Attribute Dictionary

The Attribute Dictionary defines attributes and includes references to the events and objects in which they are used.

Name	Attribute	Type	Referenced By	Description
Access Complexity	access_complexity_id	Integer	Common Vulnerability Scoring System V2 Object	The access complexity Common Vulnerability Scoring System (CVSS) metric.
Access List	access_list	String Array	Endpoint File Access Activity Event	The list of requested access rights.
Access Mask	access_result	String Array	Endpoint File Access Activity Event	The list of access check results.
Access Mask	access_mask	Integer	Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event	The access mask in a platform-native format.
Accessed	accessed_time	Timestamp	File Object	The time that the file was last accessed.
Accessor	accessor	String	File Object	The name of the user who last accessed the object.
Account UID	account_uid	String	Cloud Object, Extended User Object, User Object	The unique identifier of the account to which the user belongs (e.g. AWS Account ID).
Activity	activity	String	Endpoint Authentication Alert Event, Endpoint File Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event, File Content Protection Event	The original activity that triggered the alert event.
Activity ID	activity_id	Integer	Endpoint Authentication Alert Event, Endpoint DNS Alert Event, Endpoint File Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event, Network DNS Alert Event	The normalized identifier of the activity that triggered the alert event.
Actor Process	actor_process	Process	Account Change Audit Event, Authentication Audit Event, Endpoint Authentication Alert Event, Endpoint Boot	The process that performed the operation or action on the target object. For example, the process that could have

			Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event	created a new file or violated a policy.
Actual Permissions	actual_permissions	Integer	Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event	The permissions that were granted to the in a platform-native format.
Admin User splunk_dev	admin_users	User Array	Admin Group Info Event	The users that belong to the administrative group.
Advertised splunk_dev	is_advertised	Boolean	SMTP Transport Layer Security Object	The indication of whether the TLS protocol is advertised by the SMTP server.
Algorithm	algorithm	String	Fingerprint Object	The original hash algorithm, as reported by the event source, which was used to create the digital fingerprint.
Algorithm ID	algorithm_id	Integer	Fingerprint Object	The identifier of the normalized hash algorithm, which was used to create the digital fingerprint.
Allocated Memory splunk_dev	mem_allocated	Long	Memory Usage Event	The Java Virtual Machine® (JVM) allocated memory (in bytes).
Application Name	app_name	String	Clipboard Content Protection Event, Email Content Protection Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, File Content Protection Event, Information Protection Event, Instant Message Content Protection Event, Network Activity Event, Network Alert	The name of the application that is associated with the event or object.

			Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Policy Override Audit Event, Print/FAX Content Protection Event	
Application UID splunk_dev	app_uid	String	Policy Override Audit Event	The unique identifier of the application that is associated with the event or object.
Application Version splunk_dev	app_ver	String	Policy Override Audit Event	The version of the application that is associated with the event or object.
Assignee	assignee	String	Incident Creation Event, Incident Update Event	The name of the user who is assigned to the incident.
Attack Vector ID	attack_vector_id	Integer	Common Vulnerability Scoring System V2 Object	The attack vector Common Vulnerability Scoring System (CVSS) metric.
Attacks	attacks	Attack Array	Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Alert Event, Endpoint File Alert Event, Endpoint HTTP Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Network Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event, Incident Creation Event Finding Object	An array of attacks associated with an event.
Attempt splunk_dev	attempt	Integer	Email Delivery Activity Event, Email Delivery Alert Event	The delivery attempt.
Attributes	attributes	Integer	File Object	The bitmask value that represents the file attributes.
Auth Protocol	auth_protocol	String	Authentication Audit Event, Endpoint Authentication Alert Event	The authentication protocol as reported by the event source.
Auth Protocol ID	auth_protocol_id	Integer	Authentication Audit Event, Endpoint Authentication Alert Event	The authentication protocol used to create the user session.
Authentication ID	authentication_id	Integer	Common Vulnerability Scoring System V2 Object	The authentication Common Vulnerability Scoring System (CVSS) metric.
Autoscale UID splunk_dev	autoscale_uid	String	Virtual Machine Object	The unique identifier of the cloud autoscale configuration.
Availability Impact ID	availability_impact_id	Integer	Common Vulnerability Scoring System V2 Object	The availability impact Common Vulnerability Scoring System (CVSS) metric.

Average CPU splunk_dev	cpu_average	Long	CPU Usage Event	Average CPU.
BIOS Date	hw_bios_date	String	Device Object	The BIOS date. For example: `03/31/16`.
BIOS Manufacturer	hw_bios_manufacturer	String	Device Object	The BIOS manufacturer. For example: `LENOVO`.
BIOS Version	hw_bios_ver	String	Device Object	The BIOS version. For example: `LENOVO G5ETA2WW (2.62)`.
Base Address	base_address	String	Endpoint Memory Activity Event, Endpoint Memory Alert Event Module Object	The memory address where the module was loaded.
Bytes In	bytes_in	Long	Network Traffic Object	The number of bytes sent from the destination to the source.
Bytes Out	bytes_out	Long	Network Traffic Object	The number of bytes sent from the source to the destination.
CIS 20 List	cis20	String Array	Finding Object	The CIS 20 is a list of 20 actions and practices an organization’s security team can take on such that cyber attacks or malware, are minimized and prevented.
CVE UIDs	cve_uids	String Array	Finding Object, Malware Object	The common vulnerabilities and exposures (CVE) unique identifiers.
CVSSV2	cvssv2	Common Vulnerability Scoring System V2	Compliance Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Alert Event, Endpoint File Alert Event, Endpoint HTTP Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Network Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event	The Common Vulnerabilities Scoring System Version 2 (CVSS V2) base metrics.
Caption	caption	String	Device Object, Device Entity Object	A short description or caption of the device. For example: `Scanner 1` or `Database Manager`.
Categories	categories	String Array	Uniform Resource Locator (URL) Object	A list of categories.
Category	category	String	Base Event Rule Object	The original category of an event or object, as defined by the event source. See specific usage.

