Standards-Based Automated Remediation

A Remediation Manager Reference Implementation

Jeff Davenport

Security Automation Developer Days – Spring 2011
22-25 March 2011

Software Engineering Institute | Carnegie Mellon

Definitions*

Remediation A security-related set of actions that results in a change to a computer's configuration. May be motivated by discovered vulnerabilities or mis-configurations.

Vulnerability A state in a system that allows an attacker to

- Execute unauthorized commands
- Bypass restrictions on data access or modification
- Pose as another entity
- Affect the availability of a system resource

Mis-configuration Any configuration state that does not comply with an organization's security policy.

*Source: Wojcik, M.N., Wunder, J., Kerr, M., & Waltermire, D. (2009). *Proposed Open Specifications for Enterprise Information Security Remediation*. Bedford, MA: MITRE.

What's the Problem?

Existing methods and tools for remediating vulnerabilities and mis-configurations rely heavily on manual support, which

- Is time consuming, effort intensive, and error prone
- May result in system configurations that are out of sync with DoD policy
- Complicates compilation and reporting of current, consolidated, complete information on remediation status

Some automated remediation capabilities exist, but these may not interoperate with other tools

A standards-based approach is desired to

- Provide a common language for discussing remediation actions
- Enable interoperability between tools from multiple vendors

How Can We Solve It?

Use emerging remediation standards to support the development of interoperable, automated remediation solutions

Enable human operators to

- Obtain insight into changes tools are making to host systems
- Guide the automated remediation process by allowing operators to override policy when necessary
- Intervene when automated remediation fails

Leverage the automated process to track remediation history and enable timely, complete reporting up the chain

Four Elements of Remediation Research

Taken together, four elements of work are advancing efforts to develop standards-based, automated remediation capabilities:

- Remediation automation standards
  MITRE, NIST, SEI, SPAWAR Systems Center Atlantic
- Sample content, created in accordance with SCAP standards and emerging remediation automation standards
  G2, *MITRE, NSA, SPAWAR Systems Center Atlantic*
- A Remediation Manager reference implementation
  SEI
- A Remediation Tool reference implementation, integrated with the SCAP Compliance Checker (SCC)
  SPAWAR Systems Center Atlantic

