CDM Program's Success Relies on Data Standardization

Using more automation can help federal agencies improve quality of data.  

Kate Macri  
Fri, 10/23/2020 - 12:15

For the Department of Homeland Security’s Continuous Diagnostics and Mitigation (CDM) program to work, federal agencies need to ensure their data quality is top notch. Otherwise, their dashboards won’t offer an accurate picture of current assets and users on a federal agency’s network.
“Data quality can definitely cause issues,” said Hemant Baidwan, DHS deputy chief information security officer, at a FedInsider webinar discussing federal agencies’ progress on CDM implementation this week. “The dashboard is as good as what feeds it. If the data is not there and the quality and correlation are not there, whatever you're seeing on the dashboard is not really actionable from a risk management standpoint. It makes it difficult to make decisions.”

The CDM program focuses on four key areas of cyber risk: asset management, identity management and credentialing, network security and data protection.

Baidwan encouraged federal agencies to focus on standardizing and normalizing their data before using the CDM dashboard to monitor their networks.

“The CDM program is a collaborative vehicle,” he said. “It addresses our cybersecurity frameworks and risk management activities, and operations as well. Our CDM program within DHS has been instrumental in protecting our federal network infrastructure and providing all components with capabilities to leverage the best technologies for cybersecurity risk.”

But if you don’t have an accurate snapshot of asset and identity management each time you log into the dashboard, you can’t make critical decisions about your cybersecurity posture and risk management practices.

Most federal agencies are still in the first stage of CDM implementation, which focuses on addressing asset management, said Vijay D’Souza, director of the Government Accountability Office’s Information Technology & Cybersecurity team. This is a key time for federal agencies to normalize their data, he added.

Earlier this year, GAO released a report with an update on the CDM progress at three federal agencies: the Federal Aviation Administration, Indian Health Services and Small Business Administration.

“We looked at these agencies' ability to implement one of the four program areas of CDM, the asset management area, which is keeping track of the hardware and software on your network,” D’Souza said. “We did find it's a challenge to really nail down the software — it's harder than it seems. There were some other aspects of the program that were more successfully implemented, like tracking vulnerabilities.”
Referring to the GAO report, D'Souza said some federal agencies still have a long way to go because their data quality isn’t where it should be.

“I think long term, the dashboards will be useful,” he said. “None of the agencies we looked at were actually using the dashboards, and that was primarily because of the data-quality issues.”

Because federal agencies relying on manual reporting of data hinders data standardization, incorporating more automation functions could help accelerate and normalize the asset management process of CDM.

“If the asset management database isn't complete, the agency could be at risk,” noted Marcel Shaw, federal solutions architect at Ivanti.

At the Army, Chief Technology Officer William Robinson said working with different vendors to establish data standardization is a top priority.

“We need to be able to orient ourselves, decide and then react to whatever actions are happening on the network,” he said. “To have standardization and get everybody to look at a common picture to understand the threats is worth its weight in gold, regardless of how pretty or ugly your dashboard may look. More importantly is integration.”

Baidwan said DHS has seen much success and improvement in its cybersecurity posture due to the CDM program and is now focusing on assisting federal agencies with CDM implementation.

“Currently the CDM dashboard is providing critical functions for intelligent information and assisting security responses and risk management activities, which are critical,” Baidwan said. “The department has seen increased results and outcomes. We're looking at enhancing internal [component] dashboards and enhancing our internal cybersecurity risk-reporting throughout the department.”

While reaching 100% asset management may be somewhat unattainable, D'Souza and Robinson said agencies can still succeed as long as they’re maintaining a proactive, flexible approach. Federal agencies should do what they can, and keep building on that.
“Standardization will be key,” Robinson said. “Being able to implement a capability like this inside CDM will be critically important. All that underpinning data, understanding sensing, asset management, is going to be key. We're constantly evolving, shifting and changing to meet those needs.”

D'Souza also advised federal IT leaders to lean on DHS for support and guidance.

“The DHS management program office has a lot of valuable resources,” he said. “Really building a good relationship between yourself, DHS and a contractor is key to success.”