Continuous Diagnostics and Mitigation

Intel Security

80% OF EXPLOITS

“80% of exploits leverage known vulnerabilities and configuration management setting weaknesses. Through continuous monitoring, the US State Department cut risk by 89% after 12 months.”[1]

—John Streufert,
Director of Federal Network Resilience, Department of Homeland Security,
Continuous Monitoring: Diagnostics and Mitigation

Efficient Continuous Diagnostics and Mitigation

Challenges

Since the original FISMA, the footprint of IP-enabled devices has increased from millions to an estimated 10 billion in 2014. The number of new threats collected by McAfee Labs has increased to over 225,000 per day. Yet the number of trained practitioners and the budget for information security and privacy tools will not rise to match. Simple math shows that the methods we use to protect the mission must become more efficient. The US Department of Homeland Security (DHS) created the Continuous Diagnostics and Mitigation (CDM) Program specifically to enable practitioners to evolve their existing FISMA practices to do more with less cost and complexity.

Find the right needle in a need stack

CDM requires a shift in security infrastructure—abandoning silos in favor of interconnected systems without forcing a “rip and replace” disruption. Policy, process, system, and data integrations must span organizational, network, and system boundaries. Data collection and analysis, asset discovery and inventory, and risk management processes must happen continually, not periodically, throughout your infrastructure.

The goal is not merely to collect and publish the data. It is to turn data into actionable intelligence. Imagine your information security and privacy efforts in terms of firefighting. You have 10 fires, three buckets of water, and one firefighter. Using CDM, the first bucket of water needs to go where the greatest risk meets the most immediate need.

Constant, reliable, resilient

In the shift to CDM, aggregation and assessment of granular data across data domains become immediate and perpetual. Threat intelligence and multiple data streams—including associated risk calculations—synthesize into automated and human-assisted event analysis and incident response. As new data emerges, the CDM systems learn and adaptively respond—allowing for recalibration of system thresholds and adjustment of network policies.

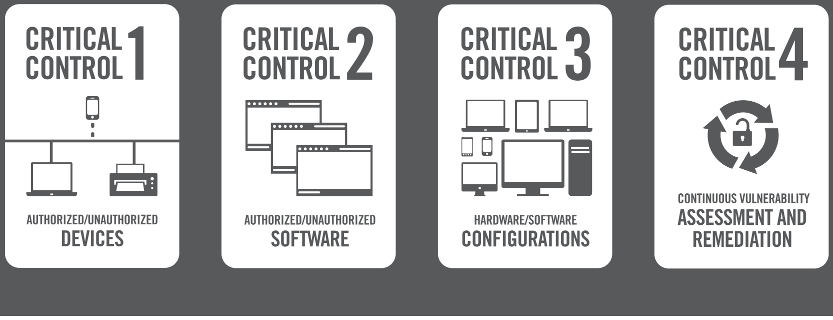
Agile and interoperable

The CDM architecture encourages cooperation between vendors using standards like SCAP, STIX, and TAXII; aggregation and sharing of intelligence; and flexible implementations. Standard interfaces link key functional components and provide ways to plug in global and local threat intelligence. This common, standards-based framework ensures maximum compatibility, agility, and ROI.

The first phase of CDM controls provides a command and control foundation. The second phase of controls builds on this to enhance protection and provide systemic tools for continuous information security risk management. Success requires support for an open, manageable, and unified environment that can span the ultimate set of 15 DHS functional requirements. Few vendors have this breadth of standards support and implementation agility.

Intel Security delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources through stronger protection, superior detection, and rapid correction. Our trusted on-premises and cloud-enabled solutions and services help secure your enterprise against advanced attacks. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. Intel Security is committed to being your number one security partner—providing a complete set of integrated security capabilities.

Download the latest resources at mcafee.com/securityconnected.



Critical Security Controls

With CDM, the government is leading the charge in adopting security best practices. The first phase of CDM maps to the first four of The 20 Critical Security Controls (formerly "SANS Top 20") —Version 4.1.

Solutions

Most organizations have baseline antivirus, operating system and application patching, vulnerability assessment, and patching solutions, along with SCAP-enabled products to evaluate FDCC/USGCB compliance. CDM forces more consistency and rigor into what may be ad hoc product deployments.

The first four functional CDM areas guide organizations to invest in a foundation for visibility and data integration. The primary functions include constant asset discovery and vulnerability management tools; integrated systems that provide for contextual risk-based analytics, intelligence-driven response, and continuous feedback; and command and control center mechanisms. Open interfaces and standard protocols help agencies minimize costs by facilitating integration of these various systems with each other and with existing network infrastructure.

