CRE and ERI
Workshop Session

IT Security Automation Conference
September 27-29, 2010

Chris Johnson
Computer Security Division
Information Technology Laboratory
The National Institute of Standards and Technology (NIST)

Agenda

- About the Workshop
- Background
- Overview
- CRE Overview
- ERI Overview
- Discussion Topics

About the Workshop

The remediation workshop is intended to be:

- Informal
- Conversational
- Informational

The remediation workshop is an opportunity to help shape the specifications by:

- Exposing new and interesting use cases
- Gathering new requirements
- Refining proposed technical approaches to remediation

Workshop Sessions

- *Session 1: Common Remediation Enumeration (CRE) and Extended Remediation Information (ERI)*
  - Time/Moderator: 10:30am-11:15am/Chris Johnson, NIST
- *Session 2: Remediation Policy*
  - Time/Moderator: 11:30am-12:15pm/Matthew Wojcik, MITRE

*************** LUNCH ****************

- *Session 3: Remediation Policy*
  - Time/Moderator: 1:15pm-2:00pm/Matthew Wojcik, MITRE
- *Session 4: Remediation Tasking*
  - Time/Moderator: 2:15pm-3:00pm/Matthew Wojcik, MITRE

*************** BREAK ****************

- *Session 5: Remediation Language*
  - Time/Moderator: 3:30pm-4:15pm/Greg Witte, G2
- *Session 6: Secstate: Integrating SCAP and Puppet for System Lockdown*
  - Time/Presenter: 4:30pm-5:15pm/Karl MacMillan, Tresys Technology

Background

Goal: Produce standardized security automation capabilities that impart greater efficiency in enterprise remediation processes

Approach: Explore the technical use cases for remediation and identify opportunities to enhance existing remediation capabilities and foster innovation through standardization

Result: A suite of 8 proposed specifications that describe naming conventions, data exchange formats, and languages for remediation

Overview
Proposed Specifications (1)

Common Remediation Enumeration (CRE)

- Common names and basic remediation information

CRE Data Exchange Format

- Exchange format for CRE content

Extended Remediation Information (ERI)

- Mappings and other supplemental remediation details

ERI Data Exchange Format

- Exchange format for ERI content

Overview
Proposed Specifications (2)

Remediation Policy

- Express remediation policy

Remediation Tasking Language

- Ability to issue remediation directives to tools

Remediation Results Format

- Common format for the outcome of remediation attempts

Open Vulnerability Remediation Language (OVRL)

- Language for constructing machine-readable instructions necessary to perform the desired remediation

Common Remediation Enumeration (CRE)

- Assign a common identifier to the set of actions that must be performed to accomplish a distinct remediation objective
- CRE entry will contain the minimum amount of information necessary to distinguish it from other CRE entries and to describe its purpose

CRE Data Fields

- Unique Identifier
- Prose description of the remediation
- Conceptual Parameters
- Supporting References
- Metadata
  - Creation/Modification Dates
  - Entry Status
  - Version
  - Provenance

CRE Use Cases
Initial Configuration

Goal: Initial configuration of a system(s) to be in compliance with a predefined policy

Success Scenario: User of a standards-based remediation tool dispatches a series of remediation tasks to bring the target system(s) into compliance. The remediation actions are identified using CREs. Remediation tool performs the remediation tasks associated with the selected CREs and issues a report indicating that the CREs were successfully performed.

Failure Condition: Remediation tool is unable to complete all the assigned remediation tasks and issues a report that identifies CREs that were successfully applied and those that failed with an accompanying error message.

CRE Use Cases
Vulnerability Remediation

Goal: Remedy software flaws (CVE) detected by an assessment scanner

Success Scenario: User of a standards-based remediation tool selects and dispatches the appropriate CRE remediation actions for the CVEs detected. The remediation tool performs the selected remediation tasks and issues a report indicating that the CREs that were successfully applied.

Failure Condition: Remediation tool is unable to complete the assigned remediation tasks and issues a report that identifies the CREs that were not successfully applied and an accompanying error message.

CRE Use Cases
Compliance Enforcement

Goal: Remedy a non-compliant configuration setting (CCE) detected by an assessment scanner

Success Scenario: User of a standards-based remediation tool selects and dispatches the appropriate CRE remediation action for the CCE detected. The remediation tool performs the selected remediation task and issues a report indicating that the CRE was successfully applied.

