Emerging Remediation Specifications: Overview

Matthew N. Wojcik & Gerry McGuire

25 March 2011

MITRE

© 2011 The MITRE Corporation. All rights reserved.

Remediation Specifications: Background

- **Goal: Increased automation, openness, interoperability of IT Remediation activities**
  - **Sometimes described as "SCAP for remediation"**

- **"Remediation" defined here as:**
  - "[A] security-relatedset of actions that results in a change to a computer's state" – NIST Interagency Report 7670 (Draft), *Proposed Open Specifications for an Enterprise Remediation Automation Framework*
  - **Footnotes:**
    - **Similarities in general configuration management**
    - **Possible applicability to network devices, etc.**

- **Approach: Develop a set of open remediation standards**
  - **Through open community discussions and developer events**
  - **Establishing consensus wherever possible**
  - **Supported by research and development, prototyping tools and content**

© 2011 The MITRE Corporation. All rights reserved.

Background Continued

- **Identified use cases include:**
  - **Scan and remediate: Address vulnerabilities and mis-configurations discovered on end systems**
  - **Configuration compliance: Bring a system in line with a baseline (e.g., DISA STIG)**
  - **Targeted remediation: Rapidly respond to emerging threats**

- **Requirements include:**
  - **Integrate with SCAP assessment**
  - **Map well onto existing commercial remediation capabilities**
  - **Accommodate legacy tools**

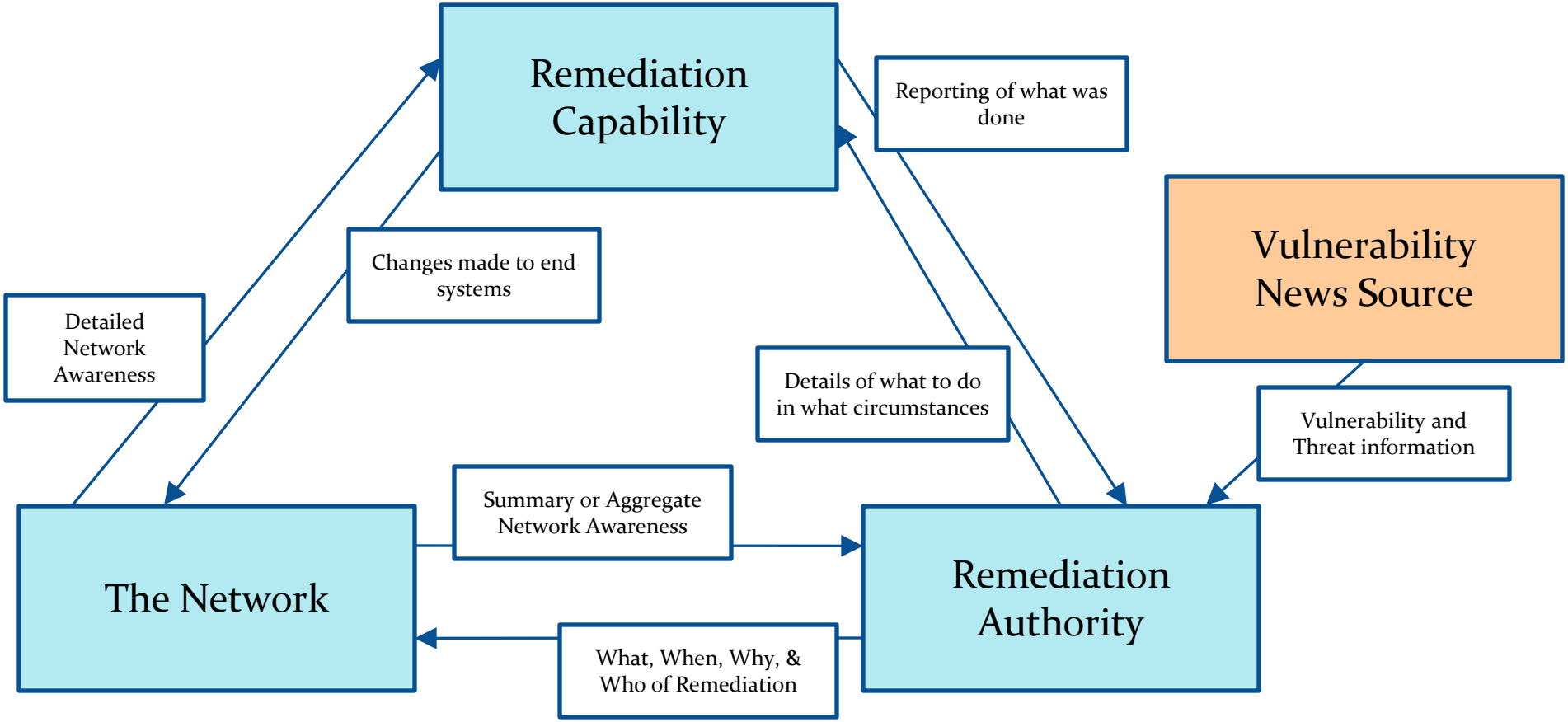
© 2011 The MITRE Corporation. All rights reserved.