Demonstrating and Maturing Remediation Standards

*SEI Role: Develop a Remediation Manager Reference Implementation**

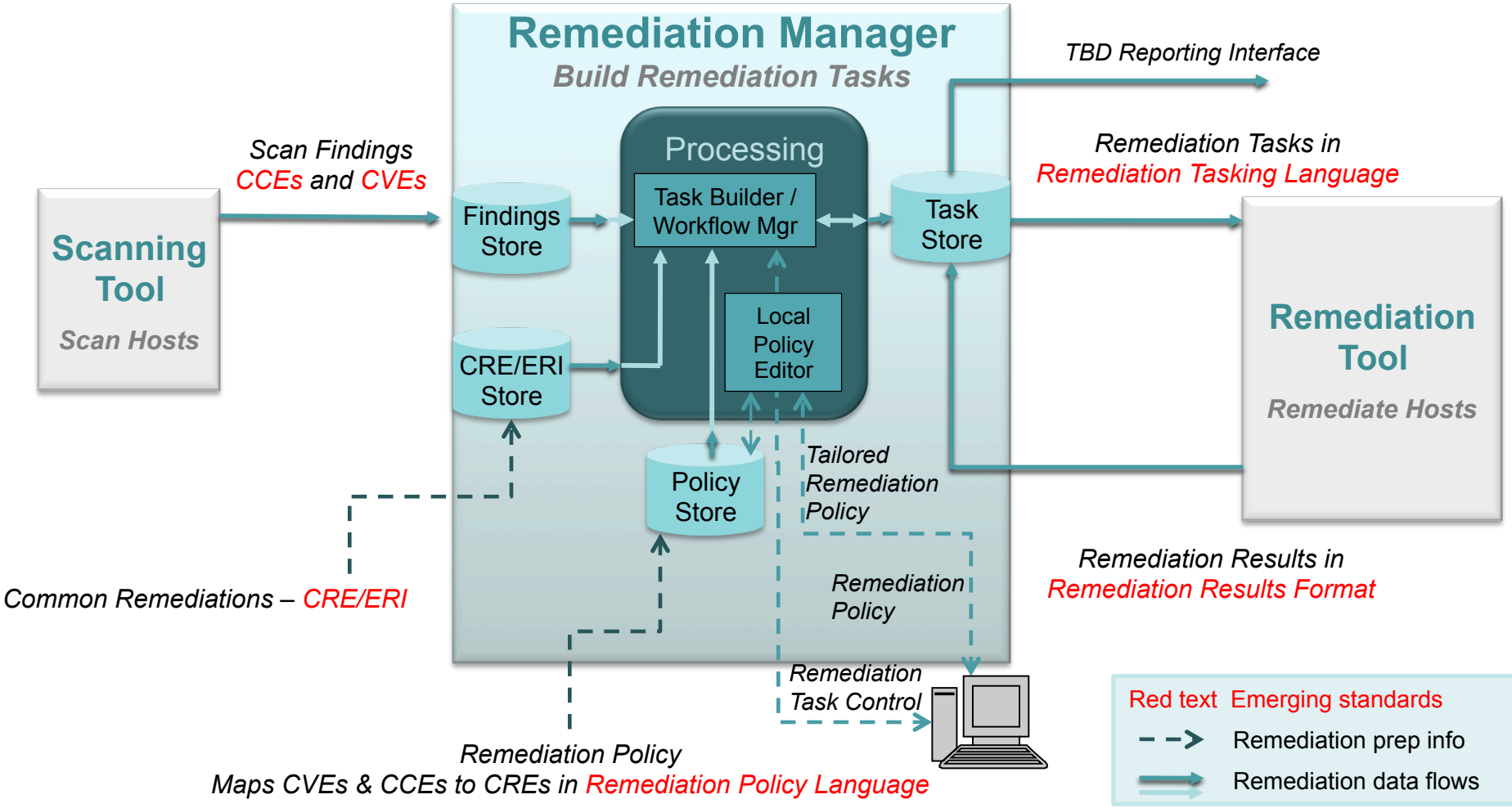
Employ emerging remediation standards to

- Ingest host scan findings in *DoD Assessment Results Format (ARF),* containing
  - Vulnerabilities, specified as *Common Vulnerabilities and Exposures (CVEs)*
  - Mis-configurations, specified as *Common Configuration Enumerations (CCEs)*
- Build remediation tasks, using *Remediation Policy Language (RPL)* to map CVEs and CCEs to *Common Remediation Enumeration (CRE)* entities
- Send remediation tasks, in *Remediation Tasking Language (RTL),* to a Remediation Tool, which executes them on the host
- Receive remediation results, in *Remediation Results Format (RRF),* from a Remediation Tool and flag failed tasks for handling by a Ticket Manager
- Manage relationships between policies, hosts, and remediations

