Asset and network modeling in HP ArcSight ESM and Express

Till Jäger, CISSP, CEH
EMEA ArcSight Architect, HP ESP
Agenda

Overview
Walkthrough of asset modeling in ArcSight ESM
More inside info about the Asset Model
Tips and tricks
Why is asset modeling important

- To get the Threat Level Formula (TLF) working more precisely (if you don’t remember it, check next slide)
- To add context to an asset, e.g., it’s a mail server or it’s identified as a SOX or Basel II relevant asset
- To get Geo Views working with private IP ranges too
- To reflect network of the organization in views and analysis and alerting
- To add customer feature for MSSPs and global organizations
What is the Threat Level Formula?

Each event is evaluated against the Threat Level Formula to determine its relative importance, or priority, to the network.

TLF calculates the priority of an event based on agent severity adjusted by four factors.

Model Confidence, can take following values:

- 0 Target is not modeled at all, target asset id is not populated
- 4 Target asset id is present, but it hasn’t been scanned for open ports or vulnerabilities
- 8 Target asset is either scanned for open ports or vulnerabilities, but not for both
- 10 Target asset is scanned for both open ports and vulnerabilities
What is the Threat Level Formula?

Relevance, which will be calculated on the following information:
Target asset has a vulnerability that is exploited by the event
Target port is open on the target asset

Severity
Takes into account whether the target has already been compromised and also whether or not prior activity from this source has been observed. All this is done using the active lists whose contents are updated by rules

Asset criticality
Measures how important the target asset is in the context of the organization. This value is a user input and influences the outcome of the TLF
Since ESM 5 – asset aging

ESM v5.0 introduced two ways in which the age of a scanned asset is taken into consideration. The age of an asset is defined as the number of days since it was last modified.

Assets can be disabled or deleted. This and assets to exclude can be set in server.properties. The ModelConfidence element will be factored by the age of an asset. It is extended to include an optional attribute, AmortizeScan.

<table>
<thead>
<tr>
<th>Asset Age (in days)</th>
<th>AmortizeScan Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>60</td>
<td>2</td>
</tr>
<tr>
<td>120</td>
<td>0</td>
</tr>
<tr>
<td>240</td>
<td>0</td>
</tr>
</tbody>
</table>
What is asset? Zone? Network? Customer?

Assets represent individual nodes on the network, such as servers, routers, and laptops.

Asset ranges represent a set of network nodes addressable as a contiguous block of IP addresses.

Zones represent portions of the network itself and are also characterized by a contiguous block of addresses.

Networks are helpful when disambiguating two private address spaces.

Customers describe the internal or external cost centers or separate business units associated with networks, if applicable to your business environment.
Event in ArcSight ESM without asset modeling

This is what an event looks like when the ArcSight ESM Asset Model is not configured

- No Customer
- No Model Confidence
- No Asset Criticality
- Priority 4
- Attacker Zone default
- Target Zone default
- No Geo Information at all
Walkthrough
How ArcSight ESM enriches events

Asset model in ArcSight ESM

In order to get the most value out of ArcSight ESM the following needs to be modeled

• Assets
• Zones
• Networks
• Customers
• Locations

These are used to increase the quality of alerts raised by ArcSight ESM

The following slides will lead you through all the steps!
How ArcSight ESM enriches events

ArcSight ESM uses Connectors to collect information from data sources
There are Connectors for more than 300 different sources

After collection, the first steps are

- **Normalization**: Events are parsed and mapped into the ArcSight ESM event schema
- **Categorization**: Classification of events based on criteria such as object type, behavior, outcome, technique, device group, and significance
How ArcSight ESM enriches events

Step 1: Add customer

The next step is to add a customer to the event

Customers describe the internal or external cost centers or separate business units associated with networks, if applicable to your business environment

This means a customer needs to be created in ArcSight ESM
How ArcSight ESM enriches events

Step 1: Adding a customer

- Go in the navigator to Customers and add a customer
- You may add additional information like address, but that won’t be used during the event enrichment process
How ArcSight ESM enriches events

Step 2: Add network

Networks are helpful when disambiguating two private address spaces

- This means a network needs to be created in ArcSight ESM
- One customer can have several networks
- Network information won’t be shown in the event
- It’s the glue between customer and zones
How ArcSight ESM enriches events

Step 2: Adding a network

- Go in the navigator to Assets and click on the Network tab
- Add a network
- Choose a customer (the one you’ve created)
How ArcSight ESM enriches events

Step 3: Add zone

- Zones represent portions of the network itself and are also characterized by a contiguous block of addresses
- The zone information will be shown in the event
- One network can have many zones
How ArcSight ESM enriches events

Step 3: Adding a zone

- Go in the navigator to Assets and click on the Zone tab
- Add a zone
- Choose a network
How ArcSight ESM enriches events

Step 4: Create asset and assign it to zone

- In the Navigator go to Assets and create a new asset
- Assets represent individual nodes on the network, such as servers, routers and laptops
- Asset ranges represent a set of network nodes addressable as a contiguous block of IP addresses
- Choose a name, IP address, zone

Do I have to do it manually?

No... In the Asset tree just right click on the asset and do an AutoZone. You have to choose a network in case there may be overlapping IP ranges.
How ArcSight ESM enriches events

Step 4: Adding an asset

- Click on Categories
- Add Criticality
How ArcSight ESM enriches events

And?

Still the same!
No asset and Zone information!

What went wrong??

The connector doesn’t know about our configuration!!
How ArcSight ESM enriches events

Step 5: Add network and customer to the connector
How ArcSight ESM enriches events

And?

That’s it! Easy, isn’t it?

