SecKit for Splunk TA Windows Documentation

Ryan Faircloth/Splunk Inc.

Mar 22, 2019

Contents:

This Success enablement content kit provides ready to deploy configuration for Windows Data Collection in a typical organization. The approach to deployment is modular designed to allow deployment of collection in such a way that valuable insights while making optimal use of your Splunk License.

The files referenced in this kit are available in our bitbucket repo

CHAPTER 1

Objectives

- Collect Windows Security Events from All Windows systems
- Collect Performance metrics from important systems such as Active Directory and DNS servers
- Collect Critical Registry key change events from all Windows systems
- Collect DHCP Lease information from Windows DHCP Servers

CHAPTER 2

Deploy the Splunk Add on (on prem)

Deploy the Splunk TA Windows to each appropriate instance of Splunk, in the following order

2.1 Splunk Search Head

- Download version Splunk TA Windows 6.0.0 from the deps folder of the repository OR from Splunk Base https://splunkbase.splunk.com/app/742/
- Expand and copy to $SPLUNK_HOME/etc/apps.
- Restart the Search Head

2.2 Splunk Search Head Cluster

- Download version Splunk TA Windows 6.0.0 from the deps folder of the repository OR from Splunk Base https://splunkbase.splunk.com/app/742/
- Remove the Splunk_TA_Windows folder from $SPLUNK_HOME/etc/shcluster/apps and push to the cluster using the appropriate command
  - non ES SHC `splunk apply shcluster-bundle`
  - ES SHC `splunk apply shcluster-bundle -preserve-lookups true`
- Expand and copy Splunk_TA_Windows to $SPLUNK_HOME/etc/shcluster/apps
- Push to the cluster using the appropriate command
  - non ES SHC `splunk apply shcluster-bundle`
  - ES SHC `splunk apply shcluster-bundle -preserve-lookups true`

2.3 Splunk Index time data processing (optional)

Optionally Splunk can be configured to process the raw logs to remove extraneous information reducing the total license consumption and in some cases improving search performance at the expense of increased CPU utilization in the indexing pipeline. See Splunk Docs

- create/update local/props.conf in the folder to be used in the following steps:

```
[source::WinEventLog:System]
SEDCMD-clean_info_text_from_winsystem_events_this_event = s/This event is␣
↪generated[\S\s\r\n]+$//g

[source::WinEventLog:Security]
SEDCMD-windows_security_event_formater = s/(?m)(^\s+[^:]+\:)\s+-?$/\1/g
SEDCMD-windows_security_event_formater_null_sid_id = s/(?m)(:)(\s+NULL SID)$/\1/g␣
↪s/(?m)(ID:)(\s+0x0)$/\1/g
SEDCMD-cleansrcip = s/(Source Network Address:    (\:\:1|127\.0\.0\.1))/Source␣
↪Network Address:/
SEDCMD-cleansrcport = s/(Source Port:\s*0)/Source Port:/
SEDCMD-remove_ffff = s/::ffff://g
SEDCMD-clean_info_text_from_winsecurity_events_certificate_information = s/
↪Certificate information is only[\S\s\r\n]+$//g
SEDCMD-clean_info_text_from_winsecurity_events_token_elevation_type = s/Token␣
↪Elevation Type indicates[\S\s\r\n]+$//g
SEDCMD-clean_info_text_from_winsecurity_events_this_event = s/This event is␣
↪generated[\S\s\r\n]+$//g

## For XmlWinEventLog:Security
SEDCMD-cleanxmlsrcport = s/<Data Name='IpPort'>0<\/Data>/<Data Name='IpPort'><\/
↪Data>/
SEDCMD-cleanxmlsrcip = s/<Data Name='IpAddress'>(\:\:1|127\.0\.0\.1)<\/Data>/
↪<Data Name='IpAddress'><\/Data>/

[source::WinEventLog:ForwardedEvents]
SEDCMD-remove_ffff = s/::ffff://g
SEDCMD-cleansrcipxml = s/<Data Name='IpAddress'>(\:\:1|127\.0\.0\.1)<\/Data>/
↪<Data Name='IpAddress'><\/Data>/
SEDCMD-cleansrcportxml=s/<Data Name='IpPort'>0<\/Data>/<Data Name='IpPort'><\/
↪Data>/
SEDCMD-clean_rendering_info_block = s/<RenderingInfo Culture='.*'>(?s)(.*)<\/
↪RenderingInfo>//

[WMI:WinEventLog:System]
SEDCMD-clean_info_text_from_winsystem_events_this_event = s/This event is␣
↪generated[\S\s\r\n]+$//g


[WMI:WinEventLog:Security]
SEDCMD-windows_security_event_formater = s/(?m)(^\s+[^:]+\:)\s+-?$/\1/g
SEDCMD-windows_security_event_formater_null_sid_id = s/(?m)(:)(\s+NULL SID)$/\1/g␣
↪s/(?m)(ID:)(\s+0x0)$/\1/g
SEDCMD-cleansrcip = s/(Source Network Address:    (\:\:1|127\.0\.0\.1))/Source␣
↪Network Address:/
SEDCMD-cleansrcport = s/(Source Port:\s*0)/Source Port:/
SEDCMD-remove_ffff = s/::ffff://g
SEDCMD-clean_info_text_from_winsecurity_events_certificate_information = s/
↪Certificate information is only[\S\s\r\n]+$//g
```