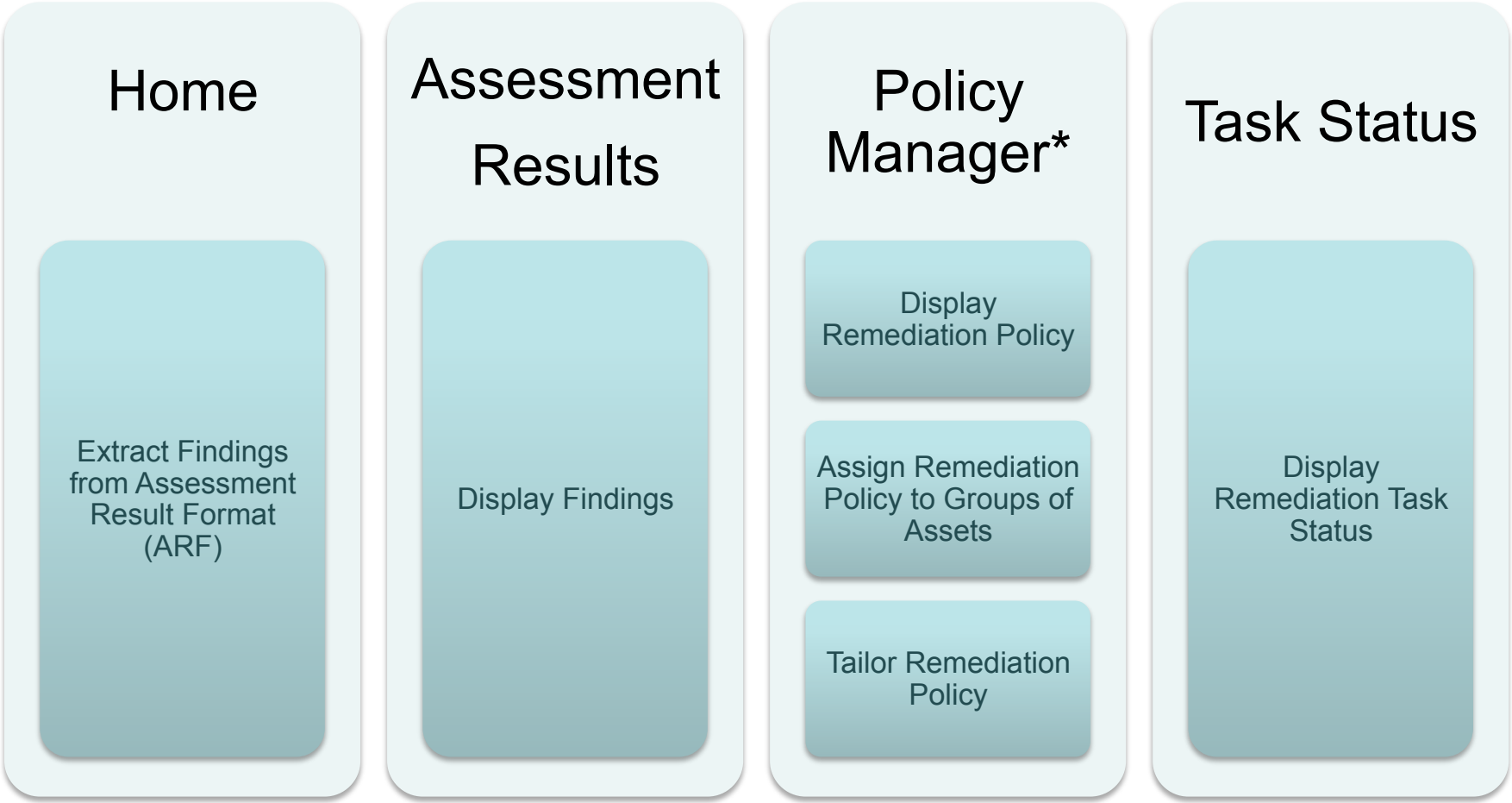
*Note: The purpose of the reference implementation is to support development of remediation standards by demonstrating their use and eliciting additional requirements the standards must meet.

Remediation Manager Standards-Based Processing

2010 Version of Reference Implementation (Simplified View)



Remediation Manager Display Screens



*Focus of today's demonstration

Policy Manager and User Interface Scenarios

We'll demonstrate an EARLY version of the functionality for the following scenarios available from the ***Policy Manager*** display screen:

1. Policy Assignment
    - Associate groups of assets with a specific set of remediation policies (i.e., assign policy groups)
2. Policy Tailoring
    - For a given finding and group of assets (i.e., policy group), choose default global or tailored local remediation policy
    - Enable the use of mitigation actions, rather than remediation, when necessary
    - Require that justification be specified for policy deviations

The purpose of demonstrating these scenarios is twofold:

1. Obtain feedback on desired functionality
2. Stimulate discussion of policy management and standards considerations in general

Remediation Manager Demonstration

Policy Manager Functions

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Host Navigation --- Next

Host ID:	1
IP:	1.0.0.0
Netbios Name:	Host0
MAC Address:	00:00:00:0

Compliance Issue	Remediation
CCE-2679-9 - TCP/IP SYN Flood Attack Protection should be properly configured.	Not yet processed
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	Not yet processed
CCE-3349-8 - The Shares that can be accessed anonymously policy should be set correctly.	Not yet processed
CCE-2679-9 - TCP/IP SYN Flood Attack Protection should be properly configured.	Not yet processed
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	Not yet processed
CCE-3349-8 - The Shares that can be accessed anonymously policy should be set correctly.	Not yet processed

