Innovating SCAP

Kent Landfield - **Director, Content Strategy, Architecture and Standards**

Dick Whitehurst – **SCAP Products Architect**

The SCAP Content Challenge

Produce an entire new set of content from scratch with no development tools, no management, maintenance or publishing infrastructure, assuring each component is completely reusable and all fully tested, being distributed via multiple channels, while using multiple formats for the content whose formats are changing based on the whim of others.

So how do we innovate SCAP without requiring immediate changes to the standards????

Overcoming Limitations of the SCAP Standards

- **McAfee OVAL Extension : Temporary proprietary extensions**
  - OVAL allows for extensions to the schema as part of the standard
  - McAfee used that capability with OVAL 5.3 time based checks
  - We notified the OVAL Working Group of our extensions
  - OVAL community adopted our extension with one very minor change that caused us to make a simple tweak to our content and code
  - No major impact at all!

- **Making SCAP globally useful : Mining the standards**
  - Designed a means to support localized SCAP Content (on third attempt)
  - Localized McAfee SCAP supplied content in 11 languages

- **Extending the relevance of SCAP results (Findings) : Contributing**
  - Providing actionable data from XCCDF/OVAL results
  - Enabling administrators to go beyond *compliant or is not compliant* results
  - Designed and integrated into McAfee Policy Auditor

Localizing SCAP Content

Making SCAP Globally Useful – Not a US-Only Standard Any Longer

SCAP Going Global

- McAfee addressed the need for I18N/L10N
  - Critical if the government truly wants COTS and GOTS solutions
- Localization of content
  - XCCDF and CPE support it
  - OVAL, well…
  - CVE has limited translations
  - Others don't
- Need to deal more than translations
  - Translations are a presentation issue
  - Able to assess a locale specific system accurately even if the presentation is in English
- Different types of content took different approaches to localizing
  - OS Patch Checks
  - Compliance and Configuration Checks
  - Application checks
- And then there are GEO specific policies that need to have benchmarks created for them
  - ACSI 33, J-SOX, EU 8th Company Law Directive on Statutory Audit, etc.

McAfee Localized SCAP Content

- McAfee developed SCAP Content
- Created localized OVAL/XCCDF compliance support
- Created locale/OS/version OVAL patch support
- Targeted OVAL application checks for desktop security products
- Designed and implemented a process to provide localized content **using the existing SCAP specifications**
  - Creation of content
  - Testing of content
  - Publication of content

McAfee Content Availability	Patches	Config Checks (Audit)	Primitives	Benchmarks	McAfee Application Checks	3rd Party Application Checks
English	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
German	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Spanish	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
French	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Italian	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Polish	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Swedish	Jan '10	Jan '10	Jan '10	Jan '10	Jan '10	Jan '10
Chinese (PRC)	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Chinese (Trad)	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Japanese	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09	Apr '09
Brazilian Portuguese	Jan '10	Jan '10	Jan '10	Jan '10	Jan '10	Jan '10

Operating System Patches

- Older operating systems are the harder to deal with
  - Windows XP and earlier Windows operating systems had the Multilingual User Interface (MUI) added on top of a locale-specific operating system
  - Windows 2000 and Windows XP, the Operating System and patches are locale-specific only insomuch as you have to apply the right locale patch to the right Operating System
  - The properties evaluated to determine compliance with patch levels are identical across locales (files, registry settings, …)
  - Locale only comes into play when determining which patch to apply (remediation)
- Newer Windows versions
  - With Windows Vista and Windows 7 the distinction between locales becomes insignificant
  - Windows Vista was designed and developed as a fully internationalized platform with a fully integrated implementation of the Microsoft MUI model. Because these Operating platforms are not locale-specific, the patches are also not locale specific

Compliance and Configuration Checks

- Configuration checks require functional localization to avoid false positives and false negatives
- Used a systematic approach to identifying the checks which required localization.
  - Categorized based on the individual OVAL tests
- Generally speaking the checks requiring localization reference security principles and are normally used to manage the built in users and groups including the “AccessToken” test, the “Group” test, and the “User” test.
- Other tests were identified as having a need or possibility of need for localization, but most of those tests have either been deprecated (e.g. the FileEffectiveRights test) or we have worked around the need for localization by finding an alternate way to find what was needed
- Moved the need for localization into the XCCDF benchmark
  - Used OVAL external variables where possible
  - Allows for the user to more readily tailor / customize the content
  - Single checks written instead of one for each supported language