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**
    MITRE, NSA, SPAWAR Systems Center Atlantic, G2
  - **A Remediation Manager reference implementation**
    SEI
  - **A Remediation Tool reference implementation and a simplified Remediation Manager**
    SPAWAR Systems Center Atlantic

© 2011 The MITRE Corporation. All rights reserved.

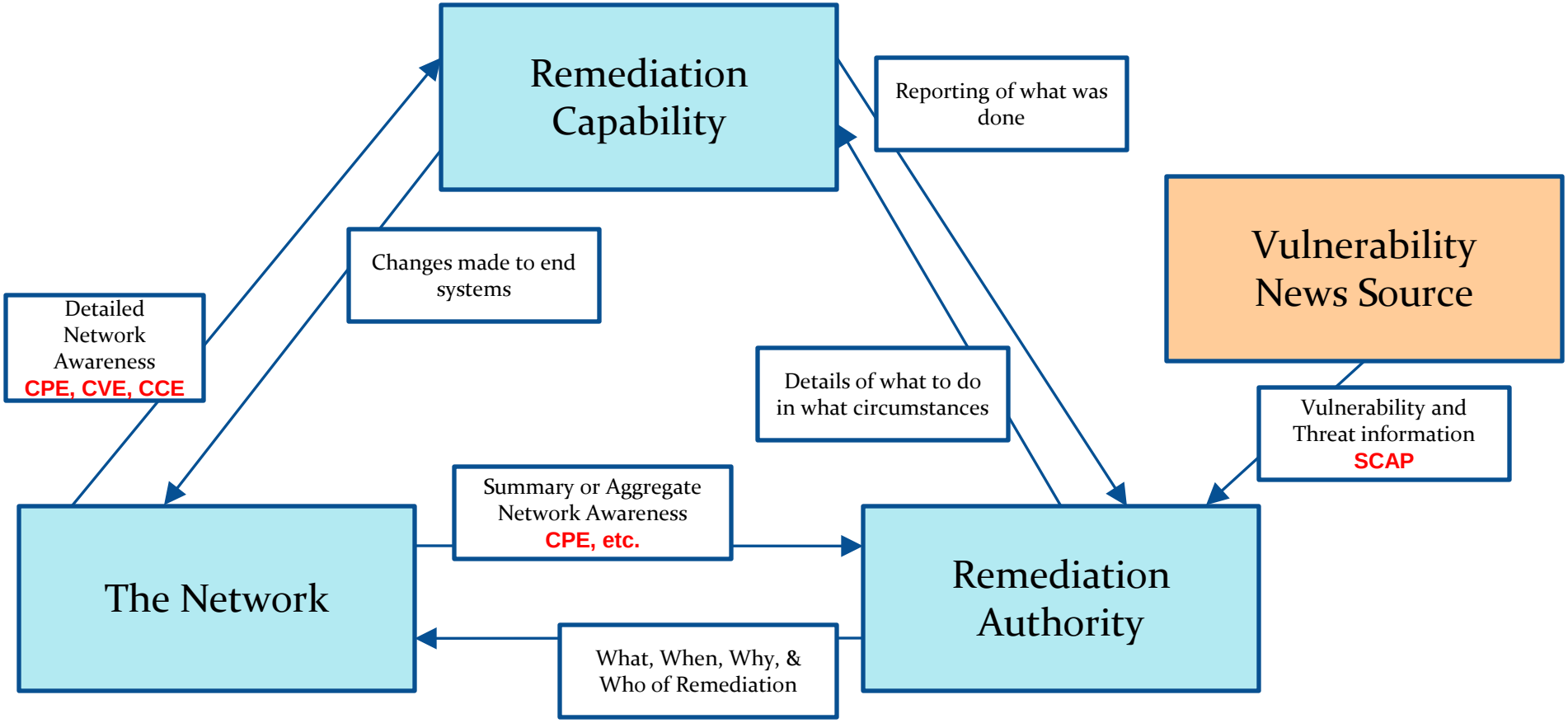
High Level Remediation Operational Concept



