
# Data Exchange Standards Specification

## *Proposed*

## Assessment Summary Results (ASR) Format

Version 0.41 Draft (Limited Distribution)

Mr. Joe Wolfkiel

December 30, 2010

# Distribution

This document presents the version 0.41 draft ASR specification in pre-release format for comment solicitation from vendors and federal partners of the DoD and is not intended for dissemination or distribution to the general public. This document may be redistributed within a single organization, but may not be distributed outside of organizational boundaries.

Requests for updated versions of this document or external distribution should be directed to Joe Wolfkiel, Joseph.Wolfkiel@disa.mil

# Table of Contents



## Table of Figures

# Acronyms and Abbreviations

| | |
|---|---|
| ARF | Assessment Results Format |
| ASR | Assessment Summary Results |
| C&A | Certification and Accreditation |
| CCE | Common Configuration Enumeration |
| CERT | Computer Emergency Response Team |
| CPE | Common Platform Enumeration |
| CRF | Common Result Format |
| CVE | Common Vulnerabilities and Exposures |
| DoD | Department of Defense |
| DNS | Domain Name Server |
| DMZ | De-Militarized Zone |
| FDCC | Federal Desktop Core Configuration |
| FQDN | Fully Qualified Domain Name |
| GUID | Globally Unique Identifier |
| IP | Internet Protocol |
| OVAL | Open Vulnerability and Assessment Language |
| OLAP | On-Line Analytical Processing |
| POA&M | Plan of Action and Milestones |
| SCAP | Security Content Automation Protocol |
| XCCDF | eXtensible Configuration Checklist Description Format |
| XML | eXtensible Markup Language |

# 1 The Summary Results Concept

The Assessment Summary Results (ASR) language is a communication vehicle for sharing information grouped by individual findings. It differs from the Assessment Results Format (ARF) in that ARF groups findings per device. Figure 1-1 shows the difference in structure between ARF and Summary Results.

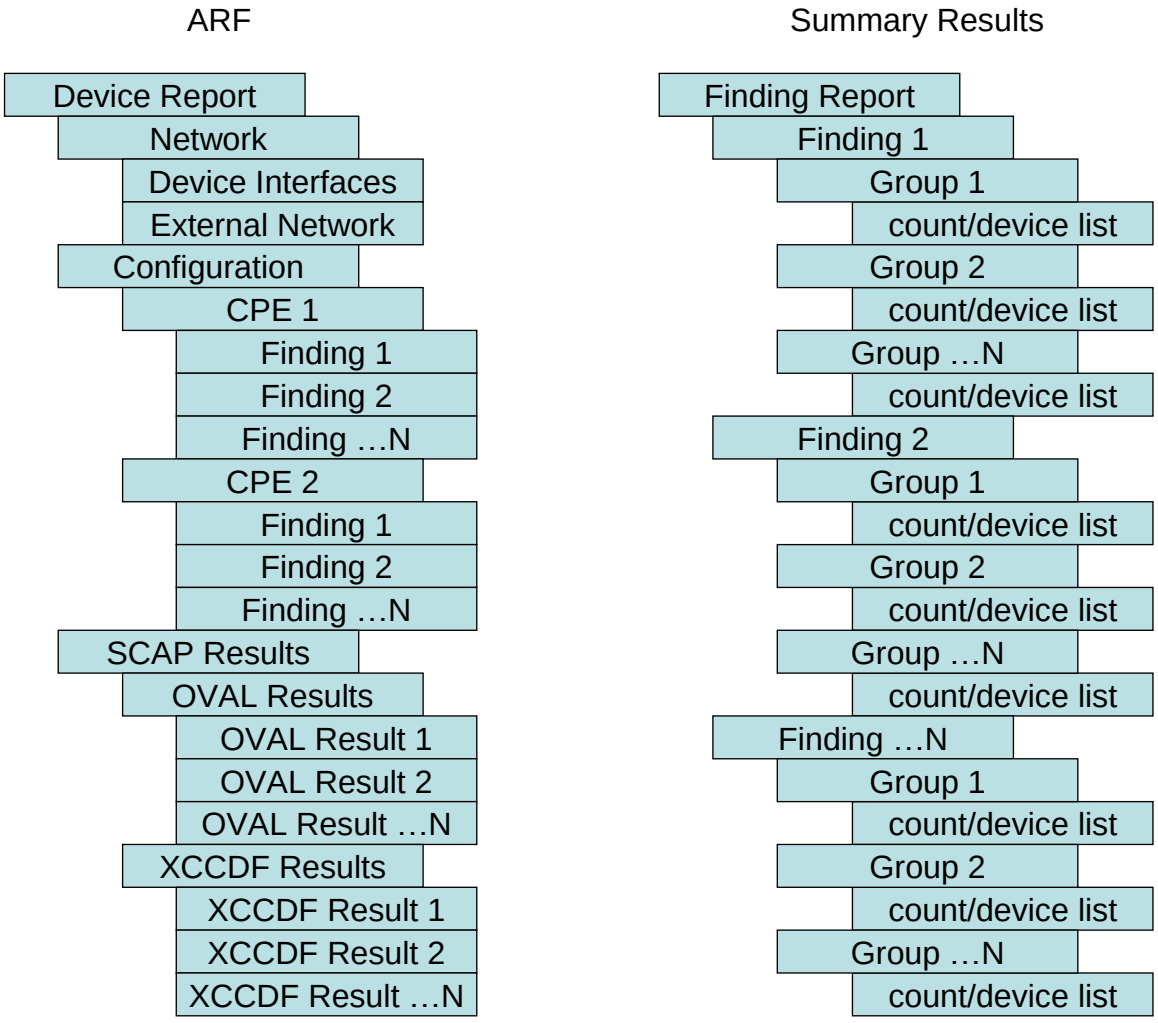


**Figure 1-1 - ARF vs ASR Concept**

# 2 The Summary Results Language

## 2.1 Summary Results Schema

As seen in Figure 2-1, the summary results format covers the major Security Content Automation Protocol (SCAP) finding types. Results can be returned using different SCAP–described conditions as the basis for reporting. For XCCDF, results include pass, fail, error, not applicable, and not tested. CPE

results will report counts or lists for each different CPE named software product that matched the input abstract CPE. In version 0.41.1, portions of ASR that were not in use (i.e. the OVAL and CCE results) were deleted in favor of a more generic schema, the System/Ident schema. The "CPE Complex" branch was also added to allow for supplying results based on combinations of installed hardware, operating systems, or applications based on the platform definition in the CPE Language schema, extended to allow for the use of a wildcard symbol "*" to allow for advanced matching capabilities.