OVAL Tests L10N Needs

- Access Token, Group Test, SID Test and User – L10N Required
  - Security Principle names are localized for built in trustees
- File Check – L10N Possibly required
  - Some extended file properties could be localized
  - Language, Product Name, possibly others
- Interface Test – L10N Possibly Required
  - Adapter name is localized – “Local Area Network” => “Conexión de área local”
  - If adapter name is used in checks, those will need to be localized
- Registry Test – L10N Possibly Required
  - These are dependent on what is being checked.
    - Dates stored by applications in the registry
    - Product names and other string data could be localized.
  - Generally, registry keys and value names are in English, value data is mixed, possible localized
  - This is most likely to occur in third party software, covered in the next major section “Application Checks – Patches and Properties”
- WMI57 Test – L10N sometimes required
  - Case-by-case, check-by-check

Localized Configuration Checks - XCCDF

- Scoring a concern
  - Using separate rules for each language and using CPE to mitigate the application of those rules could create a scoring issue where system would end up having a score skewed by the localized versions of the rules. For every check evaluated, there would be a significant number of "Not Applicable" rules that could skew the score
- Need to construct a single rule for a singular technical control that can handle all languages
- Use a complex check element within our Rule to "OR" the various localized account names to pass to the check. That way, the Rule can handle any particular language.
- The top-level complex check would consist of one or more complex checks which operationally "AND"s an inventory OVAL definition for the language we want to detect with the Log on Locally compliance definition, passing the appropriate value for the account name as necessary per our language.

Log on Locally" Rule to handle both English and French Built-in Administrator accounts

```
<Value id=" LogOnLocally_english" xml:lang="en" type="string" operator="equals" interactive="false">
      <value selector="">Administrator</value>
</Value>
<Value id=" LogOnLocally_french" xml:lang="en" type="string" operator="equals" interactive="false">
      <value selector="">Administrateur</value>
</Value>
…
<Rule id="LogOnLocally" xml:lang="en" selected="false">
    <title xml:lang="en">Log on Locally</title>
    <description xml:lang="en">Administrator log on locally.</description>
    <complex-check operator="OR" negate="false">
      <complex-check operator="AND" negate="false">
        <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" selector="">
          <check-export value-id="LogOnLocally_english" export-name="oval:com.sample:var:1" />
          <check-content-ref href="" name="oval:com.sample:def:1" />
        </check>
        <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" selector="">
          <!—This is the check for Windows is English (checked by verifying the locale_id as described in the next section)-->
          <check-content-ref href="" name=" oval:com.sample:def:1000" />
        </check>
      </complex-check>
      <complex-check operator="AND" negate="false">
        <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" selector="">
          <check-export value-id="LogOnLocally_french" export-name="oval:com.sample:var:1" />
          <check-content-ref href="" name="oval:com.sample:def:1" />
        </check>
        <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" selector="">
          <!—This is the check for Windows is French (checked by verifying the locale_id as described in the next section)-->
          <check-content-ref href="" name=" oval:com.sample:def:1001" />
        </check>
      </complex-check>
    </complex-check>
</Rule>
```

Application Checks – Patches and Properties

- Application checks are used to evaluate the patch levels and properties of various applications that may be installed on the evaluated platform

- Example:
  - Checking for a valid antivirus program, minimum version checks (Adobe Reader should be at least version XYZ), antivirus DAT age checks (antivirus DAT definitions should be no older than 10 days), checking for particular patch levels for a given application, or checking various configuration items of an application.
  - These are the types of checks that could be considered “health checks” to support technologies such as Network Access Control (NAC)

- Complexity of these checks is often high due to the breadth of software providers and the maturity of the software this content area addresses

- Some of these products are fully internationalized using common standards and methods. Others are regional applications that have not grown through the pains of localizing and internationalizing their products.

Application Checks – Patches and Properties

- Localization occurs in the OVAL instead of XCCDF Benchmark
  - Because these types of checks require less customization or tailoring, putting the localization data within the OVAL does not generally produce the usability / customization problems we see in the standard configuration checks
- Written using multiple OVAL definitions
- We use one inventory check per language or locale supported by the check.
- These inventory checks are joined with the actual technical controls to be evaluated, using the appropriate Boolean logic nested with the actual criteria element in the primary definition. This primary definition is often referred to as the “Aggregator Definition” in our own vernacular.
- The Boolean logic used is similar to the complex check logic we used in the XCCDF in the sample configuration check, but this logic is embedded in the OVAL instead of in the XCCDF.

