Continuous Diagnostics and Mitigation Program Successes

HHS: CYBERSECURITY ENHANCEMENTS TO ENSURE HEALTH PROTECTIONS FOR ALL AMERICANS

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. The Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of civilian government networks and systems.

In March 2020 when the Department of Health and Human Services (HHS) was transitioning its workforce to teleworking due to COVID-19, the department experienced a series of cyberattacks that attempted to overload the agency with computer data requests that could slow down or potentially disable its systems.

While HHS quickly addressed and nullified the attacks, the department determined that increased vigilance was needed. Safeguarding HHS pandemic-related information, particularly regarding vaccine research and related data, was essential to protect it from bad actors and foreign adversaries seeking to profit from the data.

Under the leadership of HHS Chief Information Security Officer Janet Vogel, HHS turned to the CISA's CDM Program for assistance. The effort was led by HHS Senior Security Advisor Bernard Asare and HHS Enterprise Security Architect and Manager Mark Deffenbaugh.

CDM ASSISTANCE

Before the pandemic, HHS was already working with the CDM Program to incorporate CDM's tools and capabilities to strengthen the HHS cybersecurity systems. To address heightened concern about pandemic-related data security, the HHS team requested additional assistance through the CDM Program's Request for Services (RFS) offering, which provided their CDM integrator with additional resources to address these timely needs.

"Our system integrator was already on the ground with our team incorporating CDM," recalled Asare. "They knew the HHS environment and were able to very quickly ramp up their support, identify the emergent needs to respond to these incidents, and bring in the resources, tools, and strategies to take action."

With the CDM RFS support, the HHS team began threat hunting and analysis to support their incident response program's management and mitigation activities. They also examined cloud

security tools to bolster threat hunting capabilities, identified assessment and authorization activities where patches were needed, and looked across HHS to uncover threats throughout the department's systems.

"They knew the HHS environment and were able to very quickly ramp up their support, identify the emergent needs to respond to these incidents, and bring in the resources, tools, and strategies to take action."

Bernard Asare
HHS Senior Security Advisor

IMMEDIATE IMPACT

The eight-month program delivered immediate impacts for HHS. "We're more organized, and our threat hunting capabilities have matured," said Asare. HHS has better tools to respond to and defend against future cyber threats, and its cloud security strategy is fortified to more strongly augment on-premises activity.

In addition, "the HHS Security Operations Center is working well, our cyberteams are working more cohesively, and we have better tools and services in place to support our efforts," said Asare.

THE BENEFIT OF WORKING WITH CDM

The cyberattacks in March required HHS to reprioritize its responses and systems, and the CDM Program immediately provided the support to do so seamlessly. Already working with their CDM integrator on asset management, HHS's utilization of the CDM RFS option enabled it to expand that effort to address the need that emerged in March. "The specialists that were brought in fit right in, like an extension of our own security team," said Asare.

"The project was very, very beneficial," said Asare, who credits CDM's program manager for daily oversight of the work that added needed systems and tools into the HHS cybersecurity operations. HHS also plans to accelerate adoption of CDM's suite of tools to continue to monitor for vulnerabilities and fill any gaps.

"[The CDM Program] gave us every resource we needed to defend the department while working on a vaccine to help the American public."

Janet Vogel
HHS CISO

The March cyber threats also underscored the overall importance of cybersecurity for HHS. "Cybersecurity is now a necessity," said HHS CISO Vogel. "[The CDM Program] gave us every resource we needed to defend the department while working on a vaccine to help the American public," she added.