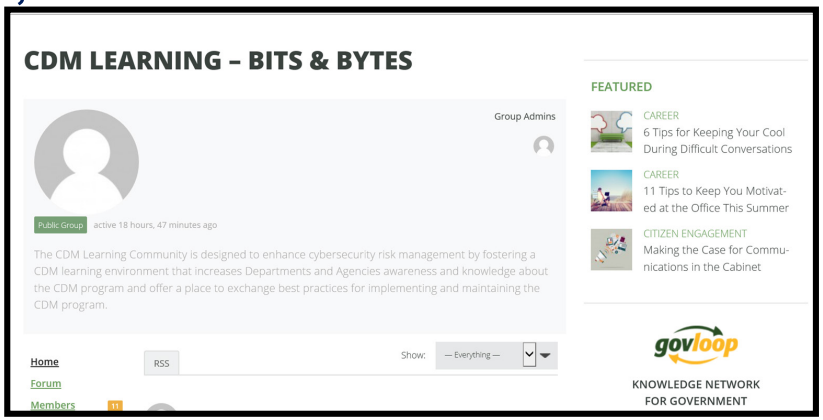
The July CDM Webinar
We will begin at 12:00PM EDT

Welcome to the CDM Webinar – Automating Assessments for Configuration Settings Management

While you wait, check out:

Our CDM Homepage
https://www.us-cert.gov/cdm/training



Our CDM Bits and Bytes Blog
https://www.govloop.com/groups/cdm-learning-bits-bytes/

Have a topic suggestion for a future event or blog post? Want to join our membership list? Please reach out to cdmlearning@hq.dhs.gov

Homeland Security

Automating Assessments for Configuration Settings Management

July 21, 2016
12:00 pm – 1:00 pm

A CDM Learning Webinar

Event Goal

The goal is to discuss automating assessments of **Configuration Settings Management** (**CSM**), focusing on:

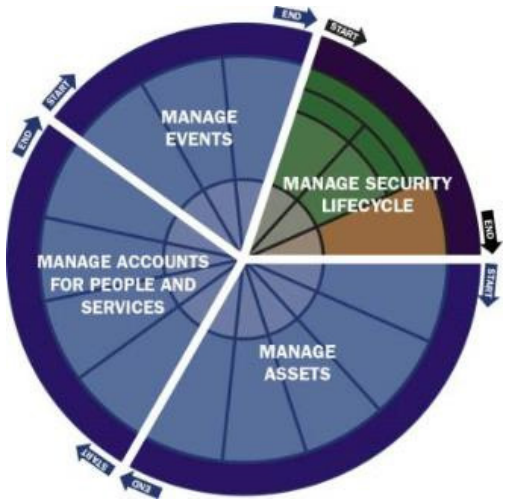
- National Vulnerability Database (NVD)
- National Checklist Program (NCP)
- Security Content Automation Protocol (SCAP)
- Common Configuration Enumeration (CCE)

CDM and Configuration Settings Management

Configuration Settings Management

- Who are the stakeholders?
- How can assessing configuration settings help to secure your environment?
- Have you securely configured your custom applications?
- Are checklists available for all your products and applications?
- How do you define CSM desired state?

CDM CSM Security Capability



Today's Speaker: Harold Booth

Computer Scientist, National Institute of Standards and Technology (NIST) Computer Security Division (CSD)

- Project lead for the National Vulnerability Database
- Leads research at NIST on the Security Content Automation Protocol (SCAP) which includes CPEs, CVEs (and CVSS) and CCE
- Involved with Security Automation Program specification development at NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SCAP™

