Asset Identification
Adam Montville, amontville@tripwire.com


Abstract:

Some standards, such as the Incident Object Description Exchange Format, provide classes used to reference external entities (such as enumeration identifiers). At the time of standardization, however, needed references may not be known, and the method of external entity identification is often left unstructured. This document describes, using IODEF as an example, a method to provide structure after the fact.
This Asset Identification specification describes a framework for how asset management processes and other specifications may identify assets using some set of information known or generated about the asset.

This specification was developed to support the immediate needs of the security automation community.

For the purposes of this specification, an asset is considered to be anything that has value to an organization.

It is expected that other standards, data formats, tools, processes, and organizations will reference this specification to describe how to represent asset identification information.
UC1 System State Assessment

Define Target System

Select Acceptable State Policy

Retrieve Data Collection Instructions

Collect Actual State Values

Compare Actual State Values

Asset Identification

<supports>

<has function>

<has function>

<has function>

<has function>
UC2
Enforcement of Accepted State

System State Assessment (single)

UC1
System State Assessment

Evaluate Compliance Level

Asset Identification

<has function>

<uses>

<supports>
UC3 Security Control Verification and Monitoring

UC1 System State Assessment

System State Assessment (sets)

Define Assessment Trigger

Define Report/Alert Criteria

Enable Continuous Assessment

Asset Identification

<supports>

<supports>

<supports>

<has function>

<has function>

<has function>
Does the Community find this work relevant?

Are there willing Authors/Editors?
Backup Slides / Technical Details
Sample Correlation Workflow
synthetic-id
locations
extended-information
timestamp

Asset

latitude:number
longitude:number
elevation:number
radius:number

LocationPoint

details:xal:AddressDetails

LocationRegion

region-name:normalizedString

Location

0-n
1
1- *

Locations

location

1
1- *

Assets

relationships
asset

1
1- *

Relationships

relationship

0-1
1
1- *

Relationship

ref:NCName
type:QName
scope:token
subject:NCName

AssetRelated

asset-ref:NCName
relationships
asset

1
1- *

1
1- *

1- *

1

1

1

<table>
<thead>
<tr>
<th>Relation</th>
<th>Domain</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>hasTerminationDevice</td>
<td>ai:circuit</td>
<td>ai:computing-device</td>
</tr>
<tr>
<td>hasServiceProvider</td>
<td>ai:circuit</td>
<td>ai:organization</td>
</tr>
<tr>
<td>hasNetworkTerminationDevice</td>
<td>ai:circuit</td>
<td>ai:network</td>
</tr>
<tr>
<td>servedBy</td>
<td>ai:database, ai:website</td>
<td>ai:service</td>
</tr>
<tr>
<td>hasServiceProvider</td>
<td>ai:service</td>
<td>ai:software</td>
</tr>
<tr>
<td>installedOnDevice</td>
<td>ai:software</td>
<td>ai:computing-device</td>
</tr>
<tr>
<td>connectedToNetwork</td>
<td>ai:system</td>
<td>ai:network</td>
</tr>
<tr>
<td>isOwnerOf</td>
<td>ai:person, ai:organization</td>
<td>ai:it-asset</td>
</tr>
<tr>
<td>isAdministratorOf</td>
<td>ai:person</td>
<td>ai:computing-device, ai:system</td>
</tr>
<tr>
<td>partOf</td>
<td>ai:person</td>
<td>ai:organization</td>
</tr>
<tr>
<td>connectedTo</td>
<td>ai:computing-device, ai:system</td>
<td>ai:system</td>
</tr>
</tbody>
</table>
Relation:

hasTerminationDevice
hasServiceProvider
hasNetworkTerminationDevice
servedBy
hasServiceProvider
installedOnDevice
connectedToNetwork
isOwnerOf
isAdministratorOf
partOf
connectedTo

description:
The circuit is terminated by the device.
The circuit is owner/operated by the organization.
The circuit ends at the network.
The database or website is served up by the service.
The service is provided by the software.
The software is installed on the computing device.
The system is connected to the network.
The person or organization owns the IT asset.
The person is the system administrator of the computing device or system.
The person is in some way a part of the organization.
The computing device or system is connected to the system.
Possible Improvements

+ Consider using Asset Identification beyond Identification

+ Specify use of IANA registry for asset type addition

+ Specify use of IANA registry for asset type extension

+ Specify use of IANA registry for relationship addition

+ Augment for internationalization