SecKit IDM Common Documentation

Ryan Faircloth/Splunk Inc.

May 21, 2019

Contents

Success Enablement Content “SecKit” apps for Splunk are designed to accelerate the tedious or difficult tasks. This application IDM Common is an add on for Splunk Enterprise Security designed to identify basic network and enrich the with information that is useful to security incident detection and response as well as compliance tracking. Following through the quick start you will be able to answer important questions for a single subnet.

- Where is the asset based on src and or dest ip?
- What is the zone of the network?
- What type of facility is the asset located in?

CHAPTER 1

Before you get started

- Complete Splunk Enterprise Security Administration training
- Review the current Assets and Identities section of the Administration Manual
- **Review the use of lookup data in Splunk**
  - Lookup Command
  - CIDR and Matching Rules
- CIDR notation splunk required all notations to be correct i.e. 10.0.0.0/16 NOT 10.0.0.1/16 and less than 32 bits.

CHAPTER 2

Support

- Reporting issues or requesting enhancements Issue tracking

CHAPTER 3

Known Issues

- Splunk Enterprise has partial support for IPv6 CIDR notation some searches may report errors such as `Invalid [fe80::/10]: 'fe80::/10' is not a valid IP address or CIDR block` There is no work around use of IPV6 in CIDR notation can be removed from the lookup files or the errors can be ignored.

3.1 Splunk System Requirements

3.1.1 Mandatory

- Splunk Enterprise >7.1.0
- Splunk Enterprise Security >5.1.0

3.1.2 Review size of lookups in memory

Splunk utilizes a default maximum size of in memory lookup tables that can be exceeded when large numbers of CIDR assets are tracked in enterprise security. If the size is exceeded a user error will appear to the effect of CIDR match lookup can not used indexed lookups. Should the impact the environment review the size of the enterprise security lookup assets_by_cdr.csv and increase the value limits.conf/[lookup]/max_memtable_bytes to 125% of the size of this file in bytes and apply the change to both the ES Search Head and the indexer tier.

3.1.3 Optional - Splunk Stream

To use Splunk Stream to discovery DHCP subnets the following patch must be applied

Listing 1: $SPLUNK_HOME/apps/Splunk_TA_stream/local/props.conf

```
[stream:dhcp]
FIELDALIAS-lease_scope = subnetmask AS lease_scope
```

3.2 Installation

Installation of the apps is intended to be minimally impactful to a Splunk ES environment. If existing assets and identities have been configured care should be take to ensure an asset or identity is only defined once.

3.2.1 Migration from legacy assets and identities

Enterprise Security does not "merge" records from multiple sources having multiple conflicting definitions can impact systems active users.

- Identify and remove the identity file definition from Splunk Enterprise Security
- Identify and remove the lookup definition from Splunk Enterprise
- Identify and remove the lookup file from disk. *Important to ensure large bundles do not impact search replication*

3.2.2 Installation

This add on is installed on the Splunk Enterprise Security Search head.

Splunk Enterprise: Choose one, note Splunk Base releases are considered stable

- Download the latest published release from SplunkBase
- Download the latest master build from bitbucket
- See installing apps This add on only requires installation on the search head in a distributed deployment.
- A search head Restart or rolling restart in the case of SHC is required.

Splunk Cloud:

- Using a service request ask for the app installation SecKit_SA_idm_common id "3055" specify version 3.0 or latter
- *WARNING* SecKit_SA_idm_common 3.x is not backwards compatible with SecKit_SA_idm_windows 2.x ensure both apps are updated in the same change if deployed together.

3.2.3 Configure ES App Imports

ES must be configured to see (import) the new application this process needs to be completed only one time

Configuration

- As an es_admin navigate to Splunk Enterprise Security
- From the Configure menu select General
- From the General menu select App Imports Update
- Click on "update_es"
- Append `|(SecKit_[ST]A_.*)` to the Application Regular Expression'
- Click Save

Verification

- As an es_admin navigate to Splunk Enterprise Security

- Click the Search menu
- Click Search again
- Execute the search `| inputlookup seckit_idm_network_masks_lookup` verify results containing netmask column are returned.

3.2.4 Initialize Lookups and Collections

Run the following searches in order. It may be necesssary to restart Splunk before all lookup tables are created.

- Navigate to a Splunk Search window
- Run the search `| from savedsearch: "seckit_idm_common_assets_networks_lookup_gen"`
- Run the search `| from savedsearch: "Identity - Asset String Matches - Lookup Gen"`
- Run the search `| from savedsearch: "Identity - Asset CIDR Matches - Lookup Gen"`

3.3 Upgrading from prior versions

3.3.1 Upgrade from version <2.0

Changes from version 1.0 are drastic, recommendation is to remove the apps, and review the contents of `local/*.conf` and lookups and port the config as if a new installation.

