Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 17, 2013

D. Waltermire, Ed.
NIST

July 16, 2012

Analysis of Security Automation and Continuous Monitoring (SACM) Use Cases
draft-waltermire-sacm-use-cases-01

Abstract

This document identifies foundational use cases, derived functional capabilities and requirements, architectural components, and the supporting standards needed to define an interoperable, automation infrastructure required to support timely, accurate and actionable situational awareness over an organization's IT systems. Automation tools implementing a continuous monitoring approach will utilize this infrastructure together with existing and emerging event, incident and network management standards to provide visibility into the state of assets, user activities and network behavior. Stakeholders will be able to use these tools to aggregate and analyze relevant security and operational data to understand the organizations security posture, quantify business risk, and make informed decisions that support organizational objectives while protecting critical information. Organizations will be able to use these tools to augment and automate information sharing activities to collaborate with partners to identify and mitigate threats. Other automation tools will be able to integrate with these capabilities to enforce policies based on human decisions to harden systems, prevent misuse and reduce the overall attack surface.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 17, 2013.

Table of Contents

1. Introduction

This document addresses foundational use cases in security automation. Portions of these use cases may be considered when establishing a charter for the Security Automation and Continuous Monitoring (SACM) working group within the IETF. This working group will address a portion of the standards needed to define an interoperable, automation infrastructure required to support timely, accurate and actionable situational awareness over an organization's IT systems. This document enumerates use cases and break down related concepts that cross many IT security information domains.

Sections [...] of this document focus on:

- Defining the key concepts and terminology used within the document providing a common frame of reference;
- Identifying foundational use cases that represent classes of stakeholders, goals, and usage scenarios;
- A set of derived functional capabilities and associated requirements that are needed to support the use cases;
- A break down of architectural components that address one or more functional capabilities that can be used in various combinations to support the use cases; and
- An inventory of existing, emerging, and needed data exchange models and communications protocols that are required to support interoperability between architectural components.

The standards identified in this document provide a foundation for creating interoperable automation tools and continuous monitoring solutions that provide visibility into the state of assets, user activities, and network behavior. Stakeholders will be able to use these tools to aggregate and analyze relevant security and operational data to understand the organizations security posture, quantify business risk, and make informed decisions that support organizational objectives while protecting critical information. Organizations will be able to use these tools to augment and automate information sharing activities to collaborate with partners to identify and mitigate threats. Other automation tools will be able to integrate with these capabilities to enforce policies based on human decisions to harden systems, prevent misuse and reduce the overall attack surface.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Key Concepts

Define/reference the major concepts included in this document.

3. Use Cases

Describe use cases, one per sub-section.

Things to consider including (but not limited to):

- Usage scenarios (e.g. Security Control Verification, Endpoint Enforcement, Incident Detection, Forensic Investigation, etc.)
- Information Domains (e.g. configuration, vulnerability, digital events, etc.)
- Characteristics of the information used (e.g. real-time/periodic, static/dynamic, etc.)

3.1. UC1: Assessment and Enforcement of Acceptable State

Controlling access to networks and services based on the assessment and analysis of host and/or network state based on machine processable content.

Possible "things" that are being measured:

- Asset information (e.g., Asset identification, ARF, ASR)
- System configuration (e.g., SCAP)
- System vulnerabilities (e.g., SCAP)
- System weaknesses
- Semi-automated human interrogation methods to assess non-automatable, technical controls (e.g., OCIL)

Possible desired outcomes to address:

- User/system is allowed access to network resources
- User/system is denied access to network resources
  - Potential mitigation actions are taken

The Network Endpoint Assessment (NEA) protocols (PA-TNC [RFC5792], PB-TNC [RFC5793], PT-TLS [I-D.ietf-nea-pt-tls], and PT-EAP [I-D.ietf-nea-pt-eap]) may be used to query and transport the things to be measured, as well as providing for manual or automated remediation and mitigation. SCAP content (XCCDF, OVAL, OCIL, etc.) may be transported over the NEA protocols to indicate which things are to be measured and send the results of the measurements. And enforcement may be implemented with RADIUS [RFC2865] or DIAMETER [RFC3588].

3.2. UC2: Behavioral Monitoring and Enforcement

Controlling access to networks and services based on the detection and analysis of host and/or user behavior using automatable information from various sources.

