REDSEAL

REDSEAL AND DHS CDM DEFEND

Government cybersecurity now includes the DHS CDM DEFEND program and task orders being announced by various federal departments. The DHS CDM DEFEND, which stands for Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense, task orders are awarded under the General Services Administration's Alliant 1 Unrestricted contract. GSA and the Department of Homeland Security (DHS) jointly run CDM to secure civilian agency ".gov" networks from cyber attacks.

RedSeal and Government Cybersecurity

RedSeal has a history of support for federal government cybersecurity initiatives. The company's network modeling and risk scoring platform is installed in numerous defense, intelligence, and civilian organizations for 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 deployments, 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 increases the value of scanning and penetration testing by prioritizing those vulnerabilities that are the most dangerous cybersecurity threats—based on how each network is put together.

The objective of the DHS CDM DEFEND program is to discover, assess and plan for 100% agency network coverage and provide context for prioritizing the closure of coverage gaps. Winners of task orders must discover all networked assets in an agency—including perimeter, cloud and mobile environments. Plus, they must develop a plan to protect all environments within six months of work commencing, and on a continuous basis after implementation. What's more, merely visualizing what's on the network isn't enough, but vendors must prioritize fixing the worst problems first.

REDSEAL AND DHS CDM DEFEND

RedSeal and DHS CDM DEFEND Solution Requirements

RedSeal supports six of the eight DHS CDM DEFEND solution requirements.

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 to see if they are secure. This includes password policies for firewalls, routers, load balancers, and wireless controllers, services enabled, logical port configurations, and networking parameters. You can also create custom checks and be notified automatically about any deviations from baselines.

Vulnerability Management: At the highest level, vulnerability management consists of two tasks: vulnerability scanning and remediation. RedSeal can determine if you have any gaps in your vulnerability scan coverage and identify the device blocking it. In addition, RedSeal has a unique ability to prioritize remediation by identifying the vulnerabilities that pose the highest risk—in each network. RedSeal combines results from top scanners (such as Rapid7 InsightVM, Tenable Nessus, and Qualys) and centralizes scoring and prioritization. Then, it overlays its detailed knowledge of all network paths 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.

Boundary Protection: Effective boundary protections are typically based on network architecture and access policies on routers, switches and firewalls. In practice, it is extremely difficult to operationalize this control, especially in multi-vendor environments. However, RedSeal Is able 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.

Incident Response: Many information sources and technical disciplines must work in concert for effective incident response. Once an indicator of compromise is identified by a SIEM, RedSeal brings network topology and reachability information to help determine how significant the risk is and what systems may be at risk. Normally this is a manual and time-consuming process, relying on traceroutes and network maps that are often out of date. Staff must comb through configurations to piece together the potential malware exploit paths. This delays an organization's ability to respond appropriately to the event, increasing both risk and the eventual overall damage. RedSeal automates this entire network investigation process, providing incident response teams with accurate information about network exploitation paths so their response can be quicker and more focused.

REDSEAL AND DHS CDM DEFEND

	REDSEAL CAPABILITIES				
CDM DEFEND Requirements	**Hardware**	**Config**	**Vuln Mgmt**	**Boundary**	**Response**
Rapid Assessment	Yes	Yes	Yes		
Boundary Architecture Changes	Yes	Yes		Yes	Yes
Evaluate multiple CDM states		Yes			
Vuln Mgmt and Triage	Yes	Yes	Yes	Yes	Yes
Change Control & L2/L3 Auditing	Yes	Yes	Yes		Yes
Incident Response	Yes	Yes	Yes		Yes

Summary

The federal government's DHS CDM DEFEND program is a response to today's cybersecurity reality. By encouraging organizations to rely less on auditing static preventive measures but instead on implementing CDM, the program better positions agencies to ensure 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.