MITRE

© 2011 The MITRE Corporation. All rights reserved.

SCAP Today in the Remediation OpCon



MITRE

© 2011 The MITRE Corporation. All rights reserved.

Key Remediation Specs Under Development

- **CRE (Common Remediation Enumeration)**
  - Unique IDs and human-oriented descriptions of remediations
  - Can be applied to workarounds or mitigations as well as "complete fixes"
  - Similar to CVE or CCE
  - Removes ambiguity or confusion when specifying remediations
  - CREs are tied to a specific platform, and are specific to the method, effect, and parameters of the remediation action

- **ERI (Extended Remediation Information)**
  - Provides additional information about CREs
  - Similar to NVD's added information about CVEs
  - Captures indicators, operational impact, pre-requisites, etc.
  - Supports remediation discovery and selection, prioritization and ordering

© 2011 The MITRE Corporation. All rights reserved.

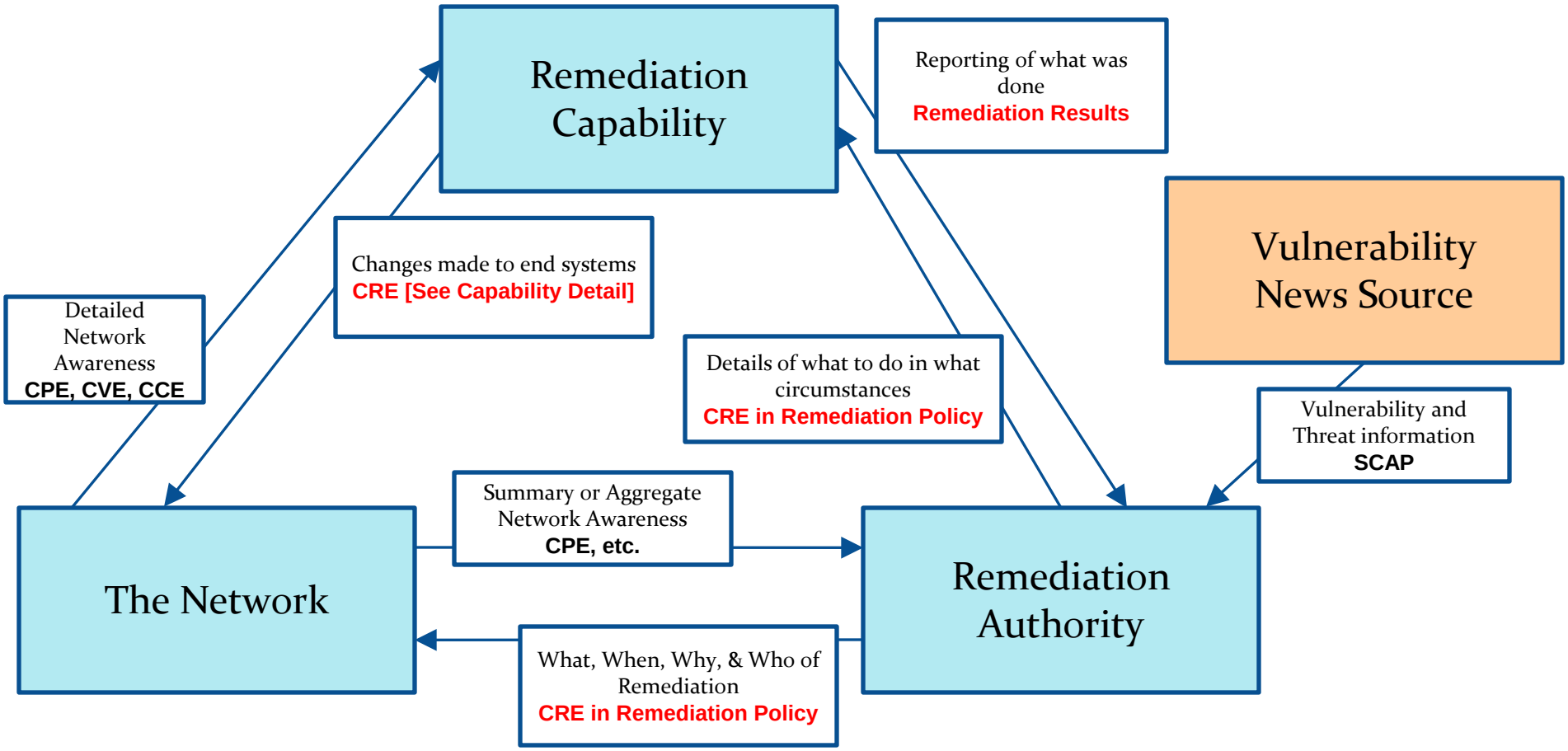
Key Remediation Specifications (continued)

