Security Automation and Continuous Monitoring WG

Terminology and Use Cases Status Report

David Harrington

IETF 88 – Nov 4 2013

Terminology Document

- This document provides common terms used in the other documents produced by SACM.
- Draft-dbh-sacm-terminology accepted as WG draft.
- Published as draft-ietf-sacm-terminology-00.
- -01- Added vulnerability, vulnerability management, exposure, misconfiguration, and software flaw.

Use Cases Document

- This document provides a sampling of use cases for collecting, aggregating, and assessing data to determine an organization's security posture.
- From use cases, we can derive common functional networking capabilities and requirements for IETF-related standards.
- The scope of this document is limited to Enterprise Security Posture Assessment . Later documents can address other scopes.
- Existing IETF technologies might be suitable to address some of these functions and requirements.

Use Cases Status -00-

- Since IETF87
- Draft-waltermire-sacm-use-cases accepted as WG draft draft-ietf-sacm-use-cases-00
- Moved terminology section into draft-ietf-sacm-terminology-00
- Removed requirements (to be put into draft-ietf-sacm-requirements-00)

Use Cases Status -01-

- Changed format of use cases to meet WG consensus
- Rewrote section 3 content regarding asset management to focus on discrete uses of asset management
- Added section 4 - Functional Capabilities
- Removed sections on asset discovery, components, composition, resources and life cycle
- Expanded asset identification, characterization, and de-confliction.
- Added asset targeting.

Use Cases Status -02-

- Changed title
- Removed section 4 – this should go into requirements document.
- Removed list of proposed functional capabilities from section 3.1
- Removed requirements language
- Rewrote the 4 use cases in this document to meet WG format preferences.

Use Cases -03-

- Expanded "typical workflow" description
- Changed use of ambiguous "assessment" to separate collection and evaluation processes.
- Added 10 use case contributions.

Use Cases -04-.

- Added 4 use case contributions.

Use Cases in -04-

- Definition and Publication of Automatable Configuration Guides
- Automated Checklist Verification
- Organizational Software Policy Compliance
- Detection of Posture Deviations
- Search for Signs of Infection
- Remediation and Mitigation
- Endpoint Information Analysis and Reporting

Use Cases in -04-

- Asynchronous Compliance/Vulnerability Assessment
- Vulnerable Endpoint Behavior
- Compromised Endpoint Identification
- Suspicious Endpoint Behavior
- Traditional Endpoint Assessment with Stored Results
- NAC/NAP connection using endpoint evaluator
- NAC/NAP connection using third-party evaluator

Use Cases in -04-

- Repository Interactions – A Full Assessment
- Repository Interactions – Filtered Data Assessment
- Direct Human Retrieval of Ancillary Materials
- Register with Repository for Immediate Notification of New Security Vulnerability Content that Match a Selection Filter

Some Use Cases from -01- not in -04-

- NIDS Response
- Historical Vulnerability
- Source Address Validation
- Event Driven Monitoring
- Periodic Monitoring
- Self-monitoring
- Do these belong in use cases document?
- Are these adequately captured in rewritten use cases?

Issues

- Should use cases be simplified?
- Do use cases need to be simplified?
- Goal of use cases is to get user feedback and to have use cases drive requirements.
- Now we need to start extracting requirements wish-list.
- Are these 18 use cases adequate for driving requirements?

Questions?