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.



Software Engineering Institute Carnegie Mellon © 2011 Carnegie Mellon University UNCLASSIFIED

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



Software Engineering Institute Carnegie Mellon

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

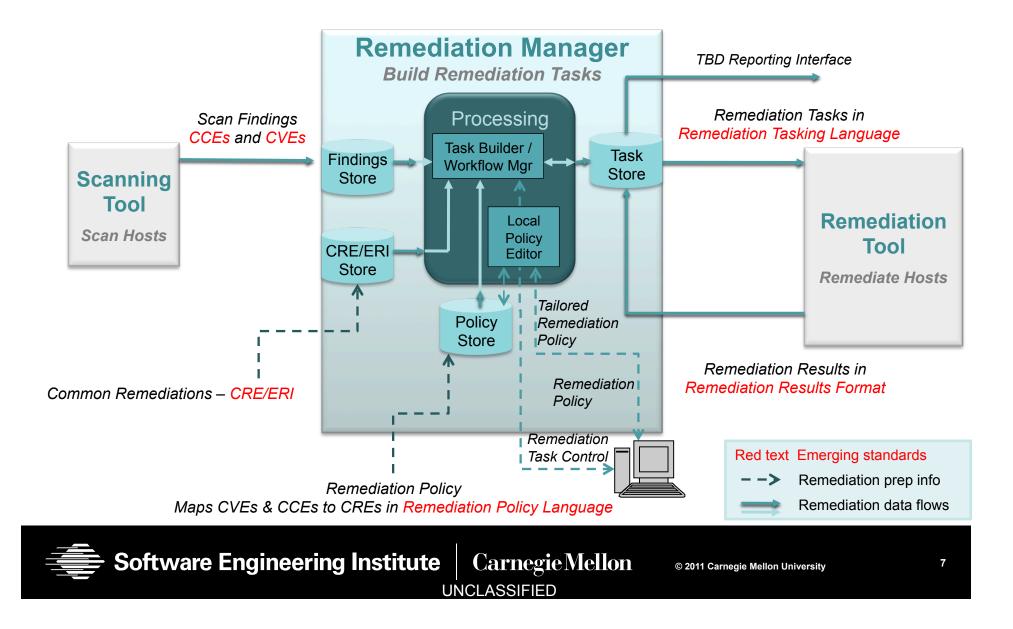
- Ingest host scan findings in DoD Assessment Results Format (ARF), containing
 - Vulnerabilities, specified as Common Vulnerabilities and Exposures (CVEs)
 - Mis-configurations, specified as *Common Configuration Enumerations* (CCEs)
- Build remediation tasks, using *Remediation Policy Language (RPL)* 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.

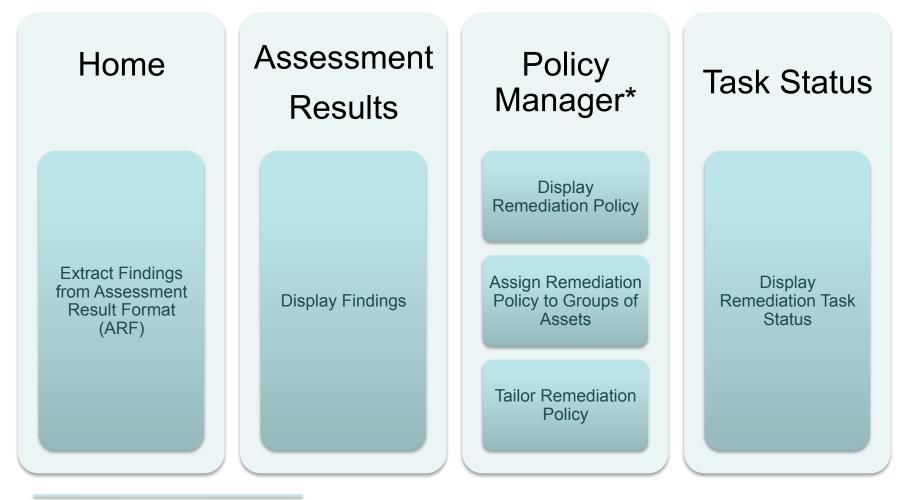


Software Engineering Institute Carnegie Mellon © 2011 Carnegie Mellon U UNCLASSIFIED