- **Remediation Policy Language**
  - Format for organizations to document allowed or required remediation actions (CREs) by host type
  - Host type defined with any combination of platform type, vulnerabilities found, configuration status, functional or organizational profile, etc.
  - Simple case: link a CRE and a parameter value with a CCE
  - Similar to XCCDF's role in assessment

- **Remediation Tasking Language**
  - Machine-readable input to remediation tool
  - "Perform <CRE list>, with <options>, on <target list>"
  - No assessment analog currently in SCAP
  - May overlap with other emerging specifications in development
  - Tasking Results also needed—Was the action attempt successful?

© 2011 The MITRE Corporation. All rights reserved.

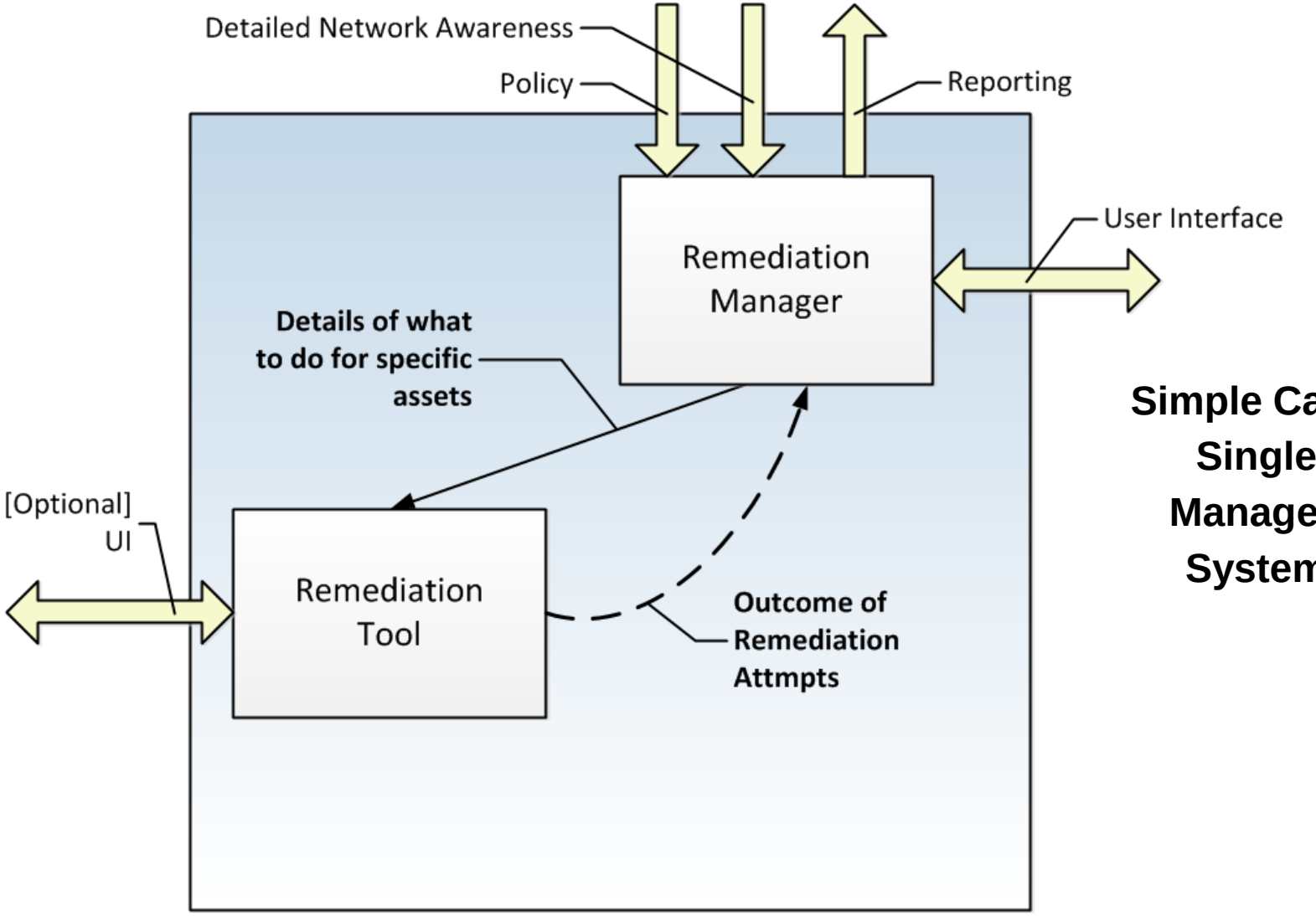
Proposed Remediation Specs in the OpCon



MITRE

© 2011 The MITRE Corporation. All rights reserved.