Category ID	category_uid	Integer	Base Event	The category identifier of the event.
Certificate Serial Number	cert_serial	String	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The Certificate Serial Number field provides a short form, unique identifier for each Certificate generated by an Certificate Issuer.
Certificate Unique Identifier	cert_uid	String	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The unique identifier of the certificate used to establish the TLS connection. For example, the AWS ARN of the certificate.
Channel splunk_dev	channel	String	Update Event, Update Available Event	The channel that was used to update the component.
Cipher Suite	cipher	String	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The negotiated cipher suite.
City	city	String	Geo Location Object	The name of the city.
Class	class_name	String	Base Event	The class name of the event.
Class	class	String	DNS Answer Object, DNS Query Object, Peripheral Device Object	The class name of the event or object.
Class ID	class_uid	Integer	Base Event	The class identifier describes the attributes available in an event. See specific usage.
Classification IDs	classification_ids	Integer Array	Malware Object	An array of malware classifications.
Classifications	classifications	String Array	Malware Object	The malware classifications.
Cleartext Credentials	is_cleartext	Boolean	Authentication Audit Event, Endpoint Authentication Alert Event	Indicates whether the credentials were passed in clear text. **Note:** True if the credentials were passed in a clear text protocol such as FTP or TELNET, or if Windows detected that a user's logon password was passed to the authentication package in clear text.
Client Cipher Suites	client_ciphers	String Array	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The client cipher suites that were exchanged during the TLS handshake negotiation.
Client TLS Alert	alert	Integer	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The integer value of TLS alert if present. The alerts are defined in the TLS specification in RFC-2246.
Cloud	cloud	Cloud	Event Origin Object	The cloud where the event was originally

				created or logged.
Command Line	cmd_line	String	Job Object, OS Service Object, Process Object, Startup Application Object	The full command line used to launch an application, service, process, or job. For example: `ssh user@10.0.0.10`
Command Name splunk_dev	command_name	String	Command Activity Event	The running process command.
Command UID splunk_dev	command_uid	String	Admin Group Info Event, Command Activity Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, Module Info Event, Module Remediation Event, Network Connection Info Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Prefetch Info Event, Process Info Event, Process Remediation Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, User Info Event, User Session Info Event, User Session Remediation Event	The unique command identifier.
Comment	comment	String	Entity Audit Event, Incident Closure Event, Incident Creation Event, Incident Update Event	The user-provided comment.
Company Name	company_name	String	Digital Signature Object, File Object	The name of the company that published the file. For example: `Microsoft Corporation`.
Compliant Device	is_compliant	Boolean	Device Object	The event occurred on a compliant device.
Component	component	String	Endpoint File Activity Event, Endpoint File Alert Event, Unscannable File Event	The name or relative pathname of a sub-component of the data object, if applicable. For example: `attachment.doc`, `attachment.zip/bad.doc`, or `part.mime/part.cab/part.uue/part.doc`.
Confidence splunk	confidence	Integer	Finding Object	The confidence of the reported finding as a percentage: 0%-100%.

Confidence ID splunk	confidence_id	Integer	Finding Object	The normalized confidence level refers to the accuracy of the rule that created the finding. A rule with a low confidence level means that the detection scope is wide and may create finding reports that may not be malicious in nature.
Confidentiality	confidentiality	String	File Object	The file content confidentiality.
Confidentiality ID	confidentiality_id	Integer	File Object	The file content confidentiality indicator.
Confidentiality Impact	confidentiality_impact_id	Integer	Common Vulnerability Scoring System V2 Object	The confidentiality impact Common Vulnerability Scoring System (CVSS) metric.
Connection Identifier	connection_uid	String	Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint File Activity Event, Endpoint File Alert Event	The network connection identifier.
Connection Info	connection	Network Connection Information	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event	The network connection information.
Container	container	Container	Event Origin Object	The container information.
Context splunk	context	String Array	Finding Object	The list of the context categories of the finding.
Context IDs splunk	context_ids	Integer Array	Finding Object	The list of the context identifiers of the finding.
Continent	continent	String	Geo Location Object	The name of the continent.
Coordinates	coordinates	Float Array	Geo Location Object	A two-element array, containing a longitude/latitude pair. The format conforms with GeoJSON. For example: `[-73.983, 40.719]`.
Correlation UID	correlation_uid	String	Metadata Object	The unique identifier used to correlate events.

Count	count	Integer	Base Event	The number of times that events in the same logical group occurred during the event **Start Time** to **End Time** period.
Country	country	String	Geo Location Object, OS Object	The ISO 3166-1 Alpha-2 country code. For the complete list of country codes see ISO 3166-1 alpha-2 codes. **Note:** The two letter country code should be capitalized. For example: `US` or `CA`.
Create Mask	create_mask	String	Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event	The original Windows mask that is required to create the object.
Creation Time	creation_time	Timestamp	Digital Signature Object, File Object, Job Object, Process Object, Public Key Certificate Object, Session Object	The time that the object was created. See specific usage.
Creator	creator	String	File Object, Session Object	The user that created the object associated with event. See specific usage.
Creator Name	creator_name	String	Incident Creation Event	The name of the user who created the incident.
Current Version splunk_dev	curr_ver	String	Update Event, Update Available Event	The updated version of the code, content, configuration or policy.
Customer UID	customer_uid	String	Event Origin Object, Virtual Machine Object	The unique customer identifier.
DKIM Domain splunk_dev	dkim_domain	String	Email Authentication Object	The DomainKeys Identified Mail (DKIM) signing domain of the email.
DKIM Signature splunk_dev	dkim_signature	String	Email Delivery Activity Event, Email Delivery Alert Event	The DomainKeys Identified Mail (DKIM) signature used by the sending/receiving system.
DKIM Status splunk_dev	dkim	String	Email Authentication Object	The DomainKeys Identified Mail (DKIM) status of the email.
DMARC Override splunk_dev	dmarc_override	String	Email Authentication Object	The Domain-based Message Authentication, Reporting and Conformance (DMARC) override action.
DMARC Policy splunk_dev	dmarc_policy	String	Email Authentication Object	The Domain-based Message Authentication, Reporting and Conformance (DMARC) policy status.
DMARC Status splunk_dev	dmarc	String	Email Authentication Object	The Domain-based Message Authentication, Reporting and Conformance (DMARC) status of the email.

DNS Answer	answers	DNS Answer Array	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Network DNS Activity Event, Network DNS Alert Event	The Domain Name System (DNS) answers.
DNS Header Flags	flags	String Array	DNS Answer Object	The list of DNS answer header flags.
DNS Header Flags	flag_ids	Integer Array	DNS Answer Object	The list of DNS answer header flag IDs.
DNS Opcode	opcode	Integer	DNS Query Object	The DNS opcode specifies the type of the query message.
DNS Query	query	DNS Query	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Network DNS Activity Event, Network DNS Alert Event	The Domain Name System (DNS) query.
DNS RData	rdata	String	DNS Answer Object	The data describing the DNS resource. The meaning of this data depends on the type and class of the resource record.
DNS UID	dns_id	Integer	DNS Answer Object, DNS Query Object	The DNS packet identifier assigned by the program that generated the query. The identifier is copied to the response.
Data	data	JSON	Incident Creation Event, Incident Update Event Enrichment Object, Managed Entity Object, Registry Value Object, TLS Extension Object	The additional data that is associated with the event or object. See specific usage.
Days Left splunk_dev	days_left	Integer	License Lifecycle Event	The number of days that remain before the license or certificate expires.
Default Value	is_default	Boolean	Registry Value Object	The indication of whether the value is from a default value name. For example, the value name could be missing.
Delivered To splunk_dev	delivered_to	Email Address	Email Object	The **Delivered-To** email header field.
Description	desc	String	Incident Creation Event Device Object, Device Entity Object, File Object, Finding Object, Geo Location Object, Group Object, Job Object, Policy Object, Rule Object	The description that pertains to the object or event. See specific usage.
Destination Endpoint	dst_endpoint	Network Endpoint	Authentication Audit Event, Authorization Audit Event, Endpoint Authentication Alert	The network destination endpoint.

			Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Network Activity Event, Network Alert Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	
Destination User	dst_user	User	Account Change Audit Event, Authentication Audit Event, Authorization Audit Event, Endpoint Authentication Alert Event	The user that was a target of an activity.
Detection Start Time	detection_start_time	Timestamp	Finding Report Event	The start time of a detection time period.
Detection Start Time	detection_end_time	Timestamp	Finding Report Event	The end time of a detection time period.
Detection Time splunk_dev	detected_time	Timestamp	Clipboard Content Protection Event, Email Content Protection Event, File Content Protection Event, Information Protection Event, Instant Message Content Protection Event, Print/FAX Content Protection Event	The time that the malware was detected.
Detection UID	detection_uid	String	Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Alert Event, Endpoint File Alert Event, Endpoint HTTP Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Network Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event	The associated unique detection event identifier. For example: detection response events include the **Detection ID** of the original event.
Detections splunk_dev	num_detections	Integer	Scan Event	The number of detections.
Developer UID	developer_uid	String	Digital Signature Object	The developer ID on the certificate that signed the file.
Device	device	Device	Event Origin Object	The device that reported the event.
Device Entities splunk	device_entities	Device Entity Array	Finding Report Event	The devices that are identified in reported the events.
Digital Signature	signature	Digital Signature	File Object	The digital signature of the file.

Direction	direction	String	Network Connection Information Object	The direction of the initiated connection, traffic, or email.
Direction ID	direction_id	Integer	File Content Protection Event Email Object, Network Connection Information Object	The direction of the initiated connection, traffic, or email.
Displayed Text splunk_dev	displayed_text	String	Policy Override Audit Event	The information that is displayed to the user that describes the impact of a client side override action.
Disposition	disposition	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Finding Report Event, Folder Info Event, Folder Remediation Event, Incident Associate Event, Incident Closure Event, Incident Creation Event, Incident Update Event, Information Protection Event, Instant	The disposition of the event, as defined by the event source.

			Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Disposition ID	disposition_id	Integer	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory	The disposition ID of the event.

			Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Finding Report Event, Folder Info Event, Folder Remediation Event, Incident Associate Event, Incident Closure Event, Incident Creation Event, Incident Update Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	

Domain	domain	String	Device Object, Device Entity Object, Endpoint Object, Extended User Object, Network Object, Network Endpoint Object, SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object, User Object, User Entity Object	The name of the domain.
Duration	duration	Integer	Base Event	The event duration or aggregate time, the amount of time the event covers from `start_time` to `end_time` in milliseconds.
Effective Date splunk_dev	effective_time	Timestamp	Policy Object	The date and time that the specific policy and rule was applied and became operational.
Email splunk_dev	email	Email	Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event	The email object.
Email Address	email_addr	Email Address	Extended User Object, User Object	The user's email address.
Email Authentication splunk_dev	email_auth	Email Authentication	Email Delivery Activity Event, Email Delivery Alert Event	The SPF, DKIM and DMARC attributes of an email.
Email UID splunk_dev	email_uid	String	Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event	The unique identifier of the email, used to correlate related email alert and activity events.
Emails splunk	emails	Email Address Array	User Entity Object	A list of emails of the person.
End Time	end_time	Timestamp	Base Event License Information Object, User Entity Object	The end time of a time period. See specific usage.
Enrichments	enrichments	Enrichment Array	Base Event	The additional information from an external data source, which is associated with the event. For example add location information for the IP address in the DNS answers: `[{"name": "answers.ip", "value": "92.24.47.250", "type": "location", "data": {"city": "Socotra", "continent": "Asia", "coordinates": [-25.4153, 17.0743], "country": "YE", "desc": "Yemen"}}]`
Entity	entity	Managed	Entity Audit Event	The managed entity that is being acted

		Entity		upon.
Entity Result	entity_result	Managed Entity	Entity Audit Event	The updated managed entity.
EtherType	ether_type	Integer		The EtherType indicates which protocol is encapsulated in the payload of an Ethernet frame.
Event ID	event_uid	Integer	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Finding Report Event, Folder Info Event, Folder Remediation Event, Incident Associate Event, Incident Closure Event, Incident Creation Event, Incident Update Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation	The event ID identifies the event's semantics and structure. The value is calculated by the logging system as: `class_id * 100 + disposition_id`.

			Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Event Name	event_name	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint	The event name, as defined by the event_uid.

			Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Finding Report Event, Folder Info Event, Folder Remediation Event, Incident Associate Event, Incident Closure Event, Incident Creation Event, Incident Update Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Event Source	event_source	Event Source		The event source from which the event originates.

Event Source splunk	source	String	Splunk Fields Object	The name of the file, stream, or other input from which the event originates. For data monitored from files and directories, the value of source is the full path, such as `/archive/server1/var/log/messages.0` or `/var/log/`. The value of source for network-based data sources is the protocol and port, such as UDP:514.
Event Time	event_time	String	Base Event	The event occurrence time, representing the time when the event was created by the event producer. **Note:** The format is ISO 8601: `yyyy-MM-dd'T'HH:mm:ss.SSSXXX`. For example: `2021-07-22T14:41:17.128-07:00`
Event Timestamp splunk	timestamp	String	Splunk Fields Object	The event's timestamp, which specifies the time at which the event occurred.
Events per Second splunk_dev	throughput_eps	Integer	Throughput Event	The number of events processed per second.
Exception splunk_dev	status_exception	String	Application Log Event, Status Event	The operating system exception message.
Exit Code	exit_code	Integer	Endpoint Process Activity Event, Endpoint Process Alert Event	The exit code reported by a process when it terminates. The convention is that zero indicates success and any non-zero exit code indicates that some error occurred.
Expiration Time	expiration_time	Timestamp	Public Key Certificate Object, Session Object	The expiration time. See specific usage.
Extended Attributes	xattributes	Object	File Object, Process Object	An unordered collection of zero or more name/value pairs where each pair represents a file or folder extended attribute. For example: Windows alternate data stream attributes (ADS stream name, ADS size, etc.), user-defined or application-defined attributes, ACL, owner, primary group, etc. Examples from DCS: • **ads_name** • **ads_size** • **dacl** • **owner** • **primary_group** • **link_name** - name of the link associated to the file. • **hard_link_count** - the number of links that are associated to the file.

