COTS JOURNAL

November 2019, Volume 21 – Number 11 • *cotsjournalonline.com*

The Journal of Military Electronics & Computing

Accelerating the Pace of Government IT Modernization

Meeting the Challenges of the 21st Century with Mil Std 1553

SPECIAL FEATURE

Accelerating the Pace of Government IT Modernization

By Brian Hajost, SteelCloud's President and CEO

For decades, the federal government has been hamstrung in its efforts to adopt new IT systems by the glacial pace of RMF accreditation and the manual processes required to secure any system connected to the outside world from security risks and inherent vulnerabilities.

Streamlining this process, however, could dramatically reshape government operations and allow for shorter-duration projects that advance the cause of government IT modernization much more quickly – including moves to the Cloud.

With government IT modernization initiatives stimulating new legislation and increasing funding opportunities, it is even more critical to address a significant and continuous drag on the system: the painstaking process of securing the system to the specifications of the Defense Information Systems Agency, a support agency for the Department of Defense (DoD)

As part of this process, systems must be hardened to standard Security Technical Implementation Guide (STIG) benchmarks. The STIGs provide configuration specifications for operating systems, database management systems, web servers and weapon system used by government agencies.

The problem is STIGs are long and detailed. Often containing hundreds of pages, adhering to or upgrading software or systems to a particular STIG has been a highly specialized manual process that can take many months to accomplish. In addition to the significant time involved, it requires well-trained engineers that are skilled in the technical system, operating system policies and security guidance.

This task adds to implementation costs and can add years before an Authorization to Operate (ATO) is issued. The task is so tedious and painstaking, and there is such a shortage of STIG experts, that it often prevents agencies from pursuing modernization projects.

"With modernization, the government is spending a lot of money upfront, but they don't get any benefit until someone can actually use the new technology in production," says Brian Hajost, president of SteelCloud and an expert in automated STIG compliance. "One of the things that must get done is the system must be 'hardened' and it has to be accredited through the RMF process before an ATO is possible."

IT modernization projects for government agencies comes in many forms. Information may be consolidated into a single, shared data center or new applications moved to a different infrastructure. Increasingly, due to the government's Cloud Smart program as well as security guidelines outlined by FedRAMP, modernization projects involve moving to the commercial cloud. The advantages for government are moving to a more agile and accessible system that can be accessed any-

where and does not require complex on-premise networks.

According to Hajost, however, the difference between deploying an application in the Cloud and a traditional data center is insignificant, at least as it relates to security hardening.

"Moving to the cloud is supposed to be relatively quick and easy, but addressing system security in the cloud is no faster or easier than it is for an on-premise environment," explains Hajost. "In our world, it isn't much different than if an application moved from one data center to another, or the application is moved from a data center to the Cloud."

Hajost says that even considering the slow pace of it, most still underestimate the expertise and time required, particularly when moving to the Cloud. A shortage of trained personnel impacts the ability to modernize, a shortage that is even more acute in classified environments.

"In a classified environment you need to hire someone with five years of information assurance (IA) that has a TS/SCI security clearance," says Hajost. "If you put out an ad, you wouldn't get one person applying for that job in six months. There just aren't many around."

Instead, settle for staff that are multi-tasking from other disciplines and specialties that have little to no STIG experience.

"Even with competent, trained people, [manually handling the STIGs] is a slow process," says Hajost. "If you use people that know nothing about the STIGs, it goes really, really slowly."

Fortunately, new automated software tools are eliminating months from the RMF accreditation process by virtually eliminating the time of the initial hardening effort while also providing the required documentation for RMF accreditation.

"With a software tool that can automate the process, you can take someone that is competent in some other aspect of IT and re-skill them to handle the STIGs in a few weeks and shave months off your project time," explains Hajost.

Fortunately, there are new STIG automations tools that can quickly identify any conflicts that an application will run into in a hardened environment.

Products such as ConfigOS from SteelCloud identify and harden all controls considered a potential security risk. As outlined in the STIGs, risks are categorized into three levels (1/2/3) with Category 1 being the most severe and having the highest priority.

The software then produces a domain-independent comprehensive policy "signature" including user-defined documentation and STIG policy waivers. In this step alone, weeks, or months of manual work can be completed in an hour.

The signature and documentation are included in a secure, encrypted signature that is used to scan endpoints (laptops, desktops, physical/cloud servers) without being installed on any of them. The time it takes to remediate hundreds of STIG controls on each endpoint is typically under 90 seconds and ConfigOS executes multiple remediations at a time.

The encrypted signature can then be transported across large and small networks,

classified environments, labs, disconnected networks, and tactical environments with connected and disconnected endpoints. No other changes are required to the network, security and no software is installed on any endpoints.

To date, ConfigOS has been licensed by just about every branch of the Department of Defense, as well as parts of DHS, HHS, and Department of Energy. The product is also used by large defense contractors and in programs for all branches of the military.

In addition to resolving issues proactively at much less cost and time, the software also provides the required documentation for RMF accreditation. This can eliminate months from what is typically a 6 to 12-month process to further speed time to production.

The STIGs are updated and evolve as well. With a new update every 90 days, automated STIG remediation software accommodates for changes in the requirements. Two business days after DISA publishes a new version of the STIGs, new production signatures are tested and made available to customers.

"New security updates are introduced periodically to account for newly discovered vulnerabilities as well as changes and updates to by the vendors supplying the major operating environment components," explains Hajost.

According to Hajost, removing this significant impediment to project completion has a greater benefit than just allowing for modernization.

"The greater benefit is the capacity to modernize is greatly expanded," explains Hajost. "Modernization shouldn't be once every 10 years – it should be a continual process. So, if automating security compliance allows you to move faster, you might be able to move more than a few systems to the cloud in the next year, maybe it can be seven or eight," says Hajost.

"Then once you can modernize more, then you get reap the benefits, which includes greater agility, more consolidated information, better access to information – with better security overall," adds Hajost.