MeriTalk
Improving the Outcomes of Government IT

SteelCloud
AUTOMATING STIG & CIS COMPLIANCE

Sparring with SteelCloud's Brian Hajost on CDM Maturation

Brian Hajost is not an MMA fighter, but he did provide us with great tips to put up a good fight against cyber adversaries. MMA: Mitigation, Mechanization, and Automation are some of the key talking points. MeriTalk sat down with Brian, President and CEO at SteelCloud, to talk about that big M in CDM – Mitigation – ahead of Brian's appearance at our CDM Central conference on December 3.

? **MeriTalk: MeriTalk released research in May that found agencies estimate just 45 percent of their current CDM processes are automated. What are some of the benefits of increased automation in the program, and what areas of government cybersecurity stand to benefit the most?**

Brian: I think we have two challenges not just in automation but getting the CDM process down. One is the cyber workforce and the other is availability of budgets. The benefits of automation here are two-pronged. Automation provides efficiencies so that agencies can meet their cyber goals with the budgets they currently have.

Secondarily, the cyber workforce is becoming a challenge across all industries. Specifically, in the Federal government, the increase in cloud migration and DoD increase in CMMC (Cybersecurity Maturity Model Certification) have drawn cyber personnel away from traditional goals. So, another thing that automation allows agencies to do is accomplish goals with the staff currently available to them.

? **MeriTalk: With that in mind, what are some new ways agencies can begin to tailor their cybersecurity approach?**

Brian: Agencies can improve their activities with a segmentation and prioritization strategy in their approach to cybersecurity. For example, instead of considering cyber vulnerabilities in one big bucket, I would offer that organizations segment cyber vulnerabilities into four quadrants. One area includes cyber vulnerabilities initiated from outside of the organization, such as zero-days, malware, and things of that nature. Then there are the vulnerabilities determined inside, as a result of risk management structure or cyber hygiene. Segment each of those into two areas: those that can be mechanized, versus those that require significant human input.

If we've segmented inside to outside, then segmented by what can be mechanized or not, you can now prioritize areas of need most effectively. In other words, let the machines do what the machines can do so that people have the bandwidth to do what only they can do.

MeriTalk: In your experience, how are agencies approaching security regulations, and what should they be taking into consideration when it comes to cybersecurity maturation?

Brian: Regarding cyber, all organizations, not just government are still searching and evaluating a set of best practices that they can execute efficiently and effectively. Organizations want to execute within the budget but also have the desired result. The task is trying not to eat the whole elephant at one time, but again, segmenting their approach to these best practices. Balance the most important cyber "fruit" with the lowest hanging fruit and aggressively go after both those. The most important fruit and highest value targets, you tackle with people, and the lowest hanging fruit with automation.

MeriTalk: Looking at the CDM Program, the various tools and sensors in the program seem to deal with the C and D of the acronym – continuous diagnostics. What about mitigation? What are things that agencies need to do to mitigate some of the risks in their environment?

Brian: Mitigation is the biggest challenge for most organizations. You can assess and diagnose issues until the cows come home, but at some point you have to actually fix your cyber problems. And just because you know your areas of weakness, does not always mean you know how to fix them effectively.

Mitigation is not a one-time event. Mitigation is a concept in which you are creating processes that both eliminate and automatically fix these cyber issues in the future. In order to achieve your cyber goals, it is important to not only mitigate those issues, but to continuously achieve mitigation. The foundation of this is found in automation, by putting processes in place to run continuously to bring your organization back from drift into compliance. Things can be checked and remediated, without human interaction. That's the way that a huge swath of the cyber issues can be mitigated while concentrating the workforce on things that can only be handled by people

MeriTalk: The new CDM dashboard infrastructure "will help agencies with risk management, getting in front of risk, and understand risk," said Kevin Cox during a virtual event. How do you see the program evolving?

Brian: Dashboards are a vital step in the CDM process. If you look at the first step of CDM, it's, "We're going to inventory what we have." The second step is to assess what we have with a dashboard. So, it's "What do I have, then how does it look?" But going back to the previous question, the most important part of the process is fixing.

A dashboard gives you an assessment, but doesn't necessarily draw you to how to fix it. So if you put the CDM process in a quality management context, things are a little backwards. Instead of assessing and then fixing, we should strive to fix then assess.

In other words, the assessment should represent the confirmation that our cyber processes are working. And, when our assessment points to issues we should address, we should go to the root cause of those issues and fix them, so they don't happen again. The dashboard is a critical component, but needs to be balanced with a mitigation and automation effort.

MeriTalk: So, how else can agencies work to build a more resilient cyber ecosystem?

Brian: We need to concentrate on building structures that limit the harm that any bad actor can have on our infrastructure. One of the key directives of zero trust architecture is creating a resilient environment. So once they've gotten through our firewalls and improved identity and access controls, that we have an infrastructure that is resilient and bad actors can only do a minimal amount of damage.

And one of the easy components of building a resilient infrastructure is conforming to either the STIGs or CIS benchmarks. This is the cookbook for how to build a resilient infrastructure.

Sometimes we tend to look at an individual control and say, "How will that help? What does it block? What bad things will not happen because of that control?" You can drive yourself crazy doing that. But if you look at the benchmark in total, you'll see it creates a formidable barrier to bad actors if it is applied consistently and generally across the organization.

Applying these benchmarks has proven to be a real challenge for Federal organizations, so this is an area where mechanization can really help. Automation mechanisms are available so that they can automatically be applied to the organization. Huge chunks of cyber benefit are achieved simply by implementing the benchmarks with a minimal amount of human effort.

This is huge when it comes to CDM. SteelCloud is excited to be part of the CDM ecosystem as a cyber tool provider. In the last 12-18 months, we've seen a significant increase in interest from agencies in moving beyond the identification and assessment stage of their CDM journey and are looking to automate the mitigation processes necessary to get compliant, stay compliant, and meet their cyber hygiene goals. So, we're just excited about helping agencies along that path.

Here's a link to the article:
https://www.meritalk.com/articles/sparring-with-steelclouds-brian-hajost-on-cdm-maturation/.

Brian Hajost, President & CEO

Brian Hajost is the President & CEO of SteelCloud. Brian transformed SteelCloud into a recognized pioneer in delivering new technologies that allow government customers and commercial enterprises to effectively meet the compliance mandates of RMF, NIST 800-53, NIST 800-171, CMMC, and IRS Pub 1075. Brian is a 30-year veteran of the hardware/software industry with extensive experience focusing on government and federal integration, financial and the securities, and mobility markets. You can reach him at bhajost@steelcloud.com.