WARNING SecKit_SA_idm_common 3.x is not backwards compatible with SecKit_SA_idm_windows 2.x ensure both apps are updated in the same change if deployed together.

3.3.2 Upgrade from version 2.x

Remove the following files from the search head they will be regenerated by the application as collections.

- `SecKit_SA_idm_common/lookups/seckit_idm_common_assets_expected_tracker.csv.*`
- `SecKit_SA_idm_common/lookups/seckit_idm_common_assets_host_expected_tracker.csv.*`

3.4 Quick Start Tutorial

The quick start procedure is simply to demonstrate the application of this solution continue reading in the using guide once your first use is complete.

3.4.1 Identify subnets for use

- Working with a knowledgeable network administrator identify one network larger than a `24/` that is located in a data center.
- For this specific data center identify - City, State/province postal code, country code (2 US letter code) - Street Address - Using Street address use a service such as google maps to identify lat, lon to 4 digits of precision

3.4.2 Configure SecKit to label the network asset

Create the initial configuration files

- Create a csv file as follows named `seckit_idm_pre_cidr_location.csv`

cidr	lat	long	city	state	country
10.0.0.0/16	37.7826	-122.3934	San Francisco	CA	US

- Create a csv file as followed name `seckit_idm_pre_cidr_category.csv` empty cells are left blank for now

cidr	cidr_pci_domain	cidr_category	cidr_priority	cidr_bunit	cidr_owner
10.0.0.0/16		facility_type:dc|zone:lan			

Update the configuration files using Enterprise Security Content Management

- As a es_admin login to Splunk Enterprise Security
- Navigate to the configure menu
- Select Content Management
- Select "SecKit SA IDM Common" from the app menu
- Find "SecKit IDM Common network location" by name and click update file upload the file created above `seckit_idm_pre_cidr_location.csv`
- Find "SecKit IDM Common network categories" by name and click update file upload the file created above `seckit_idm_pre_cidr_category.csv`

Force Merge of Assets

The following process can be used at any time to force immediate updates of asset files

- Navigate to a Splunk Search window
- Run the search `| from savedsearch: "seckit_idm_common_assets_networks_lookup_gen"`
- Run the search `| from savedsearch: "Identity - Asset String Matches - Lookup Gen"`
- Run the search `| from savedsearch: "Identity - Asset CIDR Matches - Lookup Gen"`

Verification

- As an ES user (or above) navigate to Enterprise security
- Select Security Domains from the menu
- Select Identity from the drop down
- Select Asset Center
- View the record as defined above if additional records are displayed from other sources sort/scroll to locate

3.5 Using Common Assets

Before continuing with this section ensure you have completed the quickstart tutorial.

3.5.1 Enrichment Lookups

seckit_idm_pre_cidr_location

Geolocation data is helpful context to security investigation. Location and give insight into the contextual appropriateness of actions within a network such as does the person belong in the facility involved in the event. Some discretion is advised when configuring location data to avoid creation of low value administrative burden. The lowest resolution useful should be consistently used for example the lat/long of the main entrance for a large campus rather than attempting to record building level accuracy.

Don't include VPN address ranges used by client VPN technology in the location table as the same location as the data center. Identify a fixed location for all VPN traffic not also used by a real facility.

Optional in the TOOLS folder leverage `Security Kit Location and Categories Tables.xlsx` to develop the location list.

cidr

A CIDR block allocated to a specific location the largest non overlapping block should be used

lat & long

Standard notation not more than 5 digits of precision

city

The city name

state

Postal abbreviation for state or province typically two char english uppercase

Country

Country abbreviation typically two char english upper case

seckit_idm_pre_cidr_category

cidr_priority

Minimum priority applied for notable correlation in Splunk Enterprise Security

- [blank] No value indicates no specific priority is applied to this cidr
- low
- medium
- high
- critical

cidr_pci_domain

This field is often overloaded to indicate additional specific regulatory relationships example uses

- pci = In scope for PCI assessment included wifi networks and control networks for card holder data
- cardholder = Systems contain card holder data
- GDPR = similar to PCI contains control systems but not actual data
- PII = contains personally identifiable information

cidr_bunit

Business unit or department. Splunk Enterprise security will combine all values of bunit as a multi value field. At your discretion "top" and lower level values can be applied OR should be applied only to the lowest level underwhich ther should be no smaller levels for example

10.1.0.0/20 is allocated to the "hospital" bunit however 10.1.14.0/24 is allocated to surgery. If the bunit is provided for both CIDR blocks at search time the field bunit will contain both values.

cidr_owner

The owner (typically email) of a user, group or point of contact for an asset. In most organizations this is only provided on small /22 or /24 subnets which contain systems under the responsiblity of a single group. In most cases this field is blank

cidr_category

The following categories are commonly defined in the categories configuration per cidr. The shortest reasonable string should be used for all values. Note only values matching the regex [A-Za-z0-9-_] should be used. See the categories chapter for specific examples.

