Making a Success of CDM

If there is one thing government technology professionals know, it's that no system—no matter how many tools and staff are dedicated to it—is fully secure. Agencies have spent the last two decades working hard to keep up with the changing nature and breadth of cyber-threats, but most acknowledge that it's time for a new approach.

Enter CDM. The Continuous Diagnostics & Mitigation method encourages agencies to approach cybersecurity in a more holistic, automated, measurable, and continuous way. Based on standards from NIST, CDM focuses on providing agencies with comprehensive visibility into assets and activities across the network, the ability to measure all risks, and full accountability of staff to follow plans and policies.

CDM is a deliberate attempt by government to move from the reporting rules of FISMA and the progress made through continuous monitoring to more comprehensive, effective security monitoring and mitigation. Once fully rolled out, all federal agencies will have the tools and processes to protect their networks and infrastructure from cyber-threats.

Even Congress has stressed the importance of CDM as a priority throughout government. The DHS 2015 appropriations bill specifies that part of the $140 billion set aside for the Federal Network Security program should be used "to provide adequate, risk-based and cost-effective cybersecurity to address escalating and rapidly evolving threats to information security, including the acquisition and operation of a continuous monitoring and diagnostics program".

The CDM program will be implemented in three phases. In the first phase, currently in progress, agencies are tasked with satisfying the first four of 15 functional areas: hardware and software asset management, vulnerability management, and configuration-setting compliance. During this phase, agency networks must be scanned at least once every 72 hours for potential attacks or vulnerabilities. Agencies also should install or update their sensors and start performing automated searches for potential vulnerabilities.

CDM makes the difference

Whether it's a security risk to the network, applications, data, an Internet-connected sensor, mobile device with access to network resources or a cloud-based system, CDM controls can make a big difference. They do so by providing a holistic view across the enterprise so you can understand the assets you have, the role of those assets in your organization, and where those risks are arising.

"With that information, you can quickly evaluate potential negative impacts to the organization and make sure you resolve and remediate the most potentially damaging risks first," says Robert Potter, Vice President, US Federal at security, storage and systems management solutions provider Symantec.

The key underlying concept of CDM is to fix the worst problems first, which puts the focus squarely on risk prioritization and management. That means expanding the risk management framework to fully understand critical applications, data sets, personnel and key vulnerabilities. CDM takes that up a notch with real-time monitoring, automation and big data analysis, which allows IT staff to access

From Awareness to Action

CDM isn't a concept that sprouted overnight. Instead, it's the culmination of decades of progress in cybersecurity awareness.

2002
Federal Information Security Management Act (FISMA) is enacted

2007
Department of State initiates the Cyber Security Incident Program (CSIP)

2007
NIST begins working on SCAP (Security Content Automation Protocol)

2008
Department of State launches iPost for automated scanning and continuous monitoring; it is so successful that other agencies begin to take note

2010
OMB issues mandate on continuous monitoring

information and make decisions in real-time.

"If you have visibility into vulnerabilities, patches and activities on the network in real time and can aggregate that information and display it in real time, you can understand the health of the enterprise from a risk management perspective," said Robert Osborn, Chief Technology Officer for Federal at ServiceNow, an enterprise IT cloud company.

Managing risk is the key to successful CDM. Being able to quickly pinpoint behavior or activity inside the network that is inconsistent with your policies or the behavior of the people or devices running on your network is more than half the battle in cybersecurity.

While CDM is just getting off the ground in many agencies, those that have implemented it have already reaped big benefits. The State Department, which led the charge several years ago with the first CDM-type program, reported reductions of up to 90 percent in security risk. A SANS Institute study published in August 2014 found that nearly half experienced better security as a result of the CDM controls.

CDM also has proven to improve security decision-making significantly. A recent MeriTalk study found that at least half of respondents cited improved risk assessment and acceptance, improved decision-making on when to share data with other networks, and better awareness of consequences resulting from the current state of security.

CDM: Step by Step

The Continuous Diagnostics and Mitigation program covers 15 diagnostic capabilities, which will be rolled out in three phases:

Phase 1: Endpoint integrity
- Hardware asset management
- Software asset management
- Configuration settings management
- Vulnerability management

Phase 2: Least privilege and infrastructure integrity
- Access control management (trust in people granted access)
- Security-related behavior management
- Credentials and authentication management
- Privileges
- Boundary protection (network, physical, virtual)

Phase 3: Boundary protection and event management for managing the security lifecycle
- Plan for events
- Respond to events
- Generic audit/monitoring
- Document requirements, policy, etc.
- Quality management
- Risk management

Source: Department of Homeland Security

Making sense of it all

A successful CDM approach requires paying full attention to people, processes and technology. In the technology realm, it involves upgrading or adding to the security capabilities many agencies already have in place. Some of the most important areas are:

Automation: Automation is a critical component of CDM because some threats require response within milliseconds—much faster than a human could respond. By automating as many of the known threats as

CDM promises to take cyber-protection to new heights.

