FEDERAL NEWS NETWORK

# EXECUTIVE BRIEFING SERIES:

# Continuous Diagnostics and Mitigation


Sponsored by elastic

elastic

# CDM Dashboard II
# Search. Observe. Protect.

Bring the speed and scale of Elastic to cyber threat awareness and response

Learn more at info.elastic.co/cdm.html

- See training discounts
- Read CDM whitepaper
- Watch getting started videos


## PANEL OF EXPERTS

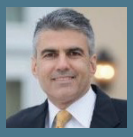
**Bernard Asare**, Acting Chief Information Security Officer (SAMHSA), HHS CDM Project Manager, Department of Health and Human Services

**Joanna Dempsey**, Director, CDM Dashboard Ecosystem Program Manager, ECS Federal

**Steven Hernandez**, Chief Information Security Officer, Director, Information Assurance Services, Department of Education

**Jason Hyer**, Continuous Diagnostics and Mitigation (CDM) Program Manager, Department of Veterans Affairs

**Gary Stevens**, Deputy Chief Information Security Officer, Executive Director, Cybersecurity Policy and Strategy, Department of Veterans Affairs



**George Young**, Vice President, Public Sector, Elastic

# New CDM dashboard data key to changing cyber behaviors

BY JASON MILLER

Most agencies are deep into the implementation and upgrading of cybersecurity capabilities through the Continuous Diagnostics and Mitigation (CDM) program after more than five years.

While the first few years of the Department of Homeland Security's program focused on filling cybersecurity gaps on agency networks, over the last year or two it's become clear CDM is more than just about data and tools.

"It's not successful unless it's changing behavior," said Jason Hyer, the CDM manager for the Department of Veterans Affairs, during a discussion sponsored by Elastic.

Hyer said that means agencies need to use data to inform decisions that lead to evolutions in cybersecurity process and policy.

"As long as we are looking at data and saying we have problems, then we have to also ask what does it matter?" he said. "All of the CDM tools are designed for a lot of things, but CDM only uses a sliver of their capabilities. We have taken tools and operationalized them so we are using them for much more than what CDM initially intended."



elastic

VA, like many agencies, holds high expectations for the data CDM can bring forward to cybersecurity and non-cyber executives through the agencywide and governmentwide dashboards. In May, 2019, DHS awarded a $276 million, six-year contract to provide a new governmentwide dashboard for the CDM program to ECS Federal. ECS has partnered with Elastic, to provide the data store and search platform for the new Dashboard capability.

## Power of the dashboard

Many civilian agencies experienced the power of the current CDM dashboard during the 2017 WannaCry ransomware attacks. Through the data, agencies knew how many Windows 7 machines they had, where PCs lived and therefore could push patches or take them offline so as not to be impacted by the cyber attack.

While the 2017 attack showed the power of the dashboard, agencies say the current version is missing some key capabilities.

"We've got three dashboards across our 12 operating agencies. When we set up CDM, we placed the stake in every single operating agency - that way, they can own and maintain their own infrastructure and their own data. And then we will roll up the CDM data to the top of the enterprise," said Bernard Asare, the CDM project manager for the Department of Health and Human Services. "If you asked us for an enterprise view, we don't have one. What I'm doing while I wait for this new dashboard is stepping into the integration layer so I can use the data there."

Asare's experience isn't unusual. Several agencies are waiting for the new CDM dashboard to consolidate existing ones and move away from relying on this integration layer, otherwise known as the middle layer of the technology stack between the public internet and the private network. It's in this layer where, for most agencies, a disparate set of cyber tools collect and report data.

"CDM is supposed to tell you how well you are doing. A CISO's job is [to understand] how well your environment is identifying threats, protecting your systems, detecting what's going on and recovering from many threats," Asare said. "When you log into the dashboard, you need to be able to see that. Since we are not seeing those things on the dashboard, we are creating that at the integration layer. We are feeding all the data that you can see or that is ingested from the CDM tools and [it tells me] how I'm looking from that point. I want to know what the ratings are before DHS comes back and tells me."

Asare said HHS currently is reviewing 14 of 104 cyber metrics through the CDM dashboard, but the data exists in other tools. He said the new dashboard will help close the metrics gap and give the agency a deeper and clearer understanding on the state of its cyber posture.

## Fine tuning the integration layer

Hyer said VA also is fine tuning the data it collects through the integration layer because this is where the agency brings all the information together from a variety of sources to be presented in the dashboard.

"There's a lot of fundamental work that has to happen behind the scenes in order to realize the vision of what the dashboard will create. And if those things are not aligned properly, then you're hamstrung what you can and cannot do with those dashboards," said Gary Stevens, the deputy CISO and executive director of cybersecurity policy and strategy at VA. "There are lots of dashboards that we have already, lots of data that gets presented in those dashboards and they're using various tiers. We need, to a certain extent, to coalesce around some common variables, common data elements that we collectively believe need to be reported in an equivalent manner so that we're all, as a federal entity, moving toward commonality in the way we report our status. When DHS does roll this all up, it is cohesive, it's equivalent and it's apples-to-apples kinds of comparisons."