Failure Condition: Remediation tool is unable to complete the assigned remediation task and issues a report that identifies the CRE that was not successfully applied and an accompanying error message.

CRE Sample Entry

Name	Value
CRE ID	cre:org.sample.cre.draft:1
CRE Description	Set the desired permissions on file sample.exe
Parameters	Desired file access permissions
Platform	cpe:/o:vendor_test:sample_os
References	http://www.sample.org/security/guidance
Entry Created	12 October 2009
Entry Modified	07 July 2010
Entry Version	2
Submitter	A3Q
Deprecated	FALSE

Extended Remediation Information (ERI)

- ERI captures additional information related to CRE entries – information that is often needed to fully support the enterprise remediation use cases described
- Capturing this supplemental data in ERI allows CRE to be much more lightweight and stable
- This approach is analogous to CVE (which carries essential identifying information about the vulnerability) and the extended data is available through the National Vulnerability Database (NVD) and its vulnerability data feeds.

ERI Data Fields

- Unique Identifier
- CRE Reference
- Indicators
- Parameter Mappings
- Supersedes
- Prerequisites
- Operational Impact
- Reboot
- Additional Metadata

ERI Use Cases
CRE Discovery based on CVE/CCE

Goal: Identify CREs that are relevant to a particular CVE (software flaw) or CCE (configuration setting)

Scenario: User submits a CVE or CCE identifier to an ERI repository as part of a query and is presented a list of candidate CREs. If the ERI repository is unable to locate an appropriate CRE for the CVE or CCE submitted an informational message is displayed.

ERI Use Cases
CRE Discovery based on CPE

Goal: Identify CREs that are relevant to a particular CPE (hardware, operating system or application)

Scenario: User submits a CPE identifier to an ERI repository as part of a query and is presented a list of candidate CREs. If the ERI repository is unable to locate an appropriate CRE for the CPE submitted an informational message is displayed.

ERI Use Cases
Operational Impact

Goal: Determine if a particular CRE has any reported operational impacts.

Scenario: User submits a CRE identifier to an ERI repository as part of a query and is presented information describing the possible operational impacts related to the CRE. If the ERI repository is unable to locate any information regarding operational impact for the CRE submitted an informational message is displayed.

ERI Use Cases
Reboot Requirements

Goal: Identify all CREs that require a reboot of the system for a particular CPE.

Scenario: User submits a CPE identifier to an ERI repository as part of a query and is presented a list of CREs for which a system reboot is required. If the ERI repository is unable to locate any CRE meeting the criteria an informational message is displayed.

ERI Sample Entry

Name	Value
ERI ID	eri:org.sample.eri.draft:101
CRE Reference	cre:org.sample.cre.draft:27
Indicators	CCE-2824-1
Parameter Mappings	Conceptual Value 1:Enable Literal Value 1:1 Conceptual Value 2:Disable Literal Value 2:0
Supersedes	None
Prerequisites	cre:org.sample.cre.draft:9
Operational Impact	None
Reboot	TRUE
Submitter	A3Q
Deprecated	FALSE

Discussion Points: Indicators

Does the CRE platform field identify where the indicator resides (CVE or CCE) or where the remediation action is to be applied?

- Sometimes the remedy is applied to another system (other than the affected system)
- This does have an impact on a use case introduced earlier (get CREs by CPE)
- CVEs are cross-platform – CREs are not
- CRE for a service pack or security rollup package will have lots of indicators

Discussion Points: Parameterization

Should system objects be parameterized, or only the characteristics of a system object included in the definition of the CRE itself?

For example, when considering setting file access permissions, should the file be specified as a parameter along with the desired permissions settings, or should separate CREs created for each file of interest, and only the desired permissions be included as a parameter?

Discussion Points: Reboot Action

Reboot Action: Should we create a separate CRE for reboot?

