OPERATIONAL INTELLIGENCE

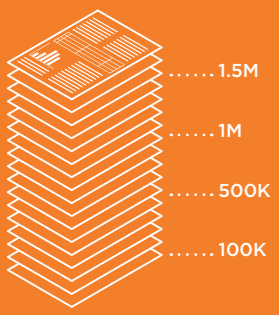
ACHIEVING MISSION SUCCESS THROUGH CDM

splunk>

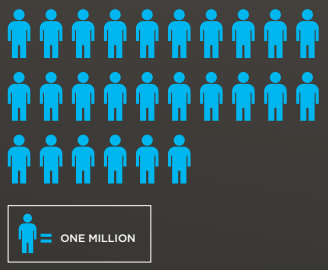
GOVERNMENT IS AN INVITING TARGET

Government systems are a trove of valuable information, and in 2014 and 2015 alone suffered major security breaches and compromised data, including:

Over **1.7 million** records at the Internal Revenue Service

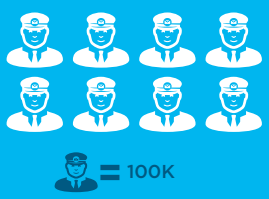


Some **26 million** government employee files at the Office of Personnel Management



Background check records of **25,000** Department Homeland Security investigators

The personal information of **800,000** US Postal Service employees



CYBERSECURITY: A TOP PRIORITY

The mission is identified (by the President) as one of the most serious economic and national security challenges we face as a nation.

THE PROBLEM IS POOR OVERALL SECURITY

The Office of Management and Budget has identified five "persistent weaknesses" at federal agencies:

1. In limiting, preventing and detecting inappropriate access to computers
2. Managing software/ hardware configurations
3. Making sure system access is not limited to just one person
4. Planning for disruptions in IT service and access
5. Implementing critical agency-wide security management programs

WHERE THE DHS CDM PROGRAM FITS

Government security is inconsistently applied, and depends on reacting to increasingly sophisticated threats. The Continuous Diagnostic and Mitigation (CDM) program will provide federal departments and agencies with a forward-looking, holistic view of their security, so they can prioritize risks and remediation.

It has three phases, each employing commercial off-the-shelf tools:

1 

Endpoint Integrity, focusing on the identification and management of local hardware and software assets, and on device configuration management

2 

Least Privilege and Infrastructure Integrity, focused more on people and managing their network access privileges, along with managing network infrastructure devices and services

3 

Boundary Protection and Event Management, which encompasses event detection and response, encryption, remote access management and access control.

THE GOAL? SUPERIOR OPERATIONAL INTELLIGENCE

You can't protect assets if you don't know how many you have and where they are. You can't identity threats and mitigate the problems caused by them if you don't have enterprise-wide visibility of networks and systems. In today's fast-moving cybersecurity environment, you also need that intelligence at your fingertips at all times.

For all of that, you need a platform that:

- Scales rapidly according to demand
- Collects and collates machine data from all available sources
- Analyzes that data in real-time

Only with that kind of resource can government CIOs and CISOs know they have the capability to protect networks and systems, detect and deal with intrusions, and quickly mitigate any potential damage thereby ensuring the agency mission can succeed.

CDM IS KEY TO BETTER INTELLIGENCE

The intent for CDM is to take the current fragmented approach to security, which leaves many unknown vulnerabilities that attackers can use, and instead provide a holistic view of an organization's security that allows for a knowledge-based, coordinated response to incidents.

To provide for that, CDM needs a solution that:

1 Integrates all point systems across all technology platforms, enabling real-time collection, indexing and correlation of any text-based data source without the constraints imposed by a backend database.

2 Aggregates machine data such as server and security events, network device logs, configuration data, and the activity of credentialed and authorized users, delivering new CDM capabilities and enhancing existing CDM.

3 Addresses emerging requirements with analytical/intelligence capabilities — provides, in real-time, indexing and search that can't be generated using traditional databases, a quick identification of trends, and the ability for root cause analysis that isn't possible with legacy relational database technology.

HOW SPLUNK FITS WITH THE DHS PROGRAM

splunk>

PHASE 1

Splunk Enterprise will help government departments and agencies to create a Master Device Record (MDR) by compiling data from their various hardware, software and configuration management tools and, along with vulnerability management data, integrate that into a single view of network and endpoint activities and behaviors.

That addresses all four of the functional requirements of this phase:

1. Hardware Asset Management
2. Software Asset Management
3. Configuration Settings Management
4. Vulnerability Management

PHASE 2

Splunk's technology will enable creation of a Master User Record (MUR) that will include all agency user identities and what level of access they have to networks and systems, if users have the appropriate level of security training for their access level, which credentials are issued to users and when, and whether users have the right access needed to do their jobs.

This addresses all four requirements for this phase:

1. Trust accorded to users
2. Behavior of users
3. Credentials assigned to users
4. Access rights granted to users

ADDITIONALLY Splunk's platform can be used to eventually integrate tools used in both Phase 1 and 2.

PHASE 3

Splunk will build a Master Systems Record (MSR) that will combine all of the device, endpoint and user data collected in previous phases of the program, with the goal of determining what happens when security events occur by focusing on such things as Internet response and anomaly detection.

The protection requirements for this phase will likely be divided into four sub-phases:

1. Boundary Protection
2. Security Event Management
3. Audit Monitoring
4. Risk Management

By the end of Phase 3, federal civilian departments and agencies will have a MDR, MUR and MSR all within the Splunk platform, correlating endpoint, user and event data across the entire enterprise.

THE END GOAL FOR CDM

Once the CDM Program is implemented across government, there will be a comprehensive, largely automated and continuous infrastructure in place to inform departments and agencies of their real-time risk from cybersecurity threats.

In particular, it will:

splunk>

For more information on how Splunk meets the needs of the federal government's CDM program, please visit **www.splunk.com/cdm**