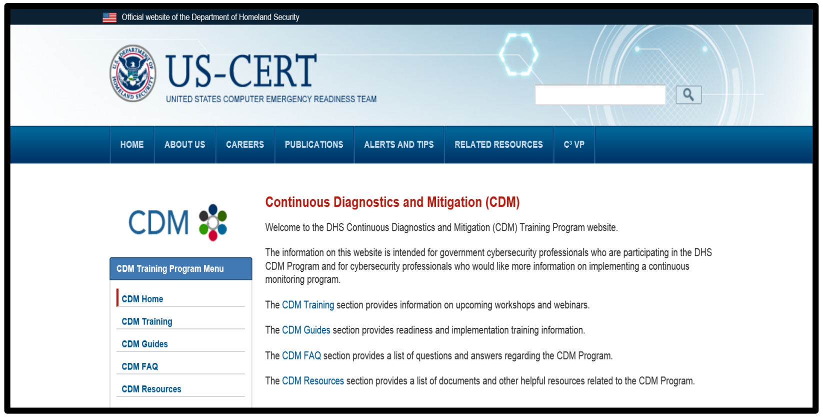
The CDM Learning Community Event (LCE) will begin at 12:00PM EST

Welcome to the ISCM Foundations: Understanding CDM's CSM Security Capability LCE

While you wait, check out:



Continuous Diagnostics and Mitigation (CDM)

Welcome to the DHS Continuous Diagnostics and Mitigation (CDM) Training Program website.

The information on this website is intended for government cybersecurity professionals who are participating in the DHS CDM Program and for cybersecurity professionals who would like more information on implementing a continuous monitoring program.

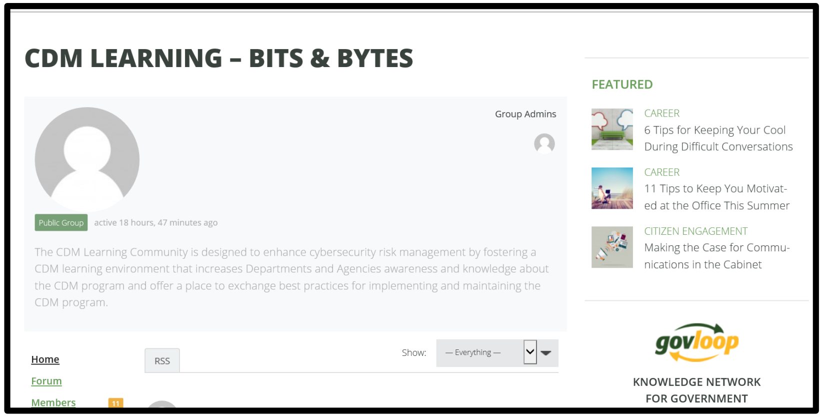
The CDM Training section provides information on upcoming workshops and webinars.

The CDM Guides section provides readiness and implementation training information.

The CDM FAQ section provides a list of questions and answers regarding the CDM Program.

The CDM Resources section provides a list of documents and other helpful resources related to the CDM Program.

Our CDM Homepage



CDM LEARNING – BITS & BYTES

active 18 hours, 47 minutes ago

The CDM Learning Community is designed to enhance cybersecurity risk management by fostering a CDM learning environment that increases Departments and Agencies awareness and knowledge about the CDM program and offer a place to exchange best practices for implementing and maintaining the CDM program.

