Subject: Re: [sacm] Proposed SACM Charter
Date: Thursday, August 2, 2012 2:15:54 PM Pacific Daylight Time
From: kathleen.moriarty@emc.com (sent by <sacm-bounces@ietf.org>)
To: shanna@juniper.net, Kent_Landfield@McAfee.com, sacm@ietf.org

+1 on Steve's comments, very good suggestions! Can these comments get into an updated version of the charter for tonight's discussion?

I also agree on not including all of the use cases in the charter. I believe UC 5 is assisting with the connection to MILE work. Where we think another WG is addressing a use case, maybe it would be good to call that out. I think it would make the most sense to have that int he use case document. ANy thoughts?

Thanks,
Kathleen

_____
From: sacm-bounces@ietf.org [sacm-bounces@ietf.org] On Behalf Of Stephen Hanna [shanna@juniper.net]
Sent: Wednesday, August 01, 2012 8:57 PM
To: Kent_Landfield@McAfee.com; sacm@ietf.org
Subject: Re: [sacm] Proposed SACM Charter

Kent,

Thanks for drafting the charter and sending it out for comments. We've got a good start here but I have a few ideas for refinement:

1. Add "remediation and response" to the first e.g. list. In the SACM Use Cases document, use cases UC1-UC4 all include response and for good reason. Automated attacks proceed quite rapidly. Automated defense must be able to do so also, with appropriate safeguards to ensure that remediation and response don't cause more problems than they solve.

2. For "i.e. specifications", I would say "i.e. data formats". We'll be creating specifications for many things, including data formats and network protocols. I believe in this instance, you're talking about data formats. Right?

3. I don't really understand the parenthetical comment "i.e. operations". I think the preceding phrase ("curating domain concept instance collections in content repositories") means "storing security automation content into databases". I don't mind using fancy words for that but I don't see what "i.e. operations" has to do with that. Maybe you mean that the security operations teams will be using that content. But I think that applies to everything we're doing here.

4. When you say "maintain an authoritative point of reference", that starts to sound like IETF or IANA would be maintaining an authoritative list of vulnerabilities and proper configurations. Of course, that isn't what you mean. I think we want to enable organizations to maintain their own content repositories. I suggest that you rewrite that sentence to fix this confusion and also change from passive voice ("It is one thing …") to active voice. Replace that sentence with "Defining a standards representation for security content is not enough. To enable interoperable security automation, we must define standard protocols for storing, retrieving, and exchanging that content."

5. In the numbered list of areas of focus for the WG, why do you say “device states” in item 1 and “systems’ state” in item 2? Those seem to be two phrases for the same thing. Also, doesn’t 2 include 1? And “response” (including remediation and mitigation) seems to be missing from this list. Do we just want to monitor our system vulnerabilities and watch them get hacked? No, I think we want to be able to use standards to fix vulnerabilities, install countermeasures and mitigations, and intervene when attacks are detected.

6. UC2, UC4, and UC5 from the use cases document do not seem to be addressed in this charter, except perhaps for the last document on “securely sharing dynamic network state information”. Maybe this omission is deliberate. I have been saying for a while that we have too many work items on our plate. If we added UC2, UC4, and UC5 to this charter, we’d probably have 3-4 times as many work items. So I’m actually OK with deciding that UC2, UC4, and UC5 aren’t in scope for this WG. But we should make that decision explicitly.

7. One of the deliverables is “A Standards Track document specifying interfaces and communication protocols used for security automation and continuous monitoring”. That sounds like several documents. Why have one document that specifies multiple protocols and interfaces? And which protocols are these, exactly? I could imagine 20 different ones that could all fit in this broad category.

As I said above, this is a good first draft. Thanks for preparing it and for welcoming comments on it. We’ve started down the path of finding the proper scope for this WG. That’s essential.

