Subject: Re: [sacm] Proposed use cases to move forward

Date: Wednesday, August 15, 2012 9:30:09 AM Pacific Daylight Time

From: david.oliva@verizon.net (sent by <sacm-bounces@ietf.org>)

To: shanna@juniper.net, sacm@ietf.org, anton@chuvakin.org

Hello all:

I think in terms on which specifications to associate with each use case.

For UC1, I can think AI and ARF for Asset Information, CCE and CCSS for system configuration, CVE and CVSS for System vulnerability.

But I just cannot see which spec in SCAP 1.2 to associate system weanesses. The only thing close to a spec that approaches these criteria are the Common Weakness Enumeration (CWE) and Common Weakness Scoring System (CWSS) that MITRE is working one. But these two specifications are not ready yet. If CWE and CWSS are part of a future version of SACM/SCAP then yes.

For UC3, I cannot see which spec in SCAP 1.2 to associate with network events. The only thing close to a spec that approaches this criterion is the Common Events Enumeration (CEE) that Dr. Chuvakin is working on.
In a short question to Dr. Chuvakin about the possibility of CEE and SCAP working together he replied "CEE can work with SCAP via OVAL, CPE, AI and ARF to report
events identifying the affected assets in a standard way". If CEE is part of a future SACM version, then yes.

David Oliva

On 08/15/12, Stephen Hanna<shanna@juniper.net> wrote:

I agree. Let's work on UC1 and UC3. The other use cases are
valuable but just doing UC1 and UC3 is plenty of work for this
group for the next year or two (maybe five!).

I saw several emails in favor of this a few weeks ago. I thought
that it was settled. I'd like to see a revised charter and use case
document, scoped down to focus on just UC1 and UC3.

What do others think? Do we have rough consensus on this?
If so, let's get moving.

Thanks,

Steve

> -----Original Message-----
> From: Adam Montville [mailto:amontville@tripwire.com]
> Sent: Wednesday, August 15, 2012 10:30 AM
> To: Adam Montville; Stephen Hanna; Luis Nunez; Omar Santos
> Cc: sacm@ietf.org
> Subject: Re: [sacm] Proposed use cases to move forward
>
> On 8/6/12 7:27 AM, "Adam Montville" <amontville@tripwire.com> wrote:
>
> > >
> > >
> > >UC1 and UC3 both require assessment of endpoint state. If not for the
> NEA
> > >ties in UC1, it seems a subset of UC3. So, we should be able to start
> > >with the main concern of UC3: Security Configuration Management.
> > >
> > >
> >
> >

> I haven't seen much activity on this thread (there was another thread,
> "Using the Frame of Reference," discussing some approaches we can use
> to
> keep us focused and meaningful).
>
> Are there any objections to tackling UC3 followed by UC1? Does anyone
> disagree with my assertion that UC3 is a subset of UC1 and that a
> reasonable starting point is Security Configuration Management?
>