Addressing the Real Impact of STIG Compliance

OVERVIEW

The U.S. Department of Defense (DoD) protects its thousands of networks by defining and implementing best practices for the installation and maintenance of its information technology (IT) resources. The Defense Information Systems Agency (DISA) develops and publishes policy in the form of Security Technical Implementation Guides (STIGs), which are used when 'hardening' DoD and mission partner systems. While significant advances have been made in the areas of threat definition and vulnerability monitoring, little progress has been made in deploying automation to address the arduous task of implementing and maintaining STIG policy on the millions of systems that support the DoD.

The PROBLEM

The lack of STIG remediation automation results in slow, costly, and inconsistent implementation of policy – creating security exposures and a substantial maintenance burden. The potential cost savings of automating STIG policy is significant - easily exceeding hundreds of millions of dollars per year. Beyond cost savings, RMF accreditation acceleration derived from automating STIG remediation should be equally important to the DoD.

The SOLUTION

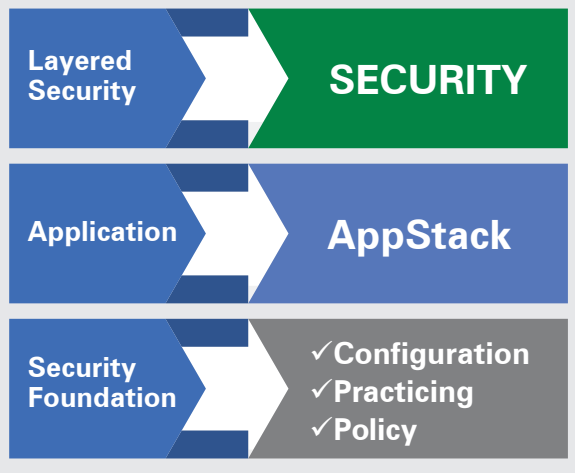
SteelCloud has been automating STIG compliance in the DoD for over twelve years. Having delivered STIG-compliant technologies across each of the Services and many DoD agencies, SteelCloud understands the operational issues involved in maintaining secure environments that also support mission goals in the most challenging DoD environments. SteelCloud has developed a new patented solution that simplifies the job of hardening controls around application stacks to create secure application baselines in just 60 minutes.

Security FOUNDATION

Best practices dictate a layered approach to providing superior endpoint security. Superior security is built on a strong foundation of Configuration, Patching, and Policy. Additional security measures will not generally compensate for deficiencies in any one of these three foundational areas.

Of the three, Policy is typically the most difficult to implement. STIG Policy can often interfere with an application's operation, especially if the application was not designed, developed, and tested in a STIG-compliant environment. Stated more directly: "STIGs break applications."

There seldom is a viable reason that well written applications should require waivers, but the reality is that they do. Because waivers can diminish the intended security posture of an environment and waivers are expensive to approve and maintain, it is imperative that STIG policy implementation be as complete as possible.



Impact of STIG Compliance on the DoD

While individual STIGs affect security, the STIGs in total have a much more pervasive impact on the DoD.
The greater STIG-related impacts on the DoD's IT infrastructure are:

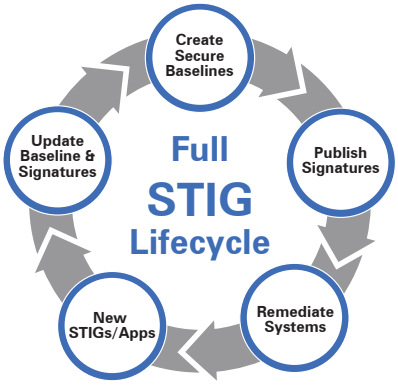
1. The timeline to accredit and rollout of new more secure technologies is extended by months, if not years;
2. Security updates to existing applications and operating systems are delayed by months;
3. Application of important new STIG security updates are not implemented quickly and consistently.