Apply the updated configuration to your assets

Update the configuration files using Enterprise Security Content Management

- As a es_admin login to Splunk Enterprise Security
- Navigate to the configure menu
- Select Content Management
- Select "SecKit SA IDM Common" from the app menu
- Find "SecKit IDM Common network location" by name and click update file upload the file created above `seckit_idm_pre_cidr_location.csv`
- Find "SecKit IDM Common network categories" by name and click update file upload the file created above `seckit_idm_pre_cidr_category.csv`

Force Merge of Assets

The following process can be used at any time to force immediate updates of asset files

- Navigate to a Splunk Search window

- Run the search `| savedsearch "seckit_idm_common_assets_networks_lookup_gen"`
- Run the search `| from savedsearch:"Identity - Asset String Matches - Lookup Gen"`
- Run the search `| from savedsearch:"Identity - Identity Matches - Lookup Gen"`

Verification

- As an ES user (or above) navigate to Enterprise security
- Select Security Domains from the menu
- Select Identity from the drop down
- Select Asset Center
- View the record as defined above if additional records are displayed from other sources sort/scroll to locate

3.5.2 Scheduled Searches and Enabled Input Tasks

Inputs

identity_manager://seckit_idm_common_assets_networks

Utilized to enable the usage of the main combined lookup by Enterprise Security Identity Manager

Scheduled Searches

seckit_idm_common_assets_networks_lookup_gen

Produces the lookup `seckit_idm_common_assets_networks_lookup` used as input in `identity_manager://seckit_idm_common_assets_networks`. The default schedule will produce a new lookup every 4 hours.

seckit_idm_combined_cidr_category_by_str_lookup_gen

Combines the csv lookup `seckit_idm_pre_cidr_category_by_str_lookup` and search managed collection `seckit_idm_common_event_cidr_category` to produced the lookup `seckit_idm_combined_cidr_category_by_str_lookup`. This lookup is utilized by the saved search `seckit_idm_common_assets_networks_lookup_gen` to produce the network assets file. The default schedule will produce a new file every 30 min.

seckit_idm_common_event_cidr_category_from_dm_network_session_dhcp

Utilizes the network session data model to identify network segments managed using DHCP to automatically categorize subnets. The default schedule will detect new subnets every 4 hours.

seckit_idm_common_event_cidr_category_age

Ages entries in the lookup `seckit_idm_common_event_cidr_category_age` where last is non zero and not updated in the prior year. The default schedule will trim the lookup once per day

seckit_idm_common_assets_expected_tracker_gen

Updates the lookup `seckit_idm_common_assets_host_expected_tracker_lookup` based on universal forwarder internal logs to identify hosts which should be set as is_expected. The default schedule search runs at the top of the hour using only the last 15m of prior data.

seckit_idm_common_assets_expected_tracker_age

Ages entries in the lookup `seckit_idm_common_assets_host_expected_tracker_lookup` not updated in the prior year. The default schedule will trim the lookup once per day.

seckit_idm_pre_cidr_category_by_str_lookup_ftr

Ensures the lookup `seckit_idm_pre_cidr_category_by_str_lookup` exists and contains the correct fields. The default schedule of the search uses a special configuration option run_on_startup and run_n_times to ensure the search runs on only once.

seckit_idm_common_assets_networks_lookup_ftr

Ensures the lookup `seckit_idm_common_assets_networks_lookup` exists and contains the correct fields. The default schedule of the search uses a special configuration option run_on_startup and run_n_times to ensure the search runs on only once.

seckit_idm_pre_host_static_lookup_ftr

Ensures the lookup `seckit_idm_pre_host_static_lookup` exists and contains the correct fields. The default schedule of the search uses a special configuration option run_on_startup and run_n_times to ensure the search runs on only once.

3.6 Customizing the add on

The add on support customization using macros

3.6.1 seckit_idm_common_event_cidr_category_from_dm_network_session_dhcp_custom

This macro is utilized in the saved search `seckit_idm_common_event_cidr_category_from_dm_network_session_dh` and can be used to add additional logic via spl to define categories to the CIDR allocations detected via dhcp.

3.6.2 Building you own lists

This add on provides a couple of macros to make the job of building out identity and assets lists a bit easier.

