SteelCloud

Going Nuclear on STIG Compliance and Achieving Game-Changing Results

CHALLENGE: Bringing greater sanity and ease to the STIG process

Key Department of Energy (DoE) groups across the nation steward our nuclear stockpile, conduct national security research, provide nuclear emergency response training and manage environmental impacts. As such, they are mandated by the Department of Defense (DoD) to protect their enterprise with the federal government's strictest and most comprehensive cybersecurity framework, Security Technical Implementation Guides (STIGs).

STIGs are used to protect the DoE's most sensitive data. Implemented properly and in a timely manner, they provide nearly impenetrable cybersecurity. They are updated quarterly as new threats and vulnerabilities develop. However, implementing them was causing a lot of frustration and delay.

One of the DoE groups used DISA's native SCAP scanner to find areas of vulnerability in their system. While this helped on certain levels, it also caused challenges in tailoring the STIGs to align with the specific operational requirements and security policies of the DoE. With no way to automate the customized remediation required, the team needed significant manual intervention to comply with mandates.

In addition, categorizing STIGs into CAT 1, 2, and 3 classifications for accurate risk assessment and remediation proved cumbersome. Overall, their SCAP scanner helped some, but lacked the intuitive functionality and comprehensive reporting capabilities required for efficient compliance management, leading to prolonged remediation cycles and potential audit delays. It also did little to help the team with the reporting requirements needed for their audits.

The team realized, as many do, that their STIG compliance was requiring more time and effort than they had on hand, keeping them behind the ball, impacting the integrity of their security and distracting members from other key cybersecurity initiatives. They had a critical need for an efficient and accurate process to tailor STIGs and enable team members to have a precise and enterprise-specific understanding of their current security posture.

SOLUTION: Transforming compliance with ConfigOS MPO, the industry's only proven unified solution

When the team started researching potential solutions, they found that very few vendors offer comprehensive solutions. As they explored various open-source alternatives, they found that they all required significant manual intervention, extensive configuration, and dedicated internal resources. Moreover, the solutions lacked the ability to generate consistent audit reports and did not help provide uniformity across different systems. All of this directly impacted efficiency, audit-readiness, and overall security consistency. There was one solution that other DoE groups were using to great success, however.

SteelCloud's ConfigOS MPO is a unified automation solution—one that integrates scanning, remediation, management and reporting into a single, purpose-built solution. Once configured and policy is set, the ConfigOS MPO STIG process is reduced to hours and days, instead of months. ConfigOS MPO produces error-free results and keeps systems audit-ready with very little human intervention.

The decision was made to implement ConfigOS MPO, then the decision-maker left the organization. As a testament to the solution's perceived value and effectiveness, the new manager embraced the choice, which was championed by the team's Information System Security Manager because of ConfigOS's ability to:

- ✓ Tailor STIG policy and remediation to meet DoE requirements
- ✓ Supply an agent-based architecture that accommodates a virtual and hybrid workforce and eases the burden on administrators
- ✓ Provide exceptional customer support, with responsive attention from SteelCloud account and support teams
- ✓ Enable future, customized enhancements as the software and its use continues to mature in the organization
- ✓ Deliver significant ROI in term of time and effort saved

OUTCOMES: Reducing effort by 75% and costs by 70% while improving compliance

The ROI the group realized from implementing ConfigOS MPO was immediate and measurable. It used to take engineers 32 hours/year to administer a single operating system. Now it takes 8 hours/year, for a 75% reduction in effort. This freed up significant time for team members to address other mission-critical activities, significantly enhancing operational efficiency and reducing resource drain on compliance-related tasks.

Better yet, prior to SteelCloud it used to cost the group $11M in tools and effort to administer their 6300 licensed endpoints. With ConfigOS, they receive a total cost avoidance of $7.8M, which translates to a savings of 70%.

What was the result of all those enterprise-wide time- and cost-savings? The group now has an enhanced security posture and improved reporting while living in a constant state of audit readiness thanks to ConfigOS's ability to maintain continuous compliance with little human intervention. They also have more ability to customize STIGs to their environment and repeat those customizations throughout their teams.

Switching to ConfigOS MPO gave the group a whole new way of interacting with STIGs, mandates and audits—all in the industry's most proven solution in sensitive environments. Today, they are looking forward to future customizations to ConfigOS and getting what equates to a bespoke solution for less than it cost them before in terms of time, effort and budget.

> **"The substantial time savings achieved through streamlined STIG tailoring and remediation allowed our personnel to reallocate valuable hours towards core mission-critical activities. In addition, SteelCloud's responsiveness and exceptional customer support were significant advantages over others in the marketplace."**
>
> *—DoE Group ISSM*

SteelCloud
20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**