Continuous Diagnostics and Mitigation Program Successes

SBA: URGENT NEED LEADS TO LONG-TERM IMPROVEMENTS

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.

As the entire nation grappled with the onset of the coronavirus pandemic, the Small Business Administration (SBA) faced a seemingly ominous challenge. Just when most Americans were forced to work from home—and when office systems and structures were upended as a result—SBA had to quickly implement a major and critical funding program for its small business community to help keep them afloat.

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into law March 27, 2020, to respond to the economic fallout of the COVID-19 pandemic in the United States. The CARES Act provided direct assistance to American workers and small businesses and authorized SBA to provide funding through the Paycheck Protection Program, Economic Injury Disaster Loans, and other debt/loan programs.

THE CHALLENGE

The SBA needed to rapidly connect economically-impacted business owners with CARES Act funds. To do so, SBA began scaling up systems and creating application materials. To support this effort, the agency's information systems needed to expand their backend infrastructure to receive, process, and secure a much greater volume of data. In addition, the number of SBA employees and contractors skyrocketed from 5,000 to nearly 20,000 in just six weeks to handle the increased workload.

As the volume of data moving through the SBA information systems increased, so did the number of cyberattacks and other security incidents. "Our cybersecurity tools were doing fine, but we did not have enough humans to address what they were identifying," said SBA Chief Information Security Officer James Saunders. The agency's use of CDM Program tools provided semi-automated monitoring of the agency's cyber risks. That monitoring required human input, and the monitoring and response team

> *"SBA works in a cloud-focused environment and working with the CDM Program Management Office allowed us to explore that to our benefit and address an immediate need we faced."*
>
> **James Saunders**
> SBA CISO

quickly became swamped as threat intelligence showed adversaries targeting the agency itself, as well as the nation's small businesses. "Our mission quadrupled quickly," said Saunders.

CDM ASSISTANCE

SBA utilized the Request for Services (RFS) offering through the CDM Program to get the security engineering operational support it needed to react to threats. Along with providing tools and capabilities that provide data on cybersecurity risk and vulnerabilities, the CDM Program also offers support for agencies to improve their day-to-day cybersecurity tracking and reporting.

SBA's RFS for this coronavirus-related challenge enabled the agency to leverage the existing CDM resources already working at SBA, which meant the agency avoided a lengthy procurement and onboarding process. "The system integrator team ramped up almost immediately, which was very impressive and critically important," Saunders recalled. With this assistance, SBA was able to augment the agency's 24/7 operations and shore up its defenses without interruptions.

IMMEDIATE IMPACT

The cybersecurity specialists working under the RFS provided SBA with senior-level expertise to support SBA's Information Security Division. They provided project plans, completed analysis of cloud-based automation and vulnerability management platform alternatives, augmented SBA's cyber threat intelligence team, and helped the CISO leadership team make stronger risk decisions "based on data," rather than on educated guesses. In addition, they helped SBA adjust its processes by turning some semi-automatic responses into automatic responses. This decreased SBA's manual workload so it could better serve its small business community's needs. By the time the short-term project was nearing completion in September, the community's needs had subsided, the funds had been allocated, and the RFS team had helped the in-house operations center absorb the new processes into existing systems and activities.

THE BENEFIT OF WORKING WITH CDM

"SBA works in a cloud-focused environment," said Saunders, "and working with the CDM Program Management Office allowed us to explore that to our benefit and address an immediate need we faced. Without this support from CDM, we would have struggled. Instead, we gained additional threat intelligence and an operational boost we needed in the short-term, and for the long-term we have gained foundational improvements that will enhance our systems well into the future."