Findings

Providing Actionable Data From XCCDF/OVAL Results

Findings

- Motivation – why is it needed
- Constraints on the architecture/design
- High Level Design
- Detailed Design
- Samples of Findings generated from XCCDF benchmarks

Motivation – Why is it needed?

- Provide data to satisfy Auditors
  - Auditors often require more detailed information about a pass or a fail
  - A configuration item passes, but what value does it have?
- Provide data needed to remediate systems
  - Why does the antivirus check fail?
    - because there is no AV?
    - Is the AV present but not a valid version?
    - Are the signature files up to date?
  - Why does the file permissions check fail?
    - Do unexpected accounts have access?
    - Does the file exist?
    - Does each expected account have proper permissions
- Simply provide clarifying data about the state of systems

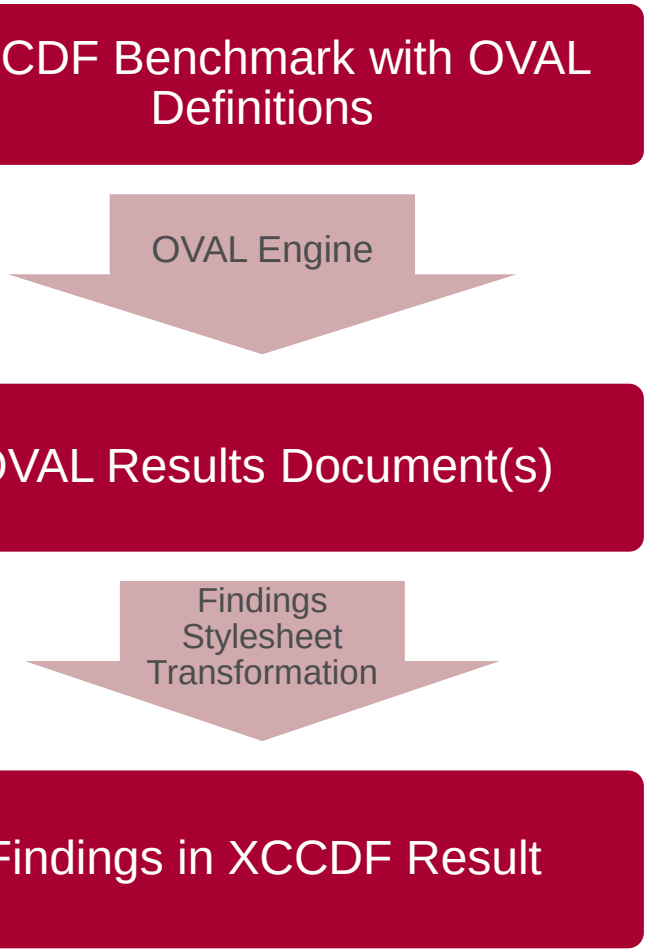
Constraints on the architecture/design

- For SCAP implementers
  - Findings must “fit in” with the rest of the SCAP infrastructure
  - Implementable with commonly available tools
- For Content Creators
  - Should have a low learning curve
- For SCAP Users
  - Should not require large resources at run time
  - Should reduce the volume of results to only significant data (high signal to noise ratio)
- For IT and Security personnel
  - Results should be clear, simple, and complete
  - Results should be localizable

High Level Design

- Process the OVAL results documents via XSL stylesheets to extract only the ‘useful’ information
- Each OVAL definition needing detailed results will have its own stylesheet
- XCCDF Results schema extended to provide a location for a Findings xml schema-compliant

High Level Design



Detailed Design (1) - Components

- Findings schema
  - Supports instance data
    - Which file
    - Which account
  - Supports actual data
    - Actual permission collected for the file/account
  - Supports input (expected) data
    - The permission the file/account was expected to have
- Findings messages
  - Substitution for instance, actual and expected data
    - For file *xyz.abc,* account *USER1* had read and execute permission when **read only** was expected
- Mapping of OVAL Definition to XSL Stylesheet
  - Our implementation used an implicit mapping
    - oval:abc.xyz:def:101 to oval_abc_xyz_def_101.xsl
- Library of reusable stylesheets
  - Example - Many definitions check for file permissions, but a single library stylesheet template can handle all of them

Detailed Design (2)

- Handle incomplete or partial results with attribute in the Findings document
- Indicate finding type (violation or compliance, and possibly others) with attribute in finding element
- Message and findings ids conventionally use URI style to provide for globally unique ids (not currently schema enforced)
- Finding messages are associated with a finding summary corresponding to the OVAL (or other) check id.