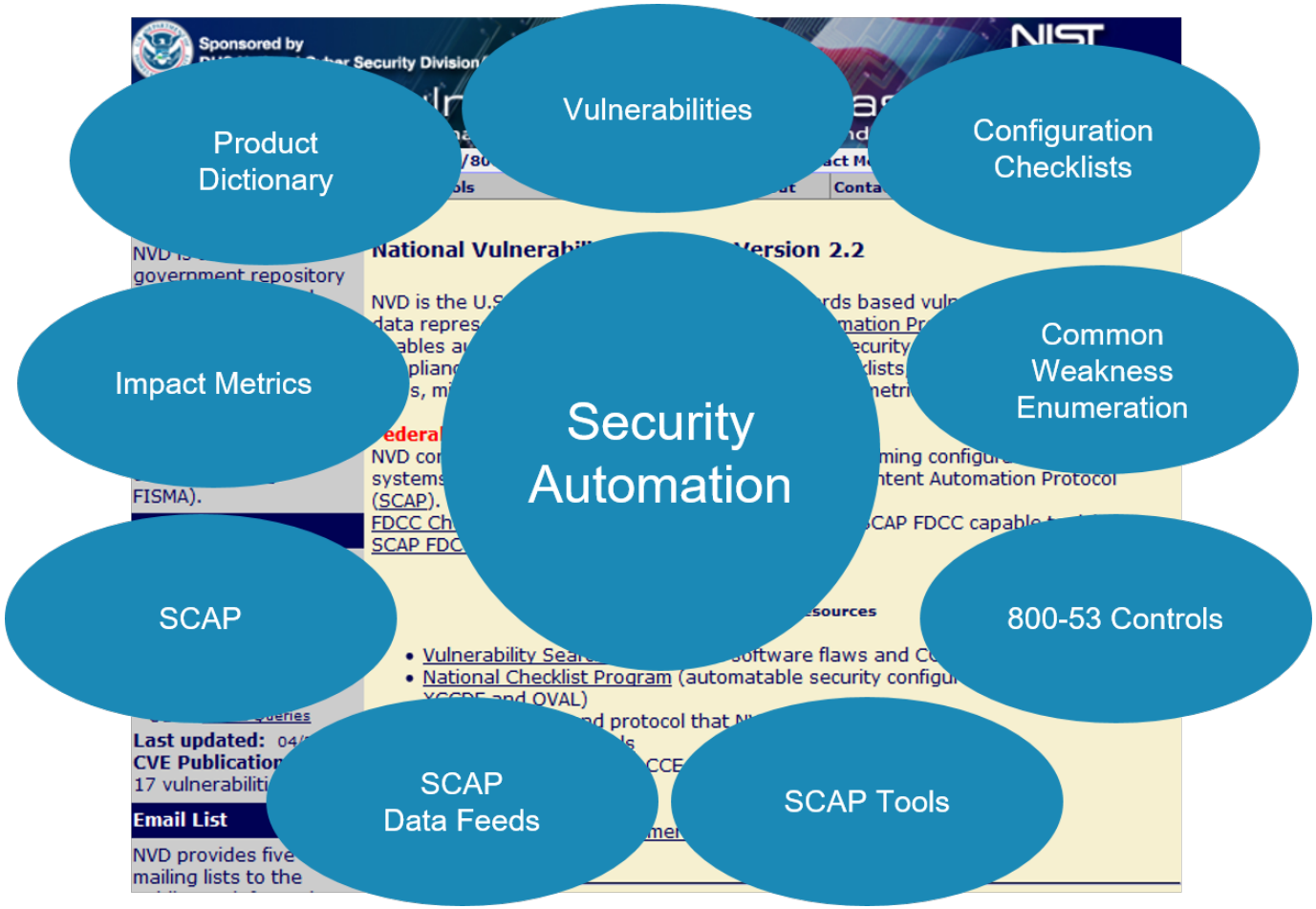
Security Automation: The National Vulnerability Database and the National Checklist Program

Harold Booth
harold.booth@nist.gov

Agenda

- Introduction and Overview of the National Vulnerability Database (NVD)
- Introduction to NVD Resources
  - Vulnerabilities
  - Product Dictionary
  - National Checklist Program
- Security Content Automation Protocol (SCAP)
- Validated Products
- Use Case

