
SecKit_IDM Documentation

Ryan Faircloth/Splunk Inc.

Oct 25, 2018

Contents:

1 Indices and tables

3

Welcome to SecKit (Success Enablement Content), the IDM add on family is designed to help the security user develop high quality enrichment for Enterprise Security's Asset and Identity Framework.

What apps are in the family today? Get started today by implementing in the following order

- [SecKit SA IDM Common](#) - This add-on provides the base functionality (library) and defines network assets at the cidr block level. Usings this add on you can gain enrichment for location data (lat/lon) as well as categorize networks by function and compliance control.
- [SecKit TA IDM Windows](#) This add on collect network configuration data for enrichment of assets in ES
- [SecKit SA IDM Windows](#) This add on discovers assets and identity data using Splunk TA for Windows.

CHAPTER 1

Indices and tables

- [genindex](#)
- [modindex](#)
- [search](#)