Facility	facility	String	Event Source Object	The subsystem or application that is providing the event data.
Facility Detail	facility_detail	String	Event Source Object	Additional detail about the source facility. For example, details could include a the name of a particular application instance (such as a database name) or a path to a monitored log file.
Facility UID	facility_uid	String	Event Source Object	The unique identifier of the facility.
Feature	feature	Feature	Event Origin Object	The feature that reported the event.
File	file	File	Email File Activity Event, Email File Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, File Content Protection Event, File Info Event, File Remediation Event, Policy Override Audit Event, Print/FAX Content Protection Event, Unscannable File Event Job Object, Module Object, OS Service Object, Process Object, Startup Application Object	The file that pertains to the event or object. See specific usage.
File Diff	file_diff	String	Endpoint File Activity Event, Endpoint File Alert Event	File content differences used for change detection. For example, a common use case is to identify itemized changes within INI or configuration/property setting values.
File Result	file_result	File	Endpoint File Activity Event, Endpoint File Alert Event	The result of the file change. It should contain the new values of the changed attributes.
Finding splunk	finding	Finding	Finding Report Event	The finding reported by detection or analytics
Fingerprints	fingerprints	Fingerprint Array	Digital Signature Object, File Object	An array of fingerprint objects associated with the certificate.
First Name splunk	first_name	String	User Entity Object	The first name of a person.
First Seen splunk_dev	first_seen_time	Timestamp	File Content Protection Event	The initial detection time of the malware.
Folder	folder	File	Endpoint Folder Activity Event, Folder Info Event, Folder Remediation Event	The folder that pertains to the event.
Folder Result	folder_result	File	Endpoint Folder Activity Event	The result of the folder change. It sould

				contain the new values of the changed attributes.
Free Memory splunk_dev	mem_free	Long	Memory Usage Event	The Java Virtual Machine® (JVM) free memory (in bytes).
From splunk_dev	from	Email Address	Email Object	The email header From values, as defined by RFC 5322.
Full Name	full_name	String	Extended User Object	The full name of a user.
Function Name	function_name	String	Module Object	The entry-point function of the module. The system calls the entry-point function whenever a process or thread loads or unloads the module.
Gateway IP Address	gateway_ip	IP Address	Network Information Object	The gateway IP address. For example: `10.0.0.1`.
Gateway MAC Address	gateway_mac	MAC Address	Network Information Object	The gateway media access control (MAC) address.
Geo Location	location	Geo Location	Device Object, Device Entity Object, Endpoint Object, Network Object, Network Endpoint Object, User Entity Object	The geographical location usually associated with an IP address.
Group	group	Group	Admin Group Info Event Device Object, Device Entity Object, Policy Object	The group object associated with an entity such as user, policy, or rule.
Group Name	group_name	String	Resource Object	The name of the group that the resource belongs to.
Groups	groups	Group Array	Extended User Object, User Object, User Entity Object, Virtual Machine Object	The groups to which user belongs.
HTTP Arguments	args	String	HTTP Request Object	The arguments sent along with the HTTP request.
HTTP Content Type	content_type	String	HTTP Response Object	The request header that identifies the original media type of the resource (prior to any content encoding applied for sending).
HTTP Headers	http_headers	HTTP Header Array	HTTP Request Object	Additional HTTP headers of an HTTP request or response.
HTTP Method	http_method	String	Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The HTTP request method indicates the desired action to be performed for a given resource. Expected values: • TRACE

			HTTP Request Object	- CONNECT - OPTIONS - HEAD - DELETE - POST - PUT - GET
HTTP Query String	query_string	String	Uniform Resource Locator (URL) Object	The query portion of the URL. For example: the query portion of the URL `http://www.example.com/search?q=bad&sort=date` is `q=bad&sort=date`.
HTTP Referrer	referrer	String	HTTP Request Object	The request header that identifies the address of the previous web page, which is linked to the current web page or resource being requested.
HTTP Request	http_request	HTTP Request	Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The HTTP Request made to a web server.
HTTP Response	http_response	HTTP Response	Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The HTTP Response from a web server to a requester.
HTTP Status	http_status	Integer	Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The Hypertext Transfer Protocol (HTTP) status code returned to the client.
HTTP User-Agent	user_agent	String	HTTP Request Object	The request header that identifies the operating system and web browser.
HTTP Version	http_version	String	HTTP Request Object	The Hypertext Transfer Protocol (HTTP) version.
Handshake Time	handshake_time	Integer	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The amount of total time for the TLS handshake to complete after the TCP connection is established, including client-side delays, in milliseconds.
Home	home_dir	Path Name	Extended User Object	The user's home folder.
Host splunk	host	String	Splunk Fields Object	The originating hostname or IP address of the network device that generated the event.
Hostname	hostname	Hostname	DNS Query Object, Device Object, Endpoint Object, HTTP Request Object, Network Endpoint Object, Network Information Object, Network Proxy Object, Uniform Resource Locator (URL) Object	The hostname of an endpoint or a device.

Hypervisor	hypervisor	String	Device Object	The name of the hypervisor running on the device. For example, `Xen`, `VMware`, `Hyper-V`, `VirtualBox`, etc.
IMEI	imei	String	Device Object	The International Mobile Station Equipment Identifier that is associated with the device.
IP Address	resolved_ip	IP Address		The resolved IP address, in either IPv4 or IPv6 format. For example, Layer 4 load balancer translated IP address.
IP Address	ip	IP Address	Device Object, Endpoint Object, Network Endpoint Object, Network Information Object, Network Proxy Object	The IP address, in either IPv4 or IPv6 format.
IP Version	protocol_ver	String	Network Connection Information Object	The Internet Protocol version.
IP Version ID	protocol_ver_id	Integer	Network Connection Information Object	The Internet Protocol version identifier.
ISP	isp	String	Geo Location Object	The name of the Internet Service Provider (ISP).
Idle CPU splunk_dev	cpu_idle	Long	CPU Usage Event	Idle CPU.
Image	image	Image	Container Object, Virtual Machine Object	The image used as a template to run a container or virtual machine.
Image Tag	tag	String	Image Object	The image tag. For example: `1.11-alpine`.
Impact splunk	impact	Integer	Finding Object	The impact of the finding, valid range 0-100.
Impact ID splunk	impact_id	Integer	Finding Object	The normalized impact of the finding.
Incident UID splunk	incident_uid	String	Incident Associate Event, Incident Closure Event, Incident Creation Event, Incident Update Event	If the event pertains to an incident, the incident unique identifier.
Index splunk	index	String	Splunk Fields Object	The name of the index in which a given event is indexed.
Injection Type	injection_type	String	Endpoint Process Activity Event, Endpoint Process Alert Event	The process injection method.
Injection Type ID	injection_type_id	Integer	Endpoint Process Activity Event, Endpoint Process Alert Event	The normalized process injection type identifier.
Instance ID	instance_uid	String	Device Object, Endpoint Object, Network Endpoint Object	The unique identifier of a VM instance.