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

Last Finding: Wed Mar 02 23:28:15 EST 2011

- # of Active Remediation Tasks: 50
- # of Unassigned Hosts: 0
- # of Unremediated Findings: 50



	Remediation Manager						
Home	Assessment Results	Policy Manager	Task Status				
	<u>Previous</u>	Host Navigat	ion	<u>Next</u>			
H	lost ID: 1						
	IP: 1.0.0.0						
	Name: Host0						
	ddress: 00:00:00:0						
Compliance		Remediation					
CCE-2679- configured	9 - TCP/IP SYN Flood At l.	tack Protection shou	ld be properly	Not yet processed			
CCE-3041- should be	Not yet processed						
	8 - The Shares that can h set correctly.	be accessed anonym	ously policy	Not yet processed			
CCE-2679- configured	9 - TCP/IP SYN Flood At l.	tack Protection shou	ld be properly	Not yet processed			
	1 - Auditing of directory enabled or disabled as a		ts on success	Not yet processed			
	8 - The Shares that can h set correctly.	be accessed anonym	ously policy	Not yet processed			



Software Engineering Institute Carnegie Mellon

UNCLASSIFIED

Remediation Manager					
	Policy Mana				
Previous Policy Gro Policy Group ID: 1	up Navigai	ion <u>Next</u>			
Name: DoD DC Standard		<u>edit</u>			
Description: Standard configurati	on for doma	ain controllers			
Inherits from: None					
Compliance Issue	Handling	Details			
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	<u>DoD</u> Policy	cre:org.mitre.draft:22 - Remediation #22	<u>edit</u> <u>delete</u>		
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:79 - Remediation #79	<u>edit</u> <u>delete</u>		
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>edit</u> <u>delete</u>		
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	<u>edit</u> <u>delete</u>		

Carnegie Mellon

UNCLASSIFIED

Create Policy for this Group



Remediation Manager						
Home	Assessment Results I	olicy Mana	ger	Task Status		
Prev	<mark>vious</mark> Policy Group Navig	gation <mark>Ne</mark>	<u>xt</u>			
Policy Grou	p ID: 1					
N	ame: DoD DC Standard	S	ubmit Q	uery		
Descrip	otion: Standard configuration for	d				
Inherits f	from: None					
Compliance	Issue	Handling	Deta	ils		
threshold p	8 - The account lockout olicy should meet equirements.	<u>DoD</u> <u>Policy</u>		rg.mitre.draft:22 - ediation #22	<u>edit</u>	<u>delete</u>
service acc	- Auditing of directory ess events on success nabled or disabled as	<u>DoD</u> Policy		rg.mitre.draft:79 - ediation #79	<u>edit</u>	<u>delete</u>

<u>DoD</u>

<u>DoD</u>

Policy

Policy

Software Engineering Institute UNCLASSIFIED

appropriate ..

appropriate.

CCE-3309-2 - Auditing of directory service access events on failure

should be enabled or disabled as

CCE-3032-0 - Use of the built-in

Create Policy for this Group

Administrator account should be

enabled or disabled as appropriate.

Carnegie Mellon

cre:org.mitre.draft:98 -

cre:org.mitre.draft:14 -

Remediation #98

Remediation #14

© 2011 Carnegie Mellon University

edit delete

edit delete

Remediation Manager						
Home Assessment Results Previous Policy Gr	Policy Mar	<i>y</i>				
Policy Group ID: 1	oup naviga					
Name: DoD DC Standard		<u>edit</u>				
Description: Standard configurat	ion for don	nain controllers				
Inherits from: None						
Compliance Issue	Handling	Details				
	DoD					
CCE-3177-3 🗘	Policy	cre:org.mitre.draft:22 🖨	Submit Query			
CCE-2715-1 CCE-2363-0 CCE-3177-3 CCE-2820-9 CCE-2820-9	<u>DoD</u> Policy	cre:org.mitre.draft:79 - Remediation #79	<u>edit</u> <u>delete</u>			
CCE-3089-0Auditing of directoryCCE-3234-2s events on failureCCE-3287-0abled or disabled as	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>edit</u> <u>delete</u>			

<u>DoD</u>

Policy



Software Engineering Institute UNCLASSIFIED

Use of the built-in

r account should be

for this Group

sabled as appropriate.

