SteelCloud

DATA SHEET

10 Reasons to AUTOMATE STIG Compliance

As you probably already know, implementing Security Technical Implementation Guides (STIGs) is a slow and repetitive process. It could take a team weeks or months to achieve compliance and authority to operate (ATO), only to have to repeat the process again three months later when updates are published. Adding to the frustration, every minute spent manually implementing STIG compliance is time you could be spending on those backlogs and new initiatives you keep meaning to address.

Automating the process with a solution like SteelCloud's ConfigOS changes all of that, reducing weeks of work to just an hour, making new things possible for your overall cybersecurity program. And that's just one benefit of automation. Here are 10 more:

1. Create New Secure Baselines.

Manually creating secure baselines for IT systems is a tedious, time-consuming task. Automating STIG compliance reduces weeks or months of manual effort to just an hour. Plus, it streamlines the incorporation of documented policy waivers to ensure flawless automated STIG remediation and compliance reporting.

2. Maintain Secure Baselines.

Even the most senior-level system administrator can only guarantee a secure baseline for a few days. Configuration drift from patches, updates, administrative changes, and new software installations constantly causes issues with maintaining compliance. And with STIGs updating every quarter, it's a daunting task. With automation, however, that cumbersome work is accomplished in about 15 minutes.

3. Simplify Compliance Scanning.

Compliance scanning isn't particularly difficult, but traditional scanning does require significant time and effort. The user ingests updated STIGs, scans for vulnerabilities, reviews volumes of compliance reports, makes corrections and considers waivers. Automation combines all these activities into a single process that scans, remediates, and reports as a single step with all the waivers already built in.

4. Minimize Training.

Manual STIG compliance work requires an experienced mid- to senior-level administrator to complete. Those administrators are hard to find, expensive, and may be a little grumpy from all that repetitive work, as well. However, automation requires no special skills or training. Junior-level administrators can scan, remediate, and report on STIG compliance after a single, short training session with a simple GUI interface.

5. Speed Implementation.

Traditional STIG implementation can take from several hours to several weeks, while automated STIG implementation generally completes in one hour or less. STIG compliance automation speed may not be the determining factor for those who only have a handful of systems, but the time and effort savings add up quickly for those who manage 100 or more systems.

6. Centralize Management.

As you may expect, manual STIG implementation has no centralized management interface for the remediation process. Automation provides the administrator with a "single pane of glass," or a single interface from which to manage all systems. The process can scan and remediate multiple systems across the network through this single interface.

7. Gain Immediate Compliance Feedback.

Rather than waiting for hours, days, or weeks for feedback on whether the hours spent on STIG controls were successful, automation makes this feedback available within minutes. Most systems can be fully hardened, the first time, within one hour, and in less than three minutes for ongoing remediation. With STIG automation, compliance feedback is virtually immediate.

8. Reduce Service Delivery Costs.

Touching every system in a network to perform hardening tasks and apply controls raises delivery costs. If an organization has 100 systems that need STIG hardening and each system requires two days to scan, remediate, test, and correct, the total human resource requirement is basically one full-time employee working for a year on nothing but STIGs! By reducing individual "touch" on every system in a network, service delivery costs are significantly reduced.

9. Increase Agility.

In IT terms, agility is a measure of how quickly an organization can respond to changes, threats, or opportunities. In a crisis where each of 100 systems requires 4 hours to scan, remediate, and test, it could take 400 hours to respond. That's not agile. With an automated solution, on the other hand, you can scan and remediate from 3,000 to 5,000 systems per hour, meaning those same 100 systems would be fully scanned and remediated within minutes.

10. Improve Quality and Consistency.

Automation delivers optimal consistency by mitigating human error. The automation tools apply controls the same way, every time, to each system. Automation delivers continuous, drift-free compliance!

Receive an immediate ROI from STIG automation.

When you consider the savings in both time and effort from automation—not to mention the value you receive from consistent, accurate compliance—a solution like ConfigOS pays for itself with its very first use. Over the course of a year, that could translate to avoiding millions in costs to remain compliant.

Manual vs. Automated Compliance Costs

Current Costs Without SteelCloud (Manual Hardening)		COMMENTS
Number of Workstations and Servers	2,491	*Number of computers supported by engineers. Assumes all computers will leverage SteelCloud for hardening due to RMF implementation.*
Maintenance in Support of System Hardening	16	*Average time (in hours) that an engineer spends administering a PC during the lifecycle of the PC (initial hardening, maintenance, audit support, etc.)*
Total Hours:	39,856	
Avg Hourly Salary Per Engineer	$100.00	*Average hourly rate for an engineer/admin*
Annual Labor Cost to Maintain All Systems:	**$3,985,600.00**	
Total Annual Costs:	**$3,985,600.00**	

Costs Using SteelCloud		COMMENTS
Labor Costs/Analysis:		
Number of Workstations and Servers	2,491	*Number of computers supported by engineers. Assumes all computers will leverage SteelCloud for hardening.*
Maintenance in Support of System Hardening	1	*Average time an engineer spends administering a PC during the lifecycle of the PC leveraging SteelCloud (initial hardening, maintenance, audit support, etc.)*
Total Hours:	2,491	
Avg Hourly Salary Per Engineer	$100.00	
Annual Labor Cost to Maintain all Systems:	**$249,100.00**	*Assumes an engineer would spend at least an hour per PC even with SteelCloud automating most of the tasks.*
Software Costs:		
Average SteelCloud Subscription Cost per Workstation:	**$125.00**	*Average price per computer to license.*
SteelCloud Foundry License:	**$7,500.00**	*Host based license that is used to create the security signatures that are deployed to the client computers.*
Total SteelCloud Subscription Annual Costs:	**$318,875.00**	
Total Annual Costs:	**$567,975.00**	

Costs Savings Annually:		COMMENTS
Total Costs Using SteelCloud:	**$567,975.00**	
Total Costs Using Manual Hardening:	**$3,985,600.00**	
Cost Savings Annually:	**$3,417,626.00**	*Cost Avoidance/Savings by implementing SteelCloud.*

Trust a proven solution for STIG compliance.

These are a few critical considerations to make when choosing a solution to revolutionize your approach to compliance. Look for a solution that is used and trusted in government agencies like ConfigOS. That way you know it is proven for Windows and Linux and all the devices and servers that are typical in government use. And you know it can work in classified and unclassified environments, tactical and weapon system programs, disconnected labs, and the commercial cloud.

See how automation works makes easy work of hardening.
Schedule a free ConfigOS demo at **www.steelcloud.com**.

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