Lumeta

SOLUTION BRIEF

Lumeta for DHS Continuous Diagnostics and Mitigation (CDM)

DHS CDM Overview

The increasing number of cyber attacks on Federal, State and Local government networks are growing more sophisticated, aggressive, and dynamic every year. Government computer networks and systems contain information on national security, law enforcement, and other sensitive data, including information about federal employees and others.

To address these threats the Department of Homeland Security (DHS) created the Continuous Diagnostics and Mitigation program (CDM, also known as "Continuous Monitoring") to fortify the cybersecurity of computer networks and systems.

The CDM program provides capabilities and tools that enable network administrators to know the state of their respective networks at any given time, understand the relative risks and threats, and help system personnel to identify and mitigate flaws at near-network speed.

The Department of Homeland Security works with technology partners, across all government and civilian departments and agencies, to deploy and maintain an array of sensors for hardware asset management, software asset management, configuration management and vulnerability management, and feed data about an agency's cybersecurity flaws and present those risks in an automated and continuously-updated dashboard.

Summary

Lumeta offers significant advantages to organizations seeking to address the DHS CDM program that involves the implementation of Critical Controls 1, 4 & 5 of the SANS Twenty Critical Security Controls for Effective Cyber Defense.

- Functional Area 1 – Hardware Asset Management
- Functional Area 4 – Vulnerability Management
- Functional Area 5 – Network Access Controls

The benefits from this technology also overreaches into other tools areas such as Functional Area 2 – Software Asset Management, with Lumeta's ability to discover unknown devices enabling other tools to be pointed at them for software asset management.

Historically, when Lumeta technology is introduced into an organization's network infrastructure (regardless of the other cybersecurity tools having been deployed), it discovers up to 20% 'more' – more network segments, more connections, and more devices than the organization was even aware of.

*Continuous Diagnostics and Mitigation Process**

*[*source: http://www.dhs.gov/cdm]*

Continuous Monitoring with Lumeta IPsonar & Lumeta ESI

With Lumeta IPsonar & Lumeta ESI (Enterprise Situational Intelligence) government and civilian department and agencies can attain a real-time, dynamic view of their network infrastructure.

- **Lumeta IPsonar** actively scans the network, on-demand; to collect all data related to Network, Host, Leak Path, and Device Discovery. Users can accurately visualize what is on the network, drill down to analyze potential areas of risk, and identify appropriate corrective actions.

- **Lumeta ESI**, running in a real-time, automated mode, delivers next-generation network discovery, leak path detection, visualization and analytics to provide full network visibility. Lumeta ESI is for organizations that want to achieve continuous situational awareness and monitor for network change and network vulnerabilities.

Highlights:

Lumeta IPsonar	Lumeta ESI
Discover the Network	
Lumeta IPsonar identifies and measures relationships between known and previously unknown network assets, including connections, routers, and firewalls.	Lumeta ESI maps the entire enterprise, discovers all networks and connections – including previously "unknown" portions of the network – and defines the network perimeter, partner connections, and cloud connectivity.
Discover the Hosts	
Lumeta IPsonar reveals all network addresses, helping IT executives align areas of visibility with areas of responsibility.	Lumeta ESI takes a census of all active devices (including IPv6 enabled network devices) attached to the network and finds "stealthy" devices.
Profile Devices	
Lumeta IPsonar provides rich data on all networked devices, delivering uniquely comprehensive data set on all devices at the network and transport levels, in addition to providing application-layer visibility.	Lumeta ESI identifies the types of devices connected to the enterprise, highlighting those devices that fall outside of policy or are considered "rogue" in nature.
Discover Network Leak Paths	
Lumeta IPsonar is crucial in the proactive fight against leaks, revealing all unauthorized connections and identifying whether access is outbound, inbound, or both.	Lumeta ESI reveals connectivity between networks (business units, partners, spin-offs, secure zones, etc.), or the corporate enterprise and the Internet. Through this intelligence IT professionals can determine whether the connectivity is authorized, or if proper security controls are in place.

Integration with CDM Tool Vendors

The Systems Integrators awarded a role on the CDM program have included a number of state-of-the-art cybersecurity tools into their offerings. Lumeta's technology aligns directly with and extends the vulnerability and management capabilities of these tools. Lumeta's technology is unique in its ability to discover and document the true boundary of the network, ensuring that enterprise network defenses are properly placed, and a full, complete 'picture' of the network exists.

For example:

- Visibility into devices or assets that are not currently under management
- Retrieving discovery-like data from agents running on deployed devices
- Endpoint protection
- Additional vulnerabilities at the perimeter of the network

With a bi-directional open API, and configurable custom attributes, Lumeta provides users the ability to seamlessly integrate active network discovery data into existing IT and security lifecycle, leveraging Lumeta's network discovery reporting and powerful network mapping engines as a front end to operational network visualization.

Lumeta fully integrates its data into third-party applications and dashboards, providing organizations with the information needed to ensure complete network availability, security, and compliance. Lumeta IPsonar & Lumeta ESI's open API is designed to enable integration with any application and the solution's network discovery results are fully extensible to a range of third-party solutions and easily translated into actionable information.

Lumeta Corporation | 300 Atrium Drive, Suite 302 | Somerset, NJ 08873 USA | +1.732.357.3500 | www.lumeta.com