- There may be times when a reboot is desired (independent of any other remediation operation)
- Allows us to use CREs within our remediation workflows
- Need to reboot will likely arise when we consider policy and tasking
- May need to consider this for restarts as well (e.g., database or web service)

Discussion Points: Reboot Alert

Reboot Alert: Should we add a field to indicate that a reboot will occur as part of the remediation process (non-discretionary reboot)

- Could we note this in the operational impact field?
- Are we aware of other remediation actions that perform

Discussion Points: Identifier Integrity

Identifier Integrity:

- Should we check digit to the identifier?
- Use a GUID?
- Do nothing and allow invalid CREs to be identified through validation and verification activities performed by the content originator

Enumeration Consistency Check

These standard algorithms provide clients with an inexpensive mechanism to ensure a correct remediation action is performed.

- Luhn check digit – Single digit checksum (CCE standard)
  - Low computational overhead (can be verified manually)
  - Detects most simple entry errors
  - Problem: will not always detect some simple errors
- Verhoeff check digit
  - Can detect a more complete set of errors
  - Problem: still a few exceptions will not be caught
  - Problem: More complex algorithm; not manually verifiable
- GUID – Globally Unique IDentifier (safety through improbability)
  - Large number space ensures values are sparse. (2^{128} possible values)
  - No runtime overhead, if ID is incorrect, conflicting entry will not be found
  - Can be generated directly by most OS and database systems
  - Problem: not suitable for manual entry

Discussion Points: Parameters

Mapping of Conceptual to Literal Parameters:

- Does this introduce excessive complexity?
- Can we effectively create and maintain such mappings?

Discussion Points: Scope of the Remediation

Scope of Remediation:

- Local vs. Domain
- Effective setting
- Persistence of change

For Additional Information

Visit the SCAP Emerging Specifications web page at:

- http://scap.nist.gov/emerging-specs/listing.html

Monitor the emerging-specs@nist.gov email list

- Announcements and technical discussions
- See http://scap.nist.gov/community.html to subscribe

NIST Computer Security Resource Center (CRSC)

- http://csrc.nist.gov/publications/PubsSPs.html

Contact the Automated Remediation Working Group Core Team:

Chris Johnson, NIST <christopher.johnson@nist.gov>

Mathew Kerr, G2, Inc. <matt.kerr@g2-inc.com>

Matthew Wojcik, MITRE woj@mitre.org

Closing Thoughts

- Thank you for participating in today's workshop!
- Please continue to provide feedback regarding the draft specifications
- We encourage your continued participation in future workshops and teleconference

Backup Slides

Remediation

A set of actions that results in a change to the state of an IT asset that may be motivated by the need to enforce organizational security policies, address discovered vulnerabilities, or to correct an improper/insecure system configuration setting

Enterprise Remediation

Describes remediation capabilities that span an organization and address the:

- Definition, application and enforcement of organizational security remediation policies
- Management of remediation tasks
- Dissemination of remediation instructions
- Reporting the results of remediation attempts

Components of Automated Enterprise Remediation

Collection of individually maintained, community developed, open specifications that can be used to identify, describe and implement system changes across the enterprise