NVD: A Collection of Resources



NVD Overview

Vulnerabilities	Product Names	Checklists	New Vulnerabilities	Checklists
77,000+	113,000+	350+	6,000+	80+
Over 77,000 CVE Entries	Product dictionary containing over 113,000 unique CPE based product names.	Over 350 checklists posted.	The NVD Analysis Team evaluates over 6,000 vulnerabilities a year.	80+ in SCAP Format (Tier III or Tier IV)

* as of July 18, 2016

NVD Data Feeds

Vulnerabilities

Configuration to 800-53 Controls

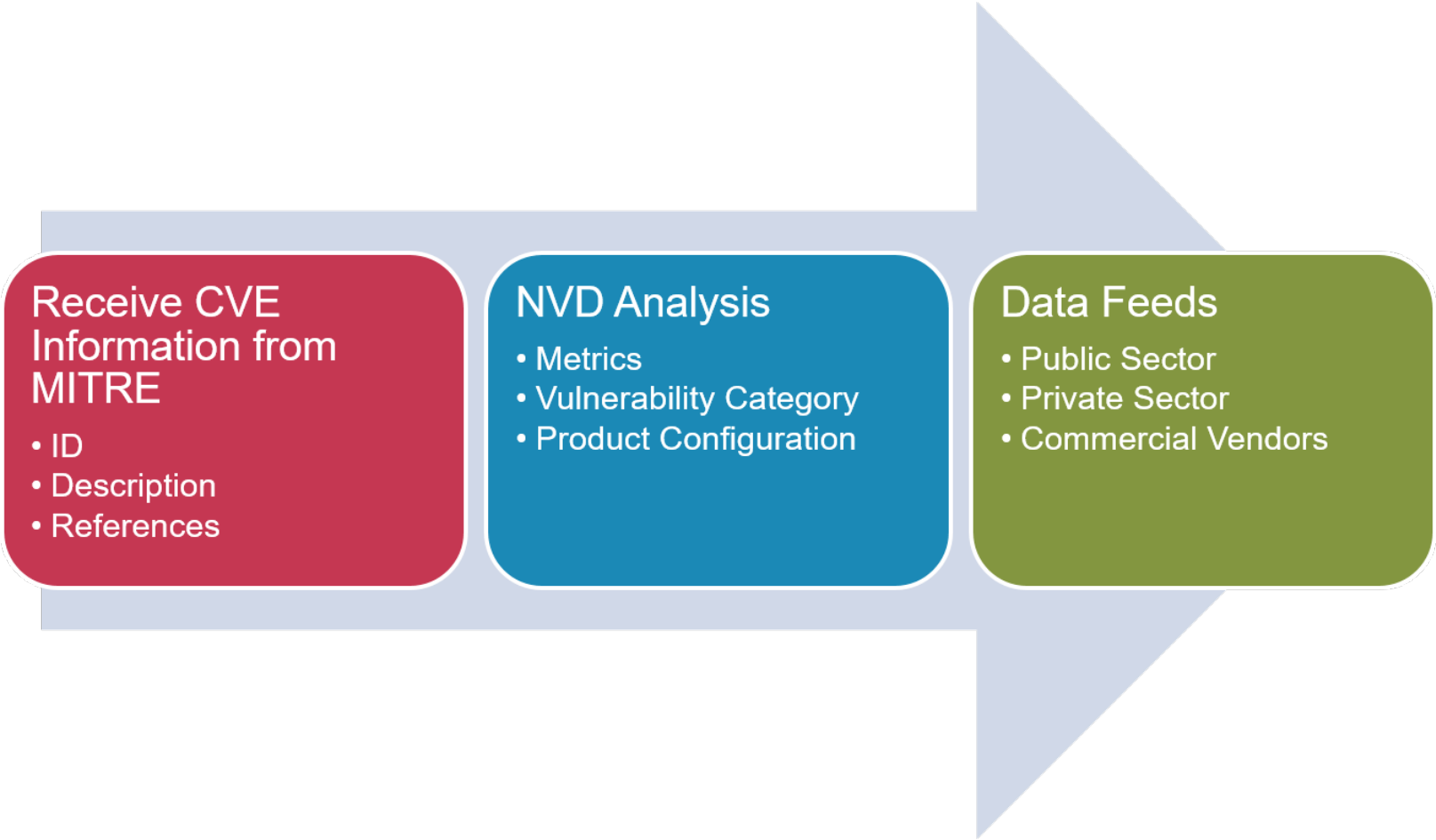
Checklists

Software Products

Common Vulnerabilities and Exposures (CVE)

- A dictionary of publicly known vulnerabilities
