(Maybe) Narrowing Information Model Elements

What Do We Really Need?

Adam Montville
IETF 97
November 15, 2016
Benchmarks (technology configuration recommendations)
Benchmarks we can analyze (they’re not just docs)
Benchmarks with at least one recommendation not automated
Scored recommendations
Automated recommendations
Distinct endpoint attribute types
OVAL test types
Distinct Operations

140 → 92 → 39

6012 → 5120 → 112 → 72 → 18
140
92 → 39
6012 → 5120 → 112 → 72 → 18 → 5  Data Types
This doesn’t feel so ominous.
Recommendations that ought to be automated but aren’t.

Except... 892
Will discovered needs have a dramatic impact?
By the way, the OVAL repository (vulnerability data set) has another 21 OVAL test types.

Still doesn’t seem too bad.
Now...

That seems like a lot.
A gap in the functionality provided by existing protocols is a generalized mechanism to allow external components to drive data collection activities through a common, protocol agnostic collection interface. This is a feature supported by the SACM architecture through the definition of a common interface on the right-hand side that allows the CC to choreograph posture collection through implementations of existing management protocols on the left-hand side.

But then again...

Seems to imply that the IM can’t be narrowed much?
Summary

Existing set of checks don’t seem too daunting

We have a large set of proposed Information Elements

The most recent architectural thoughts imply that we need to cover many
Do we need all 408 of those Information Elements?

Can we define a mapping framework to help scale?

Or, are we stuck?
Discussion