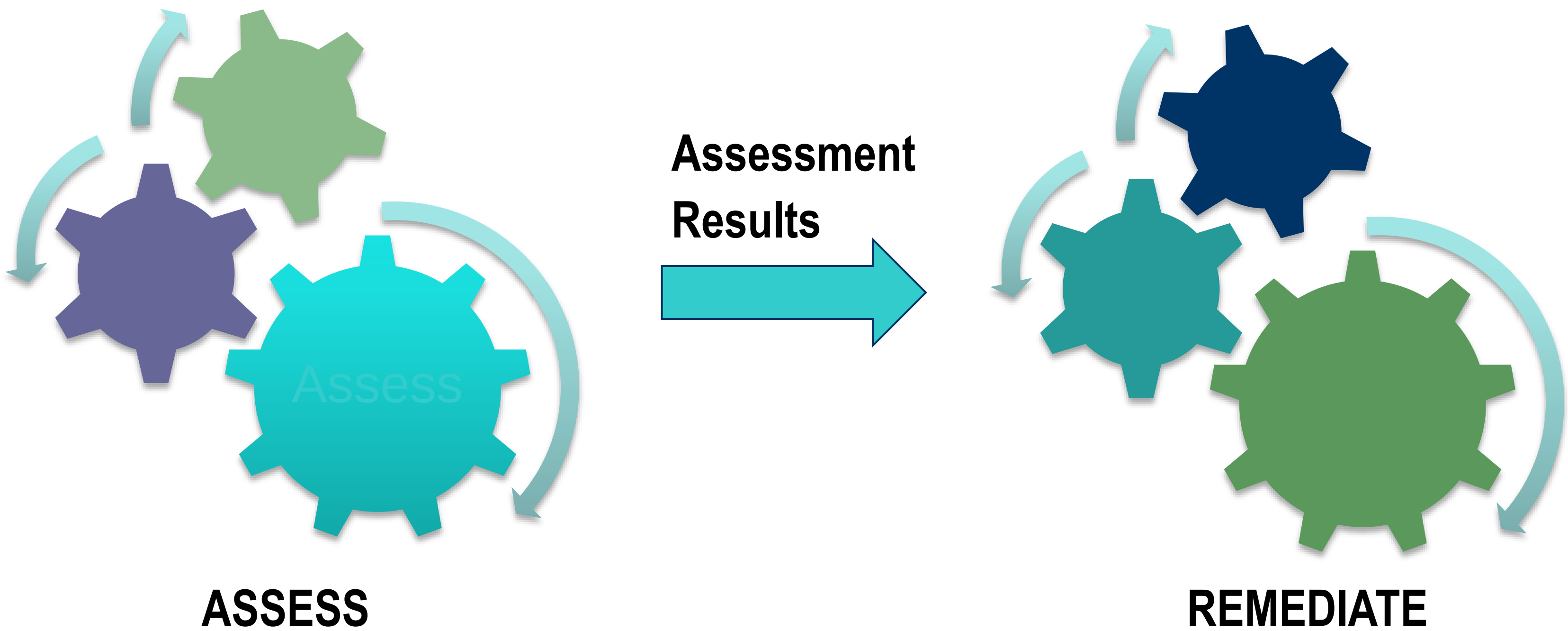
- Component specifications that establish conventions for identifying, describing, tasking and performing remediation actions
- High-level specifications define how the component specifications are used in concert to deliver capabilities to the security automation community