2011
NIST publishes SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

2012
OMB identifies continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority goals

2013
OMB issues memo requiring continuous monitoring of security by the end of FY2017

2014
NIST publishes SP 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations

FY2014
Agencies required to finalize CDM strategies

possible, humans only have to be involved when the activity is unexpected. Automation also is the only practical way to meet the CDM requirement of assessing all network assets every 72 hours. "The challenge of doing something 10 times a month instead of once a month when these agencies are already resource-constrained is completely overwhelming for solutions that don't have a high degree of automation," says Keren Cummins, Director, Federal Sales at Tripwire, a provider of risk-based security, compliance and vulnerability management solutions.

Continuous, real-time monitoring: A wide range of research shows that once an advanced persistent threat enters a network, it can quickly compromise dozens of machines, moving laterally. That makes continuous monitoring critical; by spotting breaches quickly, you have a better chance of containing and eradicating them. Most agencies already stress the importance of continuous monitoring. For example, the Defense Department relies on its Continuous Monitoring and Risk Scoring (CMRS) system to meet this goal.

Big Data analytics: Data today comes from many sources—mobile devices, sensors, email and texts, images, phone logs and more. It's critical to examine each and every piece of data interacting with the network to ensure security. With big data analytics, agencies can gain full visibility into everything in the IT infrastructure, allowing them to quickly connect the dots across different systems and applications. Doing that in real-time translates into a powerful CDM capability.

"It doesn't matter the device, or whether the resource is cloud, physical or virtual; if confidential data is involved, it represents a potential risk to the organization and must be monitored," said Joe Goldberg, Security Evangelist at Splunk, a software platform provider for real-time operational intelligence.

Ensuring that all of these capabilities are included and work together—and as required—is a difficult task. The best way to start is with a verified, tested cybersecurity framework. NIST has provided the baseline with its 800 series publications, which outline the technical controls, best practices and processes agencies need, focusing on risk management and continuous monitoring controls required to handle both advanced persistent threats and insider threats. In developing the framework, NIST included input from the public and private sector as well as SANS Institute, which contributed the 20 critical security controls.

The framework is technology-agnostic, giving agencies the freedom to choose which technologies to employ to meet the framework's goals.

The NIST framework itself is a base on which agencies can build their own CDM programs. The Defense Department has chosen to include its Continuous Monitoring and Risk Scoring (CMRS) system as part of the framework, while DHS has chosen to layer its Continuous Diagnostics and Mitigation program on top of the framework. DHS is the lead agency for the federal government on the CDM effort.

A look ahead

Once agencies are finished implementing Phase I, they must turn their attention to the next two phases. Phase II addresses issues around managing people, from training and credentials to account access and privileges. Phase III focuses on event management and boundary protection, employing technology such as forensics analysis and data loss prevention.

Along the way, threats will continue to change and technologies will continue to mature. One of the fastest-growing vulnerabilities is in the area of the Internet of Things, which involves the data sent from a variety of sensors through networks.

"Think about a military base and all of the people who live on it. If they have sensors for temperature control, refrigerators, televisions and many other things on the military network, you are potentially increasing the IP listing of that base by 30 fold," says Potter. "I don't think we have even begun to see the vast increase in sensors and the risks they could cause. That's something both agencies and vendors have to plan for now."

Strengthening the Security Posture of Government Networks

Carahsoft is pleased to support the government's CDM and cybersecurity initiatives through its partnership with a broad range of technology manufacturers, resellers and system integrators.

Akamai Cloud Security Solutions	AlertEnterprise! Security Convergence Solutions	CORE SECURITY Intelligent Network Visibility Platform	CYBERARK Privileged Account Controls & Monitoring	EMC² Secure On-Premise Storage Infrastructure
ExtraHop Wire Data Analytics Platform for Continuous Monitoring	f5 Application Security Testing & Management	FireEye Cybersecurity and Malware Protection	Gigamon Intelligent Network Visibility Platform	hp Integrated Enterprise Security Solutions
HYTRUST Cloud Under Control Virtualization Security, Compliance & Control	IMPERVA Data Center Security Solutions	Infoblox CONTROL YOUR NETWORK Automated Network Control	invincea Endpoint Security Solution	MarkLogic NoSQL Platform for Cyber Defense & Analysis
mongoDB Cross-Platform Database for Big Data Analytics	pentaho Real-Time Predictive Analytics	redhat SE Secure Linux	RSA Security, Risk & Compliance Management	SafeNet Data Protection & Software Monetization
servicenow Cloud Infrastructure Security Platform	splunk> Operational Intelligence Software	ssh COMMUNICATIONS SECURITY Data-in-Transit Security Solutions	Symantec Monitoring, Remediation & Compliance Reporting	tripwire Security Configuration & Vulnerability Management
Trustwave DbProtect Database Security & Audit Logging	VENAFI Next-Generation Trust Protection	vmware Network Virtualization & Security Platform	Vormetric Data Security Simplified Enterprise Encryption & Key Management	Xceedium Privileged Identity Management Solutions

CDM System Integrator Partners

Booz Allen Hamilton | CGI Federal | Computer Sciences Corporation | Engility Corp. | General Dynamics Information Technology | HP Enterprise Services
IBM | Knowledge Consulting Group | Kratos | Leidos | Lockheed Martin | ManTech | MicroTech | Northrop Grumman | SRA International | Technica

CDM@carahsoft.com carahsoft® carahsoft.com/cdm