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

Carnegie Mellon

cre:org.mitre.draft:14 -

Remediation #14

© 2011 Carnegie Mellon University

edit delete

Remediation Manager							
Home	Assessment Results	Policy Man	ager	Task Status			
Pr	revious Policy Gi	oup Naviga	tion	Next			
Policy Gro	oup ID: 1						
	Name: DoD DC Standard			<u>edit</u>			
Desci	ription: Standard configura	tion for dom	ain cont	rollers			
Inherit	s from: None						
Complian	ce Issue	Handling	Details				
CCE-3177-3		DoD	Groupra	mitre.draft:22 🖨	Submit Query		
LCCE-31/7-		Policy	S		Submit Query		
CCE-3041	CCE-3041-1 - Auditing of directory						

	roncy	1	-	1		
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:3 cre:org.mitre.draft:4 cre:org.mitre.draft:5 cre:org.mitre.draft:6 cre:org.mitre.draft:7		9 -	<u>edit</u>	<u>delete</u>
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:8 cre:org.mitre.draft:9 cre:org.mitre.draft:10 cre:org.mitre.draft:11 cre:org.mitre.draft:12		8 -	<u>edit</u>	<u>delete</u>
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate. <u>Create Policy for this Group</u>	<u>DoD</u> Policy	cre:org.mitre.draft:13 cre:org.mitre.draft:14 cre:org.mitre.draft:15 cre:org.mitre.draft:16 cre:org.mitre.draft:17 cre:org.mitre.draft:18 cre:org.mitre.draft:19		4 -	<u>edit</u>	<u>delete</u>
		cre:org.mitre.draft:20 cre:org.mitre.draft:21 cre:org.mitre.draft:22	•			

UNCLASSIFIED



Software Engineering Institute

Carnegie Mellon

© 2011 Carnegie Mellon University

Remediation Manager					
	Policy Mana				
Previous Policy Gro	up Navigati	on <u>Next</u>			
Policy Group ID: 1					
Name: DoD DC Standard		<u>edit</u>			
Description: Standard configuration	on for doma	in 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	<u>edit</u> <u>delete</u>		
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:79 - Remediation #79	<u>edit</u> <u>delete</u>		
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:98 - Remediation #98	<u>edit</u> <u>delete</u>		
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	<u>edit</u> <u>delete</u>		

Create Policy for this Group



Software Engineering Institute

Carnegie Mellon

UNCLASSIFIED

© 2011 Carnegie Mellon University

Remediation Manager						
Home Assessment Result		Manager 💦 Task Status				
	cy Group Na	vigation <u>Next</u>				
Policy Group ID: 2 Name: Hartford DC		edit				
Description: Governs all dor	nain controll					
Inherits from: DoD DC Standa						
	** 11.	D + 4				
Compliance Issue	Handling	Details				
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	Mitigation	Turned off lockout (VIP forgets password)	<u>edit</u> <u>stop</u> mitigating			
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:79 - Remediation #79	<u>override</u> <u>mitigate</u>			
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>override</u> <u>mitigate</u>			
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:14 - Remediation #14	<u>override</u> <u>mitigate</u>			

Create Policy for this Group

Software Engineering Institute

Carnegie Mellon

Remediation Manager						
HomeAssessment ResultPrevious PolicPolicy Group ID:2Name:Hartford DCDescription:Governs all dorInherits from:DoD DC Standard	cy Group Na nain controll	edit				
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	<u>DoD</u> 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	<u>DoD</u> <u>Policy</u>	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.	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:14 - Remediation #14	<u>override</u> <u>mitigate</u>			