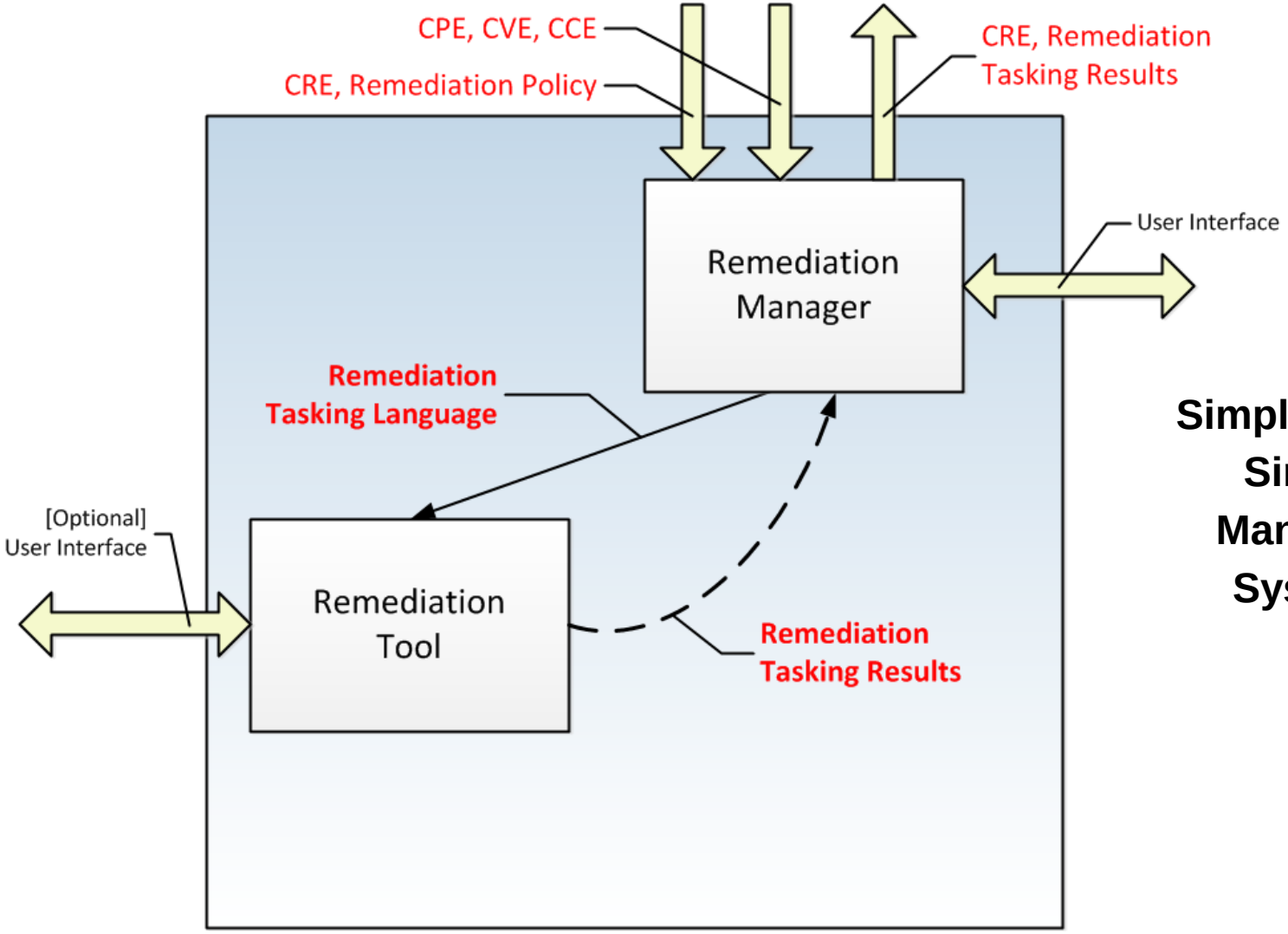
Remediation Capability: Detailed View



Simple Case: Single Managed System