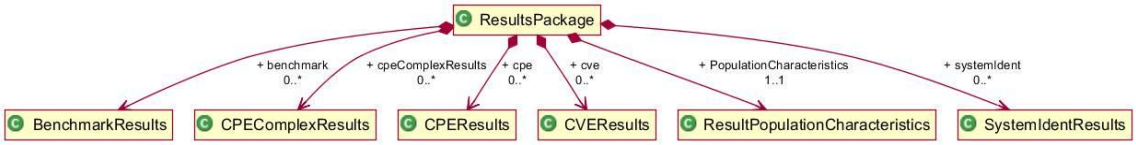


**Figure 2-1 - Summary Results Top-Level Schema**

## 2.2 Result Population Characteristics Class

Population characteristics include data about the network and types of devices that were and/or can be assessed by the tool providing the Summary Results data. A class diagram is provided in Figure 2-2. Detailed descriptions of classes, elements, and attributes can be found in the ASR Data Dictionary.

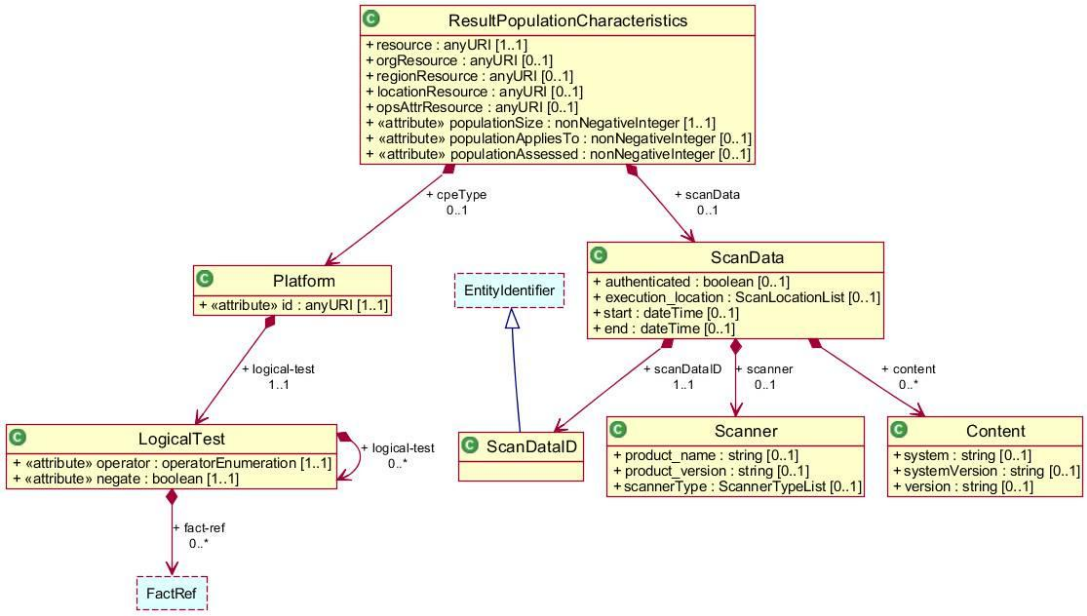


**Figure 2-2 - Result Population Characteristics Class Diagram**

Of particular note, are the new attributes, "populationAppliesTo", and "populationAssessed" in version 0.41.1. For scoring and understanding of data, it was determined that an overall population number is insufficient data about a summary results file. For relatively complete understanding, one must know first, the total amount of objects in the originating data source; second, how many a particular checking system apply to (e.g. a Windows XP benchmark would not apply to a Solaris device), and how many were actually assessed.

## 2.3 Results Values

A result value is currently a list of different results, specified by the higher-level results types that provides a count, and (optionally) a list of devices or objects, grouped by common groupBy variables. GroupBy variables are described in section 2.4.

Device records require a unique device record_identifier to be provided for each device. Other common identifiers (IP address [both IPv4 and v6], Operating System Globally Unique Identifier, Media Access Control address, and domain name) are optionally provided to enhance successful device correlation. Similarly, other objects will provide unique names, identifiers, locations, owners, etc that can be used to partition them into groups.

The Result Value UML class diagram is provided in Figure 2-3.