Integrity	integrity	String	Process Object	The process integrity (Windows only).
Integrity Impact	integrity_impact_id	Integer	Common Vulnerability Scoring System V2 Object	The integrity impact Common Vulnerability Scoring System (CVSS) metric.
Integrity Level	integrity_id	Integer	Process Object	The process integrity level (Windows only).
Intermediate IP Addresses	intermediate_ips	IP Address Array	Network Endpoint Object	The intermediate IP Addresses. For example, the IP addresses in the HTTP X-Forwarded-For header.
Interpreter splunk_dev	interpreter	String	Command Activity Event	The script interpreter used. For example: "CMD", "POWERSHELL", "VBSCRIPT", "JAVASCRIPT".
Issuer Name	issuer_name	String	Digital Signature Object, Public Key Certificate Object	The certificate issuer name.
Issuer Organization splunk_dev	issuer_organization	String	Public Key Certificate Object	The certificate issuer organization.
Job	job	Job	Endpoint Scheduled Job Activity Event, Job Info Event, Job Remediation Event	The job object that pertains to the event.
Kernel	kernel	Kernel Resource	Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Kernel Object Info Event, Kernel Remediation Event	The kernel resource object that pertains to the event.
Key Length	key_length	Integer	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The length of the encryption key.
Kill Chain Phase	kill_chain_phase	String	Finding Object	The Cyber Kill Chain® phase.
Kill Chain Phase ID	kill_chain_phase_id	Integer	Finding Object	The Cyber Kill Chain® phase identifier.
Kilobytes per Second splunk_dev	throughput_kbps	Integer	Throughput Event	The number of kilobytes of data processed per second (kB/s).
Label splunk_dev	label	String	Policy Object	The label set for the policy.
Labels	labels	String Array	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event,	The list of labels attached to an event, object, or attribute.

			Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event,	

			Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event Cloud Service Object, Device Entity Object, Image Object, Network Object, User Entity Object	
Language	lang	String	OS Object, Product Object	The two letter lower case language codes, as defined by ISO 639-1. For example: `en` (English), `de` (German), or `fr` (French).
Last Name splunk	last_name	String	User Entity Object	The last name of a person.
Last Run	last_run_time	Timestamp	Prefetch Info Event Job Object	The last run time of application or service. See specific usage.
Latency	latency	Integer	HTTP Response Object	TODO: The HTTP response latency. In seconds, milliseconds, etc.?
License splunk_dev	license	License Information	License Count Event, License Lifecycle Event	The license information.
Line Count splunk	linecount	Integer	Splunk Fields Object	The number of lines an event contains. That is the number of lines an event contains before it is indexed.
Lineage	lineage	String Array	Process Object	The lineage of the process.
Load Type	load_type	String	Module Object	The load type describes how the module was loaded in memory.
Load Type ID	load_type_id	Integer	Module Object	The load type identifies how the module was loaded in memory.
Loaded Module splunk_dev	loaded_module_name	String	OS Service Object	The name of the module loaded by the service.
Loaded Modules	loaded_modules	String Array	Process Object	The list of loaded module names.
Log Device`	log_device	Device		The device that logged the event.
Log Name	log_name	String	Metadata Object	The name of the database, index, or archive where the event was logged by the logging system.

Logged Time	log_time	Timestamp	Metadata Object	The time when the logging system collected and logged the event. This attribute is distinct from the event time in that event time typically contain the time extracted from the original event. Most of the time, these two times will be different.
Logon Process	logon_process	Process	Authentication Audit Event, Endpoint Authentication Alert Event	The trusted process that validated the authentication credentials.
Logon Type	logon_type	String	Authentication Audit Event, Endpoint Authentication Alert Event	The logon type.
Logon Type ID	logon_type_id	Integer	Authentication Audit Event, Endpoint Authentication Alert Event	The normalized logon type identifier.
MAC Address	mac	MAC Address	Device Object, Endpoint Object, Network Endpoint Object, Network Information Object	The Media Access Control (MAC) address that is associated with the network interface.
MD5	md5	File Hash	File Object	The MD5 checksum of the file content.
MIME type	mime_type	String	File Object	The Multipurpose Internet Mail Extensions (MIME) type of the file, if applicable.
Malware	malware	Malware	Email Delivery Alert Event, Email File Alert Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Alert Event, Endpoint File Alert Event, Endpoint HTTP Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Network Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event, Network Alert Event, Network DNS Alert Event, Network HTTP Alert Event	The primary malware identified by the event. **Note:** The primary malware may be the first malware found by the detection engine, or it may be the most severe malware found.
Managed By splunk	managed_by	String	Device Entity Object, User Entity Object	The distinguished name of the user that is assigned to manage this object.
Managed Device	is_managed	Boolean	Device Object	The event occurred on a managed device.
Maximum Memory splunk_dev	mem_max	Long	Memory Usage Event	The Java Virtual Machine® (JVM) maximum memory (in bytes).
Message	message	String	Base Event	The description of the event.

			HTTP Response Object	
Message UID splunk_dev	message_id	String	Email Object	The email header Message-Id value, as defined by RFC 5322.
Metadata	metadata	Metadata	Base Event	The metadata associated with the event.
Model	model	String	Peripheral Device Object	The peripheral device model.
Modified Time	modified_time	Timestamp	Incident Update Event File Object, Metadata Object, Registry Key Object, Registry Value Object	The time when the object was last modified. See specific usage.
Modifier	modifier	String	Incident Update Event File Object	The user that last modified the object associated with the event. See specific usage.
Module	module	Module	Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Module Info Event, Module Remediation Event	The module that pertains to the event.
Module Type splunk_dev	module_type	String	Module Info Event, Module Remediation Event	The type of module.
Multi Factor Authentication	mfa	Boolean	Session Object	The Multi Factor Authentication was used during authentication.
NIST List	nist	String Array	Finding Object	The NIST Cybersecurity Framework recommendations for managing the cybersecurity risk.
Name	name	String	Compliance Scan Event, Prefetch Info Event, Scan Event Cloud Service Object, Container Object, Device Object, Device Entity Object, Endpoint Object, Enrichment Object, Extended User Object, Feature Object, File Object, Group Object, HTTP Header Object, Image Object, Job Object, Kernel Resource Object, License Information Object, Malware Object, Managed Entity Object, Network Object, Network Endpoint Object, Network Information Object, OS Object, OS Service Object, Observable Object, Peripheral Device Object, Policy Object, Printer Object, Process Object, Product Object, Registry Value Object, Resource Object, Rule Object, Startup	The name of the entity. See specific usage.

			Application Object, User Object, Virtual Machine Object	
Names splunk	names	String Array	User Entity Object	The names of the person.
Namespace	namespace	String	Network Object, Network Information Object, User Entity Object	The namespace is useful in merger or acquisition situations. For example, when similar entities exists that you need to keep separate.
Network Interface ID	interface_uid	String	Device Object, Endpoint Object, Network Endpoint Object	The unique identifier of the network interface.
Network Zone	zone	String	Device Object, Endpoint Object, Network Endpoint Object	The network zone or LAN segment.
Networks Information	networks_info	Network Information Array	Networks Info Event Device Object, Device Entity Object	The network information objects that are associated with the device, one for each MAC address/IP address combination. **Note:** The first element of the array is the network information that pertains to the event.
Next Run	next_run_time	Timestamp	Job Object	The next run time. See specific usage.
Nickname splunk	nickname	String	User Entity Object	The nickname of a person.
Normalized Path	normalized_path	Path Name	File Object	The CSIDL normalized path name. For example: `CSIDL_SYSTEM\svchost.exe` (Windows only).
OS	os	OS	Device Object	The device operation system.
OS Bits	bits	Integer	OS Object	The number of processor bits. For example: `64` or `128`.
OS Build	build	String	OS Object	The operating system build number.
OS Edition	edition	String	OS Object	The operating system edition. For example: `Professional`.
OS Service splunk_dev	os_service	OS Service	Service Info Event, Service Remediation Event	The OS service that pertains to the event.
OS Service Pack	sp_name	String	OS Object	The name of the latest Service Pack.
OS Service Pack Version	sp_ver	String	OS Object	The version number of the latest Service Pack.
Observables	observables	Observable Array	Base Event	The observables associated with the event.