Create Policy for this Group



Carnegie Mellon

UNCLASSIFIED

Remediation Manager						
Home Assessment Results		Manager Task Status				
	y Group Na	vigation <u>Next</u>				
Policy Group ID: 2		1.1				
Name: Hartford DC		edit				
Description: Governs all dom		iers in Hartford CT				
Inherits from: DoD DC Standa	<u>ra</u>					
Compliance Issue	Handling	Details				
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	<u>DoD</u> Policy	cre:org.mitre.draft:21 - Remediation #21	<u>override</u> <u>mitigate</u>			
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:79 - Remediation #79	<u>override</u> <u>mitigate</u>			
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>override</u> <u>mitigate</u>			
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	override mitigate			

UNCLASSIFIED

<u>Create Policy for this Group</u>

Software Engineering Institute

Carnegie Mellon © 2011

Remediation Manager							
Home Assessment Results							
	y Group Na	vigation <u>Next</u>					
Policy Group ID: 2							
Name: Hartford DC		edit					
Description: Governs all dom		lers in Hartford CT					
Inherits from: DoD DC Standa	<u>rd</u>						
Compliance Issue	Handling	Details					
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	<u>DoD</u> 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	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>override</u> mitigate				
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	<u>override</u> <u>mitigate</u>				

Carnegie Mellon

UNCLASSIFIED

Create Policy for this Group



Remediation Manager						
HomeAssessment ResultsPolicy ManagerTask StatusPrevious Policy Group NavigationNextPolicy Group ID:2Name:Hartford DCeditDescription:Governs all domain controllers in Hartford CTInherits 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)	<u>edit</u> <u>stop</u> overriding			
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	Mitigation	Mitigation: directory access auditing di: Justification: site policy	Submit Query			
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>override</u> <u>mitigate</u>			
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	<u>override</u> <u>mitigate</u>			

UNCLASSIFIED

Create Policy for this Group



Carnegie Mellon © 2011

Remediation Manager						
Home Assessment Result	s Policy	Manager 👘 Task Status				
	cy Group Na	vigation <u>Next</u>				
Policy Group ID: 2						
Name: Hartford DC		<u>edit</u>				
Description: Governs all do		lers in Hartford CT				
Inherits from: DoD DC Stand	<u>ard</u>					
Compliance Issue	Handling	Details				
CCE-3177-3 - The account	manumg	Details				
lockout threshold policy	Local	cre:org.mitre.draft:21 -	edit stop			
should meet minimum	Policy	Remediation #21 threshhold=5 (site policy)	overriding			
requirements.		tinesinoid=5 (site policy)				
CCE-3041-1 - Auditing of						
directory service access events on success should be	Mitigation	directory access auditing	<u>edit</u> <u>stop</u>			
enabled or disabled as	migution	disabled (site policy)	<u>mitigating</u>			
appropriate						
CCE-3309-2 - Auditing of						
directory service access events on failure should be	DoD	cre:org.mitre.draft:98 -				
enabled or disabled as	Policy	Remediation #98	<u>override</u> <u>mitigate</u>			
appropriate						
CCE-3032-0 - Use of the						
built-in Administrator account	DoD	cre:org.mitre.draft:14 -	override mitigate			
should be enabled or disabled	<u>Policy</u>	Remediation #14	storrido miliguto			
as appropriate.						

