Subject: Re: [sacm] SCAM Use Case 5 "Define Security Policy"
Date: Tuesday, July 24, 2012 9:41:17 AM Pacific Daylight Time
From: Waltermire, David A. (sent by <sacm-bounces@ietf.org>)
To: kathleen.moriarty@emc.com, smullen@us.ibm.com, sacm@ietf.org
CC: s.whitlock@opengroup.org, j.hietala@opengroup.org

I am inclined to create subsections under the current use case sections. Within these subsections, we can flesh out the "building blocks" such as what Shawn has provided. Does this sound like a reasonable way to organize the material?

Sincerely,
Dave

From: sacm-bounces@ietf.org [mailto:sacm-bounces@ietf.org] **On Behalf Of** kathleen.moriarty@emc.com
Sent: Monday, July 23, 2012 10:21 AM
To: smullen@us.ibm.com; sacm@ietf.org
Cc: s.whitlock@opengroup.org; j.hietala@opengroup.org
Subject: Re: [sacm] SCAM Use Case 5 "Define Security Policy"

Shawn,

Thank you for chiming in! Would you see the proposed UC5 as a new UC1 since policy is a building block? This would just mean we have another Use case to build out the full picture. Your suggestion makes perfect sense.

From a conversation last week, we may want to have a use case on configuration management as well, before we get to enforcement, reporting, and remediation. It would be a building block along with the policy information suggested by Shawn. Any thoughts?

Thanks,
Kathleen

From: sacm-bounces@ietf.org [mailto:sacm-bounces@ietf.org] **On Behalf Of** Shawn Mullen
Sent: Monday, July 23, 2012 9:48 AM
To: sacm@ietf.org
Cc: Stephen Whitlock; j.hietala@opengroup.org
Subject: [sacm] SCAM Use Case 5 "Define Security Policy"

During the Washington DC 7/18/12 Open Group Conference Steve Hanna, John Banghart, and Kathleen.Moriarty presented the SACM overview and called for participation. In particular they ask for review and contributions to the use case definition. Therefore I am proposing the following.

Looking at this form how a enterprise would roll-out or implement a SACM environment, I belive the first use case is a simple way to define or author a security policy. This defined policy bridges the organization's security principles and goals into a policy that form that can be applied to a system or used to check a system, e.g. XML. Formally stated I suggest UC5 as follows.

3.5 UC5 Define Security Policy

This use case provides a method for IT security principles and requirements to be expressed in a common descriptive language such as XML. This common descriptive language will define the organizations security policy. The security policy definition will be at a sufficiently high level to facilitate simplicity and ease of use, It will not require the author to specify the configuration methods and commands to implementation the policy on the differing IT devices. However it will be possible for the IT devices to bridge this high security policy into actionable configuration settings.

Given the above use case, a CIO or CSO can express the security and governance requirements in a single common secruity policy xml file. This single file can be applied to all IT devices such as servers, clients, network devices, etc. Given this state, UC1 can be attained, That is we now have a common security policy which can be assessment and enforced against.

A single security policy also facilitates UC4 making GRC reporting common no matter the device being assessed. That is high level security policy not only bridges the organization security principles into a device configuration it also provides the inverse for reporting devices assessment back up to the CIO/CSO level.

My other comment is on simplicity. Just like security should be built in and not bolted on. Simplicity should be clearly defined and built in. Complexity is the enemy of security. Not only does simplicity increase adoption it also eliminates the number of components to be trusted and reduces attack surfaces.

--------- existing Use cases for reference ----------

3.1. UC1: Assessment and Enforcement of Acceptable State

Controlling access to networks and services based on the assessment and analysis of host and/or network state based on machine processable content.

3.2. UC2: Behavioral Monitoring and Enforcement

Controlling access to networks and services based on the detection and analysis of host and/or user behavior using automatable information from various sources.

3.3. UC3: Security Control Verification and Monitoring

Continuous assessment of the implementation and effectiveness of security controls based on machine processable content.

3.4. UC4: Secure Exchange of Governance, Risk and Compliance (GRC) Information

Sharing security and/or operationally relevant information within and

across trust boundaries using secure, automated communication channels and formats.

Shawn Mullen
Power Software Security Architect

cell - (512) 914-8134
11400 Burnet Road internal 9551
Austin, TX 78758-3493
office (512) 286-7683
(T/L: 363-7683)