SACM BOF
November 6, 2012
IETF-85, Atlanta

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, scribes, jabber (chairs): 5 min
- 2. Discussion on Use Cases http://tools.ietf.org/html/draft-waltermire-sacm-use-cases-02 , Adam Montville/Dave Waltermire: 20 min Clarification Questions: 5 min
- 3. Presentations on drafts to support Use cases
  - 3a. Asset Identification Draft, http://tools.ietf.org/html/draft-montville-sacm-asset-identification-00 (Adam Montville): 10 min
  - 3b. Continuous Assessment Protocol Draft, https://datatracker.ietf.org/doc/draft-hanna-sacm-assessment-protocols (Steve Hanna): 10 min
  - 3c. Assets Summary Reporting, http://tools.ietf.org/html/draft-davidson-sacm-asr-00 (Dave Waltermire): 10 min
  - 3d. Content Repository Protocols, http://datatracker.ietf.org/doc/draft-waltermire-content-repository/ , (Dave Waltermire): 10 min
  - 3e. Vulnerability Model, http://www.ietf.org/internet-drafts/draft-booth-sacm-vuln-model-00.txt (Dave Waltermire): 10 min
- 4. Feedback and Discussions: 30 min
- 5. Tough Questions: 30 min
- 6. Charter Review: 10 min

Tough Questions

- Do we understand the Problem Space?
  - Functional requirements and supported security processes
  - Architectural requirements
- Do we need Standards?
- Is the IETF the right place?
- Is a new WG the right place to do the work?
- How many people are interested to actively work (edit, review) on
  - SACM architecture
  - Protocol for carrying security automation and continuous assessment information
  - Protocol for distributing security automation content
  - Protocol and data format for securely sharing dynamic network state information among security systems
  - Assets Identification and Description Formats
  - Platform Naming and Matching

From the Charter Proposal – Scope of Work (if WG will be approved)

- This working group will develop security automation protocols and data format standards in support of information security processes and practices where practical. These standards will help security practitioners to be better utilized within their organizations by automating routine tasks related to endpoint and server security so that practitioners can focus on more advanced tasks. The initial focus of this work is to address enterprise use cases.
- The working group will achieve this by enabling the exchange of shared intelligence and continuing the security automation work already performed by various organizations around the world. The initial work has been fruitful, and the data formats previously published are ready for expansion on the international stage. Of particular interest to this working group are the security automation specifications supporting asset, change, configuration, and vulnerability management. Of additional interest to this working group are the emerging security automation interfaces and data formats relating to event management and continuous assessment. The continuous assessment capabilities enable organizational situational awareness through frequent snapshots of the operating state of their environment, with risk prioritized based on consumed information provided by shared intelligence (vulnerabilities, threats, etc.).

Work items Phase 1

- A standards track document to define a protocol for accessing content repositories
- Standards Track document specifying security automation/continuous assessment interfaces
- A Standards Track document specifying communication protocols used for security automation and continuous assessment
- A Standards Track document describing the messages and network protocols for distributing security automation content (content repository)
- A Standards Track document describing protocols and data formats for securely sharing dynamic network state information among security systems
- A Standards Track document specifying asset description format
- A Standards Track document specifying asset identification
- A Standards Track document specifying platform naming
- A Standards Track document specifying platform matching
- A Standards Track document specifying platform applicability

Work Items Phase 2

- A Standards Track document specifying a control framework representation format.
- A Standards Track document specifying benchmark configuration representation
- An Informational document stating guidelines / requirements for specifying checking languages
- Standards Track documents specifying device state checking languages
- A Standards Track document specifying an interrogative checking language
- A Standards Track document specifying asset reporting information
- A Standards Track document describing how to use the languages and other content defined in this group with the NEA protocols