SteelCloud

Simplifying AGENTLESS Operational Technology Compliance for Fortune 50 Oil & Gas company

CHALLENGE: Securing a vulnerable energy provider from cyberattack.

Our nation is under attack. And the energy sector is particularly vulnerable. The threat of cyberattack to our nation's energy concerns is elevated for three reasons:

- ✓ Cyber criminals and hacktivists want to make a statement and crippling energy supplies is an effective way to do that
- ✓ The energy sector is marked by expansive and geographical complexity that provides a greater surface for attack
- ✓ The sector's unique interdependencies between physical and cyber infrastructure make it vulnerable to attempts to commandeer operational technology (OT) and shut down operations

According to research from Gartner, "attacks on organizations in critical infrastructure sectors have increased dramatically, from less than 10 in 2013 to almost 400 in 2020 — a 3,900% change." Gartner also predicts that by 2025, "30% of critical infrastructure organizations will experience a security breach that will result in the halting of an operations- or mission-critical cyber-physical system."

Against this backdrop, a leading Oil & Gas organization chose SteelCloud's ConfigOS to harden Operational Technology (OT) endpoints and secure their process control network (PCN) using the Center for Internet Security Benchmarks (CIS) industry-standard for system-level controls.

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

Oil & Gas corporations have complex networks of critical PCN sensors and detectors that monitor refinery, exploration, and distribution infrastructures. These critical systems cannot be compromised and their system software requirements cannot be altered without express permission of the corresponding PCN vendor. The PCN platforms are typically Windows Server and Linux based systems with database and webserver software stacks together with the actual PCN specific applications.

In order to scan these 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 PCN system. Since most vulnerability scanners—including Tenable Nessus and McAfee—are all agent based, the only agentless scanning solution fit for purpose is SteelCloud's ConfigOS.

ConfigOS automates the implementation of CIS benchmarks, scanning the systems for vulnerabilities, then auditing the vulnerabilities in accordance with CIS guidelines.

The initial implementation was deployed to support the NIST security framework and includes thousands of process control and SCADA assets. While the Oil & Gas company had internal IT policies around virus protection, intrusion, and the like, it did not have a formal compliance standard for servers, printers, workstations across the enterprise. ConfigOS corrects that issue while its agentless architecture provides unique benefits to OT operators.

SteelCloud also collaborated with the company on an automated pipeline to ingest an inventory of endpoints, run compliance scans on those endpoints, and report the findings, all happening in the background.Taking this a step further, this company utilized ConfigOS DashView to gain insights into the metrics behind the reports they were automatically generating. They could then either turn alerts based on compliance issues into tickets or generate reports for overall compliance to be handed to upper management.

OUTCOMES: A successful cybersecurity initiative with more to come.

Thanks to ConfigOS and the SteelCloud team, the Oil & Gas company is now in alignment with CIS Benchmarks, significantly reducing common threats such as malware, insufficient authorization, and remote intrusion. They are so pleased with their results and are looking to add many thousand more servers to their license. They are also expressing interest in ConfigOS's agent-based solution for implementations down the road.

> ***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*