REDSEAL

CONTINUOUS DIAGNOSTICS

BEGINS WITH REDSEAL

THE MEASURE OF RESILIENCE

WHAT IS CDM?

The continuous stream of high profile cybersecurity breaches demonstrates the need to move beyond purely periodic, compliance-based approaches to IT security. Static onstructs such as "defense in depth" continue to be relevant, but can't completely stop attack penetrations. Additional controls are needed. Organizations must implement processes that monitor their security posture and remediate risks on a continuous basis. Meeting this requirement is the goal of the Continuous Diagnostics and Mitigation (CDM) program.

The DHS states that the CDM program "is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first." The CDM blanket purchase agreement is administered by the GSA and is open to federal, state, and local entities.

CDM covers a total of 15 diagnostic capabilities, organized into three phases. Phase 1 went into effect in 2013 and focused on endpoint hardening and vulnerability management. Phase 2 includes access controls and boundary protection and is expected to take effect in 2015. Phase 3 will focus on event management (cyber-attack detection and response).

The principle of continuous diagnostics is simple enough. By assessing the state of essential information security controls across the enterprise on an ongoing basis, agencies can proactively manage risk by ensuring that their cyber defenses are in place and up-todate. Automated tools can go a long way toward simplifying the process of collecting and analyzing security data while providing security officials with near-real-time information on their security posture.

CONTINUOUS DIAGNOSTICS BEGINS WITH REDSEAL

Continuous diagnostics of computing and network assets requires up-to-date knowledge of the security posture of every workstation, server and network device — including operating system and application versions and patches, vulnerabilities, and threat signatures and patterns. Information security managers will use the summary and detailed information to manage and report the security posture of their respective agencies. While each agency is required to implement continuous diagnostics, they are not required to implement a "one size fits all" solution. Each agency can implement the continuous diagnostics solution that best fits its own requirements and environment as long as its solution provides the required monthly data to the DHS repository known as CyberScope. Defense and intelligence agencies will have to provide their required security data to the Defense Department and intelligence community versions of CyberScope.

CDM GUIDING PRINCIPLES

1. Real time intelligence, context and optimal risk posture— The goal of CDM is a system that continuously visualizes critical attack risk and non-compliance in complex security infrastructures. Fundamentally, this will be achieved via real-time asset discovery and vulnerability management, intelligence-driven response, and continuous feedback to meet changing federal requirements. Open interfaces and standard protocols will help agencies integrate new and legacy systems at minimal cost. Key steps include collecting data from ongoing processes, correlating against multiple contextual factors, taking action where appropriate, and presenting the remaining issues in priority order. Lastly, prioritizing is important, so the most important and at-risk assets receive the most immediate and significant attention.

2. Automation and scalability — Automated continuous diagnostics solutions enable agencies and missions to monitor IT controls effectively and in near real time. Manual processes that involve a human dimension will not deliver the level of in-depth visibility and control IT departments need to support effective operations, and will not scale. Automated continuous diagnostics is a better approach. It can more efficiently and effectively:

a. Discover risky assets in the IT infrastructure.

b. Validate actual changes to the IT infrastructure against planned change requests.

c. dentify changes that occur without an approval.

d. Enforce policies that limit unauthorized access in the IT infrastructure.

e. Provide reports on IT infrastructure policies to highlight best practices and control violations.

3. From static and periodic to ongoing authorization — CDM transforms historically static and paper-based security control assessment and authorization process into an integral part of a dynamic risk management process. It will deliver near-real-time awareness and assessment of information security risk to support organizational risk management decisions. Most agencies have basic capabilities such as antivirus updates, operating system, and application patching assessment. CDM and DHS's Continuous Asset Evaluation expands the focus of security efforts from point compliance to an ecosystem of dynamic resilience – as you detect, you report, and take action in real-time.

CONTINUOUS DIAGNOSTICS BEGINS WITH REDSEAL

4. FISMA compliance via mission assurance — A strategically and well thought out continuous diagnostics program conserves government resources, delivers cyber situational awareness and reduces the chance of network disruption. Agencies collectively spend billions of dollars to manually monitor and report on information security programs. In the face of budget constraints and ever increasing threats, to comply with FISMA, agencies need to turn to continuous diagnostics solutions. A comprehensive approach via CDM is needed to enable agencies to monitor their entire IT environment continuously, remediate those items out of compliance, and report on compliance with federal requirements. CDM is not a FISMA replacement. Continuous diagnostics will be the single most important support for certification and authorization by providing deeper information that can be analyzed and measured over time. The trend information will be important for compliance and for overall improvements in operations, security and risk posture. Direct correlation of infrastructure performance translates to better FISMA scores. The goal is to provide network, security and risk management teams with a firm understanding of where security is working, where investment is needed, and where greatest cyber-attack risks lie. This understanding, or "security intelligence", enables organizations to allocate resources where needed most, embed best practice into daily operations, and take prioritized action when needed.

REDSEAL AND FEDERAL GOVERNMENT CYBERSECURITY

RedSeal has a history of support for federal government cybersecurity initiatives. The company's innovative software solution is installed in numerous defense, intelligence, and civilian organizations for the purpose of continuous monitoring. At the highest level, RedSeal delivers three core security controls:

- Visibility: Automated network mapping and situational awareness
- Verification: Continuous comparison of network security architecture against desired posture
- Prioritization: Analysis of vulnerability scan data and network architecture to identify the highest risk vulnerabilities that must be remediated immediately

These controls apply to both legacy deployments and new architectures. In legacy situations, RedSeal allows you to understand the existing environment and identify security control gaps. In new architectures, RedSeal validates that the network is built and operated as designed. And in all situations, RedSeal vastly increases the value of scanning and penetration testing by prioritizing those vulnerabilities that are the most dangerous cybersecurity threats.