Possible "things" that are being measured:

- System configuration
- System vulnerabilities
- Network events
- User/host behavior

Possible desired outcomes to address:

- Change in state is recorded and reported
- User/system activity is recorded and reported
- User/system access is terminated or altered

The Trusted Computing Group's [IF-MAP] protocol provides a standard way to rapidly share events and updates related to user/device behavior and network events, enabling logging or swift response such as reduced or terminated access.

Possible other things to address:

- Discuss how this could potentially be related to the IP Flow Information Export (ipfix) working group. Basically leveraging Netflow to detect network behavior. This information could be received from what the MILE WG is doing with incident response. (see UC5 and UC4)

- Relevant processes, technologies and techniques.

3.3. UC3: Security Control Verification and Monitoring

Continuous assessment of the implementation and effectiveness of security controls based on machine processable content.

Possible "things" that are being measured:

- Compliance to organizationally defined/required controls
  - System configuration
  - System vulnerabilities
  - Network events
  - Semi-automated human interrogation methods to assess non-technical controls
- Deviations from expected state

Possible desired outcomes to address:

- Compliance or non-compliance is recorded and reported

This use case extends UC1 to ensure that changes to the things measured in UC1 are rapidly detected, reported, and optionally responded to with manual or automated remediation and mitigation.

Possible other things to address:

- Relevant processes, technologies and techniques.

3.4. UC4: Secure Exchange of Risk and Compliance Information

Sharing security and/or operationally relevant information within and across trust boundaries using secure, automated communication channels and formats.

Possible "things" that are being measured:

- ???

Possible desired outcomes to address:

- Combining results from UC1-UC3, a report to an organizational authority is generated, including relevant data pertaining to the user activities, potentially along with the aggregated data from other user activities.

- Aggregate/roll-up reporting of organizational, security-oriented information in response to pre-arranged and ad hoc, automated data requests.

- Potential sharing of risk and/or threat behavioral information with partners as well as reference data and content like USGCB, NVD, IAVM, and machine-readable US-CERT alerts

- Outcome of UC4 informs back through UC1-UC3, such as updates to digitial policies, adjusted configurations, new patch data, etc.

Possible other things to address:

- Indicate the relationship of this use case to UC3 and UC5. This use case supports requests for and reporting of information generated by UC3 and UC5.

- Be sure to incorporate Incident/Security Event Exchange (UC5).

- Document how this use case supports methods to combine data sets to generate reports that would be shared between parties. This is a touch point with the MILE GRC-Exchange work. Establish the use cases for the exchange. In the following sections, discuss additional work that may be needed to tie these pieces together

- Discuss the use of content repositories in support of information exchange.

- Relevant processes, technologies and techniques.

3.5. UC5: Automated Forensics Investigation

Remote and/or local collection of organizational, network, and/or host information to generate situational awareness that will serve as an input to enhance incident detection, investigation, and response activities.

Possible "things" that are being measured:

- Scope and impact of security incident
  - Coverage of situational awareness for the assets monitored (trending as improvements are made and new data sources are added for each of the above use cases)
  - Time to detect compliance and security issues/problems from increased capabilities to automate continuous monitoring
  - Time to resolve issues/problems detected from continuous monitoring solutions and improvements (trending) to demonstrate prevention capability improvements
  - Number of low, medium, and high level threats to assets (considering the criticality of those assets) using the combined situational awareness, continuous monitoring, and feeds of known vulnerability information, static and over time.
  - Variations in behavior to enhance detection capabilities through increased situational awareness gained from UC1, UC2, and UC3
  - Impact of security incidents trending against improvements in situational awareness capabilities
  - Time to detect, quarantine, and remediate incidents, trending over time for each measurement, correlated to improvements in situational awareness and continuous monitoring.
  - Impact of security incidents measured by time, monetary impact, reputation and other factors. The trending of these measurements as improvements are made to situational awareness and continuous monitoring is a critical key performace indicator for the security program.

Possible desired outcomes to address:

- Identify the need for additional data collection from UC1-UC3 based on gaps in information currently collected
- Can be informed by UC4, such as shared risk/threat information
- Intersect data and analysis provided from UC1, UC2, and UC3 with threat and vulnerability information to enable detection of incidents via event information related to the described intersection.

