splunk>dev

TABLE OF CONTENTS

Data models used by ES

ON THIS PAGE

Splunk Enterprise Security leverages many of the data models in the Splunk Common Information Model. See Overview of the Common Information Model in the *Common Information Model Add-on Manual* for an introduction to these data models and full reference information about the fields and tags they use.

In addition to the data models available as part of the Common Information Model add-on, Splunk Enterprise Security implements and uses custom data models.

- Assets and Identities
- Domain Analysis
- Incident Management

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

	Asset lookup fields in the Enterprise Security *User* manual.		
All_Identities	For a list of extracted fields, see Identity lookup fields in the Enterprise Security *User* manual.		
All_Identities	`employedDays`	number	A calculated field based upon the identity startDate field.
All_Identities	`expiredDays`	number	A calculated field based upon the identity endDate field.
Expired_Identity_Activity	`src_user`	string	The source user name.
Expired_Identity_Activity	`src_user_endDate`	time	The source identity's end date.
Expired_Identity_Activity	`user`	string	The source user name.

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

All_Domains	expires	time	The date when the domain will expire.
All_Domains	retrieved	time	The date when the domain information was retrieved.
All_Domains	tag	string	Tags associated with the domain analysis events.
All_Domains	updated	time	The date when the domain registration was updated.
All_Domains	domain	string	The domain or IP that was scanned.
All_Domains	nameservers	string	The list of authoritative name servers for the domain.
All_Domains	registrant	string	The name of the organization or individual that registered the domain name with the registrar.
All_Domains	registrar	string	The name of the organization or individual that maintains the domain name registration.
All_Domains	resolved_domain	string	The domain name that a scanned IP address resolved to.

Incident Management

			with the original events that contributed to the notable event.
Notable_Events	owner	string	The Splunk ID of the owner of the notable event.
Notable_Events	owner_realname	string	The real name of the owner of the notable event in Enterprise Security.
Notable_Events	rule_name	string	The rule name of the notable event.
Notable_Events	security_domain	string	The security domain of the notable event.
Notable_Events	status	string	The status id of the notable event.
Notable_Events	status_group	string	The status group of the notable event.
Notable_Events	tag	string	Splunk tags associated with the notable event.
Notable_Events	urgency		

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			the suppressed notable event.
Suppressed_Notable_Events	suppression	string	The name of the suppression that suppressed this notable event.
Suppressed_Notable_Events	tag	string	Splunk tags associated with the suppressed notable event.
Suppressed_Notable_Events	urgency	string	The urgency of the notable event.
Suppressed_Notable_Events	dest	string	The dest of the notable event.
Suppressed_Notable_Events	src	string	The src of the notable event.
Incident_Review	comment	string	The review comment.
Incident_Review	owner	string	The owner of the notable event.
Incident_Review	reviewer	string	The reviewer of the notable event.

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			associated with the notable event.
Incident_Review	`urgency`	string	The urgency of the notable event.
Correlation_Search_Lookups.Correlation_Searches	See `correlationsearches.conf.spec` for descriptions of these fields.		
Correlation_Search_Lookups.Notable_Owners	`owner`	string	The Splunk user ID of a potential notable owner.
Correlation_Search_Lookups.Notable_Owners	`owner_realname`	string	The real name of a potential notable event owner in Enterprise Security.
Correlation_Search_Lookups.Review_Statuses	See `reviewstatuses.conf.spec` for descriptions of these fields.		
Correlation_Search_Lookups.Security_Domains	`is_enabled`	boolean	Whether or not the security domain is enabled.

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

Lookups.Urgencies			notable event.
Correlation_Search_Lookups.Urgencies	severity	string	The severity of the notable event.
Correlation_Search_Lookups.Urgencies	urgency	string	The urgency of the notable event, calculated based on the priority and severity.
Notable_Event_Suppressions.Suppression_Audit	action	string	The action performed on the suppression (enable/disable).
Notable_Event_Suppressions.Suppression_Audit	signature	string	The signature of the suppression audit event.
Notable_Event_Suppressions.Suppression_Audit	status	string	The status of the suppression audit event (success/failure).
Notable_Event_Suppressions.Suppression_Audit	suppression	string	The name of the suppression.
Notable_Event_Suppressions.Suppression_	user	string	The user who performed the CRUD

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

Suppressions.Suppression_Eventtypes			suppression.
Notable_Event_Suppressions.Suppression_Eventtypes	description	string	The description of the suppression.
Notable_Event_Suppressions.Suppression_Eventtypes	disabled	boolean	If the suppression is enabled or disabled.
Notable_Event_Suppressions.Suppression_Eventtypes	search	string	The notable event suppression search.
Notable_Event_Suppressions.Suppression_Eventtypes	suppression	string	The notable event suppression name.

Risk Analysis

The fields in the Risk Analysis data model describe data generated by the risk framework in Enterprise Security. This data model does not employ any tags.

