforms through the ConfigOS DashView reporting allowed the customer to rapidly determine their levels of compliance and the corresponding security risks. The ConfigOS MPO deployment quickly grew to include additional BUs, around the world, allowing its agentless architecture to provide these unique compliance reporting benefits across the enterprise.

By operationalizing the entire process, ConfigOS MPO enabled the team to measure compliance against industry standards, create custom baselines tailored to their OT environment, and report results to a dashboard with confidence—without introducing false negatives or operational risks.

This use case is strictly assessment focused. No remediation or configuration changes are performed using ConfigOS MPO. Any adjustments to OT/PCN assets are handled separately and only in coordination with the appropriate OT/PCN vendors.

SteelCloud also collaborated with the customer to build out an automated pipeline facility that allows for the ingestion of an inventory of endpoints, run compliance scans on those endpoints, and report the findings, all happening in the background. ConfigOS DashView provided insights into the metrics behind the reports they were automatically generating. They could then either turn alerts based on compliance findings into tickets or generate reports for overall compliance to be visible to security and authorization leadership.

OUTCOMES: A successful cybersecurity initiative with more to come.

Thanks to ConfigOS MPO and ConfigOS DashView and the SteelCloud team, the Oil & Gas company is now in alignment with their unique custom CIS baseline implementations, thus significantly reducing common configuration exposures and having a firm grasp on their ongoing compliance management. ConfigOS MPO is now this Oil & Gas company's standard CIS Benchmarks operationalization platform, and its footprint is ramping up rapidly to span their entire OT/PCN infrastructure across the globe.

“What we found on our STIG/CIS hardening tool search is that there are a lot of good tools out there for scanning and auditing, but not any tools for actual remediation. [SteelCloud's] ConfigOS is a fully featured GUI tool that is agentless, which is great for OT environments. It supports the scanning and remediation of systems with full HTML report outputs (amongst other formats).”

OT Cybersecurity Director