  - Predominately for, but not exclusive to, software used within the United States
  - MITRE maintains editorial control
    - Abstraction of Vulnerabilities
    - Duplication
- CVE is composed of:
  - Identifier => CVE-2013-1234
  - Description
  - References

National Vulnerability Database Role

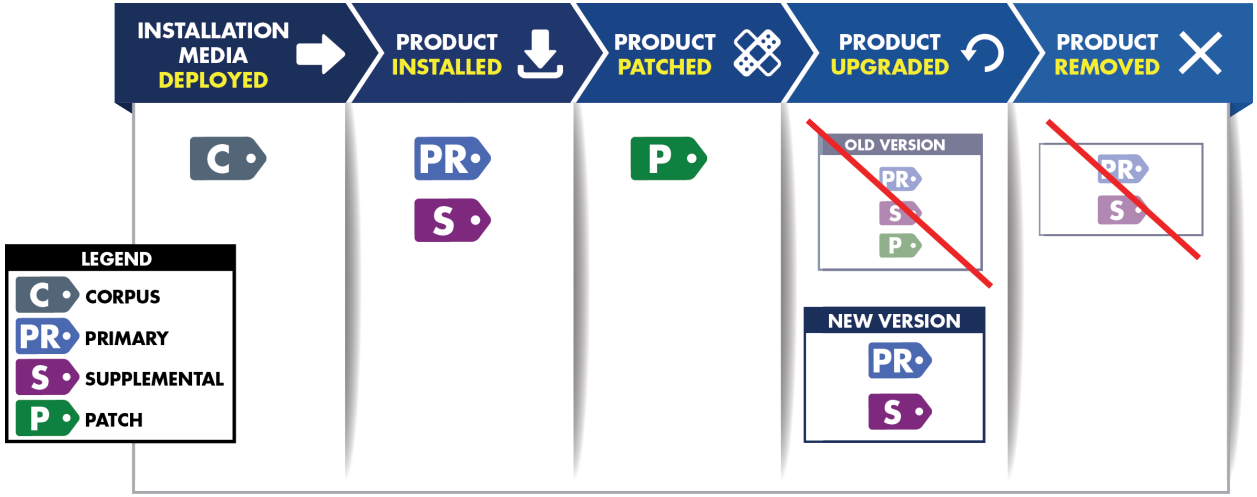


What is CPE?

- Structure naming scheme for information technology systems, software, and packages
- Includes formal name format, method for checking names against a system, and a description format for binding text and tests to a name
- The Official Common Platform Enumeration (CPE) Dictionary
  - http://nvd.nist.gov/cpe.cfm

What is SWID?

