LEVERAGING CDM TO DRIVE FEDERAL CYBER STRATEGIES

How integrated Continuous Diagnostics and Mitigation data can give agencies real-time security and added operating value.
CONTENTS

CDM system integrators filling asset-management gaps since pandemic hit
Inaccurate hardware counts were an issue at agencies even before increased telework added more devices to their networks.
By FedScoop Staff

Executive Perspective
How CDM data can drive cyber strategy and mission value
Agency leaders are starting to appreciate the added value of CDM data to improve operations as well as reduce cybersecurity risks.
By Frank Dimina

Executive Perspective
Strengthening security with automation and CDM data insights
The value of the CDM program may have a longer shelf-life than agency leaders realize if they tie in automation to analyze data and remediate vulnerabilities.
By Michael Guercio

This special report was produced by FedScoop and underwritten by Splunk.
System integrators hired to help agencies set up network monitoring tools have spent the pandemic months largely filling IT asset-management gaps, according to contractors and officials associated with the Continuous Diagnostics and Mitigation (CDM) cybersecurity program.

The transition to remote work created new holes in agencies’ awareness of hardware on their networks, said Dan Smith, vice president of the homeland security division at ManTech, one of the systems integrators that works on CDM.

ManTech and other companies found that they had to consider which devices were on federal networks before they could think about other security questions — especially because of the sudden need to protect data on employees’ mobile devices, Smith said. Addressing asset management gaps remains a top concern, especially since the Government Accountability Office found last August that agencies’ hardware counts were inaccurate, resulting in poor data quality that limited the usefulness of CDM dashboards detailing their security postures.

“Asset management turned out to be a pretty big one this year, especially with COVID-19,” Smith said during the Billington Cybersecurity Summit in September. “A lot of the pandemic response from the agencies we support, most of them moved to a telework posture pretty rapidly, and there was a pretty big shift from traditional network security to endpoint security and making sure things like their [Virtual Private Networks] were configured correctly.”

CDM works with civilian agencies to implement tools that feed data to agency and federal dashboards, informing overall cybersecurity risk management. Filling gaps in asset management — and identity and access management — is a key goal for fiscal 2021 as CDM works to ensure data quality, said Kevin Cox, CDM program manager.

“We want to make sure that the data coming up from the sensors and scanners has good reliability and is being reported in a timely fashion, so that the data is usable,” Cox said.

ManTech works on CDM with the Department of Education, Environmental Protection Agency, Department of Housing and Urban Development, Nuclear Regulatory Commission, National Science Foundation, and Small Business Administration, as well as other agencies.

Aside from asset management, ManTech has been supporting agency-specific CDM needs since the pandemic began. That includes helping them downsize their continuous monitoring toolsets to eliminate duplication and overlap.

“Part of where we’ve been trying to go with the agencies, where we’re helping with that architecture, is to help identify what the core technology needs are and then over time rationalize the tool suite so that they’ve got a smaller number of tools that are deployed more comprehensively — providing a better set of data across the board,” Smith said.

“That really helps to improve the investment profile for everybody, it keeps [operations and maintenance] costs down, it helps with licensing, and gives them additional resources to invest in areas like data protection management or cloud security brokering.”

“Inaccurate hardware counts were an issue at agencies even before increased telework added more devices to their networks.

CDM... keeps costs down, it helps with licensing and gives [agencies] additional resources to invest in areas like data protection management or cloud security brokering.

— Dan Smith

Read more of FedScoop’s coverage of CDM.
HOW CDM DATA CAN DRIVE CYBER STRATEGY AND MISSION VALUE

Agency leaders are starting to appreciate the added value of CDM data to improve operations as well as reduce cybersecurity risks.

By Frank Dimina

Since its inception, the goals of the federal government’s Continuous Diagnostics and Mitigation program have always been about visibility and reporting — and ultimately reducing cyber risks. But a growing number of agencies are on the cusp of gaining a far more powerful view of their network operations and their overall cybersecurity posture.

Early on, CDM was a much-needed initiative to help agencies identify, evaluate, and obtain a complete set of cyber tools to accomplish several vital aspects of cybersecurity. These included accurate asset counts and the identification of high-value data assets. That was followed by efforts to identify all the users on an agency’s network and understand what assets those users were actually accessing along with which access permissions users received. In its latest phase, CDM Dynamic and Mitigation program have always been about visibility and reporting — and ultimately leveraging CDM can quickly find all the applicable vulnerabilities emerged during the current pandemic.

One of CDM’s initial benefits was the way it helped remove blind spots and ambiguities about which assets were operating on agency networks.

What agencies and program leaders are starting to appreciate now, however, is how the CDM program, and the architecture behind it, is also generating a treasure trove of IT operating and security data.

That’s in large part because of the forethought and design decisions made by CDM’s architects at the outset. They created the mechanisms to collect data logs from the hardware, software devices and databases on agency networks (Layer A) — and assemble that information on agency and federal dashboards (Layer C and Layer D respectively).

The designers also created a highly valuable middle layer — Layer B — that aggregates, normalizes and integrates actual-state data from Layer A. The added insights that can be generated from Layer B enable agencies the means to fortify their overall cybersecurity posture — and make better decisions about their broader IT operations.

The added integration and analytics capability of CDM, compared to the underlying monitoring systems, is equivalent to going from looking at snapshots from a point in time to the having the fidelity of a live video feed. That’s in large part because of the forethought and design decisions made by CDM’s architects at the outset. They created the mechanisms to collect data logs from the hardware, software devices and databases on agency networks (Layer A) — and assemble that information on agency and federal dashboards (Layer C and Layer D respectively).

