IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Continuous Diagnostics and Mitigation Program Successes

DEFEND TODAY,
SECURE TOMORROW

CISA: TOOL SECURES PRIVILEGED ACCESS MANAGEMENT

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.

CISA recently deployed an industry-leading privileged access management (PAM) tool as part of its CDM implementation to transition the 30 disparate information systems it managed into a cohesive enterprise-wide approach. With this tool, CISA's security operations team found an effective solution for the results they desired and gained visibility and enhanced security throughout their organization.

THE CHALLENGE

CISA's security visibility had relied on manual data calls and monthly reporting. However, Tommy Doyle, CISA's associate chief of security operations, sought a better way to streamline, automate, and secure monitoring of the 30 systems under his watch.

To address the challenge and meet security requirements from Department and Homeland Security (DHS) and the Office of Management and Budget, Doyle and his team turned to a leading PAM tool that is part of the CDM suite of tools.

> *"I'm a big proponent of automation in IT security, rather than relying on people. Machines don't have good days and bad days."*
>
> **Tommy Doyle**
> **CISA Associate Chief of Security Operations**

This effective tool provides secure access for elevated rights and monitors and records all access continuously. It monitors the entirety of each session and provides threat analysis to prevent unauthorized access of systems. Doyle and his team were the first within DHS to use the tool's sophisticated threat analysis that examines patterns of how users access systems and alerts managers if access is being requested at a time or place that is different than the user's usual behavior.

CDM ASSISTANCE

CISA designed and implemented its cloud network enclave, VENOM, using the highest security principles available. The security operations team incorporated the PAM tool within VENOM to ensure privileged access is secured and not vulnerable to manual mistakes, escalation of privileges, or compromised account access, all of which are hallmarks of most breaches or attacks.

During the summer of 2020, integrators began to build out the design, including the PAM tool, developed documentation, and received authorization to connect to other systems. Penetration testing was conducted in fall 2020, and all tested attempts to breach the system failed. In January 2021, VENOM received authorization to operate.

Rather than add a tool to a legacy network and create centralized control issues, Doyle built the new network enclave from scratch. While a huge challenge, this approach enabled him to establish naming conventions and account standards that improved not just visibility but also standardization and overall posture. This "clean slate" approach required establishing new user accounts, moving out old systems and accounts, and providing a transition period during which trust could be built among all users.

IMMEDIATE IMPACT

Already, CISA is monitoring and recording full video capture of user sessions thanks to the new PAM tool. With a diverse set of administrative users with privileged access, such in-depth monitoring is useful for ongoing security. It also provides additional benefits including data for probable-cause investigations and random auditing, something that other agencies haven't fully realized yet.

As a software-based tool, the PAM tool also provides the agency with more flexibility in the future without the location dependencies inherent in hardware solutions. Installed in VENOM, where all the system's tools are centralized, the PAM tool ties in with the network's other tools that control access and the systems that receive data.

The security team can now also restrict access; monitor where administrators go; and alert, pause and report, or end suspicious behavior. It also can force sessions to terminate at set time lengths to prevent them from remaining open and vulnerable, and force reauthentication during sessions.

Early and immediate benefits from the new tool range from complete visibility to automated reporting. Now the security operations team has accurate, immediate, and automated user data, which has reduced the time required to compile reports by 80%. In the future, Doyle expects to fully automate reports to be issued at set time intervals and no longer require staff to produce them. Automated reporting also has eliminated data discrepancies due to human error, which frees Doyle and his team to focus on reviewing trends and changes in privileged access management metrics. This represents an important shift from simply gathering numbers to determining what they mean on a deeper level.

THE BENEFIT OF WORKING WITH CDM

For Doyle, transitioning to the new system was made much easier by working with CDM. "Beyond the initial investment by CDM in purchasing the licenses, CDM also provided specialists who helped get the software deployed and configured," he said. "They also were very helpful in the initial onboarding of users and developing platforms for different use cases for logins."

While the project required a lot of effort and patience, "it was definitely worth it," said Doyle. "It's better to have this more secure posture and have visibility on those privileged users who have the keys to the kingdom."