Splunk® Common Information Model Add-on Common Information Model Add-on Manual 5.3.2

Malware

Generated: 6/03/2024 6:54 pm

Malware

The fields in the Malware data model describe malware detection and endpoint protection management activity. The Malware data model is often used for endpoint antivirus product related events.

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 Malware event and search 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
Malware_Attacks	malware
	attack
Malware_Operations	malware
	operations

Fields for the Malware_Attacks event datasets and Malware_Operations search dataset

Malware_Attacks is mainly for searching against and creating alerts for potential malware infections in your environment. Malware_Operations is mainly for monitoring the health and operational status of your anti-virus or anti-malware solution.

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

The key for using the column titled "Notes" or "Abbreviated list of example values" is as 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	Notes
Malware_Attacks	`action`	string	The action taken by the reporting device.	• recommended • required for pytest-splunk-addon • prescribed values: `allowed`, `blocked`, `deferred`

Dataset name	Field name	Data type	Description	Notes
Malware_Attacks	`category`	string	The category of the malware event, such as `keylogger` or `ad-supported program`. **Note:** This is a string value. Use a `category_id` field for category ID fields that are integer data types (`category_id` fields are optional, so they are not included in this table).	- recommended - required for pytest-splunk-addon
Malware_Attacks	`date`	string	The time of the malware action such as when it was blocked, allowed or deferred, as it was reported by log event.	recommended
Malware_Attacks	`dest`	string	The system that was affected by the malware event. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	- recommended - required for pytest-splunk-addon
Malware_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.	
Malware_Attacks	`dest_category`	string		
Malware_Attacks	`dest_priority`	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.	
Malware_Attacks	`dest_requires_av`	boolean		
Malware_Attacks	`file_hash`	string	The hash of the file with suspected malware.	
Malware_Attacks	`file_name`	string	The name of the file with suspected malware.	required for pytest-splunk-addon
Malware_Attacks	`file_path`	string	The full file path of the file with suspected malware.	required for pytest-splunk-addon
Malware_Attacks	`severity`	string	The severity of the network protection event. Note: This field is a string. Use severity_id 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 - prescribed values: `critical`, `high`, `medium`, `low`, `informational`,
Malware_Attacks	`severity_id`	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
Malware_Attacks	`signature`	string	The name of the malware infection detected on the client (the `dest`). **Note:** This is a string value. Use a `signature_id` field for signature ID fields that are integer data types.	- recommended - required for pytest-splunk-addon - other: such as `Trojan.Vundo`, `Spyware.Gaobot`, `W32.Nimbda`
Malware_Attacks	`signature_id`	string	The unique identifier or event code of the event signature.	
Malware_Attacks	`src`	string		

Dataset name	Field name	Data type	Description	Notes
			The source of the event, such as a DAT file relay server. You can **alias** this from more specific fields, such as `src_host`, `src_ip`, or `src_name`.	
Malware_Attacks	`src_bunit`	string	The business unit of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`src_category`	string	The category of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`src_priority`	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`src_user`	string	The reported sender of an email-based attack.	
Malware_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.	
Malware_Attacks	`user`	string	The user involved in the malware event.	recommended
Malware_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.	
Malware_Attacks	`user_category`	string		
Malware_Attacks	`user_priority`	string		
Malware_Attacks	`url`	string	A URL containing more information about the malware.	
Malware_Attacks	`vendor_product`	string	The vendor and product name of the endpoint protection system, such as `Symantec AntiVirus`. This field can be automatically populated by `vendor` and `product` fields in your data.	recommended
Malware_Operations	`dest`	string	The system where the malware operations event occurred.	• recommended • required for pytest-splunk-addon
Malware_Operations	`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.	
Malware_Operations	`dest_category`	string		
Malware_Attacks Malware_Operations	`dest_nt_domain`	string	The NT domain of the `dest` system, if applicable.	recommended
Malware_Operations	`dest_priority`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	

Dataset name	Field name	Data type	Description	Notes
Malware_Operations	`dest_requires_av`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Operations	`product_version`	string	The product version of the malware operations product.	recommended
Malware_Operations	`signature_version`	string	The version of the malware signature bundle in a signature update operations event.	• recommended • required for pytest-splunk-addon
Malware_Operations	`tag`	string	The tag associated with the malware operations event.	
Malware_Operations	`vendor_product`	string	The vendor product name of the malware operations product.	• recommended • required for pytest-splunk-addon