Carnegie Mellon

UNCLASSIFIED

Create Policy for this Group

Software Engineering Institute

© 2011 Carnegie Mellon University

Remediation Manager							
Home Assessment Results		Manager 🔋 Task Status					
	y Group Na	wigation <u>Next</u>					
Policy Group ID: 2 Name: Hartford DC		o dit					
Description: Governs all dom	ain control	edit lors in Hartford CT					
Inherits from: DoD DC Standa							
mients nom. Dob De Standa	<u>1u</u>						
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)	<u>edit</u> stop overriding				
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	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	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>override</u> <u>mitigate</u>				
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:14 - Remediation #14	<u>override</u> <u>mitigate</u>				

Carnegie Mellon

UNCLASSIFIED

Create Policy for this Group

Software Engineering Institute

Remediation Manager						
Home Assessment Result		Manager Task Status				
	cy Group Na	vigation <u>Next</u>				
Policy Group ID: 2		1				
Name: Hartford DC		edit				
Description: Governs all do		lers in Hartford CT				
Inherits from: DoD DC Stand	ard					
Compliance Issue	Handling	Details				
CCE-3177-3 - The account	manumg	Details				
lockout threshold policy	Local	cre:org.mitre.draft:21 -	<u>edit</u> <u>stop</u>			
should meet minimum	Policy	Remediation #21 threshhold=5 (site policy)	overriding			
requirements.		tinesinoid=5 (site policy)				
CCE-3041-1 - Auditing of						
directory service access events on success should be	Mitigation	directory access auditing	<u>edit</u> <u>stop</u>			
enabled or disabled as	Miligation	disabled (site policy)	mitigating			
appropriate						
CCE-3309-2 - Auditing of						
directory service access	DoD	cre:org.mitre.draft:98 -				
events on failure should be enabled or disabled as	Policy	Remediation #98	<u>override</u> <u>mitigate</u>			
appropriate						
CCE-3032-0 - Use of the						
built-in Administrator account	<u>DoD</u>	cre:org.mitre.draft:14 -	ovorrido, miticata			
should be enabled or disabled	<u>Policy</u>	Remediation #14	<u>override</u> <u>mitigate</u>			
as appropriate.						

Create Policy for this Group

Software Engineering Institute Carnegie Mellon

UNCLASSIFIED

Remediation Manager						
Home Assess	ment Results	Policy Mar	nager 💦 Task Status			
Previous	Policy Gi	oup Naviga	ation <u>Next</u>			
Policy Group ID: 1						
Name: Do	D DC Standard		edit			
Description: Sta	andard configurat	tion for don	nain controllers			
Inherits from: No						
CCE-2715-1						
CCE-2363-0 = ssue		Handling	Details			
CCE-3177-3 The a	ccount lockout ould meet ents.	<u>DoD</u> Policy	cre:org.mitre.draft:21 - Remediation #21	<u>edit</u> <u>delete</u>		
CCE-3287-0 Auditi CCE-3041-1 s even CCE-3309-2 abled o CCE-3076-7	ing of directory ats on success or disabled as	<u>DoD</u> Policy	cre:org.mitre.draft:79 - Remediation #79	<u>edit</u> <u>delete</u>		
CCE-3243-3 S ever	ing of directory ats on failure or disabled as	<u>DoD</u> Policy	cre:org.mitre.draft:98 - Remediation #98	<u>edit</u> <u>delete</u>		
CCE-3257-3 CCE-3024-7 r accor	f the built-in unt should be l as appropriate.	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:14 - Remediation #14	<u>edit</u> <u>delete</u>		
		DoD Policy	•	Submit Query		

Create Policy for this Group



Software Engineering Institute UNCLASSIFIED

Carnegie Mellon

Remediation Manager						
Home Assessment Results	Policy Mar	nager 💦 Task Status				
Previous Policy Gr	oup Naviga	ation <u>Next</u>				
Policy Group ID: 1		- 10				
Name: DoD DC Standard	ion for don	edit				
Description: Standard configurat Inherits from: None	1011 101. (101)	nam controllers				
timerits from: none						
Compliance Issue	Handling	Details				
CCE-3177-3 - The account lockout threshold policy should meet	<u>DoD</u>	cre:org.mitre.draft:21 - Remediation #21	<u>edit</u> <u>delete</u>			
minimum requirements.	<u>Policy</u>	Remediation #21				
CCE-3041-1 - Auditing of directory service access events on success	DoD	cre:org.mitre.draft:79 -	edit delete			
should be enabled or disabled as appropriate	<u>Policy</u>	Remediation #79	<u>cuit</u> <u>delete</u>			
CCE-3309-2 - Auditing of directory service access events on failure	DoD	cre:org.mitre.draft:98 -				
should be enabled or disabled as	Policy	Remediation #98	<u>edit</u> <u>delete</u>			
appropriate						
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	<u>edit</u> <u>delete</u>			
CCE-3050-2	DoD Policy	cre:org.mitre.draft:95	Submit Query			

