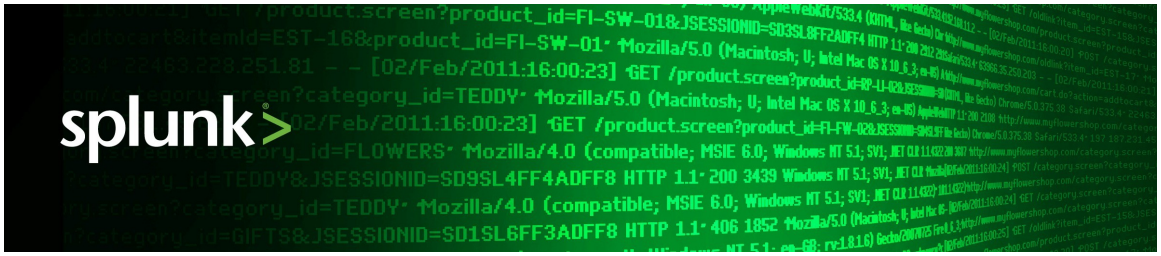

Splunk® Common Information Model Add-on Common Information Model Add-on Manual 4.11.0

Overview of the Splunk Common Information Model

Generated: 8/26/2018 1:39 pm

Overview of the Splunk Common Information Model

The Splunk **Common Information Model (CIM)** is a shared semantic model focused on extracting value from data. The CIM is implemented as an add-on that contains a collection of data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time.

The CIM add-on contains a collection of preconfigured **data models** that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. You can use these data models to normalize and validate data at search time, accelerate key data in searches and dashboards, or create new reports and visualizations with Pivot.

The add-on also contains several tools that are intended to make analysis, validation, and alerting easier and more consistent. These tools include a custom command for CIM validation and a common action model, which is the common information model for custom alert actions. See Approaches to using the CIM for more information about the tools available in the CIM add-on.

Why the CIM exists

The CIM helps you to normalize your data to match a common standard, using the same field names and event tags for equivalent events from different sources or vendors. The CIM acts as a search-time schema ("schema-on-the-fly") to allow you to define relationships in the event data while leaving the raw machine data intact.

After you have normalized the data from multiple different source types, you can develop reports, correlation searches, and dashboards to present a unified view of a data domain. You can display your normalized data in the dashboards provided by other Splunk applications such as Splunk Enterprise Security and the Splunk App for PCI Compliance. The dashboards and other reporting tools in apps that support CIM compliance display only the data that is normalized to the tags and fields defined by the Common Information Model.

The Splunk Common Information Model add-on is packaged with Splunk Enterprise Security, Splunk IT Service Intelligence, and the Splunk App for PCI Compliance.

How to use this manual

The Data Models chapter of this manual provides reference documentation for the fields and tags that make up each data model. Refer to the reference tables to determine what tags and fields are expected for each dataset in a data model as you work to normalize a new data source to the CIM. See How to use these reference tables.

This manual also provides a step-by-step guide for how to apply the CIM to your data at search time. The Using the Common Information Model chapter of the manual includes a walkthrough of the procedure you should follow to

- Use the CIM to normalize data at search time
- Use the CIM to validate your data
- Use the CIM to create reports and dashboards
- Use the common action model to build a custom alert action.

The manual also includes two detailed examples that further demonstrate how to use the CIM to normalize data at search time.

- Use the CIM to normalize OSSEC data
- Use the CIM to normalize CPU performance metrics

What data models are included

The following data models are included in the Splunk Common Information Model Add-on. You can find the JSON implementations of the data models in `$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/default/data/models`.

Data model	File name
Alerts	Alerts.json
Application State	Application_State.json
Authentication	Authentication.json
Certificates	Certificates.json
Change Analysis	Change_Analysis.json
CIM Validation (S.o.S)	Splunk_CIM_Validation.json
Databases	Databases.json
Data Loss Prevention	DLP.json

Email	Email.json
Interprocess Messaging	Interprocess_Messaging.json
Intrusion Detection	Intrusion_Detection.json
Inventory	Compute_Inventory.json
Java Virtual Machines (JVM)	JVM.json
Malware	Malware.json
Network Resolution (DNS)	Network_Resolution.json
Network Sessions	Network_Sessions.json
Network Traffic	Network_Traffic.json
Performance	Performance.json
Splunk Audit Logs	Splunk_Audit.json
Ticket Management	Ticket_Management.json
Updates	Updates.json
Vulnerabilities	Vulnerabilities.json
Web	Web.json

How the Splunk CIM compares to the DMTF CIM

The Splunk Common Information Model is an independent standard, unaffiliated with the Distributed Management Task Force CIM.

The DMTF CIM is different from the Splunk CIM. The DMTF is more hierarchical, more complex, and more comprehensive than the Splunk CIM. In the DMTF CIM, all models inherit from a single parent node, with child nodes for each model, then additional branching child nodes for sub-concepts. Thus, the DMTF's individual sub-nodes can be very complex with multiple branches in order to define most possible configurations.

In contrast, the Splunk CIM is relatively flat, simple, and flexible, because it defines only the least common denominator of concepts in a given domain rather than all possible concepts in the domain. The Splunk CIM defines fewer concepts than the DMTF CIM in order to give the developer maximum flexibility.

Prerequisites

This manual assumes you are familiar with the full data lifecycle in the Splunk platform. If you are not yet sure how to get your data in, see *Getting Data In* for

more information on how to set up the Splunk platform to accept new data or to learn about the types of data the Splunk platform can index.

Get started

To get started, see Install the Common Information Model Add-on.