Body of reference data expressed in accordance with the specifications

Exploring Some Use Cases

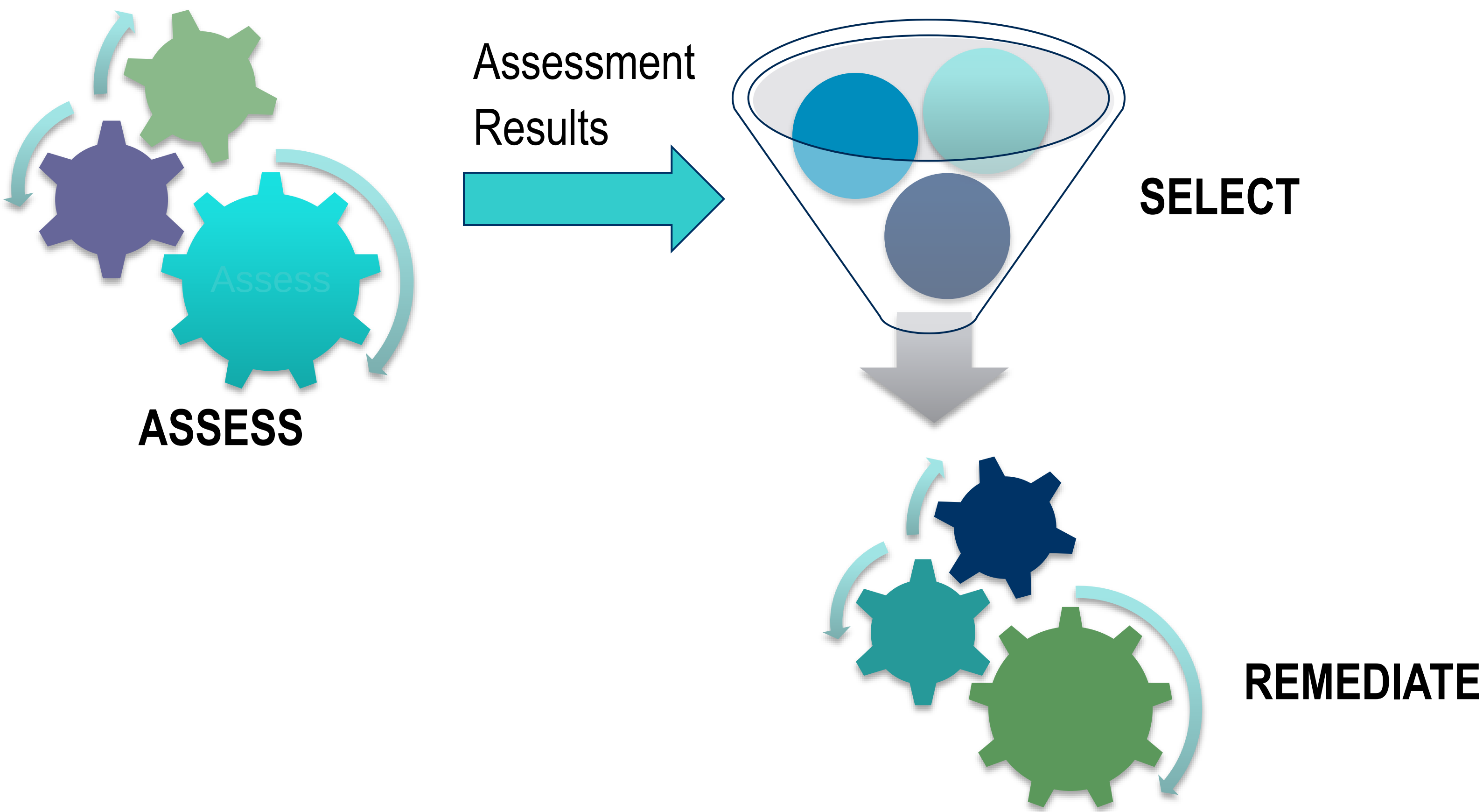
Use Case 1
Comprehensive Remediation

<u>GOAL</u>: Remediate one or more computing assets for all vulnerabilities and misconfigurations discovered during a prior assessment



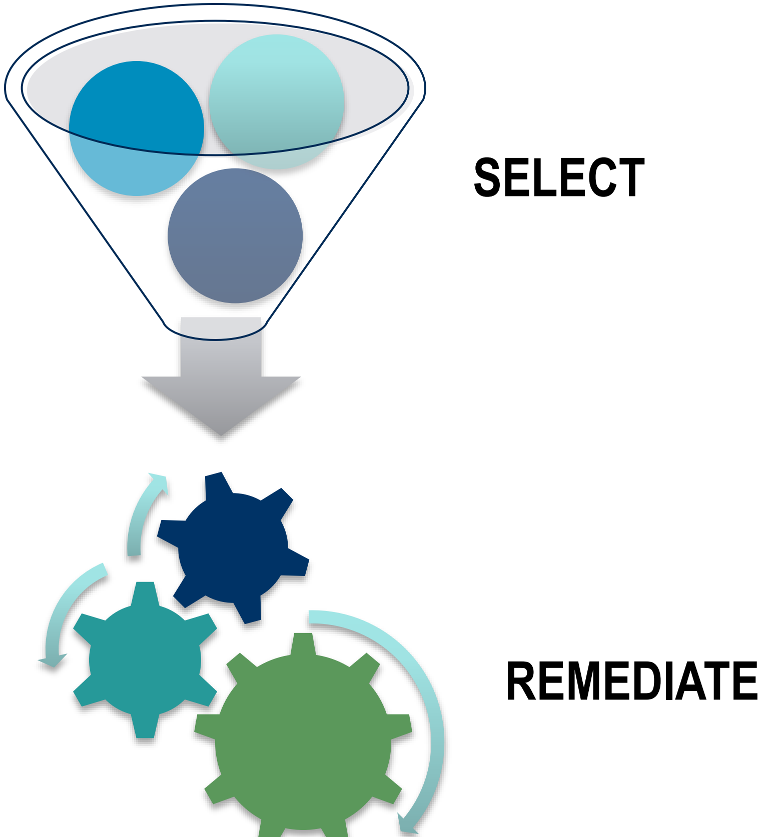
Use Case 2
Selective Remediation

<u>GOAL:</u> Remediate one or more computing assets for a subset of vulnerabilities and misconfigurations discovered during a prior assessment