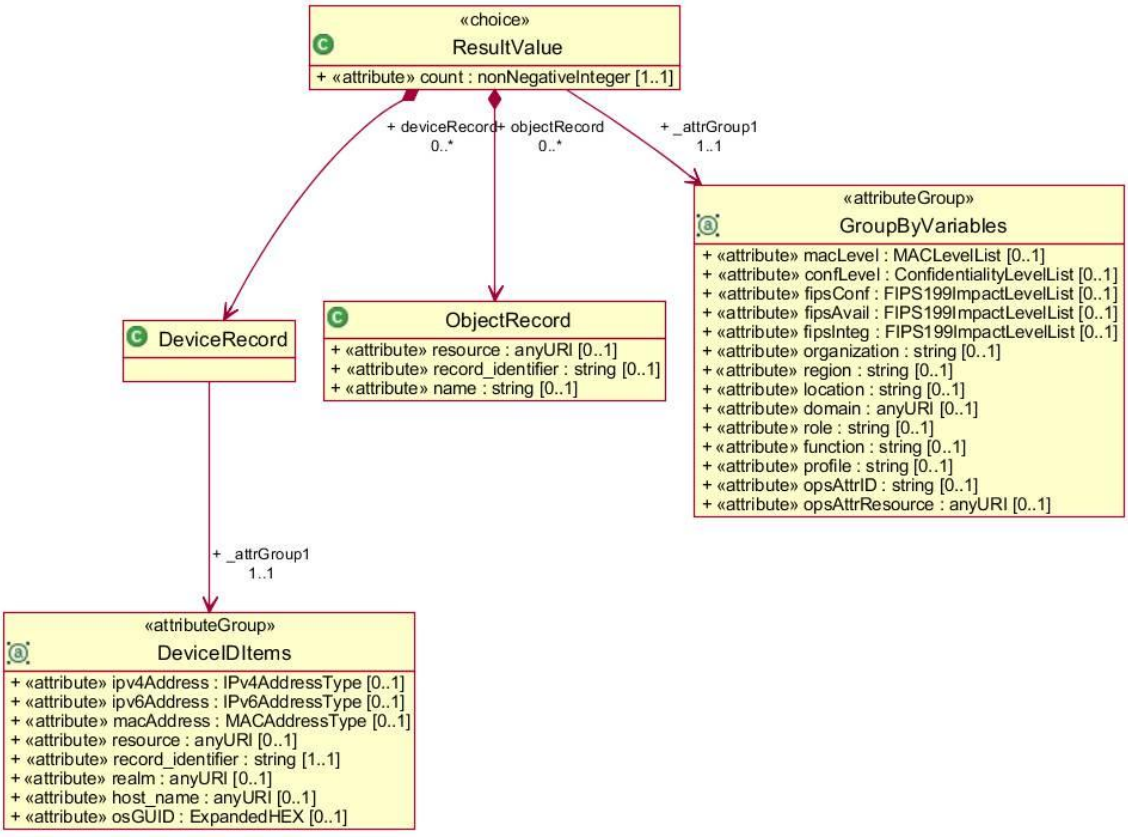


**Figure 2-3 - Result Values**

## 2.4 Group By Values

Summary Results provides the ability to group counts and lists by organization, region, domain, location, and DoD and FIPS Confidentiality, Integrity, and Availability metrics. Grouping results into these smaller segments provides the ability to construct a rough equivalent to an On-Line Analytical Processing (OLAP) cube at the receiving end to support limited drill-down capabilities as well as high-level aggregations.

In version 0.41.1, an equivalent listing for non-device objects is provided. This results list capability is expected to hold assessment result data for people, facilities, networks, organizations, and other asset types to be discovered in the future.

In version 0.41.1, the list of group-by attributes has been expanded to meet known use cases; however, if any significant amount of GroupByVariables are used, the overhead of differentiating the groups may overcome the advantage of using the ASR format. In these cases, assigning identifiers to group-by variables and associating each device or object with the appropriate group-by identifier may be a better strategy. This use case is supported by the addition of a device list element and an object list element as the final elements in the ResultsPackage base class. If this method is used, no grouping data will be supplied in the body of the ASR. Each device or object will be associated with its relevant group-by criteria in the device list or object list at the end of the ASR document.

# 3 Summary Results Creation and Usage

Initial implementation of ASR in web services has been implemented and evaluated since the release of ASR 0.41. Two primary use cases have emerged. In one case, ASR is used as an efficient transport for replicating limited data sets (e.g. benchmark results, installed software inventories, and vulnerability assessments) between sensors and centralized data stores. In this case, uses typically insert only minimum required data (e.g. no group-by variables) and additional context information is communicated using other services. In the second case, ASR is implemented for benchmark or software inventory query-response web services using SOAP. Typically, this type of web service has a user interface on the requesting side that configures a Policy Language for Assessment Result Reporting (PLARR) request that is sent to request a customized ASR response. ASR is expected to be extensively used in continuous monitoring automated data exchange in both of the previously described roles.

# 4 Usage of ASR for Reporting Known Data Types

## 4.1 Benchmark Results

The Benchmark Results construct provides information for benchmark assessments against a defined population in a defined time period.

Data about the benchmark reported on is provided, including:

- profile used
- source where the benchmark can be found
- name of the benchmark

This is followed by high level statistical data about the results population, including:

- Average Score (aveScore)

- Minimum Score (minScore)
- Maximum Score (maxScore)
- Minimum Passing Score (which can be used to divide the population into pass/fail groups) (minPassScore)
- Score Type (scoreType) as specified in the XCCDF benchmark

Benchmark compliance, at the overall benchmark level is provided, and the number of devices that passed or failed against the stated minPassScore are provided.A count of how many devices/objects met a given compliance condition is required and an optional list of device or object records can be provided if details reports are necessary.

### 4.1.1 XCCDF Benchmark Sample ASR Document

A single rule result record is provided to demonstrate usage of the benchmark rule ID and the "ident" tag, which can link to SCAP identifiers, such as CCE, CCI, or NIST 800-53 control identifiers. In ASR 0.41.1, the "system" attribute has been added so multiple benchmarks assessing against the same system can be consolidated into a common group of findings by explicitly identifying the system where the ident has meaning.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
        xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
        xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
        xmlns:cpe="http://cpe.mitre.org/language/2.0"
        xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41"
        xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="
                http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41 summary_res.xsd
                http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-core.xsd
                http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
                http://cpe.mitre.org/language/2.0 cpe-language_2.0.xsd
                http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41 scan_data.xsd ">

 <summRes:PopulationCharacteristics populationSize="500000">
  <summRes:resource>DoDIAVMReportingdB</summRes:resource>
 </summRes:PopulationCharacteristics>