FEATURED

CAREER
6 Tips for Keeping Your Cool During Difficult Conversations

CAREER
11 Tips to Keep You Motivated at the Office This Summer

CITIZEN ENGAGEMENT
Making the Case for Communications in the Cabinet

Our CDM Bits and Bytes Blog

Have a topic suggestion for a future LCE? Please send it to cdmlearning@hq.dhs.gov

Homeland Security

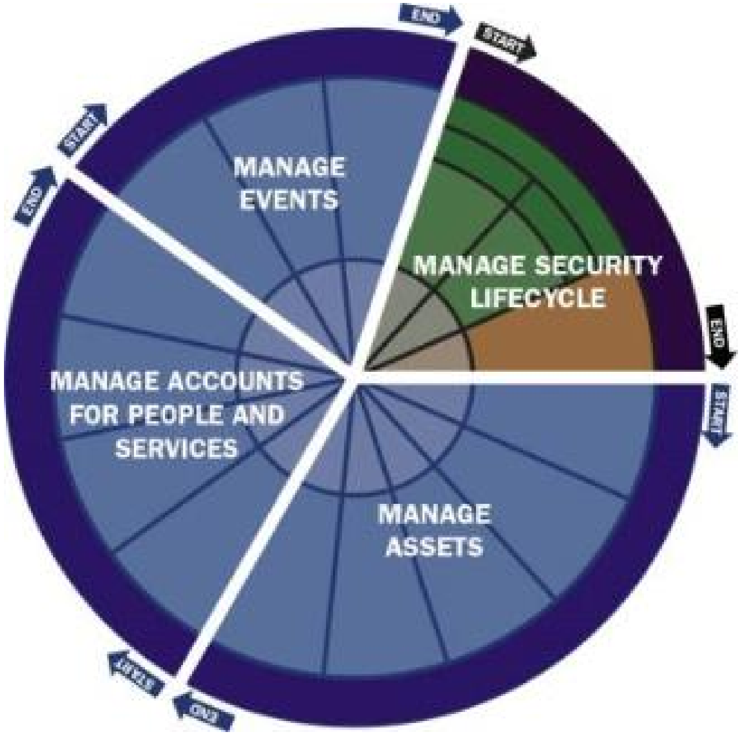
Federal Network Resilience

Homeland Security

ISCM Foundations: Understanding CDM's CSM Security Capability

August 18, 2016
12:00 pm – 1:00 pm

A CDM Learning Community Event



END
START
START
END
MANAGE EVENTS
MANAGE SECURITY LIFECYCLE
END
START
MANAGE ACCOUNTS FOR PEOPLE AND SERVICES
MANAGE ASSETS
START
END

CDM Learning Community - Roadmap

Moving Forward

	Apr-16	May-16	Jun-16	August-16	Sep-16
Webinar	CDM Readiness: Cover your Assets	Moving Forward: Automating Hardware Asset Management	Moving Forward: Automating Software Asset Management	ISCM Foundations: Understanding CDM's CSM Security Capability	Moving Forward: Automating Vulnerability Management
LCE	Federal Network Resilience: Impacting Cybersecurity through Agency Engagement	Automating Hardware Asset Management: Notes from the Field	Automating Software Asset Management: Notes from the Field		Automating Vulnerability Management: Notes from the Field

https://www.us-cert.gov/cdm/training

Event Goal

Discuss automating assessments of configuration settings management and share best practices for better risk management decision making.

Today’s Agenda

- ISCM Foundations
- Configuration Settings Management (CSM) Key Principles
- CSM Practices
- Questions and Answers
- Closing remarks

Today's Speaker

Jim Wiggins

- Cybersecurity Trainer and Information Security Practitioner
- 18 of experience in IT
- 14 of experience in IT security
- 2010 FISSEA "Educator of the Year Award"

ISCM and CSM

What is ISCM?

“Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

Source: NIST SP 800-137

How does ISCM relate to CSM (and CDM)?

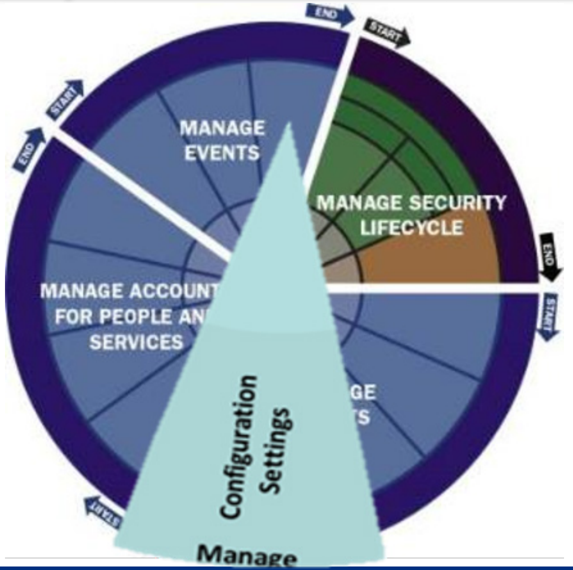
“A key goal of ISCM is to make hardware assets harder to exploit through hardware asset management, software asset management, **secure configuration management**, and vulnerability management.”

