CISA Officials Open Up About CDM Dashboard Successes

Good data and good relationships with cloud service providers can ensure maximum use of CDM dashboards.

Kate Macri
Tue, 12/08/2020 - 09:50

CISA leaders emphasized the importance of good quality data and good relationships with cloud service providers when using CDM dashboards.

Federal agencies participating in the Continuous Mitigation and Diagnostics program must trust their data in order to make the best real-time decisions about handling threats and vulnerabilities on their networks, they said. And to trust the data, you must have good data.
“The dashboard is going to be focused on being a technology enabler so we can view the data and assess the data quality,” said CISA CDM Project Manager Judy Baltensperger at a conference hosted by MeriTalk last week. “The end goal is to have each one of the agencies trust the completeness of that data and eventually the accuracy of that data. ... Eventually through that data being more complete and accurate, it will produce more accurate risk scores, which will help them find the most prioritized problem first.”

But shifting from legacy IT systems to cloud infrastructure creates new challenges for federal agencies using the CDM dashboards.

The ultimate goal is to keep critical information safe, said Kevin Cox, CDM program manager at CISA.

“What we want to dom through the pilots we've had engaging with the different cloud service providers, is make sure we have a full understanding of the data they have available, look at how the data they have available aligns with the CDM requirements, and make sure that is available to the agencies so they have that real-time understanding of the protections they have in the cloud,” Cox said at the event.

Some federal agencies also struggle with identifying and prioritizing the most critical data sets. In the event of a cyber incident, a federal agency may need to make quick decisions about dismantling threats depending on the importance of the data attacked.

“There's a lot of collaboration with the agencies to have them look at the criteria and help them make the designation for whether something is high value,” Cox said. “After the last five years, we have a good understanding of what the most important systems are in the federal dot-gov arena.”

Baltensperger said it all comes back to data quality because “data quality and decisions go hand in hand.”
“We're going to focus on helping agencies reduce their risk for the worst problems first … reduce the noise on the screen,” she said. “Everyone's immediate desire is to ingest all the data. The problem is then you become overwhelmed, and that information is not necessarily intelligent. More is not necessarily better. We want them to fix their problems as they go.”

Cox said four federal agencies have deployed upgraded versions of the CDM dashboard to monitor assets and individuals connected to their networks. The upgraded version of the CDM dashboard includes Elasticsearch, a search engine that can help federal security professionals find data and network assets in real time.