Continuous Diagnostics and Mitigation
Webinar Series

Getting Ready for Phase 2 CDM Security Capabilities: TRUST, BEHAVE, CRED, and PRIV
Introduction

• Overview of CDM and Key Concepts
• How the Security Capabilities Work Together
• Role of FICAM
• Phase 2 Security Capabilities
  • TRUST
  • BEHAVE
  • CRED
  • PRIV
CDM PMO Program Managers

No discussion or questions regarding CDM acquisition or procurement activities – this is strictly a CDM learning community activity. For agency-specific queries, contact:

- **Group A – DHS**
  - Betsy Proch (betsy.proch@hq.dhs.gov)

- **Group B – DOE, DOI, DOT, USDA, VA, OPM**
  - Derrick Williams (derrick.Williams@hq.dhs.gov)

- **Group C – DOC, DOJ, DOL, State, USAID**
  - Paul Loeffler (paul.loeffler@hq.dhs.gov)

- **Group D – GSA, HHS, NASA, SSA, Treasury, USPS**
  - Odell Blocker (odell.blocker@hq.dhs.gov)

- **Group E – Educ, EPA, HUD, NRC, NSF, SBA**
  - Matt Hartman (matthew.Hartman@hq.dhs.gov)

- **Group F – Non-Chief Financial Officer (CFO) Act Agencies**
  - Geri Clawson (geraldine.clawson@hq.dhs.gov)

- **Unsure?**
  - CDM.FNR@hq.dhs.gov
What is the CDM Program?

- Establish consistent, government-wide set of information security continuous monitoring tools to help protect .gov networks.
- Leverage the buying power of government organizations to achieve savings for cybersecurity tools and services.
- Provide dashboards to improve situational awareness, enhance agencies’ ability to identify, and respond to risk of emerging cyber threats on the agency and government-wide level.
- Support risk-based decision making for resource allocation (best bang for the buck).
How does it Work?

1. Install/Update Sensors
2. Automated Search for Flaws
3. Collect Results from Departments and Agencies
4. Triage and Analyze Results
5. Fix Worst First
6. Report Progress

Continuous Diagnostics & Mitigation (CDM)
Who is Involved?

- Departments and Agencies
- Department of Homeland Security
- Office of Management and Budget
- General Services Administration
- Federal CIO Council and ISIMC
- CMaaS Providers/Commercial System Integrators
- Federal Level Working Groups
  - PACS
Implementation Phases of CDM

What is on the Network?

Who is on the Network?

What is Happening on the Network?
Key CDM Concepts

- Security Capabilities
- Actual State
- Desired State
- Defect and Defect Check
- Objects and Attributes
- Data Format
- Dashboard
- Master User Record
- Master Device Record
Focus on Phase 2
Security Capabilities

Who is on the Network?
- TRUST
- BEHAVE
- CRED
- PRIV
Focus on Phase 2
Security Capabilities

Trust, Behave, Cred and Priv
Linkage to the User

USER is a generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

TRUST is used to validate a person’s identity and the degree to which they have been vetted.

CRED binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).

PRIV establishes the privileges associated with the credential and in turn the individual or service.

BEHAVE identifies that the individual has the proper knowledge and training for the roles they are assigned and that they remain up to date.
TRUST Security Capability

Trust

Behave

Credentials

Privileges
The TRUST CDM security capability provides the D/A visibility into the risk associated with the vetting of users.
What is the Risk?

• The agency employed mechanisms for user screening/indoctrination before granting access to sensitive data are not monitored on a regular basis nor with efficiency.

• “Key trust level attributes” are not validated and available to systems and processes that monitor/enforce access.
How the TRUST Security Capability Helps

Verifies the existence of TRUST artifacts.

<table>
<thead>
<tr>
<th>TRUST Artifacts</th>
<th>TRUST Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Clearance Determination</td>
<td>Validates existence and currency per policy</td>
</tr>
<tr>
<td>Suitability Determination</td>
<td></td>
</tr>
<tr>
<td>Fitness Determination</td>
<td></td>
</tr>
</tbody>
</table>
TRUST Planning Actions

1. Identify the stakeholders for personnel security systems.

2. Determine availability of data and policy in machine readable format (able to store in database).

3. Establish or update policies regarding how long a given trust level is valid before it expires and formal re-vetting of the user is required.

4. Define what the re-vetting and re-indoctrination policies/processes are for each trust level.
The BEHAVE CDM security capability provides the D/A insight into risks associated with non-compliance of IT related training and role requirements.
What is the Risk?