Source: FY15 FISMA Metrics Report

What is Configuration Settings Management (CSM)?

Definition

CSM identifies configuration settings on IT assets including hardware devices (both physical and virtual) and software that are likely to be used by attackers to compromise a device and use it as a platform from which to further compromise the network.



Key Concepts

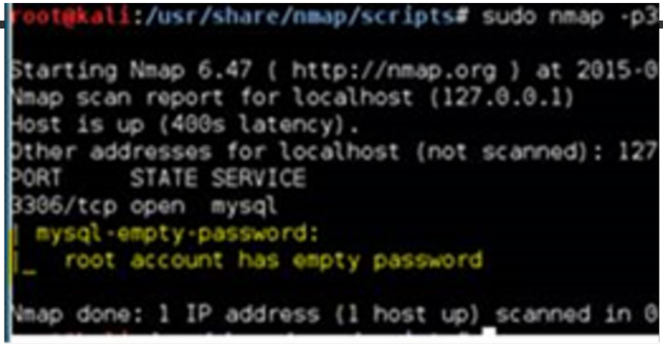
Why is it important?
Improperly configured devices result in weaknesses that can be exploited by attackers. Also, settings are often used as a means to support other capabilities, such a blocking certain software, and/or granting/denying privilege(s).

Scope
Configuration settings are inputs to a software or hardware asset that provide some control on the functionality and behavior of the product.

Differentiation
A configuration setting is a metadata about a software or a hardware asset that determines how it functions during runtime. The value can be changed by an administrator (with proper permissions), and is not hard coded in the product itself; so it can be set during installation or subsequent startups, and can be adjusted with the proper permissions.

Why employ CSM?

1 Attackers attempt to exploit software or hardware with weak or insecure configurations.



```
root@kali:/usr/share/nmap/scripts# sudo nmap -p3

Starting Nmap 6.47 ( http://nmap.org ) at 2015-0
Nmap scan report for localhost (127.0.0.1)
Host is up (400s latency).
Other addresses for localhost (not scanned): 127
PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_  root account has empty password

Nmap done: 1 IP address (1 host up) scanned in 0
```

Server / Workstation / Network Device

Misconfiguration / Weak or Unknown Configuration

2 Once configuration settings are used to compromise software or a device, further compromise of the confidentiality, integrity, and availability of resources or data residing on systems and networks may take place.

Connected Network Enclaves and Devices

3 Downstream effects (network intrusion)

How do I employ CSM?

CSM benefits from applying current cybersecurity best practices involving People, Processes, and Technology in the Configuration Management Lifecycle

People	What resources and communication are needed for continuous monitoring? What level of CSM risk situational awareness is needed from and for those resources?
Process	“What is the process used to identify, prioritize, and mitigate CSM risk?”
Technology	“What technology is deployed to identify the ‘as-is’ configurations on the network?”

