Asset Summary Reporting
draft-davidson-sacm-asr-00

David Waltermire (david.waltermire@nist.gov)
Presenting for:
Mark Davidson (mdavidson@mitre.org)
What is Asset Summary Reporting (ASR)?

An XML-based data format that facilitates the exchange of summary information about one or more sets of assets.

- ASR is vendor neutral.
- It is flexible, and suited for a wide variety of reporting applications.

ASR Goals:
- To describe summary information about one or more arbitrarily large and complex asset-related data sets in a standardized manner.
- To allow content producers the ability to choose an appropriate level of detail depending on their needs and data set size requirements.
- To reduce the complexity of producing and consuming summary result documents.

This specification defines an asset as anything that has value to an organization including, but not limited to:
- Computing devices
- Networks
- People
- Organizational units
What information does it capture?

• Data source
  – Identifies the asset pool from which the report is generated
  – Can use Asset Identification (draft-montville-sacm-asset-identification-00) to identify assets

• Record set
  – A collection of 1 or more records to report
  – An ASR record set may span multiple pages when necessary
    • Reduces risk of resending a large, single report
    • Reduces memory load of creating large, single reports

• Record set type
  – A description of how to construct a record set
  – May reference a record set type definition

• Namespace Qualified Attributes
  – Semantically well-defined attributes associated with a record
  – Controlled vocabulary approach
  – Specific data types (e.g. counts of assets, identifier types, report findings)
How does it relate to the IETF?

Security Automation and Continuous Monitoring (SACM)

Use Case 1: System State Assessment (draft-waltermire-sacm-use-cases-02)

• Asset Management (4.1.1)
  – Can provide a common vocabulary to support the exchange of asset details

• Content Management (4.1.4)
  – Record Set Type definitions are another type of content that may be exchanged
    • Provides machine-interpretable guidance that may support report generation
    • Used to validate reporting data
How does it relate to the IETF? (Cont’d)
Security Automation and Continuous Monitoring (SACM)

Use Case 2: Enforcement of Acceptable State (draft-waltermire-sacm-use-cases-02)
• Assessment Query and Transport (4.2.1)
  – Exchange of assessment results
  – Use within NEA-related protocols to provide transport?
How does it relate to the IETF? (Cont’d)
Security Automation and Continuous Monitoring (SACM)

Use Case 3: Security Control Verification and Monitoring (draft-waltermire-sacm-use-cases-02)

• Data Aggregation and Reporting (4.3.2)
  – Supports the definition and exchange of aggregate reports
  – Enables aggregation of by asset characteristics, assessment identifiers and characteristics, control identifiers, checklist identifiers, product ids or classes
How does it relate to the IETF? (Cont’d)
Managed Incident Lightweight Exchange (MILE WG)

IODEF-extension to support structured cybersecurity information (draft-ietf-mile-sci-05)

• Capable of representing observed information pertaining to various extended classes (e.g. platform, vulnerability)

• Possible candidate for inclusion in the IANA registry (Appendix II)
Possible work / How you can help?

• Develop greater consensus around reporting use cases for ASR
• Develop an IANA registry for Namespace Qualified Attributes
  – Provides future extensibility to additional reporting use cases
• Develop an IANA registry referencing definitions for common record set types
• Integrate/extend into protocols where applicable (e.g. SACM, NEA, MILE)
• JSON vs. XML
EXAMPLES
Current ASR Data Model
Example – Record Set

<asr:summary-report xmlns:ex="com.example"
xmlns:asr="http://scap.nist.gov/schema/asset-summary-reporting/1.0"
xmlns:asr-attr="http://scap.nist.gov/schema/asset-summary-reporting/1.0/attr"
page-number="1" last-page="true" report-id="d1e1">
  <asr:metadata timestamp="2011-11-08T14:27:44.97Z"/>
    record-set-type="ex:cve-report-small">
    <asr:record asr-attr:cve-id="CVE-2011-2013"
        asr-attr:inventory-finding="EXISTS" asr-attr:count="50"/>
    <asr:record asr-attr:cve-id="CVE-2011-2013"
        asr-attr:inventory-finding="NOT_EXISTS" asr-attr:count="170"/>
    <asr:record asr-attr:cve-id="CVE-2011-2013"
        asr-attr:inventory-finding="NOT_APPLICABLE" asr-attr:count="30"/>
  </asr:record-set>
  <asr:data-source id="asr:com.example:dsrc:1" resource="VulnDb.abc.com"
    population-size="250"/>
</asr:summary-report>
Example – Data Source Using Asset Identification

<asr:summary-report xmlns:ex="com.example"

...>

<asr:data-source id="asr:com.example:dsr1c:1" resource="VulnDb.example.com"

  population-size="250">

  <ai:assets>
    
    <ai:asset id="a1">  
      <ai:computing-device>  
       
        <ai:cpe>cpe:2.3:o:microsoft:windows_7:-::-x64:*:::*:::*</ai:cpe>

        <ai:fqdn>asset1.example.com</ai:fqdn>  

      </ai:computing-device>  

    </ai:asset>

    <ai:asset id="a2">  
      <ai:computing-device>  
        <ai:cpe>cpe:2.3:o:microsoft:windows_7:-::-x86:*:::*:::*</ai:cpe>

        <ai:fqdn>asset2.example.com</ai:fqdn>  

      </ai:computing-device>  

    </ai:asset>

    ...  

  </ai:assets>

</asr:data-source>

</asr:summary-report>
Example – Record Set Type

Record Set Type Name: {com.example}cve-report-small

Description: To report on the number of computers affected by a CVE. Attributes

– asr-attr:cve-id – MUST include. This is the CVE ID being reported on. Type: XML schema “string”.

– asr-attr:inventory-finding – MUST include. This is a status of the CVE for each asset in the count. Value must be one of “EXISTS”, “NOT_EXISTS”, “NOT_APPLICABLE”, “NOT_REPORTED”, “ERROR”, or “UNKNOWN”. Type: XML schema “string”.

– asr-attr:count – MUST include. Asset list is associated with this attribute. This count is the number of assets with the CVE related to the asset via the inventory-finding. Type: XML schema nonNegativeInteger.

Permit attributes not explicitly described here: no

Require asset list: not permitted

Require identifier list: not permitted