Asset Discovery and Vulnerability Management

Effective asset management combines passive and active discovery with monitoring to detect and profile every system using the network, independent of operating system, device type, or application. Passive scanning monitors traffic to see which devices are alive. Active scanning probes the network to track down idle devices. Combining the two can provide full and constant visibility into network device usage. As soon as a user installs or reconfigures a device on the network, the change is immediately recognized and the device can be re-assessed.

Effective vulnerability management will expose how devices are configured, any vulnerabilities, noncompliance with policies, and any associated risk. Since applications are common targets, this assessment must look up the software stack and across different vectors to see web and database vulnerabilities. As vulnerabilities and threats change, the system should automatically update checks to detect the latest issues and guide improvements.

Perpetual risk management

The systems should then translate this security state assessment into risk calculations that factor in current threat intelligence and other situational context.

By evaluating the criticality of assets, assigning relevant policies, and applying risk-based assessment, the systems choose appropriate responses. Where possible, a system acts nearly instantaneously, such as with a host quarantine, leaving a verifiable audit trail. Where necessary, a system triggers human intervention or investigation. Fixes like a new software .DAT or patch deploy automatically to remediate devices—at machine speed.

This ongoing risk-informed process correlates all the data collected on assets and associated vulnerabilities with live intelligence feeds, such as vulnerability research communities, the NIST National Vulnerability Database (NVD), and US CERT alerts. Two other factors come into play: the affiliated countermeasures that could nullify an identified threat or vulnerability and the mission value of the asset at stake. The optimum risk-based response to each incident should be based on that asset's threat assessment and potential loss impact on the organization's mission.

Instant information

Many indicators of compromise leave a small footprint, so yesterday's methods of looking for system state and health are ineffective. Through the addition of instant query, response, and remediation tools, up-to-date threat intelligence, effective policy controls, and constant feedback and response, a CDM program saves government resources and reduces the chance of a disruptive network event.

Best Practices Considerations

- Compliance with and reporting against standards like NIST 800-53, DISA STIG, USGCB/FDCC, CyberScope, and FISMA.
- Validated support for the current versions of the protocols within Standard Content Adaptation Protocol (SCAP), including XCCDF, OVAL, and CPE.
- FIPS 140-2, Common Criteria, USGv6, HSPD-12, and Section 508 VPAT certifications.
- Plug-and-play interoperability among task management, agent-based and agentless collection sensors, databases, presentation/reporting systems, and risk analytics systems.
- Flexible automation that streamlines workflows across these subsystems and helps guide systemic and human-assisted incident response.
- Open APIs and SDKs to extend risk-based scoring mechanisms and data to enterprise and coalition partners and support multitier networks.
- Immediate and around-the-clock threat and vulnerability feeds that drive dynamic vulnerability and risk assessment and make the CDM system more intelligent and responsive.
- Capacity to handle the speed, scope, and scale of expanding security data feeds and reporting requirements.

Continuous feedback

A command and control center based on security and information event management (SIEM) oversees all these processes in a continual improvement loop. With integrated systems acting at machine speed to analyze, assess, and take action against the bulk of events, staff can focus on potentially high-impact threats; fine-tuning policies, processes, and controls based on results; and investigating anomalous events. Flexible dashboards display information, automate workflows, and facilitate communication. The larger and more distributed the team, the greater the operational value from an accurate, contextual assessment of risk and a centralized management system that can continuously scale, adapt, and address evolving threats and vulnerabilities.

CDM provides ongoing feedback and greatly reduces the time to make a risk assessment, and—even more important—act on the findings without having a negative effect on the mission. This leap forward allows the organization's CDM system to become the core of an effective, measurable, and sustainable mission risk manager.

Value Drivers

Solutions for continuous diagnostics and mitigation need to incorporate security and compliance controls, and they also need to reduce complexity and costs. These solutions should:

- Minimize integration and maintenance costs through support for open standards, open platforms, and existing technologies.
- Reduce administrative staff, helpdesk calls, audit costs, errors, and manual compliance tasks.
- Improve detection, increase the frequency with which attacks are thwarted, and reduce the volume and impact of suspected incidents that must be responded to, investigated, and managed.
- Improve resilience through feedback loops incorporating state-of-the-art monitoring, detection, and prompt remediation.
- Enhance flexibility to respond to economic, political, and technological requirements.
- Deliver an efficient IT architecture that reduces platform hardware and software acquisition costs, power and HVAC consumption, and rack and floor space utilization.

For more information about Security Connected, visit: www.mcafee.com/securityconnected.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

[1] http://scap.nist.gov/events/2012/itsac/presentations/day2/4Oct_11am_Streufert.pdf