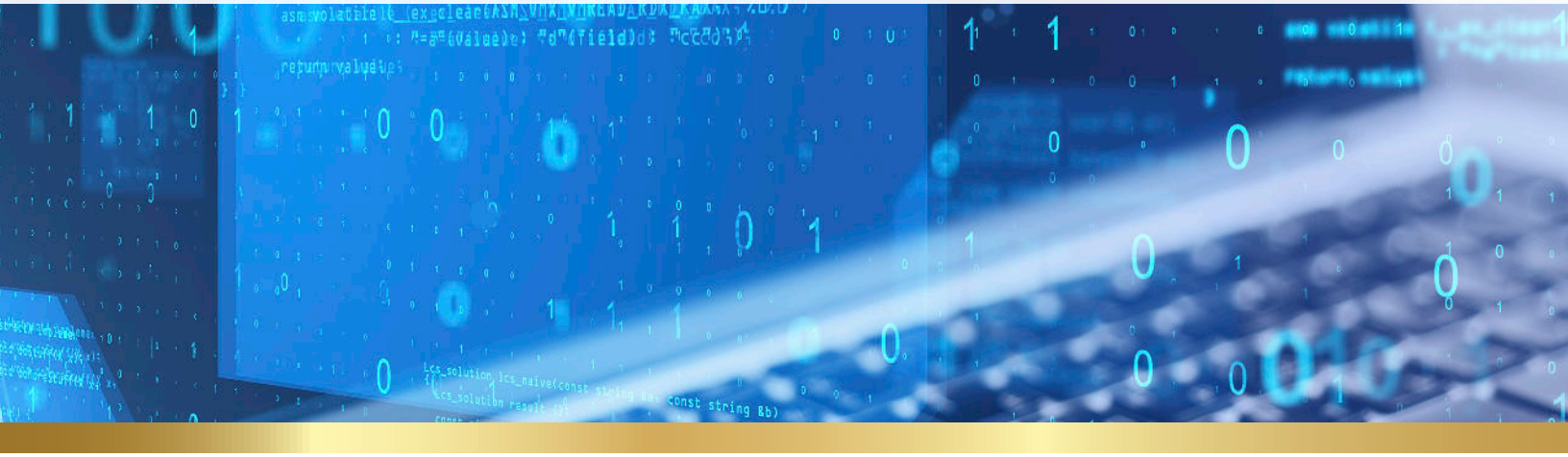
SteelCloud



WHITE PAPER

Synchronizing Cyber Compliance & IT Organizations

Unifying CIS Benchmarks Implementation Automation & Content

Purpose – There are a number of critical issues hindering an organization's ability to meet NIST 800-53 or CIS Critical Security Controls® (CIS Controls®) compliance objectives. In addition to identifying critical flaws in how these functions are automated today, this document offers a simple and convincing solution to operationalize cyber compliance through unified automation employing unified content. The result is a tight synchronization of the Risk & Compliance and IT organizations.

The Flaw - Organizations are placing a greater emphasis on streamlining the process to support continuous compliance. While a noble pursuit, this endeavor requires an organization to properly synchronize the implementation and assessment of Center for Internet Security (CIS) Benchmarks™ in the production environment. This challenge is exacerbated by the fact that assessment artifacts provided by scanning tools rarely match the controls approved to put applications into production. The resulting lack of synchronization is caused by an inherent flaw in the traditional way that CIS Benchmarks are approved, implemented, and assessed.

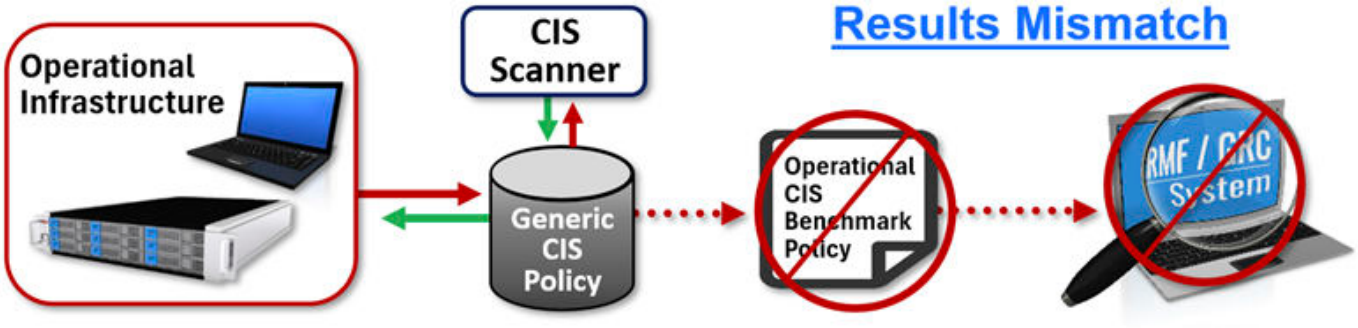
Traditional methods of cyber-compliance automation rely on multiple processes and multiple technologies from multiple vendors, which effectively isolate the processes for:

- ✓Selecting CIS Benchmarks
- ✓Implementing CIS Benchmarks
- ✓Maintaining CIS Benchmarks
- ✓Assessing CIS Benchmarks

It is easy to recognize the ongoing challenge of achieving a singular result when using multiple processes and systemswith differing CIS Benchmark content to realize that result. The challenge is magnified when one considers the compliance challenges encountered throughout an application's entire development-to-production lifecycle. Traditional means of CIS Benchmark implementation and assessment are not well suited to the efficient, accurate, and streamlined CIS compliance processes that support an enhanced production approval process – such as the Risk Management Framework (RMF).