On Premises	is_on_premises	Boolean	Geo Location Object	The indication of whether the location is on premises.
Open Mask	open_mask	Integer	Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event	The Windows options needed to open a registry key.
Org ID	org_uid	String	Cloud Object, Extended User Object, User Object	The unique identifier of the organization to which the user belongs. For example, Active Directory or AWS Org ID.
Org Unit	org_unit	String	Device Object, Device Entity Object, Network Object, User Entity Object	The name of the organization to which the user belongs.
Origin	origin	Event Origin	Base Event	The origin of the event, where the event was created.
Original Name	original_name	String	File Object	The original name of the file.
Other Malware	other_malware	Malware Array	Email Delivery Alert Event, Email File Alert Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Alert Event, Endpoint File Alert Event, Endpoint HTTP Alert Event, Endpoint Kernel Alert Event, Endpoint Memory Alert Event, Endpoint Module Alert Event, Endpoint Network Alert Event, Endpoint Peripheral Device Alert Event, Endpoint Process Alert Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Alert Event, Network Alert Event, Network DNS Alert Event, Network HTTP Alert Event	The additional malware that was detected.
Override Duration splunk_dev	override_duration	Integer	Policy Override Audit Event	The length in minutes for the override action to remain in place until restored upon expiration of time. If not provided it implies infinite duration of policy enforcement or until such time as another policy action occurs.
Owner	owner	String	File Object	The user that owns the file.
Owner Email splunk_dev	owner_email	Email Address	Clipboard Content Protection Event, Email Content Protection Event, File Content Protection Event, Information Protection Event, Instant Message Content Protection Event, Print/FAX Content Protection Event	The email address of the data owner.
Owner Name	owner_name	String	Clipboard Content Protection Event, Email Content Protection Event, File Content Protection Event, Information Protection	The name of the service or user account that owns the resource.

			Event, Instant Message Content Protection Event, Print/FAX Content Protection Event Device Entity Object, Network Object, Resource Object	
Packets In	packets_in	Long	Network Traffic Object	The number of packets sent from the destination to the source.
Packets Out	packets_out	Long	Network Traffic Object	The number of packets sent from the source to the destination.
Parent Categories	parent_categories	String Array	Uniform Resource Locator (URL) Object	An array of parent URL categories.
Parent Folder	parent_folder	Path Name	File Object	The parent folder in which the file resides. For example: `c:\windows\system32`
Parent Process	parent_process	Process	Process Object	The parent process of the `actor` process.
Path	path	Path Name	File Object, HTTP Request Object, Image Object, Kernel Resource Object, Product Object, Registry Key Object, Registry Value Object, Uniform Resource Locator (URL) Object	The path that pertains to the event or object. See specific usage.
Peripheral Device	peripheral_device	Peripheral Device	Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Peripheral Device Info Event	The peripheral device that triggered the event.
Personal Device	is_personal	Boolean	Device Object	The event occurred on a personal device.
Phones splunk	phones	String Array	User Entity Object	The list of phone numbers.
Policy splunk_dev	policy	Policy	Clipboard Content Protection Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, File Content Protection Event, Information Protection Event, Instant Message Content Protection Event, Network Policy Violation Event, Policy Change Event, Policy Override Audit Event, Print/FAX Content Protection Event, Scan Event, Unscannable File Event	The policy object.
Port	port	IP Port	HTTP Request Object, Network Endpoint Object, Network Proxy Object, Uniform Resource Locator (URL) Object	The IP port number associated with a connection. See specific usage.
Postal Code	postal_code	String	Geo Location Object	The postal code of the location.

Prefix	prefix	String	HTTP Request Object	The domain prefix.
Previous Version splunk_dev	prev_ver	String	Update Event, Update Available Event	The pre-update version of the code, content, configuration or policy.
Print Job splunk_dev	print_job	String	Print/FAX Content Protection Event	The name of the print or FAX job.
Printer splunk_dev	printer	Printer	Print/FAX Content Protection Event	The printer object.
Priority splunk	priority	Integer	Incident Closure Event, Incident Creation Event, Incident Update Event Device Entity Object, Network Object, User Entity Object	The original priority, as defined by the data source.
Priority ID splunk	priority_id	Integer	Incident Closure Event, Incident Creation Event, Incident Update Event Device Entity Object, Network Object, User Entity Object	The normalized priority. See specific usage.
Privileges	privileges	String Array	Authorization Audit Event Extended User Object, Group Object	The user or group privileges.
Process	process	Process	Application Log Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Module Info Event, Network Connection Info Event, Process Info Event, Process Remediation Event, Status Event	The process object.
Process ID	pid	Integer	Process Object	The process identifier, as reported by the operating system. Process ID (PID) is a number used by the operating system to uniquely identify an active process.
Processed Time	processed_time	Timestamp	Metadata Object	The event processed time, such as an ETL operation.
Processor Type	hw_cpu_type	String	Device Object	The processor type. For example: `x86 Family 6 Model 37 Stepping 5`.
Product	product	Product	Event Origin Object, File Object	The product that reported the event.
Project ID	project_uid	String	Cloud Object	Cloud project identifier.
Protocol Name	protocol_name	String	Network Connection Information Object	The TCP/IP protocol name in lowercase, as defined by the Internet Assigned Numbers Authority (IANA). See Protocol Numbers. For example: `tcp` or `udp`.

Protocol Number	protocol_num	Integer	Network Connection Information Object	The TCP/IP protocol number, as defined by the Internet Assigned Numbers Authority (IANA). Use -1 if the protocol is not defined by IANA. See Protocol Numbers. For example: 6 for TCP and 17 for UDP.
Provider	provider	String	Cloud Object, Device Entity Object, Enrichment Object, Geo Location Object, Malware Object, Uniform Resource Locator (URL) Object, User Entity Object	The origin of information associated with the event. See specific usage.
Proxy	proxy	Network Proxy	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Network Activity Event, Network Alert Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	If a proxy connection is present, the connection from the client to the proxy server.
Public IP	public_ip	IP Address	Device Object	The public IP address. **Note:** The **Device Public IP** is populated with the value of the *x-forwarded-for* message header, if present. .
Public Key Certificate splunk_dev	public_key_cert	Public Key Certificate	Public Key Certificate Lifecycle Event	The Public Key Certificate used to prove the ownership of a public key.
Public Network splunk	is_public	Boolean	Network Object	The indication of whether the network interface is a public IP address.
Punctuation Pattern splunk	punct	String	Splunk Fields Object	The punctuation pattern that is extracted from an event. The punctuation pattern is unique to types of events.
Quarantine UID	quarantine_uid	String	Email Delivery Alert Event, Email File Alert Event, Email URL Alert Event, Endpoint File Alert Event, Endpoint Module Alert Event, Endpoint Process Alert Event	The unique identifier of the item that was quarantined or restored from quarantine.
Query Time	query_time	Timestamp	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Network DNS Activity Event, Network DNS Alert Event	The Domain Name System (DNS) query time.
Raw Data	raw_data	String	Base Event	The event data as received from the event source.
Raw Header splunk_dev	raw_header	String	Email Authentication Object	The email authentication header.

