SACM Architecture Redux

IETF 101
Adam Montville
Center for Internet Security
An assertion...

...SACM ideally intends to enable a cooperative ecosystem of tools from disparate sources with minimal operator configuration.
Another assertion...

...[our architectural solution] approaches [are] sometimes thought to be at odds with each other - specifically ECP and XMPP-grid.
What if...

...both are relevant to us?
The Gist
ECP 1
ECP 2
ECP 3
Next...
Agents as XMPP Clients
XMPP Presence Opens Doors

[Diagram showing the flow of data between Posture Policy Source, Local Posture Policy, Repository / Dashboard, Orchestration, and various Posture Assessors connected through XMPP-Controller.]
Potential XMPP Extensions
Possible SACM Components

**Repository**
- Vulnerability Information
- Software Inventory
- Configuration Policy
- Configuration State

**Collector**
- Software Inventory Collector
- Vulnerability State Collector
- Configuration State Collector

**Evaluator**
- Software Inventory
- Vulnerability State
- Configuration State

**Orchestrator**
- Vulnerability Management
- Configuration Management
- Asset Management
Going Forward...

Welcome contributions.
Continue exploration and hackathons.
Pick one or two capabilities and associated components for focus.

AND

Consider contributions to XMPP-Grid in MILE
Or...Create XMPP-Grid+ here in SACM
Or...Do something else for message transfer