- ISO 19770-2:2015 standard
- NIST IR 8060
  - Provides example use cases
  - Implementation Guidance



Configuration Settings

- Common Configuration Enumeration (CCE)
- General CCE List:
  - https://nvd.nist.gov/cce/index.aspx
- CCE to 800-53 Mapping (Revision 3)
  - https://nvd.nist.gov/cce.cfm
- Common Configuration Scoring System (CCSS)
  - NIST IR 7502

800-53 Controls

- https://web.nvd.nist.gov/view/800-53/home

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Control Families

Families
AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS - Personnel Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

Minimum Security Controls

Minimum Security Controls
High-Impact Baseline
Moderate-Impact Baseline
Low-Impact Baseline

The National Checklist Program (NCP)

Project website: https://checklists.nist.gov

Tier 1	Tier 2	Tier 3	Tier 4
150+*	120*	70+*	9*
Tier I checklists are prose-based, such as narrative descriptions of how a person can manually alter a product's configuration.	Tier II checklists document their recommended security settings in a machine-readable but non-standard format.	Tier III checklists use SCAP to document their recommended security settings as specified in NIST Special Publication 800-126.	Tier IV checklists contain vetted mappings to controls framework such as SP 800-53 Controls for FISMA.

* as of July 18, 2016

NIST SP 800-70 Revision 3

- Governs the National Checklist Program
- Defines a checklist as a:

  "document that contains instructions or procedures for configuring an IT product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized configuration changes to the product."
- Outline a process for developing a checklist
- How to submit to the NCP

The National Checklist Program (NCP)

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: Any.....
Target Product: Any.....
Product Category: Any.....
Authority: Any.....
Keyword: Search

Checklist Results

Tier	Target Product	Product Category	Authority	Publication Date	Checklist Name (Version)	Resources
IV	• Microsoft Internet Explorer 7	• Web Browser	• Technology Infrastructure Subcommittee (TIS)	06/19/2008	USGCB Internet Explorer 7 (2.0.x.0)	• GPOs - USGCB IE7 GPOs • Prose - This is the human readable version of the USGCB settings. • SCAP 1.2 Content - USGCB Internet Explorer 7 SCAP Content using OVAL version 5.10 • SCAP 1.2 Content - USGCB Internet Explorer 7 SCAP Content using OVAL version 5.10 • SCAP 1.0 Content - USGCB Internet Explorer 7 SCAP Content using OVAL version 5.3. • SCAP 1.0 Content - USGCB Microsoft Internet Explorer 7 SCAP content using OVAL version 5.4.
	Internet	• Web	• Technology Infrastructure		USGCB Internet Explorer	• GPOs - USGCB IE8 GPOs • Prose - This is the human readable version of the USGCB settings. • SCAP 1.0 Content - USGCB Internet Explorer 8 Oval 5.3

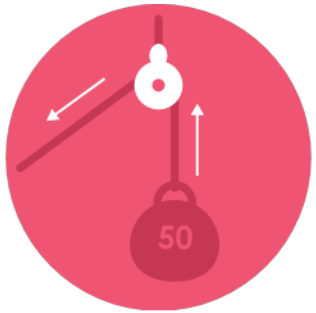
www.us-cert.gov

What is SCAP?

Security Content Automation Protocol

- Brings existing specifications together to provide a standardized approach for maintaining the security of enterprise systems
- Provides a means to identify, express and measure security data in standardized ways.
- Currently
  - Defined by Special Publication (SP) 800-126 Revision 2
  - SP 880-126 Revision 3 is now available for Public Comment
  - SP 800-117 Revision 1
  - Project website: https://scap.nist.gov

Why should I use SCAP?



Minimize Effort

Increase Interoperability

Economy of Scale and Reuse

Speed

How Does SCAP Work?

Languages

Means of providing instructions

- Community developed
- Machine readable XML
- Reporting
- Representing security checklists
- Detecting machine state

Metrics

Risk scoring framework

- Community developed
- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

Enumerations

Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings

Integrity

Conventions for applying existing and emerging XML signature standards and best practices to sign and verify content

What are SCAP Validated Products?

- Products validated by the SCAP Validation Program
- The SCAP Validation Program
  - Provides product conformance testing for Security Content Automation Protocol (SCAP)
  - Provides end users with assurance that SCAP validated tools conform to SCAP and should be capable of processing well-formed SCAP expressed checklists

SCAP 1.2 Validated Products

https://nvd.nist.gov/scapproducts.cfm

bmc

Center for Internet Security

IBM

intel Security

Microsoft

Qualys

Rapid7

redhat

tenable network security

ThreatGuard

tripwire

How do I use SCAP Validated Products?