REDSEAL SUPPORT FOR CDM

RedSeal support for CDM is focused in five of the 15 CDM diagnostics capabilities:

Hardware Asset Management: RedSeal's complete network map and network device inventory provides a framework for hardware inventory processes and discovery. The solution also provides a complete inventory of in-scope Layer 2 and Layer 3 network devices.

Configuration Settings Management: RedSeal automatically analyzes individual device configurations for compliance with best practices and baselines. The system includes over 100 out-of-the-box configuration checks for firewalls, routers, load balancers, and wireless controllers. Examples of configuration checks include password policies, services enabled, logical port configuration, and networking parameters. Custom checks are also easily defined, and deviations from baselines are identified automatically.

CONTINUOUS DIAGNOSTICS BEGINS WITH REDSEAL

Vulnerability Management: At the highest level, vulnerability management consists of two tasks: vulnerability scanning and remediation. RedSeal's contribution to the process is its unique ability to prioritize remediation by identifying the vulnerabilities that pose the highest risk. RedSeal combines results from all the top scanners (Qualys, Nessus, Rapid7, etc.) with its detailed knowledge of network path connectivity to prioritize the specific systems and vulnerabilities that could be used to do the most damage if they were exploited. Without this, organizations waste huge amounts of time remediating "high priority" vulnerabilities that could wait, because the potential damage from an exploit is very limited. And they ignore "low priority" vulnerabilities that are actually dangerous because they can be used to pivot into higher value targets in a network. RedSeal can quickly analyze the exposure of vulnerabilities discovered by the scanners and priority them based on potential feasibility, probability and severity of the exploits, thus providing users a clear prioritized list of end point vulnerabilities to remediate.

Boundary Protection: Effective boundary protections are typically based on network architecture and access policies on routers, switches and firewalls. These policies are designed around the concept of least privilege access across the boundary, and often include additional requirements such as the mandatory insertion of an intermediate system ("jumpbox") for access across the boundary. In practice, it is extremely difficult to operationalize this control, especially in multi-vendor environments. However RedSeal's most powerful capability is to analyze networks continuously and evaluate possible connectivity against desired policy. This enables even the largest organizations to implement boundary protections on multi-vendor networks in an operationally efficient manner. And this, in turn, makes it realistic to implement multi-layer segmentation policies, where assets can be isolated from the rest of the internal network to better protect sensitive data, and limit the ability of malware to spread after initial compromise.

Respond to Events: Many information sources and technical disciplines must work in concert for effective incident response. One fundamental input to the process is network topology and reachability information, as this informs the determination of how significant the risk from the event is, and what systems may be at risk. Normally this is a manual and time consuming process, relying on static information and network maps that are often out of date, and staff combing through configurations to piece together the potential malware exploit paths. This delays the ability of the organization to respond appropriately to the event, increasing both risk and the eventual overall cost of response. However this entire network analysis process is completely automated by RedSeal. Incident response teams quickly get accurate information about network exploitation path so they can respond faster and with much more focus.

REDSEAL ECOSYSTEM INTEGRATION

RedSeal's ability to deliver visibility, verification, and prioritization is driven by its industry leading integration with its network and security ecosystem. RedSeal's ecosystem can be segmented into three categories: Infrastructure, Scanners, and SIEMs.

- Infrastructure: Support for over infrastructure 15 vendors and hundreds of products, including firewalls, routers, switches, and load balancers. Support for Amazon Web Services (AWS) and VMware infrastructure, allowing hybrid clouds to be secured just as easily as traditional on premises networks.
- Vulnerability Scanners: RedSeal combines network intelligence with scan results from all the leading scanning vendors, including Qualys, McAfee, Tripwire/nCircle, Rapid7, Nessus and Symantec. This broad support not only guarantees that RedSeal prioritizes scan results and scanning patterns, but it allows organizations to adopt a multi-vendor scanner strategy with no loss of effectiveness.

CONTINUOUS DIAGNOSTICS BEGINS WITH REDSEAL

- SIEM/Log Management: Integration with the leading event correlation (SIEM) and log management systems including Splunk and HP ArcSight to deliver actionable intelligence that helps "connect the dots" and drive effective threat detection and responses.

SUMMARY

The federal government's Continuous Diagnostics and Mitigation (CDM) program attempts to confront today's cybersecurity reality. By encouraging organizations to rely less on audits of static preventive measures and instead implement CDM, the program better positions organizations to be much more aggressive in ensuring their defenses are well established at all times. The program also encourages agencies to put in place procedures to detect, evaluate, and respond to incidents, no matter when they occur. RedSeal provides a substantial contribution to the CDM framework by delivering a unique control set for boundary protection, situational awareness, vulnerability mitigation prioritization, and configuration management. And because CDM requires multiple solutions working in concert, RedSeal's wide range of integrations with dozens of security and network vendors makes it much easier to deploy an operationally efficient CDM strategy.

ABOUT REDSEAL (redseal.net)

RedSeal provides a cybersecurity analytics platform to Global 2000 organizations that certifies their evolving networks are secure and accelerates compliance initiatives. RedSeal's advanced analytics engine creates functioning network models, tests networks to identify security risks, prioritizes needed actions, and provides critical information to quickly remediate issues. The result: reduced cybersecurity risk and lower incident response and maintenance costs. With operations in North America, Europe, and Asia, RedSeal customers include leaders in finance, retail, technology, utilities, service providers, and government, all served by RedSeal's channel partner network.

REDSEAL

1600 Technology Drive, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net

AUGUST 2019