One of the challenges with existing tools has been the difficulty of looking backwards in time for newly arriving data such as threat intelligence. "One of the powers of the [new dashboard] is a search engine is that it allows you to go forward or backward. So the ability to now say, 'I got threat intelligence, so tell me if it's been anywhere on the network in the last two weeks.' Now you can do a retroactive search. It's going to be a really compelling way for people to start thinking about topics like threat hunting," said George Young, the area vice president for public sector at Elastic.

Joanna Dempsey, the program manager for the CDM Dashboard Ecosystem with ECS Federal, added agencies are interested in opportunities to collapse functions within the integration layer and the dashboard, to improve the speed with which users can view and interact with their data.

"We are trying to reduce latency between data collection at the tools and sensors layer, and the ability to view data in the dashboard," she said. "Up to this point, there has been an unwritten rule that all data has to go through the integration layer before it gets to the dashboard. But now, DHS is seeking opportunities to integrate data directly into the Dashboard, where it makes sense to do so."

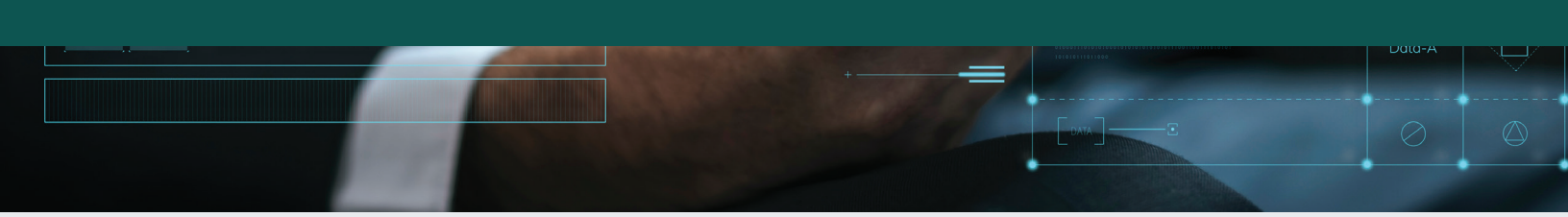
Young added the new dashboard's capabilities will bring that much-desired flexibility into not just the tools, but the data itself.

## Using the language of the data scientists

Panelists agreed that getting the right data to the right people goes back to the goal of CDM, which is to change behaviors.

Steven Hernandez, the CISO and director of information assurance services at the Education Department, said the dashboard can help with analytics or business intelligence functions to pull out the valuable bits.

"We have to also start integrating the language of our data scientists and our data friends because that's what we're running headlong into - we're running into big data and data lakes in this type of environment. What we're really talking about here is analytics, predictive analytics, machine learning, and then reporting into the dashboard," he said. "As we look into the future, we see the other data sets that are becoming increasingly valuable, especially around that behavior space. Being able to understand the models that represent behavior in our organization, how do we start to normalize that, put controls around it, but also how we can leverage that to influence and help us prioritize risk of the threats."



Elastic's Young said the new dashboard will ingest data into a common schema, which will make analytics sharing across agency bureaus or agencies much easier.

"A lot of people are trying to solve this problem including the Defense Department and the intelligence community because it's about data and speed to analytics," he said. "Dashboard users will have a library of tools to see what is best and the community can help solve cyber problems because each agency will have the opportunity to contribute and pull chips off the table."

Hernandez added the use of artificial intelligence or machine learning will make that integration of automated threat feeds easier and will do better matching. He said DHS has a "tremendous opportunity" to bring all those pieces together.

"We have to be modular in how we approach this. Whether it's visualization or analytics, as we construct the CDM architectures of the future, they have to become more data lake or big data-like," Hernandez said. "That's a different sell for the security community. That's not traditionally how we look at that problem space. We need to talk about master data management, how we will start building a common lexicon around how we are talking about data in this organization. It's a ripe opportunity because most agencies now are getting to their initial or next evolution of what their chief data officer looks like. In my agency, we are in the early discussions about how all this security data fits within the data of the agency and where might there be value that we are not realizing right now?"

## Strategies to change behavior

VA's Stevens added the data presents a picture of the environment and shows you where the critical flows are moving, which could be indicative of a problem.

"It gives you a decision tool to find where failures exist or may exist, and then correct them," he said. "In the future, it also will help you understand the trends and how they are or aren't in line with your risk appetite."

ECS's Dempsey said over the next year, their focus is to deliver a new CDM dashboard which is scalable, performant and extensible. The goal is to deliver a minimum viable product (MVP) for the Agency and Federal dashboards, which leverages Elastic's powerful search platform. The intent of a minimum viable product (MVP) is to deliver simple features, which are iteratively enhanced with user feedback. This approach emphasizes value-based delivery and reduces rework. Getting 'back to basics' with the dashboard will foster user trust in the data and allow agencies to better understand what they're looking at. Once they understand their data, they can begin to work on modifying behaviors to optimize secure operations.