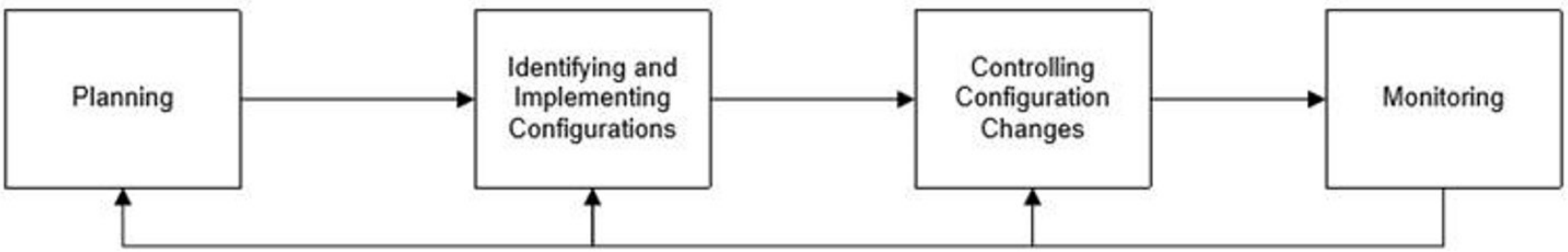
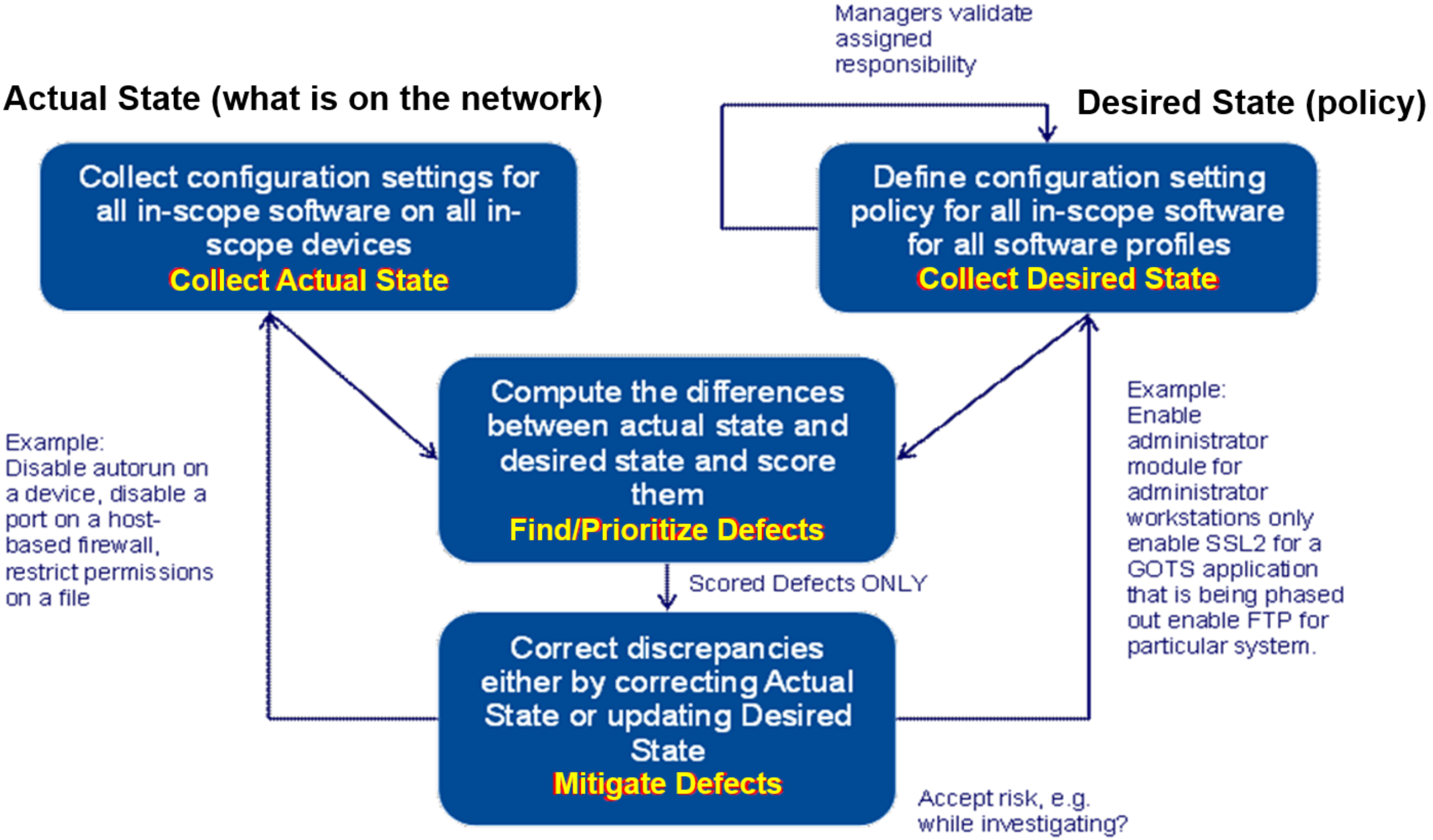