The Operational Challenge of Cyber Compliance

Traditionally, an application's CIS Benchmark specification is created as part of the approval process to put the application into production. This involves the arduous task of hardening all of the appropriate CIS Benchmarks around an application stack. Seasoned IT staff usually take weeks or months to perform this task manually. The output of that hardening process is a CIS operational policy document that is then approved for release to the production environment. An approved CIS operational policy document details all of the approved CIS Benchmark values and any deviations required and identified in the hardening process. This document is supplied to the IT/Sys Admin staff to implement the approved controls using GPOs (Group Policy Objects), various scripting tools, and/or manual processes. How often is an application's specific approved CIS Benchmark policy implemented correctly in the production environment? Rarely. Therein lies the rub. There are multiple opportunities for human error as the approved policies are translated into various GPOs and/or scripts. Furthermore, assessment tools used to "check" the implementation of CIS Benchmarks are generally not tailored to an application's specific CIS operational policy that was approved. As a result, the production implementation of CIS Benchmarks seldom match the approved Operational Policy.



Once in production, ongoing maintenance assessments are made using generic CIS Benchmark scanners with generic CIS policy content. The maintenance content is typically not tailored to the CIS specification defined in the approval process. Therefore, the generic scanner produces results that contain real failures and significant numbers of false positives and negatives.

It is clear that traditional implementations of policy controls utilize three or more policies that are not synchronized:

1. The CIS Benchmark policy that is approved in the go-live process
2. The CIS Benchmark policy that is implemented by the IT organization with the various tools available in the environment
3. The CIS Benchmark scan results that are produced using generic policies

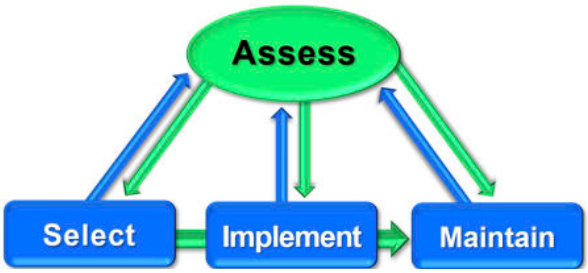
The result is an overall compliance failure requiring significant human resources to sift through results for actionable data. The burden is high enough that the reconciliation process can take days or weeks, thereby eliminating any possibility of an agile approval and monitoring process.

Addressing the Root Cause with Automation

The solution is easy to recognize. Organizations must use the same policy and automation solution for all three steps — selecting, implementing/maintaining, and assessing CIS Benchmarks. The most straightforward visualization of this process is a linear progression ending with the "assess." step.

However, in reality, the process is not linear, and assessment is not the final step. Rather, it is at the center and a key requirement of each of the component steps. So, a proper visualization would look more like a diagram where assessment is integrated into all of the steps. A compliance automation solution must operate seamlessly in both pre-production and post-production phases of the application lifecycle.

The key requirement is that a single automation tool and a single set of compliance-as-code (e.g., a collection of policies) must be able to assess and remediate systems using content that is transportable from domain to domain. This includes labs, OT/SCADA, and cloud environments.
Additionally, in each assessment step, content must be tailored to the specific app stack/system to render useful results. Generic scans against non-specific systems merely provide volumes of less-than-useful data that inhibit efficiency.



Anatomy of the Solution

Several imperatives are key to effectively automating the synchronization of the system-level controls mapping function within the IT organization:

- ✓ **Unified Operations –** The automation tool must be unified in both its automation capabilities and its ability to utilize unified CIS Benchmark content to implement, maintain, and assess controls at a granular level.
- ✓ **Hardening Process Simplification** – The hardening process needs to be simplified and automated so that non-specialized personnel can easily harden CIS Benchmarks around an app stack with minimal effort and experience. Accomplishing this will justify the creation of compliance-as-code as early in the production process as possible. Hardening automation should also accelerate both the initial CIS Benchmark deployment and periodic CIS Benchmark update activities, exercise all of the individual system-level controls, and create compliance-as-code with all deviations documented.
- ✓ **Policy Portability** – Once created in the pre-production phase, the compliance-as-code policy should be portable so it can be easily moved from domain to domain as the app stack moves from phases of development to production.
- ✓ **Approval Artifacts** – A complete solution should also produce the requisite artifacts necessary to document specific CIS Benchmark settings for specific applications.
- ✓ **Capacity and Simplification** – This is a tricky one. The automation solution and requisite policy content must be agile enough to quickly harden policy around an individual app stack/system while having the capacity to remediate and maintain thousands of systems with discrete CIS Benchmark policies tailored for each system or group of systems.
- ✓ **Policy Maintenance Automation** – An important task is the maintenance of policy. This requirement is threefold. First, the solution should be able to eliminate drift by bringing production systems into compliance while they are in production. Second, the solution should automate the periodic process of ingesting, testing, and creating new production policy baselines. Third, the solution should reliably automate the deployment of the updated policies in production by bringing the infrastructure into compliance with the new CIS Benchmark policies.

