Moving Baselines Forward

Kent Landfield

Director, Content Strategy, Architecture and Standards

Overview

- The Vision of Baselines and Benchmark Developments
  - Authoritative ownership
- Issues with Current Baselines
  - Ownership
  - Support
- Missing pieces
  - Integrity
  - Proof of authenticity
  - Sharing SCAP Content between tools
- Setting a foundation for the future
  - Repository Models

The Vision of Baselines and Benchmark Developments

- Those that create the guidance should own it
  - Authoritative ownership
  - Responsible for distribution
- Guidance documents should be fully actionable and self contained
  - Administrative Questioning
  - Technical Control Monitoring
  - Guidance Prose
- Easily accessible standardized content shared between validated products

Today's Reality

- Repositories:
  - NIST Repository
  - MITRE OVAL Repository
  - OS Vendor Repositories
  - 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.

Example

- 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…

Issues with Current Baselines

- 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?
- Support
  - Who do I call for support?
- Location
  - Where do I find a benchmark for my specific platform or need?
- Miscellaneous
  - How come some content runs and some doesn't?
  - Can we say HKEY_CURRENT_USER?

Product Approaches to Distributing Baselines

- Retrieve them yourself
  - From NIST
  - From Vendors (OS/Product)
- Vendors bundling government developed content
  - Questionable…
- There has got to be a better way…

Primary Repository Models

- Package based retrieval
  - Everything in one package to run a specific benchmark/policy
    - Checks
    - Benchmark
    - CPE support
  - Benefit
    - Consistent content a single entity
    - Ease of verification

- Component based retrieval
  - Menu based approach
    - Individual content potentially retrievable from multiple repositories
    - Checks from potentially multiple repositories
  - Benefits
    - Reuse of content

So what's Needed?

- Packaging focus
  - Documented package structure
  - Organizational information
    - Means to indicate who is authoritative
    - Contact information for support issues
    - Checksum / Signature for package
- Content Service Specification
  - Authentication (potentially optional)
  - Package registration
  - Content availability listing
  - Retrieval capabilities
- Consensus

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 a possibility
  - Availability for subscription or specific use cases

It’s time to move forward.

Kent Landfield – Kent_Landfield@mcafee.com


McAfee®