- Alteration to acceptable system state requirements necessary for UC1-UC2

- Identify the need for additional or altered controls to be addressed by UC3

- Identify the appropriate techniques and data sources necessary to build situational awareness and continuous monitoring solutions using standards to provide improved prevention and detection capabilities. This step does not perform the analysis, but provides the data and techniques to obtain the data to enable the necessary analysis capabilities.

Possible other things to address:

- Relevant processes, technologies and techniques.

- Determine standard inputs to create situational awareness, leaving analysis out-of-scope to enable innovation. The relevant techniques will be addressed in UC1-UC4.

- Determine existing sets of processes, technologies, and techniques that may be leveraged specific to increased awareness of incidents and current threats through sharing indicators of compromise. Examples include, but are not limited to:

  * RFC5070, Incident Object Description Exchange Format (IODEF)

  * RFC6545, Real-time Inter-network Defense (RID)

  * RFC6546, Transport of Real-time Inter-network Defense over HTTP/TLS

  * Extensions to IODEF such as:

    + RFC5901, Extension to IODEF-Document Class for Reporting Phishing

    + RFC5941, Sharing Transaction Fraud Data

    + IODEF-extension to support structured cyber security information:

      - http://datatracker.ietf.org/doc/draft-ietf-mile-sci/

    + Forensics extension

+ Etc.

4. Functional Capabilities

Decompose the functional capabilities needed to support the use cases, one per sub-section. Cross reference the use case dependencies where they exist.

Things to consider including (but not limited to):

- Information Views/Reports (e.g. security posture, compliance, control effectiveness)
- Data Collection (e.g. configuration state, software inventory, user and network behavior)
- Reference Information Formats (e.g. control catalogs, configuration baselines, malware characteristics, vulnerability data)

4.1. Functional Capability 1

Describe the first capability.

4.2. Functional Capability n

Describe the n capability.

5. Functional Components

Describe the abstract functional components needed to provide the capabilities described in the previous section. Describe any relationships between the components and how they can be composed to address functional capabilities. (this might be better defined in the previous section.)

Things to consider including (but not limited to):

- Topologies
- Federation Strategy

6. Data Exchange Models and Communications Protocols

Document where existing work exists, what is currently defined by SDOs, and any gaps that should be addressed. Point to existing event, incident and network management standards when available. Describe emerging efforts that may be used for the creation of new standards. For gaps provide insight into what would be a good fit for SACM or another IETF working groups.

This will help us to identify what is needed for SACM to be successful. This section will help determine which of the specifications can be normatively referenced and what needs to be addressed in the IETF. This should help us determine any protocol or guidance documentation we will need to generate to support the described use cases.

Things to address:

For IETF related efforts, discuss work in NEA and MILE working groups. Address SNMP, NetConf and other efforts as needed.

Reference any Security Automation work that is applicable.

7. IANA Considerations

This memo includes no request to IANA.

All drafts are required to have an IANA considerations section (see RFC 5226 [RFC5226] for a guide). If the draft does not require IANA to do anything, the section contains an explicit statement that this is the case (as above). If there are no requirements for IANA, the section will be removed during conversion into an RFC by the RFC Editor.

8. Security Considerations

All drafts are required to have a security considerations section. See RFC 3552 [RFC3552] for a guide.

9. Acknowledgements

The author would like to thank Kathleen Moriarty and Stephen Hanna for contributing text to this document. The author would also like to acknowledge the members of the SACM mailing list for thier keen and insightful feedback on the concepts and text within this

document.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

10.2. Informative References

[I-D.ietf-nea-pt-eap]
Cam-Winget, N. and P. Sangster, "PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods", draft-ietf-nea-pt-eap-02 (work in progress), May 2012.

[I-D.ietf-nea-pt-tls]
Sangster, P., Cam-Winget, N., and J. Salowey, "PT-TLS: A TCP-based Posture Transport (PT) Protocol", draft-ietf-nea-pt-tls-05 (work in progress), May 2012.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5792] Sangster, P. and K. Narayan, "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5792, March 2010.

[RFC5793] Sahita, R., Hanna, S., Hurst, R., and K. Narayan, "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5793, March 2010.

Appendix A. Additional Stuff

This becomes an Appendix if needed.

Author's Address

David Waltermire (editor)
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20877
USA

Phone:
Email: david.waltermire@nist.gov