Planning
Identifying and Implementing Configurations
Controlling Configuration Changes
Monitoring

Figure 2-1 – Security-focused Configuration Management Phases

(Source: NIST SP 800-128)

What I want (Desired State) and What I have (Actual State)



Managers validate assigned responsibility

Actual State (what is on the network)

Desired State (policy)

Collect configuration settings for all in-scope software on all in-scope devices
Collect Actual State

Define configuration setting policy for all in-scope software for all software profiles
Collect Desired State

Example:
Disable autorun on a device, disable a port on a host-based firewall, restrict permissions on a file

Compute the differences between actual state and desired state and score them
Find/Prioritize Defects

Example:
Enable administrator module for administrator workstations only enable SSL2 for a GOTS application that is being phased out enable FTP for particular system.

Scored Defects ONLY

Correct discrepancies either by correcting Actual State or updating Desired State
Mitigate Defects

Accept risk, e.g. while investigating?

CSM Desired State

What information is needed in your configuration settings management policy to make up a CDM Desired State that supports ongoing diagnostics and risk mitigation decisions?

- ✓ Checklists for software and hardware
- ✓ Asset information
- ✓ Use of organizational whitelists, baselines, benchmarks
- ✓ Attributes, authorization, and expiration information
- ✓ Frequency and acceptable thresholds

CSM Actual State

What settings are currently found in your environment that apply to Configuration Settings Management

- Settings for user rights on a machine
- Authentication method configured in the Windows registry (Lan Manager or NTLM v2)
- Permission set on files and folder
- System services that are enabled or disabled
- All misconfigurations on IT assets including hardware devices and software, that are likely to be exploited by a bad actor.

A CSM Defect in the Field

User wants a test WordPress web server, outside of IT change process

Hey Mr. Admin, can you help me?

↓

Administrator creates new web server with default services and credentials, ignoring baseline configuration req's

Sure thing, but it will cost you a caramel macchiato

↓

CSM tool identifies difference between *desired state* and *actual state*

DEFECT!

↓

CSM tool notifies security group of defect (dashboard, alert)

Someone failed to follow change control processes and rolled out a new WordPress webserver

Make Timely Risk Management Decisions

CSM Defect Type	Detection Rule	Mitigation Options
Misconfiguration	CSM Actual State Less Secure than CSM Desired State	• Remediate device configuration OR • Accept Risk OR • Change Desired State Specification (Rare)
Non-reporting	CSM Actual State data unavailable	• Deploy collection capability OR • Restore collection OR • Remove device

Federal Cybersecurity Metrics

Secure Configuration Management is a capability (detailed in 2.3.2, 2.3.3, and 2.3.4) of the Information Security Continuous Monitoring (ISCM) goal for the **FY16 CIO Annual FISMA Metrics**.

- Metric 2.3.2. The common security configuration baseline for each OS listed. (e.g., USGCB)
- Metric 2.3.3. Number of configuration exceptions granted.
- Metric 2.3.4. Number of assets in 2.3.1 covered by auditing for compliance with 2.3.2.