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	1
Name:	DoD DC Standard edit
Description:	Standard configuration for domain controllers
Inherits from:	None

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:22 - Remediation #22	edit delete
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	edit delete

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID: 1

Name: DoD DC Standard Submit Query

Description: Standard configuration for d

Inherits from: None

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:22 - Remediation #22	edit delete
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	edit delete

Create Policy for this Group

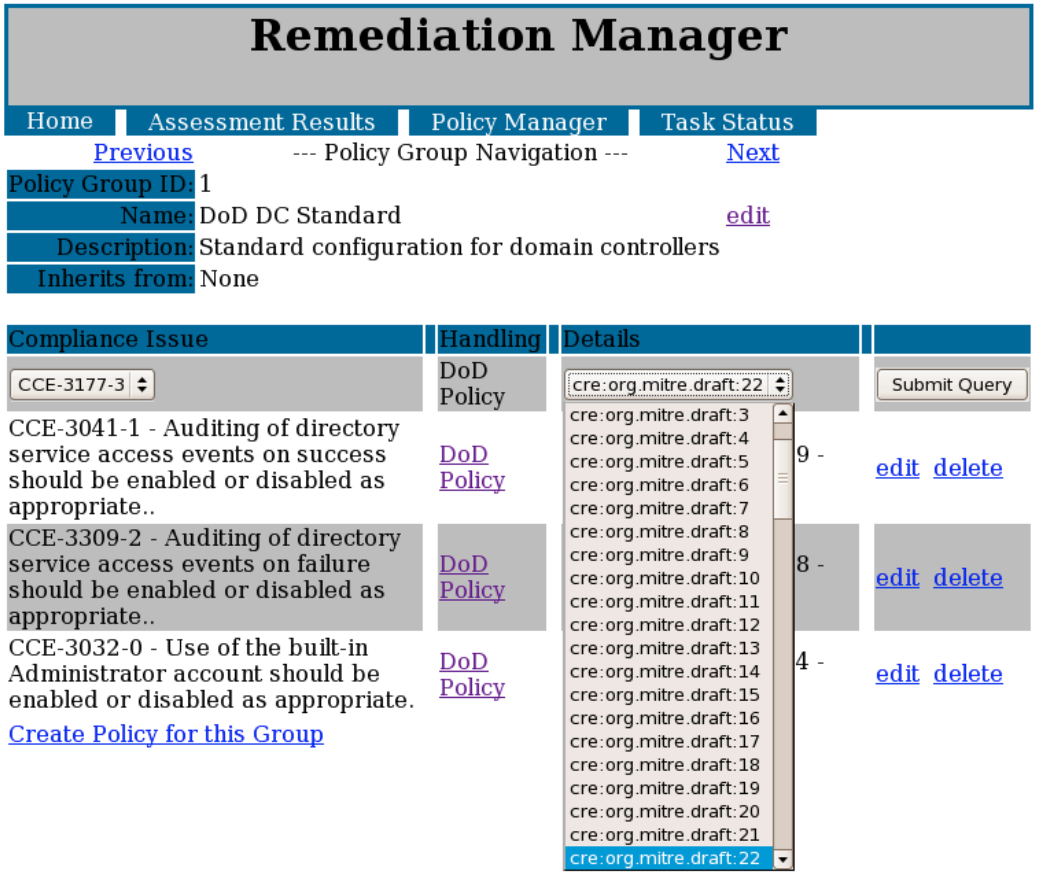
Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	1
Name:	DoD DC Standard edit
Description:	Standard configuration for domain controllers
Inherits from:	None