Create Policy for this Group



Software Engineering Institute **Carnegie Mellon**

UNCLASSIFIED

Remediation Manager					
	olicy Mana				
Previous Policy Grou	up Navigati	ion <u>Next</u>			
Policy Group ID: 1 Name: DoD DC Standard Description: Standard configuratio Inherits from: None	on for doma	<u>edit</u> nin controllers			
Compliance Issue	Handling	Details			
CCE-3177-3 - The account lockout threshold policy should meet minimum requirements.	<u>DoD</u> Policy	cre:org.mitre.draft:21 - Remediation #21	<u>edit</u> <u>delete</u>		
CCE-3041-1 - Auditing of directory service access events on success should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:79 - Remediation #79	<u>edit</u> <u>delete</u>		
CCE-3309-2 - Auditing of directory service access events on failure should be enabled or disabled as appropriate	<u>DoD</u> <u>Policy</u>	cre:org.mitre.draft:98 - Remediation #98	<u>edit</u> <u>delete</u>		
CCE-3032-0 - Use of the built-in Administrator account should be enabled or disabled as appropriate.	<u>DoD</u> Policy	cre:org.mitre.draft:14 - Remediation #14	<u>edit</u> <u>delete</u>		
CCE-3050-2 - The Screen Saver Timeout setting should be configured correctly for the current user.	<u>DoD</u> Policy	cre:org.mitre.draft:95 - Remediation #95	<u>edit</u> <u>delete</u>		
Create Policy for this Group					

<u>Create Policy for this Group</u>



Software Engineering Institute UNCLASSIFIED

Carnegie Mellon

	Remediation Manager						
Hoi	ne A	ssessment R	lesults	Policy Manager Task Status			
Task				diation 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			



Software Engineering Institute

Carnegie Mellon

UNCLASSIFIED

© 2011 Carnegie Mellon University

Remediation Manager						
Home A	Assessment Results Policy Manager	Task Status				
Previ	ous Policy Group Navigation	<u>Next</u>				
Policy Group	ID: 5					
Na	me: Policy Group #4	<u>edit</u>				
Description: This is Policy Group #4. Its a test group.						
Inherits fr	om: None					

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

UNCLASSIFIED

Software Engineering Institute

Carnegie Mellon

Remediation Manager

Home	Assessment Results	S Policy Manager	Task Status
Pr	revious Policy (Group Navigation	<u>Next</u>
Policy Gro	oup ID: 6		
	Name: Policy Group #5	5	<u>edit</u>
Desci	ription: This is Policy G	roup #5. Its a test grou	p.
Inherits	s from: Policy Group #4	<u>4</u>	

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 ()	<u>edit</u> <u>stop</u> 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)	<u>edit</u> 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)	<u>edit</u> <u>stop</u> overriding
CCE-2653-4 - Auditing of policy change events on failure should be enabled or disabled as appropriate	<u>DoD</u> Policy	cre:org.mitre.draft:88 - Remediation #88	<u>edit</u> <u>delete</u>
CCE-3181-5 - Security Audit log warning level should be properly configured.	<u>DoD</u> Policy	cre:org.mitre.draft:27 - Remediation #27	edit delete
CCE-3252-4 - The Digitally Sign Client Communication (Always) policy should be set correctly.	<u>DoD</u> Policy	cre:org.mitre.draft:67 - Remediation #67	edit delete

UNCLASSIFIED



Software Engineering Institute

Carnegie Mellon

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)



Software Engineering Institute Carnegie Mellon © 2011 Ca UNCLASSIFIED

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 <u>http://cce.mitre.org/</u>

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.