Customer ArcSight UC
Model Confidence 4
Asset Criticality 10
Priority 5
Attacker Zone populated
Target Zone populated

But:

No Geo Information
Model Confidence just 4?
How Arcsight ESM enriches events

How does this fit together?

Connector has many potentially overlapping but ordered Networks which have non-overlapping Zones representing an address range and which contain Asset ranges and Assets that fall into the address range of the zone

While the Customer always helps to distinguish between units
How ArcSight ESM enriches events

Step 6: Add more asset information

- In order to populate the Threat in an event, Vulnerabilities and Open Ports are required
- Yes, a Vulnerability Assessment Solution should be used for that!
How ArcSight ESM enriches events

Step 6: Asset information after scan
How ArcSight ESM enriches events

Event after scan

After the scan the quality of the information in the threat section is much higher

Model Confidence 10
Relevance 10
Asset Criticality 10
Priority 5

But

Why is priority still 5?
No geo information!

Because agent severity is low!
How ArcSight ESM enriches events

Step 7: Add geo information

- ArcSight ESM will automagically populate Geo Information for public networks
- For private networks you need to configure the Location
How ArcSight ESM enriches events

Step 7: Create location

- Create a location and provide the necessary parameter
- Google Earth is your friend!
- Assign it to the Network Zone
How ArcSight ESM enriches events

Event with geo information

At the end all information is present

How does it help you?

- Priority better shows what an event really means
- With Zone and Customer information filters can be created more easily
- Links in the Event Inspector go down to e.g. Asset Information
- Geo View also includes your private networks
How ArcSight ESM enriches events

Geo view
More insights about the asset model
Connectors

One or more networks can be assigned to a Connector
  • Order matters—the higher order network will be used to match an IP address first
  • Addresses can fall through to a more generic network

All zones by default belong to the hard-coded Local network, which is associated with all the connectors

The hard-coded Global network is the most generic network
  • It contains all the system zones
  • Each connector will always consult the mappings of the global network if everything else fails

Please do not edit these hard-coded networks
Quiz: Which network catches the IP?

192.168.178.31 Zone A

192.178.168.31 Catch-All Zone

10.1.10.42 Zone D
Zone population on Connectors

Connectors automatically pick up address-based zone mappings
  • Based on the network model
  • Just add networks to the list for the connector

Changes in the model are periodically synced to the connectors
  • Change in address range of a zone
  • Change in network membership of a zone
  • Change in association of network with a customer
## Asset categories for assets

### New York office

<table>
<thead>
<tr>
<th>Asset group</th>
<th>Asset range</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.242.100</td>
<td></td>
</tr>
</tbody>
</table>

### Asset categories

- Address spaces: Protected
- Business role: Computer infrastructure
- Compliance requirement: Sarbanes-Oxley
- Operating system: Windows Server 2003
- Application type: Email Exchange
- Application vendor: Microsoft Exchange
- Business role: Email Service
- Criticality: High
Categories for zones

Zones, zone groups and networks can be categorized

- Zones inherit categories from its ancestor zone groups
- Zone groups inherit categories from network
- So, zones also inherit categories from network

Assets and asset ranges do not inherit categories from zones and networks
Assets resolution for event correlation

When an event is received on the Manager each endpoint should be resolved to an asset to leverage categories in correlation and threat assessment

The endpoints in an event

- Source
- Destination
- Device
- Connectors

Each endpoint is comprised

- IP Address
- Zone Reference
- Hostname
- MAC Address
Assets in event correlation

After the endpoints are tagged with Assets in events, they are used for evaluating category and group membership

These checks are used in

• Threat assessment of the event
• Rules engine
• Data monitor evaluation for live event stream
Limitations of asset resolution

The unique identifier for the resolved assets are persisted in the database for future use by

- Active channels
- Reports
- Activity Profiler
- Interactive Discovery

If the asset model changes thereafter, the assets are not resolved again for endpoints of already processed events

We do not tag a reference to asset in the endpoint because there will be too many of those references to manage
Tips and tricks
Network model wizard

Starting with ESM v.4.5, a Network Model wizard is provided on the ESM Console (menu option Tools > Network Model).

The Network Model wizard provides the ability to quickly populate the ESM network model by batch loading asset and zone information from Comma Separated Files (CSV) files.

The wizard supports:

- Assets
- Asset ranges
- Zones

Check Admin Guide for more information
Populating the network model with assets
Auto asset creation and zone types

**ESM auto-creates assets for:**

- Assets with ESM components
- Devices discovered by a vulnerability scanner
- Devices reporting through SmartConnectors

**Static Zones**

- Devices in a static zone use static (constant) IP addresses. Must have either a unique IP address, a unique host name, or both.

**Dynamic Zones**

- Devices in a dynamic zone use dynamic addressing (such as DHCP). Dynamic zones represent assets that come and go from the network. Requires either a MAC address or a host name to identify assets in dynamic zones.
Two customers on one Connector!?

This can’t be done via the UI

This can be done using a map file ($connectorfolder/current/user/agent/map)

A map file checks for values in a field and sets another field based on that
It’s a csv file with a header that defines the ‘getter’ field(s) and the ‘setter’ field(s)...it can look like this:

- `event.sourceAddress,set.event.customerURI`
- `range.event.sourceAddress,set.event.customerURI`
- `regex.event.sourceUserName,set.event.customerURI`

Check FlexConnector User Guide and FlexConnector Development Guide for more information

Tip: Use a text editor like vi or notepad++ to show all characters incl. white spaces. White spaces will prevent the map file from working!
Please give me your feedback

Session TB3261  Speaker Till Jäger

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you