Continuous Diagnostics and Mitigation Program Successes

VETERANS AFFAIRS: EXPANDING HWAM TOOL INTEGRATION ENHANCES VISIBILITY ACROSS THE ORGANIZATION

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow. Led by CISA, the Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of civilian government networks and systems.

The Department of Veterans Affairs (VA) gained unprecedented enterprise-wide visibility into its networks through the implementation of an enhanced CDM Hardware Access Management (HWAM) capability. Once underway, the agency realized the benefits it could achieve from expanded use of the tool throughout its information technology (IT) operations—both inside and external to CISA's CDM Program. In further developing its HWAM capability, the VA has gained a web of integrated solutions that provide new data access to teams throughout the agency, which has created new and unexpected opportunities for problem-solving, enhanced analysis, and greater productivity.

CDM ASSISTANCE

The VA's initial implementation with a CDM HWAM capability, completed in 2018, provided the agency's IT security operations with centralized visibility for hardware assets across the enterprise for the first time. A follow-on effort completed in 2021 enabled the agency to meet its goal of expanding its HWAM tool to integrate with other existing security operations tools, which widened the respective visibility of each solution even further. Without needing additional sensor hardware, the HWAM solution has equipped the VA to detect even more devices connected to its network and collect a broader array of information about its assets—ultimately yielding an enriched, centralized inventory.

"Once we understood and saw the benefit of the HWAM tool, we learned we could expand its functionality throughout the agency."

Jason Hyer
CDM Program Manager and IT Specialist, VA

The HWAM tool's agentless functionality scans a network and picks up information from any device on that network, without needing to run any software. This allows the VA to perform fewer software upgrades across its enterprise and reduces its dependence on agents to monitor endpoints. The approach gives the VA wider inventory-building and reporting abilities without a significant software dependency.

Through the CDM Program, the VA was able to adopt an enhanced HWAM capability by employing additional commercial-off-the-shelf software modules and establishing multiple solution integrations with its HWAM tool. In total, five different platforms were successfully integrated through this project.

The broader access to data throughout the VA enterprise was delivered under a CDM Request for Service, managed jointly by VA and the CISA CDM Program Management Office. The different tools targeted for integration were utilized by different systems or offices within the VA, all representing a diverse set of agency stakeholders inside the largest federal civilian government agency. Through increased data enrichment and threat analytics capabilities, the agency's overall cybersecurity posture was improved, enhancing operational areas including regulatory reporting, Configuration Management Database population, incident response, and system governance.

IMMEDIATE IMPACT

The initial HWAM capability implementation provided the VA's cybersecurity operations center with visibility they had not previously had, and the expanded HWAM solution enabled greater interoperability for multiple tools and systems within the agency. Time that had previously been spent gathering data from various sources could be turned to analysis thanks to greater integration and automation. The VA's cybersecurity operations personnel are now able to leverage enhanced HWAM data and expanded use cases thanks to the additional data available.

"We integrated the HWAM tool with many other capabilities that we had for other uses, got them to talk with one another, and this interactivity enriched our data sets and the other services they were 'talking' to," said Jason Hyer, CDM Program Manager and IT Specialist at the VA. "We didn't just see value with the specific CDM solution, but other parts of the VA that wouldn't typically derive direct benefit from CDM now were enjoying increased operability and visibility."

Additionally, the agency utilized the expanded access to conduct asset inventory and assessments for its Federal Data Center Consolidation Initiative, decreasing the need to deploy individuals throughout the country for this work. "Once the team that handles this work learned that we could implement automation to provide them visibility and connectivity to sites around the VA, they were on-board," said Hyer. "Particularly during the pandemic, this touchless and virtual approach was invaluable."

Similarly, when the VA needed to capture all workstation endpoints into a login solution, the expanded HWAM capability provided the visibility needed, which avoided data standardization difficulties.

Beyond tool-specific modules, the open integration module of the HWAM tool also enabled customized development work to be accomplished. "The HWAM could talk to anything and allow us to customize its integrations in a variety of ways," said Hyer.

THE BENEFIT OF WORKING WITH CDM

The expanded HWAM capability has put the VA in a position to understand and respond to incidents with greater agility. Additionally, the HWAM tool's ability to interface with other systems has enabled a relatively quick and easy method to enhance alerting and reporting mechanisms.

The VA has gained efficiency in its implementation of comply-to-connect requirements based on the HWAM capabilities it has added. “We plan to grow that approach based on the success we have seen already,” said Benito Urbina, Network Security Service Line Manager. “We expected the expanded visibility we achieved, but we did not anticipate the level of detail that would be available to our customer groups, nor that it would continue to grow as it has to provide constantly improved and added capabilities.”

The agency has used its expanded HWAM solution to remotely monitor assets at VA site locations that are administering COVID-19 vaccines, including monitoring freezer inventory and scanning for rogue devices on the networks. The VA team was able to identify assets that did not meet government compliance regulations, leading to more informed and timely mitigation and mediation strategies.

“Prior to this project, we could not provide this support centrally and teams had to find their own solutions. Now the VA is stepping away from siloed programming and problem-solving and benefitting greatly from our centralized approach.”

Benito Urbina
Network Security Service Line Manager, VA

The expanded solution has also provided enhanced asset information to fill gaps that, in some cases, VA teams did not know existed. The agency has already utilized the expansion of its HWAM capability for the VA Engineering, Biomedical, and Operations groups’ tracking of industry Internet of Things, Operational Technology, and Internet of Medical Technology; support of emergent cybersecurity threat response, executive order deliverables, and mitigation support; and ongoing COVID-19 response support, including providing remote device inventory and VA external connection visibility that supports the VA’s identification of authorized external connections.