Recovery Key UID splunk_dev	recovery_key_uid	String	BitLocker Event	The unique identifier of the recovery key of the volume.
Reference Event Code	ref_event_code	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy	The event code/ID, as defined by the event source. It is used to identify the type of event. For example, the Windows event Code or ID.

			Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Reference Event ID	ref_event_uid	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry	The event instance identifier, as defined by the event source. It is the index of the event in an external event log. For example, the Windows EventRecordID.

			Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Incident Associate Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event Finding Object	
Reference Event Name	ref_event_name	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL	The event name, as defined by the event source.

			Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful	

			Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Reference UID	ref_uid	String	Device Object, Device Entity Object, Extended User Object, User Entity Object	The reference to a unique identifier, managed by an external system.
Region	region	String	Cloud Object, Geo Location Object, Virtual Machine Object	The name or the code of a region. See specific usage.
Registry Key	reg_key	Registry Key	Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Registry Key Info Event, Registry Key Remediation Event	The registry key.
Registry Key Result	reg_key_result	Registry Key	Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event	The result of the registry key change. It should contain the new values of the changed attributes.
Registry Value	reg_value	Registry Value	Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Registry Value Info Event, Registry Value Remediation Event	The registry value.
Registry Value Result	reg_value_result	Registry Value	Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event	The result of the registry value change. It should contain the new values of the changed attributes.
Remote	is_remote	Boolean	Authentication Audit Event, Endpoint Authentication Alert Event, User Session Info Event	The indication of whether the session is remote.
Reply To splunk_dev	reply_to	Email Address	Email Object	The email header Reply-To values, as defined by RFC 5322.
Reputation Score	rep_score	Integer	Network Information Object, Uniform Resource Locator (URL) Object	The original reputation score as reported by the event source.
Reputation Score ID	rep_score_id	Integer	Network Information Object, Uniform Resource Locator (URL) Object	The normalized reputation score identifier.
Request Headers	request_headers	HTTP Header		The additional information associated with and the HTTP request.
Request Object splunk_dev	request_obj	JSON	Unsuccessful Discovery Event, Unsuccessful Remediation Event	An object describing the request.
Requested Permissions	requested_permissions	Integer	Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event	The permissions mask that were requested by the process.

Resolutions splunk_dev	num_resolutions	Integer	Scan Event	The number of items that were resolved.
Resource	resource	Resource	Endpoint Resource Activity Event	The target resource.
Resource ID	resource_uid	String	Cloud Object	The unique identifier of a cloud resource. For example, S3 Bucket name, EC2 Instance Id.
Resource Type	resource_type	String	Uniform Resource Locator (URL) Object	The context in which a resource was retrieved in a web request.
Response Action splunk_dev	response_action	String	Clipboard Content Protection Event, Email Content Protection Event, File Content Protection Event, Information Protection Event, Instant Message Content Protection Event, Print/FAX Content Protection Event	The information protection response action taken.
Response Code	rcode	Integer	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Network DNS Activity Event, Network DNS Alert Event	The DNS server response code. See RFC-6895.
Response Code	code	Integer	HTTP Response Object	The numeric response sent to a HTTP request.
Response Headers	response_headers	HTTP Header		The additional information associated with and the HTTP response.
Response Length	length	Integer	HTTP Response Object	The HTTP response length, in number of bytes.
Response Time	response_time	Timestamp	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Network DNS Activity Event, Network DNS Alert Event	The Domain Name System (DNS) response time.
Risk	risk	Float	Common Vulnerability Scoring System V2 Object	The Common Vulnerability Scoring System (CVSS) calculated risk.
Risk Level	risk_level	String	Device Object, Extended User Object, Finding Object	The normalized risk level.
Risk Level ID	risk_level_id	Integer	Device Object, Extended User Object, Finding Object	The normalized risk level id.
Risk Score	risk_score	Integer	Device Object, Extended User Object, Finding Object	The original risk score as reported by the event source.
Role	roles	String	Observable Object	The role names of the observable.
Role IDs	role_ids	Integer Array	Observable Object	The role identifiers that classify the observable.

Rule	rule	Rule	Compliance Event, Finding Report Event, Incident Closure Event, Incident Creation Event, Incident Update Event, Network Alert Event, Network DNS Alert Event, Network HTTP Alert Event Policy Object	The rules that reported the events.
Rules splunk_dev	rules	Rule Array	Policy Object	The additional rules that are associated with the policy.
Run Count splunk_dev	run_count	Integer	Prefetch Info Event	The prefetch file run count.
Run State	run_state	String	Job Object, OS Service Object	The state of the job or service. See specific usage.
Run State ID	run_state_id	Integer	Job Object, OS Service Object	The state of the job or service. See specific usage.
Run-As User	run_as	User	Process Object	The user account the process is running as.
Runtime	runtime	String	Container Object	The runtime managing this container.
SHA-1	sha1	File Hash	File Object	The SHA-1 checksum of the file content.
SHA-256	sha2	File Hash	File Object	The SHA-256 checksum of the file content.
SMTP Banner splunk_dev	banner	String	Email Delivery Activity Event, Email Delivery Alert Event	The initial SMTP connection response that a messaging server receives after it connects to a email server.
SMTP From splunk_dev	smtp_from	Email Address	Email Object	The value of the SMTP MAIL FROM command.
SMTP Hello splunk_dev	smtp_hello	String	Email Object	The value of the SMTP HELO or EHLO command.
SMTP TLS splunk_dev	smtp_tls	SMTP Transport Layer Security	Email Object	The SMTP Transport Layer Security (TLS) attributes.
SMTP TLS Policy splunk_dev	policy_id	Integer	SMTP Transport Layer Security Object	The SMTP Transport Layer Security (TLS) policy.
SMTP To splunk_dev	smtp_to	Email Address Array	Email Object	The value of the SMTP envelope RCPT TO command.

