SecKit TA IDM Windows Documentation

Ryan Faircloth/Splunk Inc.

Jan 22, 2019

Contents

Success Enablement Content “SecKit” apps for Splunk are designed to accelerate the tedious or difficult tasks. This application TA IDM Windows is an add on for Splunk Enterprise designed to identify and enrich asset and identity information based by collection of specific information from the Windows Operating System.

- What is the static IP configuration of the host?
- Which interfaces are connected to domain networks?
- What DHCP and DNS servers are providing IPAM and DNS services for this system?

CHAPTER 1

Before you get started

- Complete Splunk Enterprise Security Administration training
- Deploy the Splunk Universal forwarder to all monitored Windows Servers and Endpoints
- Configure data collection for Windows to support the Security Monitoring and Investigation responsibilities of the organization. Review and apply the guidance as appropriate for your organization for Splunk TA Windows SecKit TA

CHAPTER 2

Support

- Reporting issues or requesting enhancements Issue Tracker
- Source

CHAPTER 3

Documentation

3.1 Splunk System Requirements

3.1.1 Mandatory

- Splunk Enterprise >7.1.0
- Splunk Enterprise Security >5.1.0
- SecKit IDM Common >=3.0.0
- Splunk TA Windows >=5.0.1

3.2 Installation

3.2.1 Splunk Enterprise

Download

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

Splunk Enterprise:

- Download the latest published release from https://splunkbase.splunk.com/app/4226/
- Download the latest master build from bitbucket

Installation

See installing apps

- Install on Search Head(s)

- Install on Indexers and Intermediate Forwarders

3.2.2 Splunk Cloud:

Using a service request ask for the app installation SecKit_TA_idm_windows id "4226" specify version 1.0 or later

3.2.3 Data Collection (Splunk Enterprise & Splunk Cloud)

- Expand the archive and install in the deployment-apps server. - Copy the inputs stanza from default to local - Set `disabled=false` - Set a index we suggest `oswinscripts`
- Add the app to a deployment server class deployed to all Windows OS UFs restart is required. If using "SecKit TA Windows guidance" utilize `seckit_all_2_os_windows_0`

3.2.4 Verify Installation

Run the following search for last 30 min records should be returned

```
index=<selectedindex> sourcetype="seckit:idm:windows:interface"
```