FEDInsider

The Value, Adoption & Implementation of CDM in Government

Agencies and members of industry share the benefits and best practices of adopting a data-driven cybersecurity program.

Featured Experts:

- **James Scobey**
  Chief Information Security Officer, U.S. Securities & Exchange Commission

- **Wilbert Vaughn**
  CDM Program Branch Chief, STRAT, OIS, Department of Health & Human Services

- **Garland Garris**
  Quantum Lead, Accenture Federal

- **Andrew Manos**
  Director, Commercial Services, True Zero Technologies

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation (CDM) program was first introduced in 2012 to provide a dynamic approach to strengthening government networks' cybersecurity. Today, it includes new cybersecurity tools, integration services and dashboards that help agencies improve their security posture.

The program also helps agencies reduce their threat surface, increase visibility, improve response capabilities and streamline required security reporting. Thought leaders from government and industry spoke at a recent FedInsider webinar to discuss how CDM is evolving, and its role in meeting cybersecurity mandates.

THE VALUE CDM

The CDM program provides federal agencies with the tools, processes and expertise to continuously monitor, identify and mitigate cybersecurity threats and vulnerabilities in their environment.

"Gaining real-time visibility into the network and assets with newer platform technologies, helps overcome gaps created by legacy technologies that haven't been able to securely and effectively address the explosion of distributed workforces and the speed and advancement of adversaries seeking to exploit weaknesses in enterprise computing environments. Advancements in newer platform technologies focused on converged endpoint management are giving federal agencies better visibility and rapid remediation for emerging threats. The CDM program affords opportunities in a programmatic and consistent way," said Andrew Manos, director of commercial services at True Zero Technologies.

CDM also plays a vital role in protecting sensitive government data and systems from cyberattacks, while providing the ability to standardize tools for overall resilience. This is particularly helpful in meeting Federal Information Security Management Act mandates.

CDM also plays a key part in supporting the president's executive orders on information security and continuous monitoring across all of the federal agencies, like the one on improving the nation's cybersecurity.

"The overall intent of an agency CDM program is to assure that the federal government as a whole is protected," said Garland Garris, quantum lead at Accenture Federal. "That only happens if each federal agency has the tools that they need to assure their data is secure, and that they can actually share information appropriately to [chief information security officers] and other federal agencies."

And because CDM data reports are shared at the agency and federal level, CISA can identify any threats and notify other agencies so they can deploy the proper protections.

CDM IMPLEMENTATION HURDLES

Garris said that one of the most common challenges with implementing CDM in agencies is finding the time and resources to do so. "Agency leadership has to make CDM a priority," he said. This can be particularly hard for large federal agencies with multiple systems, high-value assets and a large attack surface. "Having credible information, and information about security gaps and vulnerability, is not always easy to orchestrate," Garris said.

Relying on manual data recording, rather than automated compliance checks, also leaves room for latency and error. Even when accurate reporting is achieved, sharing that data can also be challenging depending on what can and can't be shared and how.

The Department of Health and Human Services had to bring all department networks

and programs under a unified CDM program. Wilbert Vaughn, Continuous Diagnostics and Mitigation program branch chief, STRAT, OIS, at HHS, said they did so by deploying the CDM program and tools to every operational division under this umbrella. "Each one operates independent of each other. Each has a visibility into their own environment and can take necessary steps to control that risk," Vaughn said.

According to Vaughn, all the agency CDM programs are tied together within HHS and the CDM enterprise network. All data at the agency level is collected and reported up to the enterprise network level, and then displayed at the agency-level dashboard.

Another challenge around the influx of data, as it pertains to CDM, comes with the cloud. James Scobey, CISO for the Securities and Exchange Commission, said adopting the cloud means leveraging APIs, meaning more visibility and more data to store.

"There is a need to get those logs and the telemetry from the devices in real-time," Scobey said. "All of that means more data to manage, which means more expensive storage costs, more expensive licensing and slower processing across the much larger data sets that we have to deal with. That means the capability has to be constantly upgraded. And we have to figure out better ways to do that."

Considering the amount of data, the ability to sift and parse through that data in real-time to detect threats is also a challenge. "It is a double-edged sword that I think we will have to come to terms with now and in the future," Scobey said.

PREPARING FOR CDM

The first step in addressing the above challenges and adopting a CDM program is investing in personnel, making sure there is proper workforce training and building the skillsets needed to operate new technologies that must be implemented.

"I don't think we even know yet what those new technologies and techniques that we need to train on are," Scobey said. "I think that really spending some time with it right now, taking a look at the workforce . . . and then figuring out what the training path looks like -- not just for FY24, but to prepare for that transformation -- I think it is going to be critical to meeting the challenges."

To help tackle the data-driven security problem, Manos recommends reducing the number of applications collecting information, and training employees so that a specialist isn't needed for every single tool. "Organizations have been piling on different agents that complicate managing technology stacks, makes it harder for operations teams to stay up to date on all the technologies, and can cause unnecessary performance issues on those endpoints that confuses and limits accuracy of data and decision-making. With newer technologies, organizations can reduce the number of agents sitting on endpoints, collect data more effectively and efficiently, and address threats more accurately and timely," he said.

Also, Manos suggests adopting a tool that provides visibility into the environment and integrates the workflow to act and remediate. "Converged endpoint management solutions on the market today that give teams the ability to pivot from visibility to action (or remediation) with speed and ease to more quickly reduce risks. Being able to see what's on the network, the state of vulnerabilities and compliance, and the power to patch and manage in a single integrated workflow exists," Manos said. "And being able to access that information in real-time is more important than ever because the volume and speed of attacks is only accelerating."

Still, every agency is different – and the time it takes to prepare for a CDM program depends on the agency's cyber maturity. No federal agency is starting from scratch, said Garris. "There is existing information with existing security programs...that we can work from."

Rather that starting with nothing, the required process is more like integrating CDM into an agency's existing programs. Agencies should start with assuring the auto logs are being captured, and that data must be centralized so it can be analyzed and reported on, which is a process in itself. "For the agencies that are just starting out with CDM, you have to prioritize high value assets and your critical systems," Garris said. "You want to migrate as much as you can, detect as much as you can, and make it as difficult as you can for the adversaries to take advantage of vulnerabilities."

And if you can do all that, then you are well on your way to a good CDM program, Garris added.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190
Contact: **The Tanium Team at Carahsoft**

(703) 673-3560
Tanium@Carahsoft.com
www.Carahsoft.com/Tanium
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

True Zero Technologies

True Zero Technologies
5116 Kenwood Drive
Annandale, VA, 22003
Contact: **Andrew Manos**

(410) 300-6526
AManos@truezerotech.com
www.truezerotech.com
Linkedin.com/company/true-zero-technologies
@truezerotech