Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Manage assets and identities to enrich notables in Splunk Enterprise Security

Generated: 5/19/2022 11:32 pm

Manage assets and identities to enrich notables in Splunk Enterprise Security

When asset and identity correlation is enabled, Splunk Enterprise Security compares indexed events with asset and identity data in the asset and identity lists to provide notable enrichment and context. The comparison process uses automatic lookups in the `props.conf` file. You can find information about automatic lookups in the Splunk platform documentation:

- For Splunk Enterprise, see Make your lookup automatic in the Splunk Enterprise *Knowledge Manager Manual*.
- For Splunk Cloud Platform, see Make your lookup automatic in the Splunk Cloud Platform *Knowledge Manager Manual*.
- See Modify priority and rank in the Asset and Identity Framework in the *Use Splunk Enterprise Security* manual for further information about how ranks, correlations, and automatic lookups affect notable event urgency.

Asset and identity correlation enriches notable events with asset and identity data at search time in the following ways:

- Asset correlation compares events that contain data in any of the `src`, `dest`, or `dvc` fields against the merged asset lists for matching IP address, MAC address, DNS name, or Windows NT host names. Asset correlation no longer occurs automatically against the `host` or `orig_host` fields.
- Identity correlation compares events that contain data in any of the `user` or `src_user` fields against the merged identity lists for a matching identity.
- Enterprise Security adds the matching output fields to the event. For example, correlation on the asset `src` field results in additional fields such as `src_is_expected` and `src_should_timesync`.

You can also format asset and identity data to identify unique assets and identities and enrich notable events. For more information on formatting an asset and identity list as a lookup, see Format an asset or identity as a lookup in Splunk Enterprise Security.

Asset and identity correlation lets you determine whether multiple events can relate to the same asset or identity. You can also perform actions on the identity and asset fields added to events to open additional searches or dashboards scoped to the specific asset or identity. For example, you can open the Asset Investigator dashboard on a `src` field.

You can choose from the following options:

- Disable for all sourcetypes
- Enable selectively by sourcetype
- Enable for all sourcetypes

Prerequisites

Perform the following prerequisite tasks before starting on these settings:

1. Collect and extract asset and identity data in Splunk Enterprise Security.
2. Format the asset or identity list as a lookup in Splunk Enterprise Security.
3. Configure a new asset or identity list in Splunk Enterprise Security.

Disable asset and identity enrichment for all sourcetypes

Disabling asset and identity correlation completely prevents notable events from being enriched with asset and identity data from the asset and identity lookups. This might prevent correlation searches, dashboards, and other functionality from working as expected. Consult with Splunk Professional Services or Splunk Support before disabling asset and identity correlation. If in doubt, keep asset and identity correlation enabled.

To disable correlation for all sourcetypes, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Correlation Setup** tab.
3. Click the **Disable for all sourcetypes** radio button.
4. Click **Save**.

Enable asset and identity enrichment selectively by sourcetype

Enable correlation selectively by sourcetype if you know the specific sourcetypes and corresponding lookups that you need for populating your correlation searches, dashboards, and other functionality. To enable correlation selectively by sourcetype, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Correlation Setup** tab.
3. Click the **Enable selectively by sourcetype** radio button.
4. Click **+ Add a new sourcetype**.
5. Enter the name of the sourcetype.
6. Toggle **Enable asset correlation** or **Enable identity correlation**.
7. Click **Done**.
8. Click **Save**.

Enable asset and identity enrichment for all sourcetypes

Enable correlation for all sourcetypes for ease of management if you don't have performance concerns and if you don't know specifically which sourcetypes you need for populating your correlation searches, dashboards, and other functionality. To enable correlation for all sourcetypes, complete the following steps:

1. From the Splunk Enterprise Security menu bar, select **Configure > Data Enrichment > Asset and Identity Management**.
2. Click the **Correlation Setup** tab.
3. Click the **Enable for all sourcetypes** radio button.
4. Click **Save**.

Enable correlation and entity zones

When correlation and entity zones are both enabled, the `cim_entity_zone` field is used to find the correct asset in the correct zone. Identifying the correct asset in the correct zone enables you to more accurately enrich your search results and notable events fields. For details about entity zones, see Enable entity zones for Assets or Identities.