Compliance Issue	Handling	Details	
CCE-3177-3	DoD Policy	cre:org.mitre.draft:22	Submit Query
CCE-2715-1 CCE-2363-0 CCE-3177-3 CCE-2820-9 CCE-3089-0 CCE-3234-2 CCE-3287-0 CCE-3041-1 CCE-3309-2 CCE-3076-7 CCE-2970-2 CCE-2724-3 CCE-3243-3 CCE-2746-6 CCE-2653-4 CCE-2322-6 CCE-3257-3 CCE-3024-7 CCE-2927-2	Auditing of directory ss events on success abled or disabled as	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
	Auditing of directory ss events on failure abled or disabled as	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
	Use of the built-in r account should be isabled as appropriate. for this Group	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	edit delete



Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	1
Name:	DoD DC Standard edit
Description:	Standard configuration for domain controllers
Inherits from:	None

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:21 - Remediation #21	edit delete
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	edit delete

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Mitigation	Turned off lockout (VIP forgets password)	edit stop mitigating
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	override mitigate
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Mitigation	Mitigation: Turned off lockout Justification: VIP forgets password	Submit Query
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	override mitigate
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:21 - Remediation #21	override mitigate
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	override mitigate
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Local Policy	cre:org.mitre.draft:21 - Remediation #21 Parameter: threshhold=5 Justification: site policy	Submit Query
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	override mitigate
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Local Policy	cre:org.mitre.draft:21 - Remediation #21 threshhold=5 (site policy)	edit stop overriding
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	Mitigation	Mitigation: directory access auditing dis Justification: site policy	Submit Query
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Local Policy	cre:org.mitre.draft:21 - Remediation #21 threshhold=5 (site policy)	edit stop overriding
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	Mitigation	directory access auditing disabled (site policy)	edit stop mitigating
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Local Policy	cre:org.mitre.draft:21 - Remediation #21 threshhold=5 (site policy)	edit stop overriding
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	override mitigate
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group

Remediation Manager

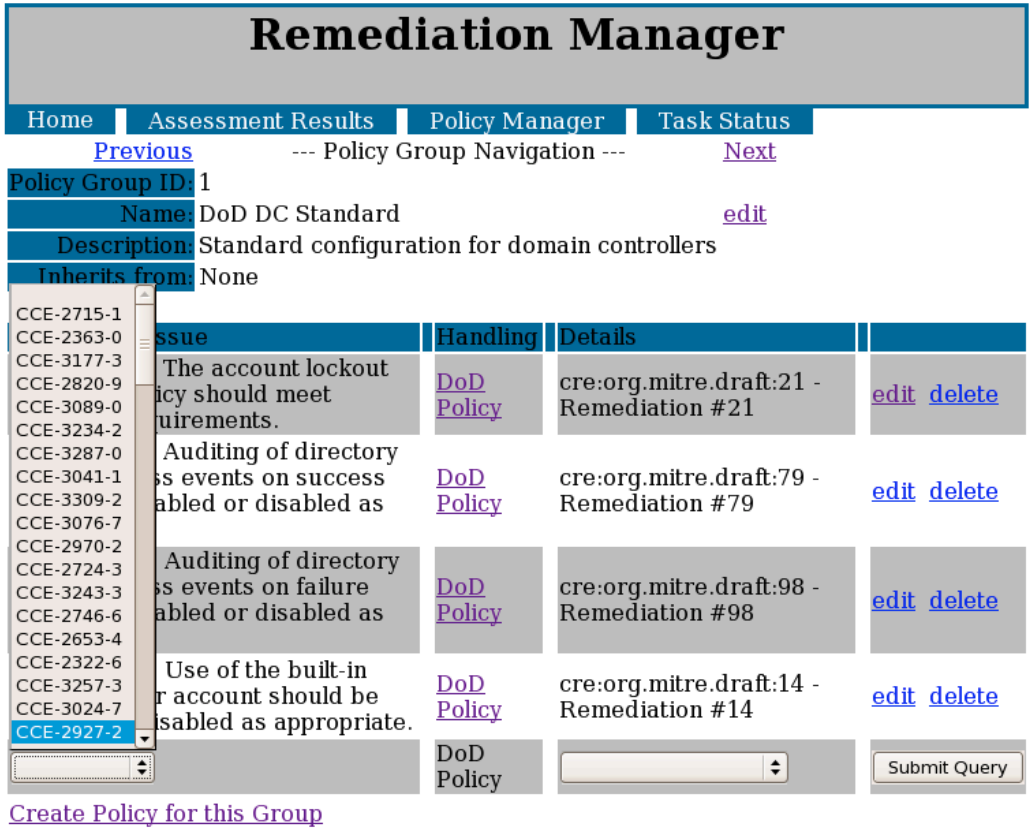
Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	2
Name:	Hartford DC edit
Description:	Governs all domain controllers in Hartford CT
Inherits from:	DoD DC Standard