Source: FY16 CIO Annual FISMA Metrics

Supporting IT Standards/Protocols

SCAP CCE:

- Supports identifying configurations
- Can be used to build the CSM Desired State/policy

National Checklist Program (NCP):

- CIS Benchmarks
- STIGs
- USGCB

SWID: supports CSM to identify software configurations

- NISTIR 8060: Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

Defensive Configurations

What *should* a baseline configuration policy have in it?

- Minimum changes to access and authorization
- Minimizing the attack surface
- Frequency of “diagnosing” the configuration
- Process for mitigating any risks

CSM within the CDM Readiness & Planning Guides

CDM Guides:

- https://www.us-cert.gov/cdm/guides

How is CSM addressed? Readiness practices were identified:

- IT lifecycle management (Practice 1)
- Baseline configurations (Practice 2)
- IT change control (Practice 3)

Practice: Separate IT testing and production environments

Are configurations tested before production?

- “Is there a development and testing environment that is separate from the production environment?”
- “How often do we validate and verify configurations?”
- “Do we have policies that address configuration establishment, maintenance, and approval/authorization for software development and testing?”

Practice: Baseline Configuration Maintenance

Start at the beginning of the IT lifecycle

- “What baselines are used across our organization?”
- “How do we validate the baseline?”

Where do baselines fit in?

- “How do we manage software configuration?”
- “What configuration attributes do we collect?”

Additional considerations

- “What is the mean time it takes us to identify a misconfiguration?”
- “If there is a misconfiguration identified, what is the median time to repair it?”

Practice: Configuration Change Control

“What change control roles and processes exist for our organization?”

More focused:

- “What process do we use for software configuration updates?”
- “How often do we update the baseline configuration?”

Are configuration changes integrated into other IT processes:

- “How are configuration baselines and configuration checks integrated into the policies, configuration management process, and software management process?”

Open Discussion

What is the impact of …??

What about ….??

How did the stakeholders adjust to ….??

What would you do differently about ….??

What should I do about ….??

What would you recommend for ….??

How much time did it take to ….??

How are you maintaining 95% compliance with HWAM CAP….??

How did you handle … (latency, centralization, control issues, etc.) ??

Event Conclusion

Thank you for attending today's

CDM Learning Community Event (LCE)!

- A certificate of attendance will be available to download on the CDM Learning Program website at www.us-cert.gov/cdm/training, within one week of today's event
- Visit our website to learn more about the CDM Learning Program and upcoming events at www.us-cert.gov/cdm
- For any questions, comments, or suggestions for future topics, please email us at cdmlearning@hq.dhs.gov
- Please take a moment to fill out our 4 question survey

The CDM Learning Program

CDM Learning Program – What's in it for you:

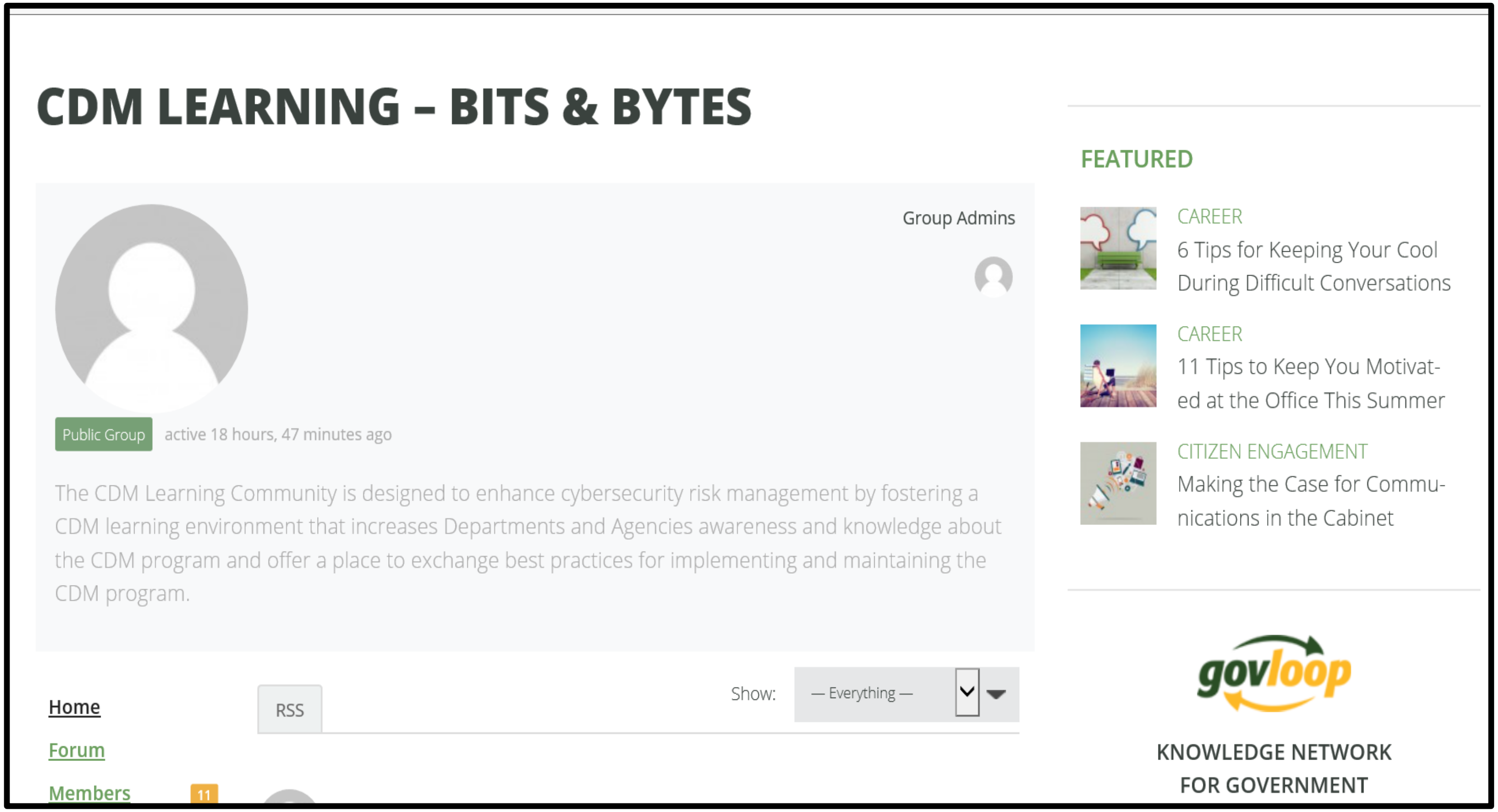
- Learning Community Event (CDM-LCE)
  - CDM leaders and implementers discuss relevant CDM topics in-depth, either in a live face-to-face session or using a virtual platform such as AvayaLive!
  - CDM experts deep-dive into specific CDM topics and participants are able to ask relevant questions using a text-chat function
- Weekly CDM Bits & Bytes
  - Short email awareness tips that link to additional content posted to the CDM Learning forum on GovLoop
- Online Vignettes
  - Short video vignettes which allow the learner to develop foundational knowledge around key CDM concepts and topics

Resources Available: https://www.us-cert.gov/cdm

Sign up to receive information on Learning Community Events by emailing cdmlearning@hq.dhs.gov

Sign up for our blog!

https://www.govloop.com/groups/cdm-learning-bits-bytes/



CDM LEARNING – BITS & BYTES

Group Admins

Public Group active 18 hours, 47 minutes ago

The CDM Learning Community is designed to enhance cybersecurity risk management by fostering a CDM learning environment that increases Departments and Agencies awareness and knowledge about the CDM program and offer a place to exchange best practices for implementing and maintaining the CDM program.

Home

Forum

Members 11

RSS

Show: — Everything —

FEATURED

CAREER
6 Tips for Keeping Your Cool During Difficult Conversations

CAREER
11 Tips to Keep You Motivated at the Office This Summer

CITIZEN ENGAGEMENT
Making the Case for Communications in the Cabinet

govloop

KNOWLEDGE NETWORK FOR GOVERNMENT