- End users purchasing a tool from the validated products list has assurance that the product has met the test requirements defined in NIST IR 7511 and should process SCAP expressed checklists.
- https://nvd.nist.gov/scapproducts.cfm

Use Case: Configuration Assessment

https://nvd.nist.gov/scapproducts.cfm

Authenticated Configuration Scanner

https://usgcb.nist.gov

https://checklists.nist.gov

Use Case: Configuration Assessment

```
<!-- ~~~
```

Use Case: Configuration Assessment

```
<entry id="CCE-9308-8">
    <config:cce-id>CCE-9308-8</config:cce-id>
    <config:published-datetime>2010-09-24T16:44:34.730Z</config:published-d
    <config:last-modified-datetime>2012-05-25T03:59:21.197Z</config:last-mo
    <config:summary>The 'Account lockout duration' setting should be config
    <scap-core:control-mappings>
        <scap-core:control-mapping last-modified="2011-04-18T20:18:49.687Z"
            <scap-core:mapping published="2011-04-18T20:18:49.687Z">AC-7</s
        </scap-core:control-mapping>
    </scap-core:control-mappings>
</entry>
```

- CCE-to-800-53 Mapping
  - CCE-9308-8
  - AC-7 From NIST SP 800-53 Revision 3

Use Case: Configuration Assessment


```
- <controls:control>
    <family>ACCESS CONTROL</family>
    <number>AC-7</number>
    <title>UNSUCCESSFUL LOGON ATTEMPTS</title>
    <priority>P2</priority>
    <baseline-impact>LOW</baseline-impact>
    <baseline-impact>MODERATE</baseline-impact>
    <baseline-impact>HIGH</baseline-impact>
  - <statement>
      <description>The information system:</description>
    - <statement>
        <number>AC-7a.</number>
      - <description>
          Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and
        </description>
      </statement>
    - <statement>
        <number>AC-7b.</number>
      - <description>
          Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays
          attempts is exceeded.
        </description>
      </statement>
    </statement>
  - <supplemental-guidance>
    - <description>
        This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by infor
        delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those compone
```


- 800-53 Controls File
  - AC-7

Resources and Websites

- **NVD Homepage**
  - https://nvd.nist.gov
- **National Checklist Program**
  - https://checklists.nist.gov
- **SCAP Homepage**
  - https://scap.nist.gov
- **SCAP Validated Products**
  - https://nvd.nist.gov/scapproducts.cfm
- **NIST Computer Security Resource Center (CRSC) Documents**
  - http://csrc.nist.gov/publications/PubsSPs.html
  - http://csrc.nist.gov/publications/PubsNISTIRs.html

CSM, the NVD and SCAP

- Think about your current tools and processes—do they support SCAP?
- Ask your CMaaS integrator how their tools support SCAP—work together with them to get this information from tool vendors
- Think about the CDM CSM desired state—what are the appropriate configurations on your networks
- Think about how sensors can use SCAP content to determine actual state and report configuration settings defects
- How can the NVD (and CPE/CCEs) help define CSM desired state and defect priority?
- How can they help with automated assessments?

Questions and Answers

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 CSM CAP….??

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

Questions and Answers

Q: Will SCAP 1.3, which entails XCCDF 1.2, accommodate SWID? The XCCDF 1.2 constraint makes this awkward.

A: We did look at using SWID for some of the inventory management and we do have a bit in there on how one could use OVAL which is one of the checking tools to look for SWID tags on a system and extract that information and relate that to a CPE. The primary mechanism right now for SCAP will be through CPE. There is a way interoperate between CPE and SWID in a somewhat automated way. We have an outline for that within 800-126 Rev 3. The relationship between a particular product and the checklist does make SWID a bit difficult absent additional standards. The current way SCAP addresses that is to use CPE and will continue to do that going forward into SCAP 1.3.

