Subject: Re: [sacm] SACM Use Cases Updated
Date: Monday, July 23, 2012 7:14:56 AM Pacific Daylight Time
From: kathleen.moriarty@emc.com (sent by <sacm-bounces@ietf.org>)
To: osantos@cisco.com, david.waltermire@nist.gov, sacm@ietf.org

Thanks, Omar!

Those are good suggestions. I agree some will go to UC5, where some of the work (drafts to support the use cases) is handled in MILE and SACM will have relationships with the work in MILE (we may need SACM to have drafts supporting these relationships). Some of this updated version of UC4 will get handled through MILE as well, I suspect. It is good to build out the bigger picture in this document though, thanks!

Best regards,
Kathleen

-----Original Message-----
From: sacm-bounces@ietf.org [mailto:sacm-bounces@ietf.org] On Behalf Of Omar Santos (osantos)
Sent: Sunday, July 22, 2012 9:03 PM
To: Waltermire, David A.; sacm@ietf.org
Subject: Re: [sacm] SACM Use Cases Updated

Hi Dave/team,

My apologies for the delay. The following are a minor suggestion/feedback
for the SACM Use Cases (draft-waltermire-sacm-use-cases).

Under 3.4. UC4: Secure Exchange of Risk and Compliance Information

Perhaps we can add "new reports of potential zero-day vulnerabilities to
vendors."

I know that we have the following:

o Potential sharing of risk and/or threat behavioral information
   with partners as well as reference data and content like USGCB,
   NVD, IAVM, and machine-readable US-CERT alerts

However, it may be a good use case expand on the notification to vendors
of potential zero-day vulnerabilities and also the coordination/exchange
of information of potential industry-wide vulnerabilities (i.e., protocol
vulnerabilities; or any other issue that may affect multiple vendors).

We can also include some language about the aforementioned under "3.5.
UC5: Automated Forensics Investigation"

Regards,

Omar Santos

Incident Manager, PSIRT
Security Research and Operations
Cisco Systems, Inc.
Email: os@cisco.com
Phone: +1 919 392 8635
PGP Key: 0x3AF27EDC

Cisco.com - http://www.cisco.com <http://www.cisco.com/>
Cisco Security Advisories and Notices - http://www.cisco.com/go/psirt

On 7/16/12 5:43 PM, "Waltermire, David A." <david.waltermire@nist.gov>
wrote:

> I just posted an updated SACM use cases document based on all the contributions and comments to date. Thanks for all the input! Links to the updated document are below. I'd appreciate any feedback.
>
> Sincerely,
> Dave
>
> -----Original Message-----
> From: internet-drafts@ietf.org [mailto:internet-drafts@ietf.org]
> Sent: Monday, July 16, 2012 5:38 PM
> To: Waltermire, David A.
> Subject: New Version Notification for
> draft-waltermire-sacm-use-cases-01.txt
>
> A new version of I-D, draft-waltermire-sacm-use-cases-01.txt
> has been successfully submitted by David Waltermire and posted to the
> IETF repository.
>
> Filename:	draft-waltermire-sacm-use-cases
> Revision:	01
> Title:		Analysis of Security Automation and Continuous Monitoring (SACM)
> Use Cases
> Creation date:	2012-07-16
> WG ID:		Individual Submission
> Number of pages: 13
> URL:
> http://www.ietf.org/internet-drafts/draft-waltermire-sacm-use-cases-01.txt
> Status:
> http://datatracker.ietf.org/doc/draft-waltermire-sacm-use-cases
> Htmlized:
> http://tools.ietf.org/html/draft-waltermire-sacm-use-cases-01
> Diff:
> http://tools.ietf.org/rfcdiff?url2=draft-waltermire-sacm-use-cases-01
>
> Abstract:

> This document identifies foundational use cases, derived functional capabilities and requirements, architectural components, and the supporting standards needed to define an interoperable, automation infrastructure required to support timely, accurate and actionable situational awareness over an organization's IT systems. Automation tools implementing a continuous monitoring approach will utilize this infrastructure together with existing and emerging event, incident and network management standards to provide visibility into the state of assets, user activities and network behavior. Stakeholders will be able to use these tools to aggregate and analyze relevant security and operational data to understand the organizations security posture, quantify business risk, and make informed decisions that support organizational objectives while protecting critical information. Organizations will be able to use these tools to augment and automate information sharing activities to collaborate with partners to identify and mitigate threats. Other automation tools will be able to integrate with these capabilities to enforce policies based on human decisions to harden systems, prevent misuse and reduce the overall attack surface.
>
> The IETF Secretariat
>
> ____
> sacm mailing list
> sacm@ietf.org
> https://www.ietf.org/mailman/listinfo/sacm

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

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