SACM Scope Discussion
IETF-92 Meeting

March 23, 2015

Dave Waltermire

Adam Montville

Background

- Targeting by endpoint class became a point of discussion
- Class of endpoint may effect which attributes can be relied on for identifying that endpoint
- Seemed to be consensus within that design team to agree on defining endpoint classes

Paraphrased SACM's Charter

- **Collect** and **verify** security configurations
- First address **enterprise use cases** for endpoint posture assessment

SACM Goals Are To Define:

1. A set of standards to enable assessment of endpoint posture [in the enterprise context].
2. A set of standards for interacting with repositories of content related to assessment of endpoint posture [in the enterprise context].

Let's Categorize Devices And Pick

- Traditional
- Mobile
- Network Devices
- Constrained (e.g. ICS, IoT)

SUPPORTING MATERIAL

RFC 5209: Endpoint Definition

Any computing device that can be connected to a network. Such devices normally are associated with a particular link layer address before joining the network and potentially an IP address once on the network. This includes: laptops, desktops, servers, cell phones, or any device that may have an IP address.

RFC 5209: Posture Definition

Configuration and/or status of hardware or software on an endpoint as it pertains to an organization's security policy.