(continues on next page)

(continued from previous page)

```
SEDCMD-clean_info_text_from_winsecurity_events_token_elevation_type = s/Token␣
↪Elevation Type indicates[\S\s\r\n]+$//g
SEDCMD-clean_info_text_from_winsecurity_events_this_event = s/This event is␣
↪generated[\S\s\r\n]+$//g
```

2.4 Splunk Non Clustered Indexers, Windows Heavy Forwarders, Intermediate Forwarders

- Download version Splunk TA Windows 6.0.0 from the deps folder of the repository OR from Splunk Base https://splunkbase.splunk.com/app/742/
- Copy to $SPLUNK_HOME/etc/apps.

2.5 Splunk Clustered Indexers

- Download version Splunk TA Windows 6.0.0 from the deps folder of the repository OR from Splunk Base https://splunkbase.splunk.com/app/742/
- Expand and Copy to $SPLUNK_HOME/etc/apps.
- Create the following indexes in accordance to the standard practices for index definition in your organization by added to or created an indexes.conf file in the most appropriate app in master-apps. If no standard location we suggest `$SPLUNK_HOME/master-apps/Splunk_TA_windows_SecKit_Indexes/local/indexes.conf`
  - `appmsadmon`: Used for Active Directory change data capture.
  - `oswin`: Windows OS events generally used by IT operations and Application Support some events may have security relevance.
  - `oswinreg`: Windows OS registry key changes captured by the Windows UF
  - `oswinsec`: Windows OS Security Event log, may also be used for additional event log types primarily used by Security Monitoring
  - `oswinscript`: Windows Scripted inputs used to collect additional information about the Windows OS, useful to many types of users
  - `oswinperf`: Windows Performance data as events
  - `oswinmetrics`: Windows Performance Metrics data, ** This must be a metrics index **
  - `epintel`: Endpoint Intelligence index contains information which can be used to identify the behaviors of malicious code and users.

2.6 Splunk Deployment Server

- Download version Splunk TA Windows 6.0.0 from the deps folder of the repository OR from Splunk Base https://splunkbase.splunk.com/app/742/
- Expand and Copy to $SPLUNK_HOME/etc/deployment-apps
- Download src/Splunk_TA_windows_SecKit_DS and copy to $SPLUNK_HOME/etc/apps

- Download src/Splunk_TA_windows_SecKit_<n>* and copy to $SPLUNK_HOME/etc/deployment-apps
- Restart the deployment server

CHAPTER 3

Deploy the Splunk Add on (Splunk Cloud)

- Request installation of version 6.0.0 of Splunk_TA_windows on all appropriate search heads
- Manually create the indexes prescribed above
- Deploy to intermediate forwarders and Windows heavy forwarders as prescribed above
- Configure deployment server as prescribed above.

