Standardizing Access to Organizational SCAP Content

Dave Waltermire, NIST
Kent Landfield, McAfee

SCAP Developer Days 2012

Session Overview

SCAP content needs to be delivered internally within an organization. Today, the SCAP vendors cannot share a single local site security policy without the site staff having to go to each of the individual products and figuring out how to inject that new or updated policy into that product's delivery mechanisms. This session will describe means to address this by creating a content repository access specification.

Purpose

Today we have created a standardized content format used by multiple SCAP tools from multiple vendors. What we have not addressed is the actual distribution of standardized content.

Organizations are developing, customizing and tailoring content without a means to distribute, reuse and manage it.

For larger sites with multiple SCAP products, changes to content can be painful in assuring all the SCAP products are using and reporting on the same content.

This interactive discussion will focus on defining requirements for creating a standardized means for accessing and distributing content from a central service within an organization.

What this session does not focus on

- Commercial / Industry Content Aggregation Repositories
- Content Ownership
- Vendors proprietary means of distributing content

Repository Directions

- More authoritative ownership
  - Vendor Hardening guides
  - Software and Hardware products providing per product configurations
  - Guidance Authors understanding the benefits of actionable content
- Decentralized content availability
  - No longer solely a NIST Checklist focus
  - Yes, this is a good thing
- Commercial content a possibility
  - Availability for subscription or specific use cases

Organizational Distribution Problem

- Large organization (insert an agency or Fortune 500 name here) has multiple SCAP validated tools in their environment with many different sites and departments
- Tools they own are a mixture of point products and enterprise tools
- The organization wants to create their own SCAP-based site security policy which they would like scheduled to run weekly
- Each time they make a change they need to go to each of their tools (and potentially systems) and update the content
- Extremely laborious and time consuming from a staffing perspective…

Guidance Author Distribution Problem

- An organization develops a set of benchmarks and the associated checks that target a specific set of guidance for which they are authoritative for
- They want to maintain control over the content and its distribution to assure they can update the content rapidly as needed to support their community
- They want to be able to widely distribute updated content quickly to assure their community is using the most current guidance
- Do not or cannot rely on an external organization to facilitate the distribution of their content

Content Location / Version Problem

- Standardized Content is available from many sources
- User community has no means to be made aware of what content is available to be used in their SCAP enabled products
- No means to search for the desired content
- Users feel they need to create their own because they do not know where to go find what they need
- Extremely laborious and time consuming from a searching / finding perspective…
- Then when they do find what they are looking for, they have to manually continually monitor the location for any updated versions

Organizational Content Servers

- Exists on local network
- Could be set up in a hierarchy in the organization if needed
- Holds the actual content to be retrieved by the SCAP products or Content development tools
- Can be an authoritative server for local organizational or site security policy content
  - Can be authoritative within the organization without registering with an external repository index
- Caching server for external content
- Manages the content allowed or required to be retrieved within the organization
    - What is the default to be used? How do we indicate that, by platform, subnet, ? Do we need to at all?
- Querying
- Injecting Content at a component or package level

So what is needed ?

Need a means:

- To allow content to be distributed globally via automated means and not via manual means
- For guidance authors to be able to register their content as authoritative and publish that content so it can be retrieved and used by the interested or affected community
- For organizations to be able to locate new content and track existing content for updated versions
- For different SCAP products within an organization to be able to retrieve the organization's approved content to be used in evaluating the state of the local network
- To assure the content being retrieved is the guidance author's approved version
- To be able to identify the support contact information if issues are encountered with the retrieved content
- To manage the registration process at a global level
- To manage the organizational repository