- `seckit_idm_common_output_identities(lookup_name,key_field,tag)` used to output a list suitable for identity merge. Accepts events utilizing the standard field names. - lookup_name - the defined lookup destination for the data must exists - key_field - not used set to nick, - tag use to attach a a category to trace the source of an identity - identity - multivalve field (makemv identity) list valid account names for the identity - nick - the unique key for the record should not be repeated in any other source - category - a multivalve

field (makemv category) list of categories to apply - priority - may be a single or multivalve field the highest priority found will apply

- `seckit_idm_common_output_assets(lookup_name,key_field,tag)` used to output a list suitable for asset merge. Accepts events utilizing the standard field names. - lookup_name - the defined lookup destination for the data must exists - key_field - not used set to nick, - tag use to attach a a category to trace the source of an asset - field notes - category - a multivalve field (makemv category) list of categories to apply - priority - may be a single or multivalve field the highest priority found will apply - should_timesync,should_update,requires_av single or multi value fields. Any value of true will result in true for the final output
- `seckit_idm_common_get_asset_geo` used by add on packages to enrich ip address with internal geo coding.

3.7 Common Categories

The following categories are commonly defined in the categories configuration. The shortest reasonable string should be used for all values. Note only values matching the regex [A-Za-z0-9-_] should be used. This reference is shared by the SecKit IDM family of tools each example is marked if it is appropriate for CIDR, a single ASSET, or BOTH

3.7.1 facility_id:<value> CIDR

The facility_id is typical a short identification string defined by the organizations facility management department. This would be associated to a real physical location under the control of the organization.

3.7.2 facility_type:<value> CIDR

The facility type reflect the general purpose of the facility common examples

- DC = Data Center
- COLO = Colocation
- STORE = Retail Store
- OFFICE = General Office
- PLANT = Plant

3.7.3 known_scanner BOTH

A known scanner will regularly trigger vuln scanner detection this category is applied to all types of scanners.

3.7.4 known_scanner:<value> BOTH

In addition to known_scanner this category with a value gives context to the expected type of scanner.

- vuln = Network vulnerability scanner such as rapid7 or nessus
- app = Application scanner such as burp suite used to detect application vulnerabilities
- ping = Ping scanner typically used to monitor uptime for IT operations
- alive = Application is alive scanner typically can understand application level response

- asset = Asset discovery or collection system

3.7.5 net_assignment:<value> CIDR

The network address management method for the segment

- static = IP address is assigned locally
- dyndhcp = IP address is issued by a DHCP server
- dynvirt = IP address is issued by a virtualization system such as docker, AWS, hyper-v or vcenter and rarely changes

3.7.6 net_type:<value> CIDR

The network type

- RFC1918 (Reserved per RFC)
- CGNAT (Carrier Grade NAT)

3.7.7 pf:<value> BOTH

The PF or primary function of a device is a specific identifier relates to the role of a asset in a service. This is most commonly applied to a specific asset but may apply to a CIDR

3.7.8 svc:<value> BOTH

The SVC or Service is a identifier indicating the service this asset participates in providing for example. The service DNS “svc:DNS” would typlically be made up of a combination of “pf:ms_dns” or “pf:BIND” AND “pf:dns_rbl” “pf:dns_recursive”

3.7.9 zone:<value> CIDR

The network zone type for the network segment common values are as follows

- LAN = Wired lan
- DMZ
- WLAN = Wireless Lan
- WWLAN = Mobile or wireless private networking (Rare)
- VPN = Client VPN
- PartnerVPN = Site 2 Site VPN network with a partner
- Storage = Storage area network
- Guest = Guest network wired or wired
- Vendor = Vendor equipment network (devices not managed by org)
- IC = Industrial Controls
- SAFETY = Life or Safety systems

3.7.10 zone_name:<value> CIDR

Many organizations have more than one of a specific type of zone particularly DMZ, and VPN zones the name this field can be used to specifically identify those zones.

Apply the updated configuration to your assets

Update the configuration files using Enterprise Security Content Management

- As a es_admin login to Splunk Enterprise Security
- Navigate to the configure menu
- Select Content Management
- Select "SecKit SA IDM Common" from the app menu
- Find "SecKit IDM Common network location" by name and click update file upload the file created above `seckit_idm_pre_cidr_location.csv`
- Find "SecKit IDM Common network categories" by name and click update file upload the file created above `seckit_idm_pre_cidr_category.csv`

Force Merge of Assets

The following process can be used at any time to force immediate updates of asset files

- Navigate to a Splunk Search window
- Run the search `| savedsearch "seckit_idm_common_assets_networks_lookup_gen"`
- Run the search `| from savedsearch:"Identity - Asset String Matches - Lookup Gen"`
- Run the search `| from savedsearch:"Identity - Identity Matches - Lookup Gen"`

Verification

- As an ES user (or above) navigate to Enterprise security
- Select Security Domains from the menu
- Select Identity from the drop down
- Select Asset Center
- View the record as defined above if additional records are displayed from other sources sort/scroll to locate