 <summRes:benchmark profile="Gold">

  <summRes:benchMarkID>
   <cndc:resource>vms.dod.mil</cndc:resource>
   <cndc:record_identifier>winXPSTIGv2.53</cndc:record_identifier>
  </summRes:benchMarkID>

  <summRes:benchmarkStats aveScore="62.0" minScore="2.0" maxScore="93.0" minPassScore="62.3"
scoreType="flat"/>

<!-- Compliance lists and counts at the overall benchmark level -->

  <summRes:benchmarkComplianceItem benchmarkResultStatus="pass">
```

```
    <summRes:result count="375231">
      <summRes:deviceRecord record_identifier="asset1" ipv4Address="192.168.3.5"/>
      <summRes:deviceRecord record_identifier="asset2" ipv4Address="192.168.3.7"/>
      <summRes:deviceRecord record_identifier="asset3" ipv4Address="192.168.3.11"/>
    </summRes:result>
  </summRes:benchmarkComplianceItem>

<!-- Compliance lists and counts at the individual rule level -->

  <summRes:ruleResult ruleID="rule1">
    <summRes:ident system=”http://cce.mitre.org”>CCE-20075-7</summRes:ident>

    <summRes:ruleComplianceItem ruleResult="pass">
      <summRes:result count="3">
        <summRes:deviceRecord record_identifier="asset1" ipv4Address="192.168.3.5"/>
        <summRes:deviceRecord record_identifier="asset2" ipv4Address="192.168.3.7"/>
        <summRes:deviceRecord record_identifier="asset3" ipv4Address="192.168.3.11"/>
      </summRes:result>
    </summRes:ruleComplianceItem>

    <summRes:ruleComplianceItem ruleResult="fail">
      <summRes:result count="3">
        <summRes:deviceRecord record_identifier="asset4" ipv4Address="192.168.3.12"/>
        <summRes:deviceRecord record_identifier="asset5" ipv4Address="192.168.3.13"/>
        <summRes:deviceRecord record_identifier="asset6" ipv4Address="192.168.3.14"/>
      </summRes:result>
    </summRes:ruleComplianceItem>

  </summRes:ruleResult>

 </summRes:benchmark>
</summRes:ResultsPackage>
```

## 4.2 CPE Results

CPE results are intended to provide counts/lists of devices that contain an operating system or application that match a CPE mask, using the matching algorithm in the CPE specification. For devices with a matching OS or application, the cpeFinding attribute will be set to “true” and the platformName attribute will be set to the CPE name of the OS or application found. For devices that do not have matching CPEs or were not successfully assessed, appropriate OVAL error and exemption statuses may be used (false, unknown, error, not evaluated, not applicable).

In general, CPE results with multiple matching values for a given CPE mask should have a list of devices under each fully specified CPE. However, this behavior should be tailored by the requestor of the ASR document.

### 4.2.1 CPE Results Sample ASR Document

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
        xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
        xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
```

```
        xmlns:cpe="http://cpe.mitre.org/language/2.0"
        xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41"
        xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="
        http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41 summary_res.xsd
        http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-core.xsd
        http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
        http://cpe.mitre.org/language/2.0 cpe-language_2.0.xsd
        http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41 scan_data.xsd ">

  <summRes:PopulationCharacteristics populationSize="250">
    <summRes:resource>http://cpeDb.dod.mil</summRes:resource>
  </summRes:PopulationCharacteristics>

  <summRes:cpe>

<!-- First line "platform" defines the CPE mask that is the basis of the CPE results report -->

    <summRes:platform>cpe:/a:adobe:flash</summRes:platform>

<!-- Each CPE Result item record gives a count and may provide a list of products that match the
        "platform" defined above.  Also count/list of devices that don't have any products
        that match the platform mask. -->

    <summRes:cpeResultItem cpeFinding="true" platformName="cpe:/a:adobe:flash:1.02">
      <summRes:result count="50"/>
    </summRes:cpeResultItem>

    <summRes:cpeResultItem cpeFinding="true" platformName="cpe:/a:adobe:flash:1.05">
      <summRes:result count="50"/>
    </summRes:cpeResultItem>

    <summRes:cpeResultItem cpeFinding="true" platformName="cpe:/a:adobe:flash:1.20">
      <summRes:result count="100"/>
    </summRes:cpeResultItem>

    <summRes:cpeResultItem cpeFinding="false" platformName="cpe:/a:adobe:flash">
      <summRes:result count="50"/>
    </summRes:cpeResultItem>

  </summRes:cpe>
</summRes:ResultsPackage>
```

### 4.3 CPE Complex Results

CPE Complex results are intended to provide counts/lists of devices that contain a uniquely specified combination of operating systems or applications that match a CPE Platform definition as defined in the CPE Language specification. For devices with matching OSs and applications, the cpeFinding attribute will be set to “true” and the platform element will repeat the platform definition that triggered the ASR report.

In general, only true values are supplied for a CPE Complex report along with a single listing is supplied of all devices that contain any combination of CPEs that match the platform definition. More advanced cases may be supported, but the behaviors for how

an ASR should be constructed in response to a platform match request should be defined between the requester and report generator and is out of scope for this document.