DATASET NAME	FIELD NAME	DATA TYPE	DESCRIPTION

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations._all	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations.cis20	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations.mitre_attack	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations.mitre_attack.mitre_detection	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations.mitre_attack.mitre_tactic_id	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations.mitre_attack.mitre_technique_id	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

			security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	annotations.nist	string	If you are usin security framework annotations, t field is automatically provided by correlation features of applications li Splunk Enterprise

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			that calculate the risk_score risk_factor_a and risk_factor_m fields for a tot score. This is derived from t fields in the da model.
All_Risk	`control`	string	The value is assigned with PCI-specific r base searches For example, `control=1.2.` for the search PCI - 1.2.3 - Unauthorized Wireless Devi Detected - Ru
All_Risk	`creator`	string	If the modifier was created a hoc, this is the Splunk user ID that created t modifier.

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	dest_category	string	This field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe

			automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	`governance`	string	The value is assigned with PCI-specific r base searche For example, `governance=p i` for the sear of PCI - 1.2.3 - Unauthorized Wireless Devi Detected - Ru
All_Risk	`risk_factor_add`	number	The expressic that calculate

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			that calculate the multiplication for risk factor
All_Risk	`risk_factor_mult_matched`	number	The human readable nam of the risk factors that matched for t `risk_factor_ult` field.
All_Risk	`risk_message`	string	This field provides a wa for customizi risk created from a search
All_Risk	`risk_object`	string	The object fo which the risk modifier appli

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

	unit of the risk_object involved in the event, or who initiated the event. For authentication privilege escalation events this should represent the user targeted the escalation This field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fo this field whe writing add-o

splunk>dev

TABLE OF CONTENTS

	the risk_objec involved in the event, or who initiated the event. For authenticatio privilege escalation events this should represent the user targeted the escalatior This field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field wher writing add-o

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

splunk>dev

TABLE OF CONTENTS

	the risk_objec involved in the event, or who initiated the event. For authenticatio privilege escalation events, this should represent the user priority targeted by th escalation. Th field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			calculating th description field.
All_Risk	src	string	The object tha is the source o the risk event
All_Risk	src_bunit	string	This field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fo this field wher writing add-on
All_Risk	src_category	string	This field is automatically provided by asset and identity

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	tag	string	Splunk tags associated wi the risk modifiers.
All_Risk	threat_object	string	The field in th search results that contains potential indicator of compromise, such as a malicious process, file

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			threat object, which is typically the same type provided by tl ES threat intelligence framework, su as file_hash, domain, ip, an so on.
All_Risk	`user`	string	The user involved in the risk event.
All_Risk	`user_bunit`	string	This field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe writing add-o
All_Risk	user_priority	string	This field is automatically provided by asset and identity correlation features of applications li Splunk Enterprise Security. Do n define extractions fc this field whe

Threat_Activity	dest_priority	string	The destination asset priority.
Threat_Activity	src_bunit	string	The source asset business unit.
Threat_Activity	src_category	string	The source asset category.
Threat_Activity	src_priority	string	The source asset priority.
Threat_Activity	threat_match_field	string	The name of the field for which Enterprise Security found a threat match.
Threat_Activity	threat_match_value	string	The value Enterprise Security matched on.
Threat_Activity	threat_collection	string	The collection of intelligence Enterprise Security matched on.
Threat_Activity	threat_collection_key	string	The KV store key of the intelligence Enterprise Security matched on.
Threat_Activity	threat_key	string	The key for the threat attribution associated with the intelligence Enterprise matched on.
Threat_Activity	dest	string	The destination of the event that Enterprise Security matched on.

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

		TYPE	
All_UEBA_Events	action	string	The recommended action to take in response to a threat in Splunk UBA.
All_UEBA_Events	app	string	A multi-value attribute with the names of all the applications associated with the anomaly or threat.
All_UEBA_Events	category	string	The category or categories associated with an anomaly.
All_UEBA_Events	description	string	The long description of an anomaly.
All_UEBA_Events	dvc	string	A multi-value attribute with the names of all devices associated with an anomaly or threat.
All_UEBA_Events	link	string	The link to view the

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			threat in Splunk UBA.
All_UEBA_Events	uba_event_id	string	The internal id for an anomaly or threat in Splunk UBA.
All_UEBA_Events	uba_event_type	string	An anomaly or threat.
All_UEBA_Events	uba_host	string	The UBA host sending the threats and anomalies.
All_UEBA_Events	url	string	A multi-value attribute with the names of all domains associated with an anomaly.
All_UEBA_Events	user	string	A multi-value attribute with the names of all users associated with an anomaly.
All_UEBA_Events	uba_time	time	The time the anomaly or threat was forwarded to Enterprise Security.

Developer Guide

Reference

Tutorials

Downloads

Examples

Search

			Splunk UBA model that detected the anomaly.
All_UEBA_Events.UEBA_Anomalies	`uba_model_version`	string	The version of the Splunk UBA model that detected the anomaly.