Findings generated from XCCDF benchmarks

- The account Power Users access to C:\WINDOWS\wmsetup.log is XRQNWATBDE(Modify) access, but no access is expected.
- The account Users access to C:\WINDOWS\wmsetup.log is XRQNE(Read&Execute) access, but XRQNWATBDE(Modify) is expected.

```
<findings xmlns="http://results.pa.mcafee.com/findings/5.2” id="oval:com.mcafee.oval:def:89558“>
    <finding isViolation="true“  messageId="com.mcafee.pa.msg.winfilenonerightsviolation">
        <instanceValue key="account">Power Users</instanceValue>
        <instanceValue key="filename">C:\WINDOWS\wmsetup.log</instanceValue>
        <actualValue key="permissions">XRQNWATBDE(Modify)</actualValue>
    </finding>
    <finding isViolation="true" messageId="com.mcafee.pa.msg.winfilerightsviolation">
        <instanceValue key="account">Users</instanceValue>
        <instanceValue key="filename">C:\WINDOWS\wmsetup.log</instanceValue>
        <instanceValue key="permissions">XRQNWATBDE(Modify)</instanceValue>
        <actualValue key="permissions">XRQNE(Read&amp;amp;Execute / List Folder Contents)<actualValue>
    </finding>
    <findingsSummary isViolationSetComplete="1" totalViolations="3"/>
</findings>
```

Findings generated from XCCDF benchmarks

- The account Users access to C:\WINDOWS\help\ is XRQNE(Read & Execute / List Folder Contents) access, but RQNE(Read) is expected.

```
<findings xmlns="http://results.pa.mcafee.com/findings/5.2 " id="oval:com.mcafee.oval:def:89206">
    <finding isViolation="true" messageId="com.mcafee.pa.msg.winfilenonerightsviolation">
        <instanceValue key="account">Power Users</instanceValue>
        <instanceValue key="filename">C:\WINDOWS\help\</instanceValue>
        <actualValue key="permissions">XRQNWATBDE(Modify)</actualValue>
        </finding>
</findings>
```

Findings generated from XCCDF benchmarks

- Password history length should be 6 or greater but is set to 0. (Failure)

```
<findings xmlns= "http://results.pa.mcafee.com/findings/5.2" id="oval:com.mcafee.oval.win:def:6001" >
   <finding isViolation="true" messageId="com.mcafee.pa.msg.winpasswdhistlengreaterthansetting">
      <instanceValue key="inputValue">6</instanceValue>
      <actualValue key="actualValue">0</actualValue>
   </finding>
   <findingsSummary isViolationSetComplete="1" totalViolations="1"/>
</findings>
```

Findings generated from XCCDF benchmarks

- Maximum password age should be less than 3888000 seconds (45 days) and is set to 3710851 seconds (43 days.) (Pass)

```
<findings xmlns="http://results.pa.mcafee.com/findings/5.2" id="oval:com.mcafee.oval.windows:def:17">
    <finding isViolation="false" messageId="com.mcafee.pa.msg.winmaxpasswdagelessthansetting">
        <instanceValue key="inputValue">3888000 seconds (45 days) </instanceValue>
        <actualValue key="actualValue">3710851 seconds (43 days) </actualValue>
    </finding>
    <findingsSummary isViolationSetComplete="1" totalViolations="0"/>
</findings>
```

Status of Findings Today

- An integrated feature in the McAfee Policy Auditor 5.2 and 5.3 versions
- Being actively used by iPost today
- Extends the integration of OVAL and XCCDF to provide users with a missing capability
- Makes SCAP content more useful to customers without forcing them to munge XML results to get what they operationally need
- Being contributed to extend the SCAP set of standards
- Open specification is being provided to not just customers but to the community for others to integrate and benefit from

Innovating SCAP Standards

- **Don’t always look to the standards committees to provide you with innovative ways to improve your SCAP capabilities**
- **Use the architecture the standards provide**
  - Don’t be afraid to create extensions you feel are valuable
- **Mine the standards**
  - There’s a great deal there and you may not be looking at the standards in the right way
- **Design, expand and contribute where needed**
  - If you find something missing and needed you can bet others will need it as well
- **Participate!**

SCAP innovation can occur outside the standards groups if people only look and understand what they are developing in. McAfee is and has been doing innovative things extending SCAP to a global marketplace while making substantive enhancements to the foundations of SCAP for the community to use.

Questions ???

Kent Landfield – Kent_Landfield@mcafee.com
Dick Whitehurst – Richard_Whitehurst@mcafee.com


McAfee®