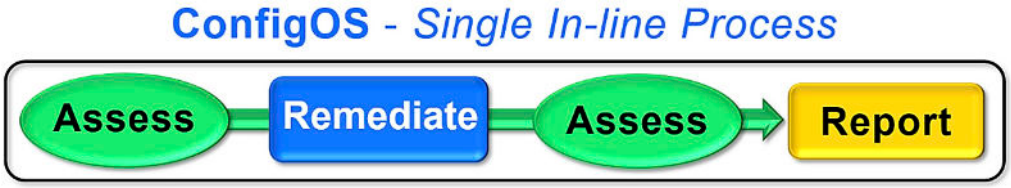
SteelCloud's ConfigOS – Checking All the Boxes

The ConfigOS cyber automation solution is elegantly designed software that easily allows organizations of any size to meet their compliance objectives. It is effortless for any systems administrator with basic operating system skills to implement and operate SteelCloud's compliance solution. The key to its effectiveness is twofold—ConfigOS has unified automation for both assessment and remediation. It performs its tasks with unified content built for selection, implementation/maintenance, and assessment of CIS Benchmarks. ConfigOS also provides a comprehensive set of reporting and JSON file output. It has been proven in hundreds of installations over more than a decade to accelerate and automate compliance in virtually any type of environment, from the commercial cloud to air-gapped SCADA/OT networks.

Accelerating the Application Approval Process with Unified Automation and Policy Content

Historically, creating compliance-as-code in the pre-production phases of an app stack's lifecycle has been challenging to accomplish and hard to justify. ConfigOS dramatically simplifies the process of hardening and creates compliance-as-code as an automatic by-product of the hardening process. With unified content and advanced automation, ConfigOS routinely allows a user to harden all CIS Benchmarks around an app stack in 30-60 minutes versus weeks or months via traditional manual methods.

The real advantage of the ConfigOS hardening process is that it automatically produces unified compliance-as-code policy baselines that scan, remediate, and report. This policy baseline includes descriptions of control waivers/deviations and the identification of controls to be remediated versus those that are scan-only. Once created and approved, the ConfigOS compliance-as-code policies can be moved directly into the production environment to implement and maintain the approved Operational Policies for specific systems or groups of systems.



In summary, ConfigOS delivers the following advantages:

- ✓ Provides unified policies that are used to select, implement/maintain, and assess CIS Benchmarks.
- ✓ Accelerates the approval process by automating the technical tasks to harden app stacks and produce required artifacts.
- ✓ Produces approved compliance-as-code as an automatic byproduct of the hardening process.
- ✓ Enables approved policies to be deployed directly into production to implement and maintain compliance with approved CIS Benchmarks for specific systems or groups of systems.

Closing the Loop – The Synchronization of Approved Policy and Production Compliance

Using a single CIS Benchmark automation solution together with unified content ensures that all infrastructures and compliance activities are wholly coordinated and synchronized. Production infrastructures' compliance always matches approved CIS Benchmark policies, and the results reported back to the cyber risk organization match what was approved in both form and detail.

Conclusion – Unified Automation with Unified Content

The key to bringing about this fundamental improvement is creating compliance-as-code policy as an output of the application risk approval process. Traditional single-purpose automation tools cannot efficiently or effectively achieve that goal. However, a comprehensive automation solution that unifies policy content ensures that control selection, implementation, and assessment are automatically and continually in sync.

About SteelCloud

SteelCloud develops innovative software that delivers near-impenetrable endpoint security with minimal effort. Our patented ConfigOS platform is the industry leader in optimizing readiness by automating the implementation of NIST (National Institute of Standards and Technology) and STIG (Security Technical Implementation Guide) security controls and CIS (Center for Internet Security) Benchmarks.

ConfigOS has been proven over more than a decade to streamline and accelerate the hardening process by automatically detecting vulnerabilities and remediating issues—eliminating the complexity traditionally associated with endpoint hardening.

What once took weeks of manual effort is now completed in about an hour. ConfigOS and ConfigOS MPO make it effortless to maintain secure baselines in any environment, laying a critical foundation for Zero Trust architectures and other advanced cybersecurity strategies.

SteelCloud can be reached at 703.674.5500. Additional information is available at www.steelcloud.com or by email at info@steelcloud.com.