© 2011 The MITRE Corporation. All rights reserved.

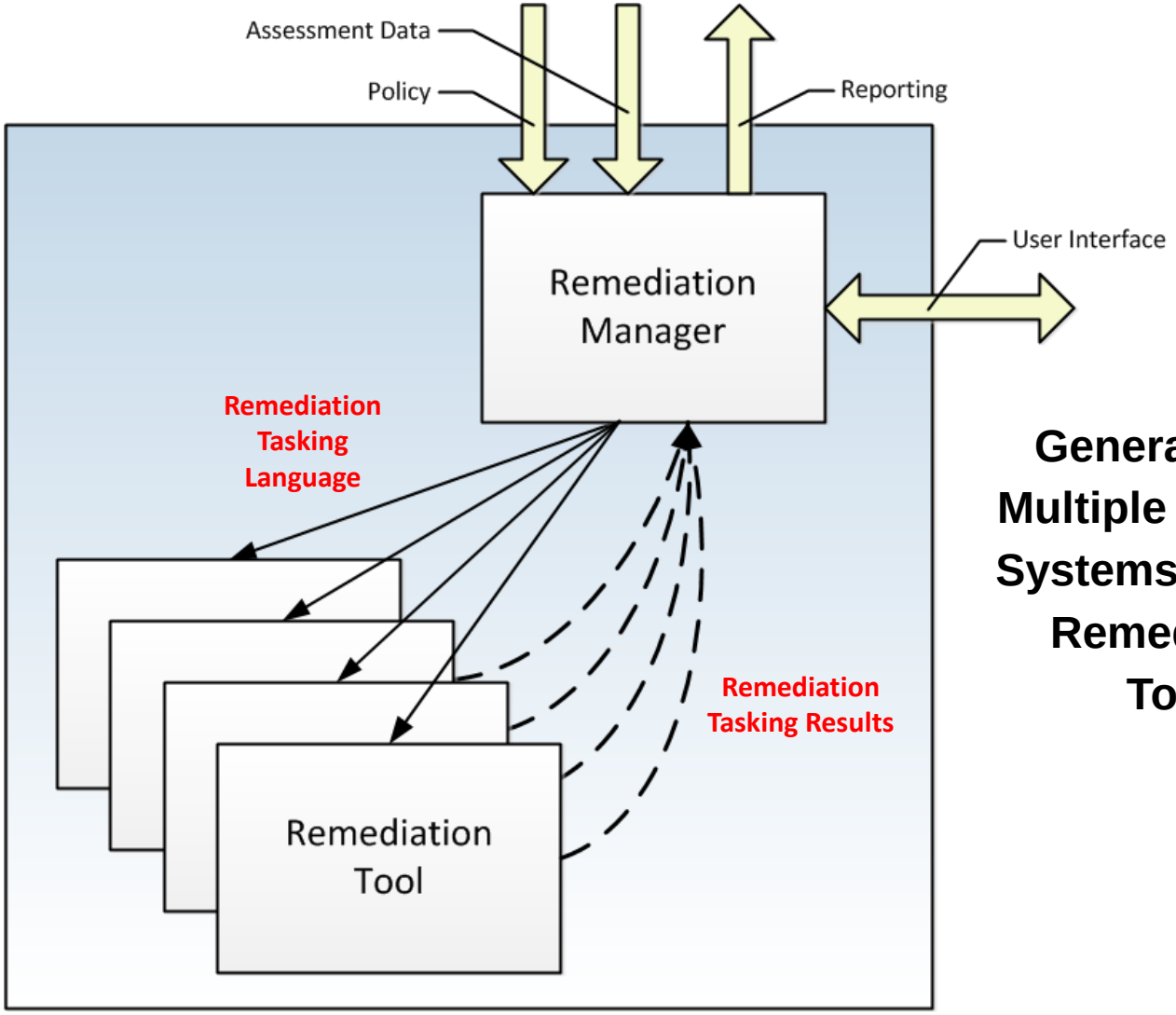
Capability Detail: SCAP and Proposed Specs