- Users are granted access to facilities, systems, resources, information (sensitive data) without:
  - Current policy
  - Appropriate security training
  - Demonstrated skill specialty
  - Knowledge
  - Certification
  - Completing proper security-related documentation or training
  - Signed agreements
What is the Risk?

Poorly trained users can engage in behaviors that compromise systems, expose sensitive data, or subvert security policies meant to mitigate risk.

• Examples
  – Ineffective training
  – Users have not been assigned the proper training for the access
How the BEHAVE Security Capability Helps

Verifies the existence of BEHAVE artifacts.

<table>
<thead>
<tr>
<th>User Behavior</th>
<th>BEHAVE Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete awareness training at least annually</td>
<td>Validates Existence and Currency per Policy</td>
</tr>
<tr>
<td>Complete role-based training as required</td>
<td></td>
</tr>
<tr>
<td>Read and accept rules of behavior or other types of system agreements</td>
<td></td>
</tr>
<tr>
<td>If testing is utilized, set a passing score, such as meeting an 80% level for passing</td>
<td></td>
</tr>
</tbody>
</table>
1. Identify stakeholders for BEHAVE artifacts.
2. Determine whether BEHAVE artifacts are in “data format” – if not, how to get in data format.
3. Review or establish policies about mandatory training attributes, such as:
   • How long the training is valid
   • Grace period for not completing training
   • Refresher training requirements
   • Testing requirements
CRED Security Capability

Trust
Behave
Credentials
Privileges

WHO IS ON THE NETWORK?

Phase 2
The CRED CDM security capability provides the D/A insight into risks associated with weaknesses in its management of credentials and the mechanisms used to authenticate users to facilities and systems.
What is the Risk?

• Authentication, reissuance, and revocation activities are not in compliance with policy and introduce risks.
• Users are not authenticated appropriately for access to facilities, systems, and information.
• Authentication, reissuance, and revocation policies are incurring more risk than deemed acceptable by the agency.
How the CRED Security Capability Helps

Verifies the existence of CRED artifacts.

<table>
<thead>
<tr>
<th>CRED Artifacts</th>
<th>Cred Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER attributes identifying a credential being issued to each user</td>
<td></td>
</tr>
<tr>
<td>USER attributes identifying date and state of issuance, revocation, reissuance, or suspension</td>
<td>Validates Existence and Currency per Policy</td>
</tr>
<tr>
<td>Credential (account) attributes identifying the associated user(s) and authentication mechanisms</td>
<td></td>
</tr>
<tr>
<td>Credential attributes for usage, complexity, duration, and grace period</td>
<td></td>
</tr>
<tr>
<td>Credential attributes for revocation</td>
<td></td>
</tr>
</tbody>
</table>
How the CRED Security Capability Helps

Verifies the existence of CRED artifacts.

<table>
<thead>
<tr>
<th>CRED Artifacts</th>
<th>Cred Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication mechanism for every account</td>
<td>Validates Existence and Currency per Policy</td>
</tr>
<tr>
<td>Default accounts/passwords enabled</td>
<td></td>
</tr>
</tbody>
</table>
CRED Planning Actions

1. Review or establish policies for the following:
   • How long a given credential type is valid before it expires
   • Reissuance, revocation, or suspension for each credential type
   • Credential requirement policies for systems, facilities, and services
   • Credential quality
   • Non Person Entity credentials and policy compliance
2. Determine if the following user account attributes are in data format on the system:
   • Account identifier
   • System or applications that account is allowed to access
   • Authorized user and authorization status
   • Date first authorized, date last authorized
   • Date revoked, suspended
PRIV Security Capability

Trust
Behave
Credentials
Privileges

WHO IS ON THE NETWORK?

Phase 2
The PRIV CDM security capability provides the D/A insight into risks associated with the privilege(s) granted to a credential(s) issued to user(s) of facilities systems and services.
What is the Risk?

• Credentials that are no longer needed to perform a function are NOT disabled or deleted.
• Privileges accumulated over time or through role changes are not removed.
• Credentials have excess access.
• Credentials have excess privileges.
How the PRIV Security Capability Helps

Verifies the existence of PRIV artifacts.

