Content Repositories:

Operational Approaches and Commercial Directions

Kent Landfield - McAfee

Aharon Chernin – SCAP.com

Chandrashekhar B - Secpod

Agenda

- Overview of the issues and operational approaches in the future
- Aharon Chernin introduces SCAP.com and it's approach and attitude towards developing community repositories
- Chandrashekhar B presents Secpod's approach, attitude and what they are doing with the Secpod Content Repository
- Request for participation

Problem

- 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.

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…

Today’s Reality

- Retrieve it yourself on a per-product basis
  - NIST Repository
  - MITRE OVAL Repository
  - OS Vendor Repositories
  - Vendor Product Content
- Content integrity validation missing
- No way to prove authenticity
- Kludgy ways for an organization distribute the same SCAP content to multiple SCAP validated products on the same network
- Vendors have their proprietary way (or no way) of doing this in an enterprise

Wasn’t the goal of SCAP to provide standardized content between products? While the internals work, the distribution does not.

Current Content Distribution Issues

- Ownership
  - Confusion around centralized repositories
  - Is the content authoritative?
  - Is this content really ready to be used or still under development?
  - What content should I run for what situation?
  - How come some vendors include others peoples content in their product and some don’t

- Support
  - Who owns the content?
  - Who do I call for support for content issues?

- Location
  - Where do I find a benchmark for my specific platform or need?
  - Is there anyway to see what those outside my organization have created?
  - If I want to build a benchmark do I need to write all the checks myself?

Repository Directions

- More authoritative ownership
  - Vendor Hardening guides
  - Software and Hardware products providing per product configurations
  - Guidance Authors will understand the benefits of actionable content

- Decentralized content availability
  - No longer solely a NIST Checklist focus
  - Yes, this is a good thing

- Commercial content becoming a possibility
  - Availability for subscription or specific use cases

Aharon Chernin

SCAP.com

Chandrashekhar B

SCAP Content Repository - Preview

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 organizational repository

Request for participation

- New Content Repository / Distribution Mailing list
  - Sign up at
    http://www.scap.com/mailman/listinfo/scapcontentdistribution_scap.com

- Forming a working group around addressing the repository design and development

- Effort will be more focused on fast prototyping

- Looking forward to your participation!