Thanks,

Steve

From: sacm-bounces@ietf.org [mailto:sacm-bounces@ietf.org] On Behalf Of Kent_Landfield@McAfee.com
Sent: Tuesday, July 31, 2012 6:12 PM
To: sacm@ietf.org
Subject: [sacm] Proposed SACM Charter

Hi all,

Here is an initial cut at the proposed SACM Working Group charter. The intent of this is to be a starting point for the conversation. Comments are expected, encouraged and welcomed.

Security Automation Continuous Monitoring (SACM)

Proposed Working Group Charter

Chairs:
TBD
TBD

Security Area Directors:
Stephen Farrell <stephen.farrell@cs.tcd.ie<mailto:stephen.farrell@cs.tcd.ie>>
Sean Turner <turners@ieca.com<mailto:turners@ieca.com>>

Security Area Advisor:
Sean Turner <turners@ieca.com<mailto:turners@ieca.com>>

Mailing Lists:
General Discussion: sacm@ietf.org<mailto:sacm@ietf.org>
To Subscribe: http://www.ietf.org/mailman/listinfo/sacm
Archive: http://www.ietf.org/mail-archive/web/sacm

Description of Working Group

Securing information and the systems that store, process, and transmit that information has become a challenging task for organizations of all sizes, and we find that security practitioners spend most of their time on manual processes relegating them to ineffectiveness. Security automation is the key to escaping this rut. This working group will enable security automation standards in support of information security processes and practices where practical, such that security practitioners can be better utilized within their organizations and we can meet the more advanced needs of the security community (e.g. information sharing, continuous monitoring, result aggregation and analysis). The initial focus of this work is toaddress enterprise and SOHO use cases. The working group will achieve this by consuming and continuing (with cooperation) the security automation work already performed by various organizations around the world.

The initial work has been fruitful, and the specifications previously published are ready for expansion on the international stage. Of particular interest to this working group are the security automation specifications supporting asset, change, configuration, and vulnerability management. Of secondary interest to this working group are the emerging security automation specifications relating to event management and continuous monitoring.

By undertaking this work, we recognize that there are multiple categories of problems in the security automation domain: defining expressions for particular domain concepts (i.e. specifications), curating domain concept instance collections in content repositories (i.e. operations), and enabling interoperability through the development and use of interfaces and communications protocols. It is one thing to define an expression for vulnerabilities and configuration items, but it is quite another to maintain an authoritative point of reference upon which tools (and their users) can rely and support the automated exchange of vulnerability and configuration information.

This working group will provide solutions to these categories of problems and the main areas of focus for this working group are described as follows:

1. Define, either by normative reference, adoption, or creation, a set of standards that can be used for the purpose of assessing, aggregating and comparing device states against expected values,and reporting on those results in a predefined or ad hoc manner.

2. Define, either by normative reference, adoption, or creation, a set of standards that can be used to continuously monitor and report on systems' state and security process effectiveness in a pre-defined or ad-hoc manner.

3. Create relationships between existing operations management standards to enable a comprehensive view of security automation, leveraging existing work and implementations.

This working group will produce the following:

* An Informational document providing an overview of security automation and continuous monitoring to include a reference model
* A Standards Track document specifying benchmark configuration representation
* An Informational document stating guidelines / requirements for specifying checking languages
* Standards Track documents specifying device state checking languages
* A Standards Track document specifying an interrogative checking language
* A Standards Track document specifying platform naming, matching and applicability
* A Standards Track document specifying asset identification and reporting information
* A Standards Track document specifying interfaces and communication protocols used for security automation and continuous monitoring

* A Standards Track document describing the messages and network protocols for distributing Security Automation Content
* A Standards Track document describing integrating security automation and Network Endpoint Assessment capabilities
* A Standards Track document describing protocols and data formats for securely sharing dynamic network state information among security systems

Goals and Milestones

Needs to be developed.

Kent Landfield

McAfee | An Intel Company
Direct: +1.972.963.7096
Mobile: +1.817.637.8026
Web: www.mcafee.com<http://www.mcafee.com/>