<table>
<thead>
<tr>
<th>PRIV Artifacts</th>
<th>PRIV Security Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical access authorizations issued to each credential</td>
<td>Validates Existence and Currency per Policy</td>
</tr>
<tr>
<td>Credential restrictions implemented</td>
<td></td>
</tr>
<tr>
<td>Privileges enabled for each credential</td>
<td></td>
</tr>
</tbody>
</table>
PRIV Planning Actions

1. Review or establish policies for the following:
   • Separation of duties
   • How long a given authorization and credential type are valid before they expire
   • Applicable reauthorization
   • Credential restrictions, such as time of day, duration, etc.
   • Locking credentials
   • Disabling credentials
   • Physical access
2. Identify where existing attributes are in data format for the following:

- Separation of duties
- Account authorization and type validation
- Account restrictions, such as time of day, duration, etc.
- Locking accounts
- Disabling accounts
- Physical access
How the Phase 2 Security Capabilities Work Together

Who is on the Network?
Trust
Behave
Credentials
Privileges
How the Phase 2 Security Capabilities Work Together

Trust, Behave, Cred and Priv Linkage to the User

BEHAVE
- Maintain identity

TRUST
- Establish identity

PRIV
- Requires

CRED
- Requires
- Access
- Represent identity

Requires
Role of FICAM

Trust, Behave, Cred and Priv Linkage to the User

BEHAVE

TRUST

CRED

PRIV

Identity, Credential, and Access Management

Access Management
The processes and technologies used to govern and authorize access.

Authorization
Run-time decisions on whether an identity is trusted

Monitoring
Dynamically checking and evaluating the efficiency of access controls and conducting remediation activities

Risk Assessment
Evaluate potential threats to establish security mechanisms and policy for a resource

Policy Management
The processes for determining and maintaining access rules to digitally protected resources

Provisioning
Management of accounts and privileges for access to applications and facilities

Credential Management
The processes for managing objects that authoritatively bind an identity to a token

Identity Management
The processes for establishing and maintaining the identity state of an individual.

Digital Identity
The bits that make a person or thing unique

Credentials
An object that digitally or physically represents a person or thing

Identity, Credential, and Access Management

Credential Management

Identity Management

Data Integration

Access Management

Authentication

Authorization

Monitoring

Provisioning

Policy Management

Risk Assessment
FICAM

• Provides architecture and implementation guidance to address concerns related to:
  – Identity
  – Credential
  – Access Management
Summary

Who is on the Network?
Trust
Behave
Credentials
Privileges
Additional Resources

GSA Site
- http://www.gsa.gov/cdm

US-Cert Site
- http://www.us-cert.gov/cdm

Additional Upcoming Activities

- January 21, 2016
  - CDM Learning Community Event
    CDM: Awakening the Force of Automated Assessments
    Time: 1:00 pm – 3:00 pm
    Location: Arlington, VA
    Registration Information - https://www.us-cert.gov/cdm/training
CDM PMO Program Managers

No discussion or questions regarding CDM acquisition or procurement activities – this is strictly a CDM learning community activity. For agency-specific queries, contact:

- **Group A – DHS**
  - Betsy Proch (betsy.proch@hq.dhs.gov)
- **Group B – DOE, DOI, DOT, USDA, VA, OPM**
  - Derrick Williams (derrick.Williams@hq.dhs.gov)
- **Group C – DOC, DOJ, DOL, State, USAID**
  - Paul Loeffler (paul.loeffler@hq.dhs.gov)
- **Group D – GSA, HHS, NASA, SSA, Treasury, USPS**
  - Odell Blocker (odell.blocker@hq.dhs.gov)
- **Group E – Educ, EPA, HUD, NRC, NSF, SBA**
  - Matt Hartman (matthew.Hartman@hq.dhs.gov)
- **Group F – Non-Chief Financial Officer (CFO) Act Agencies**
  - Geri Clawson (geraldine.clawson@hq.dhs.gov)
- **Unsure?**
  - CDM.FNR@hq.dhs.gov
Questions and Answers
Survey Questions

- Please help us improve these events by answering the 5 survey questions
CUE/CPE Information

- Thanks for attending today’s session!

- A generic Webinar completion certificate can be downloaded from the following site: https://www.us-cert.gov/sites/default/files/cdm_files/course_certs/Phase2OverviewCourseCompletionCertificate_nofitsi.pdf

- Hold onto the following:
  - Completion certificate after filling in your name
  - A copy of the email confirmation showing you registered for the Webinar
Contact Information

THANK YOU FOR ATTENDING OUR WEBINAR.

Contact: cdm.fnr@hq.dhs.gov