CHAPTER 4

Begin Data Collection

Data collection is managed through the deployment server configured above. The default configuration will collect the minimum reasonable data from all Windows Instances. Using the software deployment solution for your organization ensure the Windows version of the Splunk UniversalForwarder is deployed to all Windows systems. ** NOTE: Best Practices for security deployment of the UF should be followed **

4.1 Active Directory Servers

Active Directory is a critical service for the IT Operations and Security user communities. Use the following search to identify all Hosts where the Splunk Universal Forwarder has been installed and correctly configured for managed by the deployment server above.

```
index=* sourcetype=winhostmon source=roles Name="Active Directory Domain Services"
|  stats latest(_time) as _time by host
```

- Review the list of hosts with the appropriate Active Directory Administrator(s) to confirm no hosts have been omitted.
- Utilize the following search to generate a white list of all Active Directory Servers

```
index=* |  stats latest(_time) as _time by host
|  fields + host
|  mvcombine host
| eval host=mvjoin(host,",")
```

- On the deployment server create/update the following stanza in $SPLUNK_HOME/etc/apps/Splunk_TA_windows_SecKit_DS/loc

```
[serverClass:seckit_all_2_os_windows_dc]
whitelist.0 = comma,seperated,list,of,hosts,identified,above
```

- Review the list of servers with the appropriate Active Directory Administrator(s). Identify two (2) domain controllers for each domain preferably located in the same data centers as Splunk Indexer

sites and NOT FSMO role holders. On the deployment server create/update the following stanza in $SPLUNK_HOME/etc/apps/Splunk_TA_windows_SecKit_DS/local/serverclass.conf

```
[serverClass:seckit_all_2_os_windows_dc_admon_sync]
whitelist.0 = comma,seperated,list,of,hosts,identified,above
```

4.2 Non Active Directory Server Windows DNS

- Review the following search to determine if any Microsoft DNS Servers exist which are NOT also Microsoft Active Directory Servers configured above.

```
index=* sourcetype=winhostmon source=roles Name="Active Directory Domain Services" OR␣
↪ Name="DNS Server"
|  stats values(Name) by host
| search Name="Active Directory Domain Services" NOT Name="DNS Server"
```

- If any servers are identified. Run the following search to produce a white list

```
index=* sourcetype=winhostmon source=roles Name="Active Directory Domain Services" OR␣
↪ Name="DNS Server"
|  stats values(Name) by host
| search Name="Active Directory Domain Services" NOT Name="DNS Server"
|  mvcombine host
| eval host=mvjoin(host,",")
```

On the deployment server create/update the following stanza in $SPLUNK_HOME/etc/apps/Splunk_TA_windows_SecKit_DS/local/serv

```
[serverClass:seckit_all_2_os_windows_dns]
whitelist.0 = comma,seperated,list,of,hosts,identified,above
```

4.3 Microsoft DHCP

- Review the following search to determine if any Microsoft DHCP Servers exist.

```
index=* sourcetype=winhostmon source=roles Name="DHCP Server"
| stats lates(_time) by host
```

- If any servers are identified. Run the following search to produce a white list

```
index=* sourcetype=winhostmon source=roles Name="DHCP Server"
|  stats values(Name) by host
|  mvcombine host
| eval host=mvjoin(host,",")
```

On the deployment server create/update the following stanza in $SPLUNK_HOME/etc/apps/Splunk_TA_windows_SecKit_DS/local/serv

```
[serverClass:seckit_all_2_os_windows_dhcp]
whitelist.0 = comma,seperated,list,of,hosts,identified,above
```

4.4 Collect Additional Microsoft EventLogs

Beginning with Windows 7, Microsoft began logging important events to EventLogs other than the traditional Application System and Security destinations. In addition minimal performance counters, and registry keys known to be abused by malware for persistence are captured. Determine if the additional events collection by the extended event logs input are useful to your organization and within license budget then update the white list below by providing a * to for all systems, white list regex or whitelist lookup.

```
[serverClass:seckit_all_2_os_windows_1]
whitelist.0 = *
```

CHAPTER 5

Indices and tables

- genindex
- modindex
- search