Security Automation and Continuous Monitoring WG

Use Cases Status Report

David Harrington

IETF 87 – Aug 2 2013

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

- Dave Harrington added as editor
- Modified text to reflect charter and WG consensus
  - Introduction describes the focus
  - Organized by asset, config, change, and vulnerability management
  - Focus on Enterprise use cases
  - Focus on UC1 – Endpoint Posture Assessment
  - Removed UC2 – Enforcement of Acceptable State
  - Removed UC3 – Security Control Verification and Monitoring

Use Cases Status

- Editorial changes
  - Removed references to WG and charter
  - Moved NIST acknowledgement to Acknowledgements
  - Removed discussion of chapters; we have Table of Contents
  - Modified IANA and Security Considerations sections
  - Removed some marketing claims to focus on technical analysis
  - Moved terms to the front; combined with RFC 2119 text
  - Removed "Key Concepts"; not used in document, better in arch
  - Moved (partly) to an IETF-style use case approach

Use Cases

- Asset Mgmt
  - Asset Discovery – subnet, IP addresses
  - Asset Characterization – system, components, host resources
- Config Mgmt
  - Config – hardware/software component mappings, resources, interfaces
- Change Monitoring
  - Change monitoring – DHCP addressing, RADIUS services, NAT logging, syslog authorization warnings

Use Cases

- Vulnerability Mgmt
  - NIDS Response
  - Historical Vulnerability
  - Source Address Validation

Use Cases to be Added

- A number of additional use cases have been sent to the list for discussion, but are not yet added in -05-
  - Suspicious Endpoint Behavior
  - Vulnerable Endpoint Behavior
  - Batch Assessment
  - Event Driven Monitoring
  - Periodic Monitoring
  - Self-monitoring

Issues

- Should our use cases be limited to our constrained focus, or show the larger general environment in which the constrained focus fits?
- Should we be collecting/gathering requirements now, or after we have gathered use cases?
- What is the appropriate descriptive level for our use cases? Should we be identifying which parties rely on what functionality, and what data is required, to be successful?
- Should discussions be taken to more public fora (trade shows)?

Issues

- Should our use cases be limited to discussions of interactions relevant to IETF?
  - User actions should relate to Internet protocols

Questions?