Questions and Answers

Q: Why not just follow the STIGs? (Susan Hansche) Concerns that Federal agencies are supposed to follow NIST and not DOD, but if they are in the checklist program, can they use those? (Specifically related to CCEs)

A: STIGs are one type of checklist and they are actually enumerated in NCP. A lot of them are using SCAP or bits of SCAP. They are just another type of checklist that are provided by DISA (DOD). May be appropriate for some agencies, but not for all. NIST is a non-regulatory agency and provide recommendations and guidance, but say that you should follow your sector-specific checklist first. In federal agencies you would follow DISA, NSA or NIST checklists, but take into account your environment. However, DISA NSA and NIST checklists may not be appropriate for your environment, where they are more focused on security than functionality and may not fit in with the mission of a specific agency and what they are trying to accomplish. As far as STIGS for CCE, I think you may probably be referring to CCIs [Control Correlation Identifier]. Higher order level of abstraction above CCE. CCI are often used by DISA STIG CCEs are a much lower level talking about technical control itself. CCI is getting at a particular state that one wants to reach. Two different concepts trying to answer related concepts and are definitely related where more than one CCE can be mapped to one CCI.

Questions and Answers

Q: NIST SP 800-126 does not discuss metrics or scoring. Is there a separate document that addresses these?

A: 800-126 talks about interoperability of the various specifications and which version of specifications are in scope for a particular version of SCAP. The actual specification itself talks about those metrics. For instance, CVSS is maintained by Forum of Incident Response and Security Teams (FIRST) and that specification is described there. CCSS is for example an NISTIR, 7502. So those various specifications are discussed in their own documents.

Questions and Answers

Q: If we're purchasing risk prevention/mitigation tools, are we required to use SCAP validated products?

A: This is policy-related and [NIST] does not do policy. (Susan Hansche) If this question related to whether or not CMaaS Vendor is purchasing tools, then the PMO will likely say go back to your tool provider, integrator. If you are talking generally, DHS will always promote that we have to get to the automation of controls assessment. It’s just too much to do manually. They will probably recommend that any tool you purchase would have to be on the approved list of tools and have automation. That would include these SCAP validated products.

Questions and Answers

Q: If we're purchasing risk prevention/mitigation tools, are we required to use SCAP validated products?

A: This is policy-related and [NIST] does not do policy. (Susan Hansche) If this question related to whether or not CMaaS Vendor is purchasing tools, then the PMO will likely say go back to your tool provider, integrator. If you are talking generally, DHS will always promote that we have to get to the automation of controls assessment. It’s just too much to do manually. They will probably recommend that any tool you purchase would have to be on the approved list of tools and have automation. That would include these SCAP validated products.

Questions and Answers

Q: SCAP files did not work with Tenable's Security Center last year - the results contained many false positives. It was recommended to use "Security Content Automation Protocol (SCAP) Compliance Checker" instead. Is that still valid, or has Tenable's Security Center been fixed?

A: Can’t speak to a particular product/tool. If you are having a problem with a particular validated product reach out to SCAP@nist.gov and someone should be able to help you out with that.

Questions and Answers

Q: Is the RSA Archer Governance, Risk, and Compliance (GRC) a validated SCAP tool? If not what kind of tool is it considered?

A: Archer would not be. We don't currently have validation for the kind of tool Archer is. SCAP is trying to something a little different than what Archer is trying to do, so at the moment we don't have any way to categorize the Archer tool. We are looking at standardizing the types of things the Archer tool is achieving but we hope to have something like that in the future. (Susan Hansche) The RSA Archer Risk and Compliance tool that is being customized for the CDM Dashboard is taking the feeds from the tools and then they are displaying that.

Questions and Answers

Q: Besides software vulnerabilities, what other vulnerabilities are in the NVD? Can you provide some examples of how agencies are using it to understand the non-software vulnerabilities?