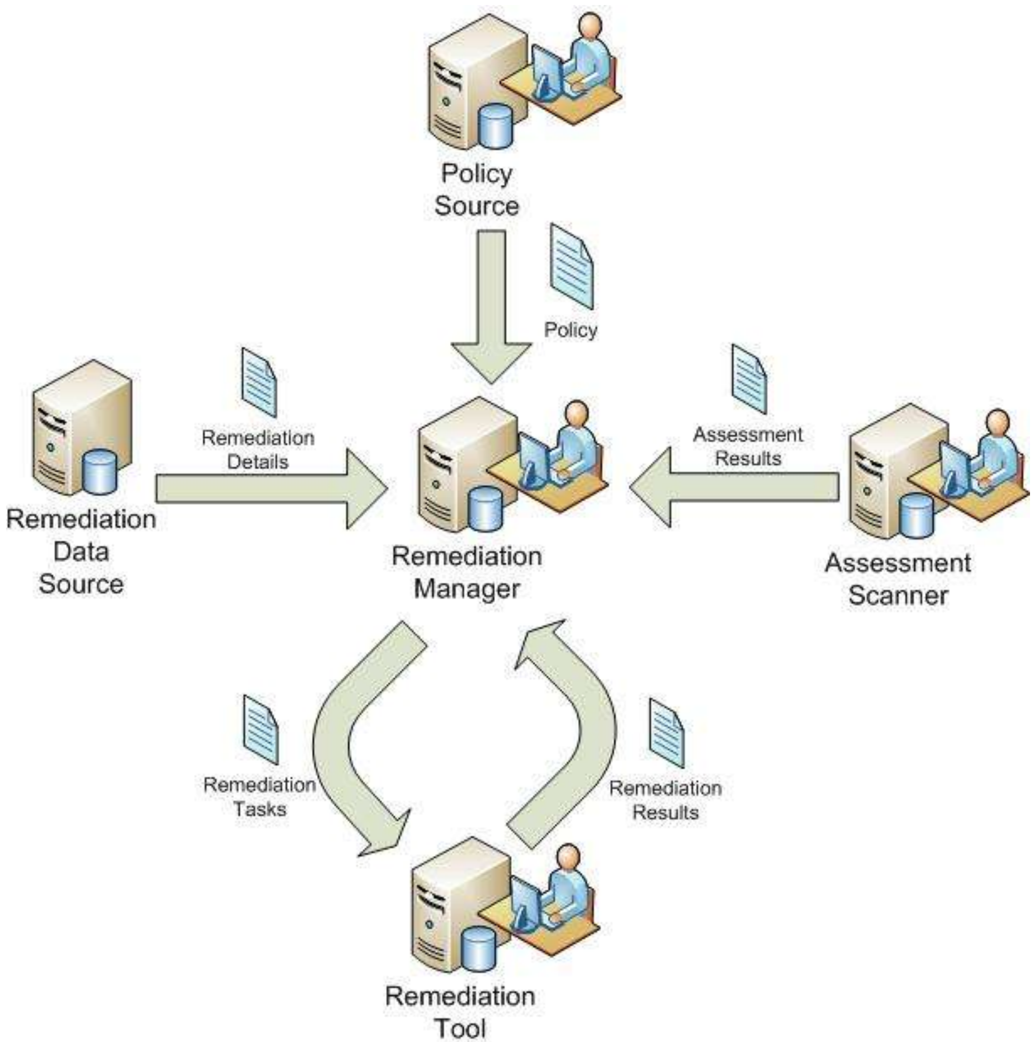
Use Case 3
Independent Remediation

<u>Goal:</u> Apply one or more remediations to one or more computing assets regardless of their current security state (as determined by an assessment scanner).



Enterprise Remediation Logical Workflow Diagram

Remediation Information could originate from a product vendor, security tool database, third-party source, or it may reside in a local repository within the organization



An Additional Note on CREs

A desired end state can often be reached in multiple ways - for example, a service may be disabled by:

- Commenting out the service startup command in a configuration file
- Changing the file permissions on the executable associated with the service
- Removal of the executable associated with the service

A separate CRE would be issued for each of these examples because the method and parameters for implementing the change are unique.