### 4.3.1 CPE Complex Results Sample ASR Document

```
<?xml version="1.0" encoding="UTF-8" ?>
<summRes:CPEComplexResults xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
xmlns:cpe="http://cpe.mitre.org/language/2.0"
xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41"
xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
      http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41 summary_res.xsd
      http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-core.xsd
      http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
      http://cpe.mitre.org/language/2.0 cpe-language_2.2.xsd
      http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41 scan_data.xsd"
      singleListing="true">
       <summRes:platform negate="false" operator="AND">
          <cpe:logical-test negate="false" operator="OR">
            <cpe:fact-ref name="cpe:/o:microsoft:vista" />
            <cpe:fact-ref name="cpe:/o:microsoft:windows_xp" />
            <cpe:fact-ref name="cpe:/o:microsoft:windows_7" />
          </cpe:logical-test>
         <cpe:fact-ref name="cpe:/a:adobe:flash" />
           </summRes:platform>
       <summRes:cpeResultItem cpeFinding="true">
       <summRes:result count="5">
            <summRes:deviceRecord record_identifier="device1" />
            <summRes:deviceRecord record_identifier="device2" />
            <summRes:deviceRecord record_identifier="device3" />
            <summRes:deviceRecord record_identifier="device4" />
            <summRes:deviceRecord record_identifier="device5" />
        </summRes:result>
       </summRes:cpeResultItem>
</summRes:CPEComplexResults>
```

## 4.4 CVE Sample ASR Document

CVE results documents only allow lists for each possible result from the OVAL results enumeration list (true, false, unknown, error, not evaluated, not applicable). Otherwise, they function much like CPE results documents.

### 4.4.1 CVE Sample ASR Document

CVE results documents only allow lists for each possible result from the OVAL results enumeration list (true, false, unknown, error, not evaluated, not applicable). Otherwise, they function much like CPE results documents.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
          xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
          xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
          xmlns:cpe="http://cpe.mitre.org/language/2.0"
```

```
        xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41"
        xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="
        http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41 summary_res.xsd
        http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-core.xsd
        http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
        http://cpe.mitre.org/language/2.0 cpe-language_2.0.xsd
        http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41 scan_data.xsd ">

<summRes:PopulationCharacteristics populationSize="250">
<summRes:resource>DoDVulnDb.dod.mil</summRes:resource>
</summRes:PopulationCharacteristics>

<summRes:cve cveID="CVE-2009-0001">

   <summRes:cveResultItem cveFinding="true">
     <summRes:result count="50"/>
   </summRes:cveResultItem>

   <summRes:cveResultItem cveFinding="false">
     <summRes:result count="170"/>
   </summRes:cveResultItem>

   <summRes:cveResultItem cveFinding="not applicable">
     <summRes:result count="30"/>
   </summRes:cveResultItem>