The bottom line is that the traditional manual approach to STIG compliance is slow and expensive and does not achieve the goal of making the DoD more secure. Today, STIG-related efforts are buried deep within thousands of DoD and program budgets, making it more difficult to appreciate the significant dent that STIG automation can have on the billions of dollars that the DoD spends annually on STIG compliance. SteelCloud believes this should be a Tier One security concern for DoD executives - and now there is a simple, proven solution.

Defining the SOLUTION

Since 2008, SteelCloud has delivered automation technology to set up and maintain physical, virtualized, and cloud STIG-compliant infrastructures. We have learned that the task of evaluating and determining the right STIG controls cannot be eliminated, but the process can be made exponentially easier and more consistent with automation. To this end SteelCloud developed our patented STIG remediation automation tool – ConfigOS. Tremendous thought has gone into the design and development of ConfigOS. SteelCloud has built-in unique capabilities that allow ConfigOS to automate STIG remediation given the complexities that exist within the DoD's diversity of networks and infrastructures. ConfigOS has been implemented across the DoD in classified environments, tactical deployments, air-gapped labs, cloud, and on stand-alone systems. ConfigOS requires no changes in infrastructure or connectivity.
In concept, ConfigOS is very simple. It accomplishes three primary functions:

1. ConfigOS allows any competent systems administrator to determine the correct ("securely perfect") STIG controls for an application environment in about an hour;
2. ConfigOS documents the effort to set up the proper STIG controls by automatically creating a machine executable XML signature that is secured using FIPS-validated encryption;
3. Using ConfigOS in combination with this compact secure signature, a system anywhere in the world can be remediated to the targeted security standards in a matter of seconds – without system failure or unexpected downtime.



The best technology in the world is only as good as an organization's ability to install, support, and use it. SteelCloud fully recognizes the challenges that the DoD encounters because of the size/complexity of its organization and infrastructure. Therefore, what sets ConfigOS apart from other security technologies is the sheer speed and simplicity with which it operates. ConfigOS remediates more STIG controls than SCAP or ACAS validate. ConfigOS, with its optional command line interface, can easily be managed by a security framework or discrete systems management tool. Examples of the speed and simplicity of ConfigOS are as follows:

- ✓ The ConfigOS software installs in a fully STIG-compliant environment in 60 seconds;
- ✓ ConfigOS allows an administrator to reduce the time it takes to harden STIG controls around an application by 90% (60 minutes vs. days/weeks), while creating a signature documenting the hardening effort as an automatic byproduct of the effort;
- ✓ ConfigOS will remediate a Windows system in under 45 seconds and a Linux system in under 2 minutes – while automatically building a complete rollback file and writing an audit log in the process;
- ✓ The ConfigOS Builder allows a user to build an application-specific signature in as little as 2 minutes;
- ✓ ConfigOS has an immediate payback, typically pays for itself the first time it is used – freeing up current-year budget for other projects.

ConfigOS embodies agility and is one of the easiest technologies the DoD will ever implement. It can quickly remediate Windows and Linux systems across security boundaries, in networked, constrained, and disconnected networks. There is nothing inherent in ConfigOS that limits it to STIG policy. ConfigOS can be applied to virtually any organizational policy. The ConfigOS design philosophy allows it to easily address requirements more/less stringent than the STIGs. With the inherent flexibility of ConfigOS, the DoD is now able to set variable ranges of security policy standards based on application, location, and/or security domain.

CONCLUSION

The STIGs cast a much greater shadow over maintaining DoD infrastructure security than the total of the individual controls themselves. The operational impact of STIG compliance slows the adoption of new security technologies, and slows the installation of critical security updates, operating system service packs, and other endpoint-related security enhancements. ConfigOS can dramatically decrease the negative impact that STIG compliance has on the DoD's IT agility. SteelCloud is eager to apply its revolutionary technology to raise security, lower costs, and improve agility for the DoD and its mission partners.

SteelCloud®
20110 Ashbrook Place, Suite 170 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**