A: Primarily it contains software vulnerabilities, even ones that are normally considered hardware based driven by firmware. Don't think we have any that are hardware based. Most are fixable in that they require firmware or patch update. The only space where we may have vulnerabilities for (hardware) are in the ICS <Industrial Control Systems> space.

Questions and Answers

Q: Can you talk a little about the planned evolution of CCEs and CCSS?

A: We are still trying to figure out the best approach. For CCEs (more generally configuration settings and configuration items), we are looking how to break things apart better, so we are looking at things like (DISA) CCIs. And how do you map those to control frameworks. Going from there to CCI all the way down to the low level configurations settings for a particular product and mapping those. Then allow people to specify them at the Policy level. Looking at how to enable all that, so once its set up an agency can identify what a settings desirable state is. For CCSS, it's a bit more complicated because the interaction of the various configuration items is important. We are still looking at how to talk about the importance of the requirements for the controls framework instead of the settings themselves. That are too low level to be much useful. This is something we are still research and if you have a great answer we'd love to have a conversation from you about that.

Questions and Answers

Q: Are such feeds to Archer defined in a format that (1) is the same as SCAP 1.2/1.3, or (2) in some other format?

A: They are in a different format, and there is no normative reference for such a format either. That is an area we are looking at. I would describe what Archer does is collection all of the information dealing with A&A and the appendix F&G controls and address each one for a particular baseline Archer will help you go through and collect information and produce a report. And apparently CDM has their own custom version of the Archer tool. (Susan Hansche) This is exactly what this kind of webinar is intended to do—help you answer those questions. Because your CMaaS integrator is the team responsible for taking those CDM sensor feeds and putting them into the CDM agency dashboard. So you need to talk your organization CDM POCs and get them engaged with it to know how it's going to fit in and work within your organization.

Questions and Answers

Q: There are obvious dependencies between hardware, software asset management, vulnerability management and configuration settings management. What, in your experience, are the most critical dependencies to remember when implementing and automated configuration settings assessment?

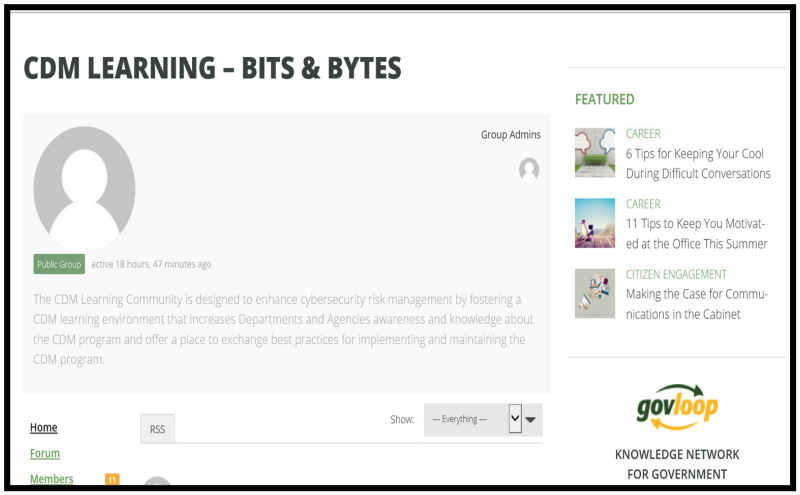
A: The most important thing is understanding what you have installed on your endpoints (assets) you have because everything else flows from that.

The CDM Learning Program

CDM Learning Program

- Monthly Learning Community Event (CDM-LCE)
- Monthly Webinars
- Weekly CDM Bits & Bytes
- Online Vignettes

Sign up for the CDM learning blog: https://www.govloop.com/groups/cdm-learning-bits-bytes



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

Sign up to receive event information:
cdmlearning@hq.dhs.gov

Event Conclusion

Thank you for attending today's

CDM Webinar!

- 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