  </summRes:cve>

</summRes:ResultsPackage>
```

## 4.5 System/Ident Results

System/Ident results are a new construct in version 0.41.1, specifically built to support unanticipated data requirements. Initially the System/Ident construct was intended to enable requesting multiple CCE values across multiple benchmarks. However, on evaluation, many other data sharing requirements, particularly non-SCAP based requirements, can be addressed by using the System/Ident construct. Within the context of this document, "system" will be synonymous with "measurement system" and should not be confused with IT systems or other types of systems.

### 4.5.1 The "System" Concept

In order for the System/Ident ASR to function, a system must be defined with well understood values for unique identifiers generated within that system. Existing SCAP systems, such as XCCDF Benchmark, CCE, CPE, CVE, and CPE Platform are well understood and already supported in ASR 0.41. However, all of these systems can be easily translated into the System/Ident branch of ASR and other, new, systems can be introduced by specifying a unique system name and what rules are used within the system for associating meaning with results mapped to unique identifiers.

Three types of results are recognized within the systems supported in the System/Ident branch. Inventory results associate counts and lists of objects with specific values that are explicitly discovered. Boolean results associate absence or presence of a set of one or more logically-related conditions based on OVAL results, primarily true or false. Compliance results return an assessment of whether an assessed condition complies with a policy using XCCDF results, primarily pass or fail. A type, titled "ComplexInventoryFinding" has been inserted into the schema for potential future uses, but is not envisioned for use in the near future. Its purpose is to hold inventory results that require multiple elements and attributes to describe (e.g. the list of all public key values in the trusted Certificate Authority key store).

### 4.5.2 Idents

Within the System/Ident construct, there are two types of "idents." Simple idents can be expressed as a single line of text within the constraints of an XML attribute. Complex idents require multiple elements and/or attributes to fully express a unique ident value. An example of a simple ident would be a CPE or CCE ID. A complex ident example would be a CPE Language platform definition. Idents are expected to be unique within a system, so any object that claims a relationship to an ident within a system will be considered to have the same inventory, Boolean, or compliance relationship as any other object claiming the same ident and value and can be added to the same count or list in an ASR document, regardless of whether they were collected in the same assessment or benchmark. For use in continuous monitoring systems, where a risk score is supplied for not reporting, the value of "not_reported" has been added to both the Boolean and compliance result types to convey information about devices or other objects that should have returned results, but did not.

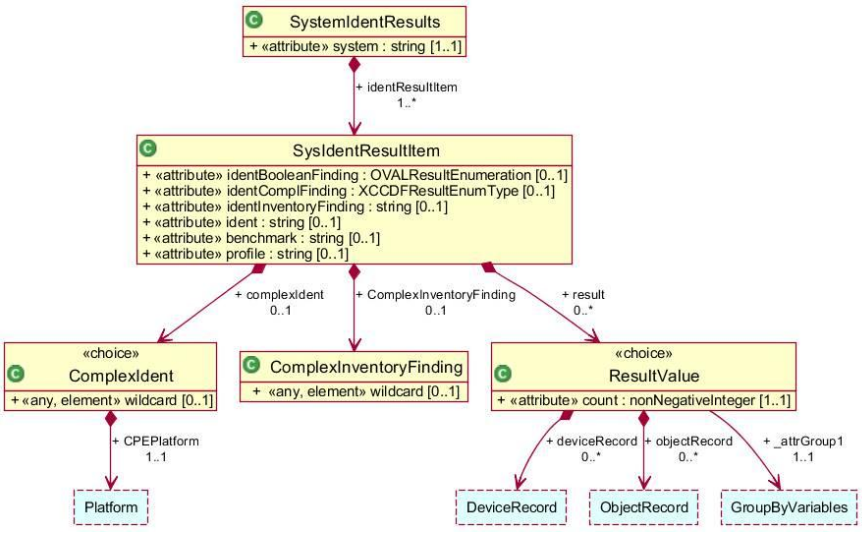


**Figure 4-1 System/Ident Results UML Diagram**

In general, it is anticipated that any data that can be shared using an ASR System/Ident report with simple idents can be converted into an XCCDF results file if necessary. In general, the conversion can be completed by converting the Boolean or inventory value into a single-value compliance expression and only returning "pass" values. E.g. if the system for inventory was "birthday" and an ASR was constructed with inventory values

where birthday=2/2/2002, birthday=3/1/2010, the same data could be converted into XCCDF benchmark formats by converting the idents into birthday_eq_2-2-2002=pass and birthday_eq_3-1-2010=pass.

### 4.5.3 CPE Example

To reduce complexity in future versions of ASR, CPE expressions may be eliminated and be replaced using the system/ident model. Again, it is critical that all users of the system/ident ASR scheme share a common understanding of how a given system is to be used and what a specific ident within the system is conveying.

In the following "simple" CPE sample, the request was submitted to return all device IDs that match any pattern of the CPE "**cpe:/o:microsoft:win_xp".** The resulting ASR shows that 10 devices were found that contained software matching the CPE mask. Of the 75000 devices assessed, 5 had been assessed as having the "**cpe:/o:microsoft:win_xp::sp2"** software installed and 5 contained the CPE "**cpe:/o:microsoft:win_xp::sp3".** It should also be noted that the CPE system returns, by default, a listing of all devices that contain any matching software against the request mask and they are listed in separate groups under the fully specified CPE they contain.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <summRes:ResultsPackage xmlns:cia-
    enum="http://scap.nist.gov/schema/cia_enums/0.1"
    xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-
    core/0.41"
    xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan
    _data/0.41"
    xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/sum
    mary_res/0.41" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://metadata.dod.mil/mdr/ns/netops/net_defense/su
    mmary_res/0.41 summary_res.xsd
    http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-
    core.xsd http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
    http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
    scan_data.xsd">
- <summRes:PopulationCharacteristics populationSize="120000"
    populationAppliesTo="80000" populationAssessed="75000">
  <summRes:resource>http://armyT0CMDB.army.smil.mil</summRes:resource>
- <summRes:scanData>
- <scan_data:scanDataID>
  <cndc:resource>http://armyT0CMDB.army.smil.mil</cndc:resource>
  <cndc:record_identifier>2010-12-17-1300</cndc:record_identifier>
    </scan_data:scanDataID>
  <scan_data:start>2010-12-11T12:00:00</scan_data:start>
  <scan_data:end>2010-12-16T12:00:00</scan_data:end>
    </summRes:scanData>
    </summRes:PopulationCharacteristics>
- <summRes:systemIdent system="http://cpe.mitre.org">
- <summRes:identResultItem ident="cpe:/o:microsoft:win_xp"
    identInventoryFinding="cpe:/o:microsoft:win_xp::sp2">
- <summRes:result count="5">
```

```
      <summRes:deviceRecord record_identifier="1" />
      <summRes:deviceRecord record_identifier="2" />
      <summRes:deviceRecord record_identifier="3" />
      <summRes:deviceRecord record_identifier="4" />
      <summRes:deviceRecord record_identifier="5" />
        </summRes:result>
        </summRes:identResultItem>
    - <summRes:identResultItem ident="cpe:/o:microsoft:win_xp"
         identInventoryFinding="cpe:/o:microsoft:win_xp::sp3">
    - <summRes:result count="5">
      <summRes:deviceRecord record_identifier="6" />
      <summRes:deviceRecord record_identifier="7" />
      <summRes:deviceRecord record_identifier="8" />
      <summRes:deviceRecord record_identifier="9" />
      <summRes:deviceRecord record_identifier="10" />
        </summRes:result>
        </summRes:identResultItem>
        </summRes:systemIdent>
        </summRes:ResultsPackage>
```

In the following "complex" CPE sample, the request was submitted to return all device IDs that match any pattern that matches the platform described as follows:

```
    - <summRes:platform negate="true" operator="AND">
    - <cpe:logical-test negate="false" operator="AND">
      <cpe:fact-ref name="cpe:/o:microsoft:vista" />
        </cpe:logical-test>
      <cpe:fact-ref name="cpe:/a:adobe:flash" />
        </summRes:platform>
```

The resulting ASR shows that 8 devices were found that contained software matching the CPE platform definition. It should also be noted that the CPE-complex system returns, by default, a listing of all devices that contain the platform described and they are listed in a single listing unless group-by criteria are supplied.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
      xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
      xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
      xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data
/0.41"
      xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res
/0.41"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="
            http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41
summary_res.xsd
            http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-
core.xsd
            http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
```

```
            http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
scan_data.xsd ">


  <summRes:PopulationCharacteristics populationSize="120000"
populationAppliesTo="80000" populationAssessed="75000" >
    <summRes:resource>http://armyT0CMDB.army.smil.mil</summRes:resource>
    <summRes:scanData>
      <scan_data:scanDataID>
        <cndc:resource>http://armyT0CMDB.army.smil.mil</cndc:resource>
        <cndc:record_identifier>2010-12-17-1300</cndc:record_identifier>
      </scan_data:scanDataID>
      <scan_data:start>2010-12-11T12:00:00</scan_data:start>
      <scan_data:end>2010-12-16T12:00:00</scan_data:end>
    </summRes:scanData>
  </summRes:PopulationCharacteristics>

