CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

ASSET MANAGEMENT – What is on the Network?

OVERVIEW OF ASSET MANAGEMENT

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. 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.

The Asset Management capability is aimed at providing agencies with a centralized overview of their network devices and the risks associated with such devices. 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 discovers and enables management of hardware on the network. This capability finds and records each hardware device and its key attributes using passive and active scanning methods. Additionally, this capability collects appropriate data to match actual findings to an authorized agency-approved hardware inventory. HWAM is able to gather this information through the use of hardware discovery scanning tools.

Software asset management

SWAM discovers and enables management of software on the network. This capability 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 and reports the misconfiguration of assets on the network. The goal of this capability is to help reduce the misconfiguration of assets 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. These tools allow agencies to adapt their networks to the modern era where mobile devices are crucial and inevitable.

CURRENT STATE OF CDM ASSET MANAGEMENT DEPLOYMENT

Foundational to the CDM Program, Asset Management was the first capability deployed; as such, it has the widest coverage across the agencies participating in the CDM Program. As agencies' networks expand and contract, the CDM Program will continue to work with them to evaluate their Asset Management needs. Given that network assets must be regularly scanned and monitored, Asset Management will be continuously updated in response to security changes within their organizations. Asset Management is reported to the CDM Agency Dashboard (which enables agencies to see all hardware and software assets on their network) and the Federal Dashboard (which provides summary information about assets on agency networks across the Federal Government).

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