Using assets as an example, consider the following source file with the same `ip`, `mac`, and `nt_host` in different zones:

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av,cim_entity _zone
192.0.2.94,00:00:5e:16:a7:7a,host,splunk.com,owner1,priority1,,,city1,country1,bunit1,,,,,,,zone1
192.0.2.94,00:00:5e:16:a7:7a,host,splunk.com,owner2,priority2,,,city2,country2,bunit2,,,,,,,zone2
```

With entity zones enabled, the behavior is not to merge key fields such as `ip`, `mac`, and `nt_host` that are in different zones.

You may use the search preview for **asset_lookup_by_str** that returns results as shown in the following table:

asset	cim_entity_zone	ip	mac	nt_host	dns	owner	priority	city	country	bunit
00:00:5e:16:a7:7a host	zone1	192.0.2.94	00:00:5e:16:a7:7a	host	splunk.com	owner1	priority1	city1	country1	bunit1
00:00:5e:16:a7:7a host	zone2	192.0.2.94	00:00:5e:16:a7:7a	host	splunk.com	owner2	priority2	city2	country2	bunit2

For more information on how to use the search preview to test the merge of assets and identities, see Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security.

With correlation and entity zones both enabled, search results are displayed with the events enriched by the `cim_entity_zone` field.

The following search:

```
index="main" sourcetype="sourcetype_you_enabled_for_correlation"
```

displays the following search results:

i	Time	Event
>	6/9/2020 6:06:05.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone1" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner1" dvc_priority="priority1" dvc_country="country1" dvc_city="city1" dvc_bunit="bunit1" asset_tag="bunit1" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"
>	6/9/2020 7:06:07.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone2" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner2" dvc_priority="priority2" dvc_country="country2" dvc_city="city2" dvc_bunit="bunit2" asset_tag="bunit2" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"

The results display two devices of 192.0.2.94 in two different `cim_entity_zone` zones with events that occurred an hour apart. The `cim_entity_zone` field is used to find the correct asset in the correct zone.

Disable entity zones

When entity zones are disabled, With entity zones disabled, the default behavior is to merge by the key fields, such as `ip`, `mac`, and `nt_host`.

You may use the search preview for **asset_lookup_by_str** that returns results as shown in the following table:

asset	ip	mac	nt_host	dns	owner	priority	city	country	bunit	asset_tag
00:00:5e:16:a7:7a host	192.0.2.94	00:00:5e:16:a7:7a	host	splunk.com	owner1 owner2	priority2	city1 city2	zone1_country zone2_country	bunit1 bunit2	bunit1 bunit2

For more information on how to use the search preview to test the merge of assets and identities, see Use the search preview to test the merge of asset and identity data in Splunk Enterprise Security.

With correlation and entity zones both disabled, the merged search results are displayed with the events that are not enriched by the `cim_entity_zone` field.

The following search:

```
index="main" sourcetype="sourcetype_you_enabled_for_correlation"
```

displays the following search results: The results display the same device 192.0.2.94 enriched with the same multivalue fields in events that occurred an hour apart. The `cim_entity_zone` field is in the raw event (if defined). However, with entity zones disabled, it is not used in correlation searches, saved searches, or dashboards.

i	Time	Event
>	6/9/2020 6:06:05.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone1" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner1 | owner2" dvc_priority="priority2" dvc_country="country1 | country2" dvc_city="city1 | city2" dvc_bunit="bunit1 | bunit2" asset_tag="bunit1 | bunit2" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"
>	6/9/2020 7:06:07.000 PM	example event dvc="192.0.2.94" cim_entity_zone="zone2" host="host" dvc_asset="host | 00:00:5e:16:a7:7a" dvc_ip="192.0.2.94" dvc_asset_id="123456789" dvc_owner="owner1 | owner2" dvc_priority="priority2" dvc_country="country1 | country2" dvc_city="city1 | city2" dvc_bunit="bunit1 | bunit2" asset_tag="bunit1 | bunit2" source="example_source" sourcetype="sourcetype_you_enabled_for_correlation"