Subject: Re: [sacm] Using the Frame of Reference

Date: Wednesday, August 15, 2012 7:26:52 AM Pacific Daylight Time

From: Adam Montville (sent by <sacm-bounces@ietf.org>)

To: Moriarty, Kathleen, Waltermire, David A., sacm@ietf.org

On 8/7/12 2:25 PM, "Moriarty, Kathleen" <kathleen.moriarty@emc.com> wrote:

> The configuration check languages are validating after the configurations
> have been set. Other systems are used to manage configurations that may
> be vendor/product dependant.

Managing the configuration expressions is something that is critical to our overall success, and I would say that managing such content - to include creation, selection, tailoring of specific checks - is therefore important to us. It would be very useful to keep this in mind as we would expect the other systems Kathleen mentioned to work with our expressions.

> -----Original Message-----
> From: Waltermire, David A. [mailto:david.waltermire@nist.gov]
> Sent: Tuesday, August 07, 2012 5:16 PM
> To: Moriarty, Kathleen; Adam Montville; sacm@ietf.org
> Subject: RE: Using the Frame of Reference
>
> +1 on clearly defining our assumptions.

Agreed.

>> -----Original Message-----
>> From: sacm-bounces@ietf.org [mailto:sacm-bounces@ietf.org] On Behalf Of
>> Waltermire, David A.
>> Sent: Tuesday, August 07, 2012 4:10 PM
>> To: Adam Montville; sacm@ietf.org
>> Subject: Re: [sacm] Using the Frame of Reference
>> Are your 5 aspects of SCM controls or activities?

Well, they're really both depending on your perspective (this is why I'd like us to continuously define common vocabulary). They are activities, but that activity itself is a control, or, at the very least, substantiates a control, from the perspective of a control framework.

>> I would argue more
>> so that latter. I also like how you have broken down the different
>> "layers" of information for each of the 5 aspects. In my mind the
>> initial scope of this effort should focus on the "Observable Model" and

> > lower which I would interpret as being the data formats that describe
> > what is to be observed, how to observe it, and how to report those
> > observations.

I would prefer to describe what is to be observed, but not necessarily require an expression of how to make the observation.

> > Things like tasking are the protocol bits to ensure that
> > the right observations are made and that the results are provided (or
> > not provided) to specific network components.

I see a potential distinction here. Tasking involves scoping and instructing, and it's the scoping piece that helps ensure the right observations are made, and the instructing that tells a sacm-compliant (can I say that?) tool to go do something.

> > I would argue that "Configuration Assessment" might have a
> > "configuration compliance" model above "assessment" that would be a
> > peer to "vulnerability". This would put the configuration state in
> > context within the enterprise, just like the "vulnerability model"
> > does.

I'm not sure I'm understanding this, but I haven't tried to draw it out (short on time at the moment). It seems that what you're suggesting is that what I've written as "assessment model" would be decomposed into a parent and child, where the parent is the "configuration compliance" piece and the "assessment" aspect is then the child?

Also, when you say "configuration compliance," I want to be clear that you're talking about expressing a platform-level checklist of configuration settings, and then harvesting the data to measure an instance of that platform against that checklist - in other words, you're not talking about compliance to control frameworks, but to something I would generally call benchmarks (not measuring to NIST 800-53, but to a DISA STIG, for example).

> > It is at the scoring/risk layer that we may want to tie-in control
> > frameworks. But what does this really mean? Does it mean that you are
> > demonstrating successful implementation of a control through the
> > collection of supporting data? Does it mean providing data that
> > indicates that the use of the control is effective in reducing security
> > exposure or risk? There are many other considerations as well.
> > It might be enough for this effort to ensure that the results from the
> > assessment/remediation model/layer is capable of being associated with
> > the controls they implement.

I have found it helpful to look at this from two perspectives: auditor and security operations. As an auditor, it's my job to ensure that the benchmarks (tests) being applied to in-scope systems substantiate the controls and control objectives described in a given framework. So, the answer to your second question is yes.

As a security operations guy, I want to ensure that the benchmarks being applied to in-scope (all, really) systems effectively treat the risk of attack, compromise, breach (put your word here). So, the answer to your third question is also yes (but we'll need help from other efforts to do so).

A first step, as I think you would agree (judging based on your last sentence above), is to clearly get benchmark-level content clearly associated with particular controls and control objectives.

> -----Original Message-----
> From: sacm-bounces@ietf.org [mailto:sacm-bounces@ietf.org] On Behalf
> Of Adam Montville
> Sent: Monday, August 06, 2012 9:08 PM
> To: sacm@ietf.org
> Subject: [sacm] Using the Frame of Reference
>
> All:
>
> Here's how I would envision using the frame of reference using
> Security Configuration Management (SCM) as an example.
>
> SCM is really five controls often assisted by technical toolsets
> (depending on who you ask, so this is just one perspective):
>
>   1. Configuration Assessment (password length is set to x)
>   2. Patch and Vulnerability Assessment (software package x is at
> version
>   a.b.c)
>   3. Configuration Remediation (set password length to x)
>   4. Patch Remediation (bring software package x to at least version
>   a.b.c)
>   5. Rate of Change (how are the files, registry entries, and other
>   Settings changing over time
>
> Because asset management is critical to the success of these
controls,
> I assert that we should revisit what we have today in the way of
> models and where we need improvement (gaps or less than ideal
coverage).
> Appropriate asset models are required for each of SCM's constituent
> parts, as listed below.
>
> We might assert the following information model relationships:
>
>   o Security Configuration Management is composed of

>   o Configuration Assessment, which requires a/an
>   - Asset Model (information/characterization)
>   - Observable Model,
>   - Assessment Model (checklists),
>   - Scoring/Risk Model;
>   o Patch and Vulnerability Assessment, which requires a/an
>   - Asset Model,
>   - Observable Model,
>   - Assessment Model,
>   - Vulnerability Model,
>   - Scoring/Risk Model;
>   o Configuration Remediation, which requires a/an
>   - Asset Model,
>   - Observable Model,
>   - Remediation Model;
>   o Patch Remediation, which requires a/an
>   - Asset Model,
>   - Observable Model,
>   - Remediation Model.
>
> Note that some of the Supporting Concepts would be helpful here as
> well.
> Tasking/Workflow, is one example (consider assessing an endpoint,
> remediating, then reassessing).
>
> The Observable Model should be one that describes that which can be
> technically observed on an endpoint and which is able to provide
> contextual information with respect to that observable (either
> directly or through use of another model). For example, if I'm
> looking at a the Account Lockout Duration setting for a Windows
Server
> 2008 R2 machine Group Policy Object, then we should provide the means
> for content producers to include acceptable values for that
> configuration item, such that implementers using these specifications
> can provide guidance to their users with respect to that particular
setting.
>
> Something that seems lacking here is tying back to control frameworks
> (control in the ISO 27000/NIST 800-53 sense of the term). In the
case
> of SCM, we could use any number of the available control frameworks
to
> guide us. For example, the third SANS Top 20 Critical Control,
> "Secure Configurations for Hardware and Software on Laptops,
> Workstations, and Servers" might require one or more SCM constituents
as defined above.
>
> I'm particularly interested in this because it has been shown that,
to
> date, security automation efforts have been rather shotgun in their
> approach and have not necessarily done a good job ensuring that
> requirements derived from top-level scenarios are being satisfied.
> Also, knowing the exact needs of these controls can help us focus on
> what that which must be done, rather than upon that which could be

> > > done.
> > >
> > > Regards,
> > >
> > > Adam

____

sacm mailing list
sacm@ietf.org
https://www.ietf.org/mailman/listinfo/sacm