# SACM BOF
# March 14, 2013
# IETF-86, Orlando

# Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

# Agenda

- 1. Note Well, Note Takers, Jabber Scribes, Agenda Bashing - 5 min
- 2. SACM Use Cases - David Waltermire, Adam Montville - 30 min http://www.ietf.org/id/draft-waltermire-sacm-use-cases-04.txt
- 3. SACM Architecture - David Waltermire - 25 min http://www.ietf.org/id/draft-waltermire-sacm-architecture-00.txt
- 4. Solutions Contributions * (* there are three 10 min available slots, slot times will be allocated based on new Internet-Drafts submitted after IETF-85)
- 5. Scope and Charter Discussion - 20 min
- 6. BOF Questions - 10 min

# Solutions Contributions

- Submitted prior to IETF-85 and presented and discussed in the first BOF:
  - http://datatracker.ietf.org/doc/draft-booth-sacm-vuln-model/
  - http://datatracker.ietf.org/doc/draft-davidson-sacm-asr/
  - http://datatracker.ietf.org/doc/draft-hanna-sacm-assessment-protocols/
  - http://datatracker.ietf.org/doc/draft-montville-sacm-asset-identification/
  - http://datatracker.ietf.org/doc/draft-waltermire-content-repository/

# Proposed Charter

Name: Security Automation and Continuous Monitoring (SACM)
AREA: Security

Chairs:
TBD
TBD

Security Area Directors:
Stephen Farrell <stephen.farrell at cs.tcd.ie>
Sean Turner <turners at ieca.com>

Security Area Advisor:
Sean Turner <turners at ieca.com>

Mailing Lists:
General Discussion: sacm at ietf.org
To Subscribe: http://www.ietf.org/mailman/listinfo/sacm
Archive: http://www.ietf.org/mail-archive/web/sacm

Description of Working Group

Securing information and the systems that store, process, and transmit that information is a challenging task for organizations of all sizes, and many security practitioners spend most of their time on manual processes relegating them to ineffectiveness. The key to escaping this rut is security automation to collect, verify, and update system configurations with the ability to prioritize risk based on timely information about threats. This working group will develop security automation protocols and data format standards in support of information security processes and practices. These standards will help security practitioners to be more effective by automating routine tasks related to client and server security freeing them to focus on more advanced tasks. The initial focus of this work is to address enterprise use cases pertaining to the assessment of endpoint posture (using the definitions of Endpoint and Posture from RFC 5209).

The working group will, whenever reasonable and possible, reuse existing protocols and mechanisms. Of particular interest to this working group are the security automation specifications supporting policy asset, change, configuration, and vulnerability management.

There are multiple categories of problems in the security automation realm: enabling interoperable data exchanges through standardized protocols, defining expressions for particular domain concepts (i.e. data formats), establishing a standards-based foundation supporting the curation and exchange of security automation content collections in content repositories, and enabling interoperability through the development and use of standard interfaces and communication protocols. Content based on rich and extensible data standards and protocols will provide the authoritative instructions needed by data-driven tools to enable the automated collection of configuration and vulnerability data pertaining to enterprise assets. Information produced by these tools will provide accurate and timely situational awareness in support of organizational decision making.

# Proposed Charter (2)

The data exchange protocols will need to support several exchange types including requesting assessments and reporting on assessment results. Exchanging information across organizational boundaries will not be within scope for this effort at this time.

This working group will provide solutions to these categories of problems and the main areas of focus for this working group are described as follows:

1. One or a set of standards to enable assessment of endpoint posture.
   This area of focus provides for necessary language and data
   format specifications.

2. One or a set of standards for interacting with repositories of content
   related to assessment of endpoint posture.

In accordance with existing IETF processes, the group will communicate with and invite participation from other relevant standards bodies and groups, and if necessary reuse existing liaison relationships or request the establishment of new liaison relationships,

This working group will achieve the following milestones:

- An Informational document on Use Cases and Requirements
- An Informational document on SACM Architecture
- A Standards Track document to define a protocol for interacting
  with content repositories
- Standards Track documents specifying communication protocols and
  data formats used for assessment of endpoint posture

After these work items have been submitted to and approved by the IESG, the WG will recharter or close.

# BOF Questions

- A. Should IETF take-up the work described by the Scope and Charter**? (yes, no, no opinion) (** with possible modifications discussed today)
- B. Indicate your intent to actively contribute to this work in IETF***. (yes, no, no opinion) (*** if taken-up in the approximate form described)