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Local Policy	cre:org.mitre.draft:21 - Remediation #21 threshhold=5 (site policy)	edit stop overriding
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	Mitigation	directory access auditing disabled (site policy)	edit stop mitigating
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	override mitigate
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate

Create Policy for this Group



Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	1
Name:	DoD DC Standard edit
Description:	Standard configuration for domain controllers
Inherits from:	None

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:21 - Remediation #21	edit delete
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	edit delete
CCE-3050-2	DoD Policy	cre:org.mitre.draft:95	Submit Query

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	1
Name:	DoD DC Standard edit
Description:	Standard configuration for domain controllers
Inherits from:	None

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:21 - Remediation #21	edit delete
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	DoD Policy	cre:org.mitre.draft:14 - Remediation #14	edit delete
CCE-3050-2 - The Screen Saver Timeout setting should be configured correctly for the current user.	DoD Policy	cre:org.mitre.draft:95 - Remediation #95	edit delete

Create Policy for this Group

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Task ID	Host Id	Host Name	Remediation Id	Remediation Reference
1	551	Host550	65	cre:org.mitre.draft:64
2	271	Host270	80	cre:org.mitre.draft:79
3	552	Host551	88	cre:org.mitre.draft:87
4	523	Host522	54	cre:org.mitre.draft:53
5	293	Host292	86	cre:org.mitre.draft:85
6	783	Host782	75	cre:org.mitre.draft:74
7	956	Host955	11	cre:org.mitre.draft:10
8	539	Host538	13	cre:org.mitre.draft:12
9	677	Host676	2	cre:org.mitre.draft:1
10	477	Host476	80	cre:org.mitre.draft:79
11	763	Host762	10	cre:org.mitre.draft:9
12	545	Host544	15	cre:org.mitre.draft:14
13	482	Host481	77	cre:org.mitre.draft:76
14	617	Host616	80	cre:org.mitre.draft:79
15	858	Host857	68	cre:org.mitre.draft:67
16	263	Host262	80	cre:org.mitre.draft:79
17	460	Host459	43	cre:org.mitre.draft:42
18	107	Host106	57	cre:org.mitre.draft:56
19	853	Host852	65	cre:org.mitre.draft:64
20	942	Host941	66	cre:org.mitre.draft:65
21	255	Host254	67	cre:org.mitre.draft:66
22	54	Host53	91	cre:org.mitre.draft:90
23	952	Host951	11	cre:org.mitre.draft:10
24	181	Host180	40	cre:org.mitre.draft:39

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID:	5
Name:	Policy Group #4 edit
Description:	This is Policy Group #4. Its a test group.
Inherits from:	None

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	DoD Policy	cre:org.mitre.draft:21 - Remediation #21	edit delete
CCE-2820-9 - Auditing of account logon events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:76 - Remediation #76	edit delete
CCE-3234-2 - Auditing of account management events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:31 - Remediation #31	edit delete
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:79 - Remediation #79	edit delete
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:98 - Remediation #98	edit delete
CCE-2746-6 - Auditing of policy change events on success should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:43 - Remediation #43	edit delete

Remediation Manager

Home | Assessment Results | Policy Manager | Task Status

Previous --- Policy Group Navigation --- Next

Policy Group ID: 6

Name: Policy Group #5 edit

Description: This is Policy Group #5. Its a test group.

