Splunk® Common Information Model Add-on Common Information Model Add-on Manual 4.20.0

Intrusion Detection

Generated: 6/28/2022 1:11 pm

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Intrusion Detection

The fields in the Intrusion Detection data model describe attack detection events gathered by network monitoring devices and apps.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Intrusion Detection event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
IDS_Attacks	ids
	attack

Fields for Intrusion Detection event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Abbreviated list of example values" follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
IDS_Attacks	`action`	string	The action taken by the intrusion detection system (IDS).	• required for pytest-splunk-addon • prescribed values: `allowed`, `blocked`
IDS_Attacks	`category`	string	The vendor-provided category of the triggered signature, such as `spyware`. This field is a string. Use a `category_id` field (not included in this data model) for category ID fields that are integer data types.	• recommended • required for pytest-splunk-addon
IDS_Attacks	`dest`	string	The destination of the attack detected by the intrusion detection system (IDS). You can **alias** this from more specific fields not included in this data model, such as `dest_host`, `dest_ip`, or `dest_name`.	recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
IDS_Attacks	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
IDS_Attacks	dest_category	string		
IDS_Attacks	dest_priority	string		
IDS_Attacks	dest_port	number	The destination port of the intrusion.	
IDS_Attacks	dvc	string	The device that detected the intrusion event. You can **alias** this from more specific fields not included in this data model, such as dvc_host, dvc_ip, or dvc_name.	• recommended • required for pytest-splunk-addon
IDS_Attacks	dvc_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
IDS_Attacks	dvc_category	string		
IDS_Attacks	dvc_priority	string		
IDS_Attacks	file_hash	string	A cryptographic identifier assigned to the file object affected by the event.	
IDS_Attacks	file_name	string	The name of the file, such as notepad.exe.	
IDS_Attacks	file_path	string	The path of the file, such as C:\\Windows\\System32\\notepad.exe.	
IDS_Attacks	ids_type	string	The type of IDS that generated the event.	• recommended • required for pytest-splunk-addon • prescribed values: network, host, application, wireless
IDS_Attacks	severity	string	The severity of the network protection event. This field is a string. Use a severity_id field (not included in this data model) for severity ID fields that are integer data types. Also, specific values are required for this field. Use vendor_severity for the vendor's own human readable severity strings, such as Good, Bad, and Really Bad.	• recommended • required for pytest-splunk-addon • prescribed values: critical, high, medium, low, informational
IDS_Attacks	severity_id	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
IDS_Attacks	signature	string	The name of the intrusion detected on the client (the src), such as PlugAndPlay_BO and JavaScript_Obfuscation_Fre. This is a string value. Use a signature_id field (not included in this data model) for numeric indicators.	• recommended • required for pytest-splunk-addon
IDS_Attacks	signature_id	string	The unique identifier or event code of the event signature.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
IDS_Attacks	src	string	The source involved in the attack detected by the IDS. You can **alias** this from more specific fields not included in this data model, such as src_host, src_ip, or src_name.	recommended
IDS_Attacks	src_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
IDS_Attacks	src_category	string		
IDS_Attacks	src_priority	string		
IDS_Attacks	src_port	string	The port number of the source.	
IDS_Attacks	tag	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
IDS_Attacks	transport	string	The OSI layer 4 (transport) protocol of the intrusion, in lower case.	
IDS_Attacks	user	string	The user involved with the intrusion detection event.	recommended
IDS_Attacks	user_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
IDS_Attacks	user_category	string		
IDS_Attacks	user_priority	string		
IDS_Attacks	vendor_product	string	The vendor and product name of the IDS or IPS system that detected the vulnerability, such as HP Tipping Point. This field can be automatically populated by vendor and product fields in your data.	recommended