  <summRes:systemIdent system="http://cpe-complex.mitre.org">
  <summRes:identResultItem identBooleanFinding="true">
    <summRes:complexIdent>
      <summRes:CPEPlatform id="">
        <summRes:logical-test negate="false" operator="AND">
          <summRes:logical-test negate="false" operator="OR">
            <summRes:fact-ref name="cpe:/o:microsoft:vista"/>
            <summRes:fact-ref name="cpe:/o:microsoft:windows_xp"/>
            <summRes:fact-ref name="cpe:/o:microsoft:windows_7"/>
          </summRes:logical-test>
          <summRes:fact-ref name="cpe:/a:adobe:flash"/>
        </summRes:logical-test>
      </summRes:CPEPlatform>
    </summRes:complexIdent>
    <summRes:ComplexInventoryFinding/>
    <summRes:result count="8">
      <summRes:deviceRecord record_identifier="1"/>
      <summRes:deviceRecord record_identifier="2"/>
      <summRes:deviceRecord record_identifier="3"/>
      <summRes:deviceRecord record_identifier="4"/>
      <summRes:deviceRecord record_identifier="5"/>
      <summRes:deviceRecord record_identifier="6"/>
      <summRes:deviceRecord record_identifier="7"/>
      <summRes:deviceRecord record_identifier="8"/>
    </summRes:result>
  </summRes:identResultItem>
  </summRes:systemIdent>
</summRes:ResultsPackage>
```

### 4.5.4 CCE Example

In the following CCE sample, the request was submitted to return compliance results for the CCE ident "cce-1098-4". The resulting ASR shows that 15 devices were found that contained software that should have returned compliance results for cce-1098-4. Of those, 5 devices passed, 5 failed, and 5 did not report results for cce-1098-4.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
```

```
      xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
      xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
      xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data
/0.41"
      xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res
/0.41"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="
            http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41
summary_res.xsd
            http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-
core.xsd
            http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
            http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
scan_data.xsd ">


  <summRes:PopulationCharacteristics populationSize="20" populationAppliesTo="15"
populationAssessed="10" >
    <summRes:resource>http://armyT0CMDB.army.smil.mil</summRes:resource>
    <summRes:scanData>
      <scan_data:scanDataID>
        <cndc:resource>http://armyT0CMDB.army.smil.mil</cndc:resource>
        <cndc:record_identifier>2010-12-17-1300</cndc:record_identifier>
      </scan_data:scanDataID>
      <scan_data:start>2010-12-11T12:00:00</scan_data:start>
      <scan_data:end>2010-12-16T12:00:00</scan_data:end>
    </summRes:scanData>
  </summRes:PopulationCharacteristics>

  <summRes:systemIdent system="http://cce.mitre.org">

    <summRes:identResultItem ident="cce-1098-4" identComplFinding="pass"
benchmark="winxp_fdcc" profile="max security">
      <summRes:result count="5">
        <summRes:deviceRecord record_identifier="1"/>
        <summRes:deviceRecord record_identifier="2"/>
        <summRes:deviceRecord record_identifier="3"/>
        <summRes:deviceRecord record_identifier="4"/>
        <summRes:deviceRecord record_identifier="5"/>
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="cce-1098-4" identComplFinding="fail"
benchmark="winxp_fdcc" profile="max security">
      <summRes:result count="5">
        <summRes:deviceRecord record_identifier="6"/>
        <summRes:deviceRecord record_identifier="7"/>
        <summRes:deviceRecord record_identifier="8"/>
        <summRes:deviceRecord record_identifier="9"/>
        <summRes:deviceRecord record_identifier="10"/>
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="cce-1098-4" identComplFinding="not_reported"
benchmark="winxp_fdcc" profile="max security">
      <summRes:result count="5">
```

```
        <summRes:deviceRecord record_identifier="11"/>
        <summRes:deviceRecord record_identifier="12"/>
        <summRes:deviceRecord record_identifier="13"/>
        <summRes:deviceRecord record_identifier="14"/>
        <summRes:deviceRecord record_identifier="15"/>
      </summRes:result>
    </summRes:identResultItem>

  </summRes:systemIdent>

</summRes:ResultsPackage>
```

### 4.5.5 AV-DOT-DAT Example

In the following AV-DOT-DAT example, a custom system was created where the request was submitted to return compliance results for the dates of common antivirus signature files or "dat" files. Within this system, identifiers contain the date of the dat files as part of the ident, and are returned using compliance results; however, in this system, only "pass" and "not reported" are produced. The resulting ASR shows that 12 total devices were in the source population, 12 devices should have returned av dat dates, but only 8 devices did. Of those, 4 passed for the date 2010-12-16 and 4 passed for the date 2010-12-17. Four did not report dat dates, but should have.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
      xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
      xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
      xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data
/0.41"
      xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res
/0.41"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="
            http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41
summary_res.xsd
            http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-
core.xsd
            http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
            http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
scan_data.xsd ">


  <summRes:PopulationCharacteristics populationSize="12" populationAppliesTo="12"
populationAssessed="8" >
    <summRes:resource>http://armyT0CMDB.army.smil.mil</summRes:resource>
    <summRes:scanData>
      <scan_data:scanDataID>
        <cndc:resource>http://armyT0CMDB.army.smil.mil</cndc:resource>
        <cndc:record_identifier>2010-12-17-1300</cndc:record_identifier>
      </scan_data:scanDataID>
      <scan_data:start>2010-12-11T12:00:00</scan_data:start>
      <scan_data:end>2010-12-16T12:00:00</scan_data:end>
    </summRes:scanData>
  </summRes:PopulationCharacteristics>
```

```
  <summRes:systemIdent system="http://av-dat-date.dod.mil">

    <summRes:identResultItem ident="av-dat-2010-12-16" identComplFinding="pass">
      <summRes:result count="4">
        <summRes:deviceRecord record_identifier="AABCC-EE-FFF-AAB" />
        <summRes:deviceRecord record_identifier="AABCC-EE-FFF-AAC" />
        <summRes:deviceRecord record_identifier="AABCC-EE-FFF-AAD" />
        <summRes:deviceRecord record_identifier="AABCC-EE-FFF-AAF" />
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="av-dat-2010-12-17" identComplFinding="pass">
      <summRes:result count="4">
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAG" />
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAH" />
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAI" />
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAJ" />
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="av-dat-not_reported"
identComplFinding="not_reported">
      <summRes:result count="4">
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAK" />
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAL" />
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAM" />
        <summRes:deviceRecord record_identifier="BABCC-EE-FFF-AAN" />
      </summRes:result>
    </summRes:identResultItem>


