Remediation Discussion Issues

CRE, ERI, and Remediation Policy

Matthew N. Wojcik

April 1, 2011

MITRE

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.

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

CRE Search, Selection, Prioritization and ERI

- The Platonic ideal of a CRE list would be an entry for every remediation action we commonly take for any security-motivated reason
- Remediation Policy allows an organization to specify which CREs {should, may, must, must not} be taken in response under various conditions
- Problem: How does an organization find the CREs they need to consider for inclusion in their policy? How do they decide between them?
- Current answer: ERI
  - But how? What metadata do we need about CREs?

Platforms and the Search Problem

- A Group Policy CRE might be set on a Windows Server 2008 R2 machine, but applied to address an issue on a Windows 7 client
  - You want to fix Windows 7
  - You know what domain server versions you have
- What kind of search criteria will you use?
- What results do you want to see?
- What data do we need to support that?

Discussion: Human Readability

- Generate human-readable policy, or just machine-readable?
- Having one source document avoids maintenance problems
- Certain level of readability required for selecting between remediations allowed by policy, and potentially adjusting values
- Readability will be required if any manual tasks should be supported (e.g., help desk tickets)

Discussion: Remediation Preference

- Should policy support saying that remediations are:
  - Required?
  - Preferred?
  - Allowed?
  - Disallowed?
- Express preference order?

Discussion: Asset Types

- What categories of asset types should be supported?
  - Installed operating system or applications
  - Discovered vulnerabilities
  - Current configuration of software or hardware
  - Organizational unit
  - Network location
  - Geographical location
- How should these be expressible?
  - By SCAP “fact” IDs, such as CPE, CVE, CCE
  - By OVAL definition or ID, for arbitrary machine-measurable statements of applicability
  - By OCIL questionnaire or ID
  - By other conventions for system metadata (IF-MAP or similar?)
  - Free text, for human use?
  - N.B. – Earlier proposal for expanding CPE Language scope

MITRE

Discussion: CRE Parameters in Policy

- CREs are parameterized
  - E.g., one CRE for setting the file permissions on a particular file
  - Policy will have to specify parameter values
- Remediation Tasks will have to include parameter values in a predictable, parseable format
- Humans tailoring policy or selecting between CREs during task selection will need "friendly" values
- Implies policy should map between human- and machine-readable parameters
  - This topic was anticipated earlier this week
  - Similar problems faced in SCAP today
  - Current theory: conceptual in CRE, how to map in ERI, both in policy, literal in tasking

Discussion: Dates, Deadlines, Deferment

- What dates are needed for the policy itself?
  - Creation, modification, effective on, expires on
- Are deadlines needed in remediation policy, or are compliance deadlines sufficient?
  - Possible deadlines:
    - Issue tasks by date
    - Receive task result
    - Receive “success” result
- Remediation tasks are often deferrable by end-users
  - Opportunity to save work
  - Don’t interrupt a presentation or deadline crunch
  - How should policy specify what deferral is allowed?

Discussion: Authority, Scope, Exceptions

- Who issued the policy?
- Who does it apply to?
- Is it mandatory or optional?
  - In whole or in part?
- What is their authority?
- Should the policy indicate when and how an exception must be reported?
  - Or are exceptions handled as part of compliance checking?
  - Decision not to comply may be because the remediation options allowed/required by policy are unworkable in the local environment