Simple Case: Single Managed System

© 2011 The MITRE Corporation. All rights reserved.

Remediation Capability: General Case



General Case: Multiple Managed Systems, Multiple Remediation Tools

© 2011 The MITRE Corporation. All rights reserved.

Questions for You

- Does the framework described make sense?
- Can you imagine applying the framework to your remediation use case(s)?
- Do you think the framework could be integrated with SCAP results? More fully integrated with SCAP?
- …with other network information currently used in your remediation activities?
- Can you imagine ever applying this framework to remediation activities involving actions performed other than on the end systems?
  - Active Directory, LDAP, etc?
  - Firewall rule changes? Host-based or otherwise?
  - Router, switch, etc. configuration changes?
- Do you think that would be useful to you?
  - In one year? In five years? In 10?

© 2011 The MITRE Corporation. All rights reserved.

For More Information

- **Review NIST IR-7670: Overview NIST Interagency Report**
  - **Describes the proposed remediation standards framework**
  - **See http://csrc.nist.gov/publications/PubsNISTIRs.html**

- **Monitor the emerging-specs@nist.gov email list**
  - **Announcements and technical discussions**
  - **See http://scap.nist.gov/community.html to subscribe**

© 2011 The MITRE Corporation. All rights reserved.

Contact Information

- **Standards Discussion Moderators**
  - **Matthew N. Wojcik <woj@mitre.org>**
  - **Gerry McGuire <gmcguire@mitre.org>**
  - **Matt Kerr <Matt.Kerr@g2-inc.com>**
  - **David Waltermire <david.waltermire@nist.gov>**
- **R&D Reference Prototype Development**
  - **SPAWAR Systems Center Atlantic team, c/o Jack Vander Pol <jack.vanderpol@navy.mil>**
  - **Software Engineering Institute team, c/o Rita Creel <rc@cert.org>**
  - **MITRE team, c/o Matthew Wojcik <woj@mitre.org>**
- **Sponsor POC: Mike Kinney**

© 2011 The MITRE Corporation. All rights reserved.

Backup Slides

© 2011 The MITRE Corporation. All rights reserved.

CRE Entry Example

ID	cre:org.example.cre:513
DESCRIPTION	Enable or disable ICMP Redirects via the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect registry key.
Parameters	enable / disable
PLATFORM	cpe:/o:microsoft:windows_7
REFERENCES	(1) Microsoft Security Compliance Manager Windows 7 Baseline
Created	2010-10-15
Modified	2010-10-15
Deprecated	False
Version	1
Submitted By	ACME Inc.

© 2011 The MITRE Corporation. All rights reserved.

ERI Example

ID	eri:com.example.eri:37
CRE REFERENCE	cre:org.example.cre:513
INDICATORS	CCE-8513-4
PRE-REQUISITES	None
SUPERSEDES	None
OPERATIONAL IMPACT	Disabling ICMP redirects may interfere with normal network operations.
PARAMETER MAPPING	enable = 1; disable = 0
REBOOT	False
Created	2010-10-15
Submitted By	ACME Inc.
Deprecated	False

© 2011 The MITRE Corporation. All rights reserved.