The designers also created a highly valuable middle layer — Layer B — that aggregates, normalizes and integrates actual-state data from Layer A. The added insights that can be generated from Layer B enable agencies the means to fortify their overall cybersecurity posture — and make better decisions about their broader IT operations.

For agency IT and security teams, that ultimately means gaining greater situational awareness and control over their networks. Moreover, by aggregating and unifying often incompatible data formats from different security tools into Layer B, agencies now have greater ability to harness machine learning and artificial intelligence to assess and respond to potential threats in seconds, rather than days, weeks or months. That in turn increases their ability to more quickly adjust and continually strengthen their cyber strategy.

Another, less-appreciated dimension of CDM that agencies are also starting to take advantage of is the ability to automate a variety of repetitive security tasks, using the CDM tools agencies already have installed.

These automation CDM tools can reduce a significant number of trivial tasks that security staffs might otherwise have to perform manually — and redirect valuable analysts’ focus to higher-quality security issues.

A number of agencies have already experienced the power of “operationalizing” CDM data as new vulnerabilities emerged during the current pandemic. Now, when DHS identifies an uptick in advanced attacks against a software vulnerability, agencies that are leveraging CDM can quickly find all the applicable assets and patch them as well as track the patching as it is occurring.

What has traditionally been a very manual and cumbersome process that could easily take weeks to determine whether assets had been exposed can now be completed in a matter of minutes or hours.

Ultimately, the true value of CDM is the ability it provides agencies — and those responsible for managing agency security operation centers — to fuse CDM data with other datasets, such as EINSTEIN and TIC (Trusted Internet Connection) network perimeter information to gain a greater holistic view and operational control over their agency’s high-value assets.

But all that potential value depends on agency leaders providing their teams with the support they need and a simple directive: Don’t let all that data go to waste.

Learn more about how Splunk can help your agency tap the potential of CDM.

Frank Dimina is Vice President, Americas & Public Sector at Splunk. He has more than 20 years of experience leading technology organizations and currently oversees Splunk’s americas, federal, state and local government and higher education businesses.
Through the Continuous Diagnostics and Mitigation program over the last five years, agencies have been working diligently to deploy various types of sensors and tools within their environments to gain better visibility across the network. That includes capabilities like asset discovery, vulnerability scanning, configuration checks and remediation.

Currently the Department of Homeland Security is funding the CDM program, however as planned since the inception of the program, this funding period is nearly at its end. When this happens, agency IT leaders are going to need to prove the value of keeping these tools, even as they continue to face a variety of technical challenges these CDM tools can bring.

One of those challenges lies in managing the explosion of data flowing into the security and network operation centers from these new sensors and tools. Security and operation staff are overwhelmed with information making it difficult to identify the top risks organizations are currently facing and attempt to mitigate these risks, along with new, yet-to-be discovered attack vectors and security vulnerabilities.

Additionally, each CDM tool has its own data model which allows each tool to operate. There’s a lot of extraneous data attributes inside each of these tools that are needed in order for each tool to function. But the tools don’t necessarily enrich a common data model, which is why it’s important to bring all generated data into a central location to stitch these “data-components” into a complete and logical picture.

Another challenge stems from remediating vulnerabilities. While there are policies and procedures in place today, for some, remediation is still a manual process that requires IT teams to allocate valuable time and resources.

That’s where one of CDM’s underappreciated capabilities comes into play. In addition to the ability to stitch together information from multiple sources, CDM’s tools also provide the ability to automate the execution of identification and potential responses, based on agencies’ most critical threats, their risk posture and their risk threshold. This may be the easiest way for IT leaders today to demonstrate the ongoing value of CDM and also realize important gains in their agency’s cybersecurity posture.

An example of this is the CDM capability involving the use of network access controls (NAC) to unify user or system authentication. Advanced NAC automation capabilities give agencies a powerful tool to have machines conduct multiple validation tests against an asset or a person trying to authenticate on the network. This can include scanning software version controls as well as vault scans, and various other tool scans.

Specifically, Splunk’s Phantom platform provides an orchestration automation and response technology to help correlate data and create a single picture of the agency’s cybersecurity posture. It also can automate remediation processes and augment existing NAC technologies across the tool stack. It doesn’t matter if an agency is using ForeScout, or if they’re using Cisco ISE, or even both within a more federated agency’s IT organization. Phantom provides the automation of these tools into one service so that agencies have a single, easy-to-interpret view with checks and downstream actions initiated without human intervention.

Additionally, Phantom’s architecture supports scaling for massive bursts. For example, when large percentages of the workforce begin to login at 8 or 9 in the morning, Phantom supports advanced NAC tools to scale up to or even exceed 50,000 events within an hour. That not only improves the agency’s security posture, but also the user experience to gain access to the network or system.

Though CDM implementation is a work in progress, the continued push to add more capabilities to the cloud, as well as the need for remote capabilities, means that agencies can no longer wait to implement more robust automation capabilities. These integration capabilities are available today and can be achieved — while bolstering security and speed — without re-engineering the entire process.

Learn more about how Splunk is helping leaders make confident decisions with better data insights.
Splunk is the CDM data integration and security analytics platform of choice enabling real-time visibility, reduced threat risks, and operational efficiencies.