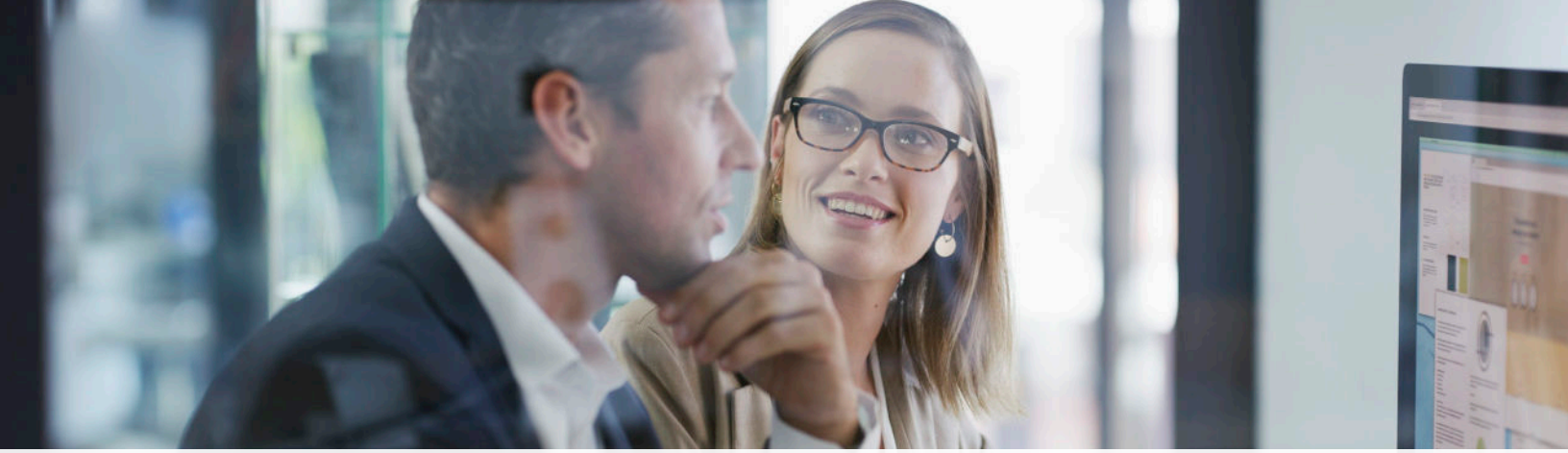

SteelCloud

Becoming True Believers in Automation After Failing a CORA Audit

CHALLENGE: Recovering from an unsuccessful CORA.

When you're a lab contracting to the Department of Energy (DoE), and you're designing, producing and assembling non-nuclear components for national programs, your mission is critical to national security. These components include precise electrical, mechanical and engineered materials for our nation's nuclear weapons stockpile and other defense applications for our warfighters. And if you fail your Cyber Operational Readiness Assessment (CORA), it puts that mission at risk. That's the precarious situation a key team found themselves in after their audit.

Loss of contracts, financial harm, operational disruption, damage to their reputation and a loss of customer trust were very real consequences this DoE lab could face as a result. The auditors gave them a short window to fix things. If they failed again, they would be brought in front of the Quarantine Review Board and could, possibly, have their contracts terminated.

The situation was dire. They knew their current system of SCAP scanning, manual remediation and Excel sheet reporting to comply with STIG, CORA and RMF requirements was no longer tenable. Auditors told them they needed to overhaul their cyber security polices, enhance employee training and invest in substantial security program improvements. And they needed to move quickly to get it all done before the auditors returned for a follow up in six months.

SOLUTION: Implementing compliance automation without significantly changing the way the team works.

The team knew they needed help from automation and other tools to fully comply with CORA in such a short timeframe. They reviewed their use of SCAP and Excel, as well as new-to-them solutions like STIG Viewer. But all fell short. The tools still required manual effort and manpower they didn't have on hand. They could be burdensome and tedious. And there just wasn't the time or resources needed to correct their CORA issues using those tools.

That's when they turned to SteelCloud. Other DoE labs were using SteelCloud's automation solution to great success, so they decided to follow suit. SteelCloud's automation platform, ConfigOS MPO, scans, remediates, maintains and reports on STIG and RMF compliance from a single, integrated solution. Once implemented, the compliance process is automated, requiring very little human intervention to remain continuously compliant. With ConfigOS MPO, the team would beat their audit deadline and their systems would be more secure than ever.

Another benefit of ConfigOS MPO was that the team did not want an intrusive solution that was hard to learn, nor did they want to completely change the way they worked. They just wanted to bring automation to what they were already doing. ConfigOS MPO answers that need. It's the only unified solution proven across the government's and DIB's most sensitive environments for over a decade.

Now, the team can significantly improve the security of their lab and their systems with the staff they have on hand.

OUTCOMES: Avoiding $2.6M in costs each year while substantially reducing effort.

The results of implementing ConfigOS were significant and measurable. Not only did the team pass their CORA audit with flying colors, they saved time and effort doing it.

Prior to implementation, engineers would spend an average of 20 hours administering an endpoint over its lifecycle. With ConfigOS, engineers will spend three hours per endpoint. This 20:3 ratio adds up to significant time savings across all the endpoints in their systems and frees engineers to focus on other security initiatives like implementing Zero Trust.

Perhaps more significant is the cost savings that come from using ConfigOS. The lab has realized an estimated total cost avoidance of $2.6M per year in costs and labor for STIG, RMF and CORA compliance in their classified environment. In fact, their CIO and CISO speculate the actual cost avoidance is higher. This equates to an overall reduction in spending of at least 60%-75%, which is fairly typical for ConfigOS MPO.

Today, ConfigOS is considered a mission critical solution in the lab's classified environments. In fact, it's known as a force multiplier across all the DoE's National Nuclear Security Administration (NNSA) labs. It keeps teams secure, compliant and audit-ready with very little human intervention.

It's a seismic shift from where the team was before ConfigOS MPO. As a result, they are considering expanding their licensing to capture additional endpoints in their unclassified systems in the future. Now true believers, they have approached DoE/NNSA leadership to consider enterprise licensing of Config OS/Config OS MPO across all the labs in the system.