Inherits from: Policy Group #4

Compliance Issue	Handling	Details	
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Local Policy	cre:org.mitre.draft:21 - Remediation #21 ()	edit stop overriding
CCE-2820-9 - Auditing of account logon events on success should be enabled or disabled as appropriate..	Local Policy	cre:org.mitre.draft:76 - Remediation #76 --Parameter Values Go Here-- (null)	edit stop overriding
CCE-2746-6 - Auditing of policy change events on success should be enabled or disabled as appropriate..	Local Policy	cre:org.mitre.draft:43 - Remediation #43 --Parameter Values Go Here-- (null)	edit stop overriding
CCE-2653-4 - Auditing of policy change events on failure should be enabled or disabled as appropriate..	DoD Policy	cre:org.mitre.draft:88 - Remediation #88	edit delete
CCE-3181-5 - Security Audit log warning level should be properly configured.	DoD Policy	cre:org.mitre.draft:27 - Remediation #27	edit delete
CCE-3252-4 - The Digitally Sign Client Communication (Always) policy should be set correctly.	DoD Policy	cre:org.mitre.draft:67 - Remediation #67	edit delete

Questions & Discussion

Purpose of Remediation Manager Development

Build a reference implementation of an automated remediation manager that will enable us to

- Develop, demonstrate, and mature remediation standards, e.g.,
  - Common Remediation Enumeration (CRE)
  - Extended Remediation Information (ERI)
  - Languages and formats for remediation policy, tasking, and results
- Learn more about which remediation functions can be automated – and which will require manual intervention
- Identify and resolve challenges associated with standardizing remediation information and automating the remediation process
- Share interim results and obtain feedback

What's Next for the Remediation Manager? - 1

Extend the reference implementation to include additional capabilities

- Local policy editing – further development
- Standards-based interfaces with additional remediation tools
- Deadlines
- Prioritization (e.g., of multiple CREs per host)
- Ticketing
- Other capabilities

What's Next for the Remediation Manager? - 2

Consider other factors important to an operational RM

- Scaling issues
- Quality attributes
- Deployment options
- Other…

Discuss challenges and seek community input in charting the way forward

- Balance between automation and manual intervention
- Approach to centralized coordination of remediation for DoD
- Support for consolidated, complete reporting of remediation status
- Methods for managing policy deviations and conflicts
- Other…

Remediation Manager Top-Level Capabilities

System-Level Requirement
Accept input scan results formatted as ARF (implemented); and ASR, XCCDF, and OVAL (possible future)
Accept input policy instructions per standards-derived requirement DR 5 (MITRE, 2009; NIST, 2011; NSA, 2010). (partially implemented)
Output a directive to apply a remediation per standards-derived requirement DR 6 (MITRE, 2009; NIST, 2011; NSA, 2010). (partially implemented)
Allow users to choose which remediation to apply when multiple options are included in the policy. (future)
Determine the most efficient method of remediation (e.g., apply a single patch to fix multiple vulnerabilities). (possible future)
Decide how to remediate when multiple remediation systems, including network-oriented systems, are available. (possible future)
Allow a user to tailor remediation policy for a given set of assets as well as accept some risks (i.e., decide not to remediate). (partially implemented)
Assist users in building POA&Ms for policy deviations. (future)
Provide capability to publish POA&M messages consistent with Netops data standards. (future)
Accept Remediation Tool results per standards-derived requirement DR7 (MITRE, 2009; NIST, 2011; NSA, 2010). (partially implemented)
Republish findings received from the RT with notations on fixes made (e.g., updating XCCDF results type to “fixed”; adding “info” messages to OVAL). (future)

References

MITRE. (2009). Wojcik, M.N., Wunder, J., Kerr, M., & Waltermire, D. *Proposed Open Specifications for Enterprise Information Security Remediation*. Bedford, MA: The MITRE Corporation.

MITRE. (2011a). *Common Vulnerabilities and Exposures*. Retrieved January 7, 2011 from http://cve.mitre.org/

MITRE. (2011b). *Common Configuration Enumeration*. Retrieved January 7, 2011 from http://cce.mitre.org/

NIST. (2011). Waltermire, D., Johnson, C., Kerr, M., Wojcik, M., & Wunder, J. *Proposed Open Specifications for Enterprise Information Security Remediation – Draft*. NIST Interagency Report 7670.

NSA. (2010). *Integrated Statement of Work for FY2010 Remediation Concept Development.*