  </summRes:systemIdent>

</summRes:ResultsPackage>
```

### 4.5.6 Patch Example

In the following patch example, a custom system was created where the request was submitted to return Boolean results for the presence or absence of a patch on devices running relevant Microsoft operating systems or applications. Within this system, identifiers consist of the Microsoft Knowledge Base numbers for patches and updates associated with Boolean results indicating whether a given patch is installed. The resulting ASR shows that 50 total devices were in the source population, 15 devices should have returned patch installation status, but only 10 devices did. Of those, 5 resolved to "true" for the patch with the ident "kb1234567", five resolved to "false" and five did not report results for the patch, but should have.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
      xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
      xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
      xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data
/0.41"
```

```
      xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res
/0.41"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="
            http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41
summary_res.xsd
            http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-
core.xsd
            http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
            http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
scan_data.xsd ">


  <summRes:PopulationCharacteristics populationSize="50" populationAppliesTo="15"
populationAssessed="10">
    <summRes:resource>http://armyT0CMDB.army.smil.mil</summRes:resource>
    <summRes:scanData>
      <scan_data:scanDataID>
        <cndc:resource>http://armyT0CMDB.army.smil.mil</cndc:resource>
        <cndc:record_identifier>2010-12-17-1300</cndc:record_identifier>
      </scan_data:scanDataID>
      <scan_data:start>2010-12-11T12:00:00</scan_data:start>
      <scan_data:end>2010-12-16T12:00:00</scan_data:end>
    </summRes:scanData>
  </summRes:PopulationCharacteristics>

  <summRes:systemIdent system="http://patch.microsoft.com">

    <summRes:identResultItem ident="kb1234567" identBooleanFinding="true">
      <summRes:result count="5">
        <summRes:deviceRecord record_identifier="1"/>
        <summRes:deviceRecord record_identifier="2"/>
        <summRes:deviceRecord record_identifier="3"/>
        <summRes:deviceRecord record_identifier="4"/>
        <summRes:deviceRecord record_identifier="5"/>
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="kb1234567" identBooleanFinding="false">
      <summRes:result count="5">
        <summRes:deviceRecord record_identifier="6"/>
        <summRes:deviceRecord record_identifier="7"/>
        <summRes:deviceRecord record_identifier="8"/>
        <summRes:deviceRecord record_identifier="9"/>
        <summRes:deviceRecord record_identifier="10"/>
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="kb1234567" identBooleanFinding="not_reported">
      <summRes:result count="5">
        <summRes:deviceRecord record_identifier="11"/>
        <summRes:deviceRecord record_identifier="12"/>
        <summRes:deviceRecord record_identifier="13"/>
        <summRes:deviceRecord record_identifier="14"/>
        <summRes:deviceRecord record_identifier="15"/>
      </summRes:result>
    </summRes:identResultItem>
```

```
  </summRes:systemIdent>

</summRes:ResultsPackage>
```

### 4.5.7 Network Security Event Example

In the following patch example, a custom system was created where the publishing endpoints construct a summary of antivirus (AV), antimalware (AM), and host-based intrusion prevention system (HIPS) alerts every five minutes and publish an inventory System/Ident ASR report with the identifiers being the source of the event data and the inventory finding being the ID of the event within the vendor alert identification system. The sample ASR shows that 120000 total devices were in the source population. Across that population, 3 Symantec AV alerts recorded with counts of how many devices triggered those alerts. For McAfee Antivirus and HIPS alerts, two HIPS alerts were triggered, and two AV alerts were triggered with respective counts of each.

```
<?xml version="1.0" encoding="UTF-8"?>
<summRes:ResultsPackage
      xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
      xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
      xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data
/0.41"
      xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res
/0.41"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="
            http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41
summary_res.xsd
            http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-
core.xsd
            http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
            http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
scan_data.xsd ">


  <summRes:PopulationCharacteristics populationSize="120000">
    <summRes:resource>http://armyT0SIM.army.smil.mil</summRes:resource>
    <summRes:scanData>
      <scan_data:scanDataID>
        <cndc:resource>http://armyT0SIM.army.smil.mil</cndc:resource>
        <cndc:record_identifier>2010-12-11-1200</cndc:record_identifier>
      </scan_data:scanDataID>
      <scan_data:start>2010-12-11T12:00:00</scan_data:start>
      <scan_data:end>2010-12-11T12:05:00</scan_data:end>
    </summRes:scanData>
  </summRes:PopulationCharacteristics>

  <summRes:systemIdent system="http://host-event-summary.dod.mil">

    <summRes:identResultItem ident="symantec_av" identInventoryFinding="12598">
      <summRes:result count="4">
      </summRes:result>
    </summRes:identResultItem>
```

```
    <summRes:identResultItem ident="symantec_av" identInventoryFinding="67386">
      <summRes:result count="200">
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="symantec_av" identInventoryFinding="66842">
      <summRes:result count="52">
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="mcaffee_hips" identInventoryFinding="mac529">
      <summRes:result count="31">
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="mcaffee_hips" identInventoryFinding="mac324">
      <summRes:result count="7">
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="mcaffee_av" identInventoryFinding="mac666">
      <summRes:result count="27">
      </summRes:result>
    </summRes:identResultItem>

    <summRes:identResultItem ident="mcaffee_av" identInventoryFinding="mac852">
      <summRes:result count="39">
      </summRes:result>
    </summRes:identResultItem>

  </summRes:systemIdent>

</summRes:ResultsPackage>
```