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

CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

ASSET MANAGEMENT – What is on the Network?

DEFEND TODAY, SECURE TOMORROW

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures by delivering better visibility and awareness of their networks and defending against cyber adversaries. The CDM Program ultimately reduces the threat surface and improves federal cybersecurity response through four capability areas: Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management.

OVERVIEW OF ASSET MANAGEMENT

The Asset Management capability provides agencies with a centralized overview of their network devices and the risks associated with such devices. Asset Management identifies hardware and software located on or having access to an agency's network. Asset Management enables an agency to maintain and improve its cyber hygiene through five capabilities: Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), Vulnerability Management (VUL), and Enterprise Mobility Management (EMM). Asset Management is the foundation of a strong cybersecurity strategy—it allows agencies to supervise network assets as they are being configured and deployed on the network, which ensures the assets are properly configured and that vulnerabilities have been identified and remediated.

CDM's automated asset management tools have been deployed to federal civilian agencies since 2014. These tools continue to be important today as shadow Information Technology (IT) (i.e., hardware/software that is on the network but is managed outside of, and without the knowledge of, the primary IT department) at agencies continue to expand.

BENEFITS OF ASSET MANAGEMENT

Asset Management identifies hardware and software located on or having access to an agency's network. Once identified, CDM-provided tools validate that the assets are inventoried, while simultaneously scanning the assets for vulnerabilities and configuration weaknesses. Asset Management also assists agencies in creating and maintaining approved device and software inventory lists and keeping software versions updated. This capability allows agencies to comply with their organizational security policies and aids in incident-response activities.

ASSET MANAGEMENT CAPABILITIES

Asset Management is comprised of five distinct capabilities to evaluate what is on the network.

Hardware Asset Management

HWAM finds and records each hardware device and its key attributes using passive and active scanning methods. Additionally, HWAM collects appropriate data to match actual findings to an authorized agency-approved hardware inventory.

Software Asset Management

SWAM finds and records installed software and its key attributes running on each hardware device on the network. It helps identify and report unauthorized software which could be vulnerable and exploited as a pivot to other network assets. Tools within SWAM include software discovery tools, version scanning tools, and license management tools.

Configuration Settings Management

CSM detects, reports, and reduces the misconfiguration of assets on the network through interrogation of devices for compliance against security configuration benchmarks. CSM includes Security Content Automation Protocol (SCAP-) compliant assessment tools for security benchmarks like the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

Vulnerability Management

VUL detects and reports vulnerabilities in assets on the network. This capability is focused on Common Vulnerabilities and Exposures (CVEs) that are listed in the National Vulnerability Database (NVD). The goal of this capability is to help system administrators quickly mitigate these vulnerabilities using tools such as vulnerability scanners.

Enterprise Mobility Management

EMM enables agencies to secure the use of mobile devices within the agency network. This capability enforces the supervision of mobile devices and mobile applications by using Mobile Application Vetting (MAV), Mobile Threat Defense (MTD), and mobile identity management tools.

CURRENT STATE OF CDM ASSET MANAGEMENT DEPLOYMENT

As the first capability deployed, Asset Management has the widest coverage at the agencies participating in CDM. Implementation of all capabilities remains underway and will continue as agencies networks expand and contract based on mission. The program is working with agencies to fill remaining gaps and ensure quality in data reporting. Asset Management will be continuously updated in response to security changes within their organizations.

For more information on Asset Management capabilities and/or the CDM Program, please contact the CDM Program Management Office at CDM@cisa.dhs.gov.