SPF Status splunk_dev	spf	String	Email Authentication Object	The Sender Policy Framework (SPF) status of the email.
SSID	ssid	String	Network Information Object	The name of the wireless network, or Service Set Identifier (SSID).
Sandbox	sandbox	String	Process Object	The name of the containment jail (i.e., sandbox). For example, hardened_ps, high_security_ps, oracle_ps, netsvcs_ps, or default_ps.
Scan Name splunk_dev	scan_name	String	File Content Protection Event, Unscannable File Event	The administrator-supplied or application-generated name of the scan. For example: • "Home office weekly user database scan" • "Scan folders for viruses" • "Full system virus scan"
Scan Type splunk_dev	scan_type	String	File Content Protection Event	The type of scan.
Scan UID splunk_dev	scan_uid	String	Admin Group Info Event, Compliance Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, Module Info Event, Module Remediation Event, Network Connection Info Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Prefetch Info Event, Process Info Event, Process Remediation Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, User Info Event, User Session Info Event, User Session Remediation Event	The unique identifier of a scan job.
Scanned Files splunk_dev	num_files	Integer	Scan Event	The number of files scanned.
Scanned Folders splunk_dev	num_folders	Integer	Scan Event	The number of folders scanned.
Scanned Network Items splunk_dev	num_network	Integer	Scan Event	The number of network items scanned.

Scanned Processes splunk_dev	num_processes	Integer	Scan Event	The number of processes scanned.
Scanned Registry Items splunk_dev	num_registry	Integer	Scan Event	The number of registry items scanned.
Schedule UID splunk_dev	schedule_uid	String	Compliance Scan Event, Scan Event	The unique identifier of the schedule associated with a scan job.
Scheme	scheme	String	Uniform Resource Locator (URL) Object	The scheme portion of the URL. For example: `http`, `https`, `ftp`, or `sftp`.
Seats splunk_dev	seats	Integer	License Information Object	The number of seats.
Security Descriptor	security_descriptor	String	File Object, Registry Key Object	The object security descriptor.
Sender Email splunk_dev	sender_email	Email Address	File Content Protection Event	The email address of the sender.
Sender Host Name splunk_dev	receiver_hostname	Hostname	Email Delivery Activity Event, Email Delivery Alert Event	The host name of the receiving email server.
Sender Host Name splunk_dev	sender_hostname	Hostname	Email Delivery Activity Event, Email Delivery Alert Event	The host name of the sending email server.
Sender IP Address splunk_dev	sender_ip	IP Address	Email Delivery Activity Event, Email Delivery Alert Event	The IP address of the sending email server, in either IPv4 or IPv6 format.
Sender IP Address splunk_dev	receiver_ip	IP Address	Email Delivery Activity Event, Email Delivery Alert Event	The IP address of the receiving email server, in either IPv4 or IPv6 format.
Sequence Number	sequence	Integer	Metadata Object	Sequence number of the event. The sequence number is a value available in some events, to make the exact ordering of events unambiguous, regardless of the event time precision.
Serial Number	serial	String	Peripheral Device Object, Public Key Certificate Object	The serial number that pertains to the object. See specific usage.
Server Cipher Suites	server_ciphers	String Array	SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The server cipher suites that were exchanged during the TLS handshake negotiation.
Service	service	Cloud Service	Cloud Object	The cloud service that pertains to the event.
Service Name	svc_name	String	Network Endpoint Object	The service name in service-to-service connections. For example, AWS VPC logs the pkt-src-aws-service and pkt-dst-aws-service fields identify the connection is

				coming from or going to an AWS service.
Session	session	Session		The session information.
Session UID	session_uid	String	Authentication Audit Event, Authorization Audit Event, Endpoint Authentication Alert Event, Policy Override Audit Event, User Session Info Event, User Session Remediation Event Extended User Object, User Object	The unique ID of the user session, as reported by the OS.
Severity	severity	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License	The original event severity, as defined by the event source. The severity is a measurement the effort and expense required to manage and resolve an event or incident.

			Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Severity ID	severity_id	Integer	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint	The normalized event severity. The normalized severity is a measurement the effort and expense required to manage and resolve an event or incident. Smaller numerical values represent lower impact events, and larger numerical values represent higher impact events.

			Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Shell	shell	String	Extended User Object	The user's login shell.
Signature Serial Number	serial_number	String	Digital Signature Object	The object serial number.
Size	size	Long	Endpoint Memory Activity Event, Endpoint Memory Alert Event	The size of data, in bytes.

			Email Object, File Object	
Skipped splunk_dev	num_skipped	Integer	Scan Event	The number of skipped items.
Source Endpoint	src_endpoint	Network Endpoint	Authentication Audit Event, Endpoint Authentication Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Network Activity Event, Network Alert Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The network source endpoint.
Source Incident UID splunk	ref_incident_uid	String	Incident Creation Event	The unique incident identifier, as defined by the event source.
Source Type splunk	sourcetype	String	Splunk Fields Object	The format of the data input from which the event originates, such as \`access_combined\` or \`cisco_syslog\`. The source type controls how the Splunk platform formats incoming data. [List of pretrained source types - Splunk Documentation] (https://docs.splunk.com/Documentation/Splunk/8.2.3/Data/Listofpretrainedsourcetypes)
Source User	src_user	User	Account Change Audit Event, Authentication Audit Event, Endpoint Authentication Alert Event, Entity Audit Event	The existing user from which an activity was initiated.
Splunk Server splunk	splunk_server	String	Splunk Fields Object	The name of the Splunk server containing the event. Useful in a distributed Splunk environment.
Stack Trace splunk_dev	status_stack_trace	String	Application Log Event, Status Event	The list of calls that the application was making when an exception was thrown.
Start Time	start_time	Timestamp	Base Event License Information Object, User Entity Object	The start time of a time period. See specific usage.
Start Type splunk_dev	start_type	String	OS Service Object, Startup Application Object	The start type of the service or startup application.
Start Type ID splunk_dev	start_type_id	Integer	OS Service Object, Startup Application Object	The start type ID of the service or startup application.

Startup Application splunk_dev	startup_app	Startup Application	Startup Application Info Event, Startup Application Remediation Event	The startup application that pertains to the event.
State splunk	state	String	Incident Closure Event, Incident Creation Event, Incident Update Event	The state of the event or object, as defined by the event source. See specific usage.
State ID splunk	state_id	Integer	Incident Closure Event, Incident Creation Event, Incident Update Event, Network Connection Info Event	The state ID of the event or object. See specific usage.
Status	status	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info	The event status, as reported by the event source.

			Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event HTTP Response Object	
Status Details	status_detail	String	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory	The status details contains additional information about the event outcome.

			Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Status ID	status_id	Integer	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage	The cross-platform normalized status of the activity or alert reported by the event.

			Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry	

			Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Subject splunk_dev	subject	String	Email Object	The email header Subject value, as defined by RFC 5322.
Subject City splunk_dev	subject_city	String	Public Key Certificate Object	The certificate subject city.
Subject Country splunk_dev	subject_country	String	Public Key Certificate Object	The certificate subject country.
Subject Email splunk_dev	subject_email	Email Address	Public Key Certificate Object	The certificate subject email.
Subject Name splunk_dev	subject_name	String	Public Key Certificate Object	The certificate subject name.
Subject Org Unit splunk_dev	subject_org_unit	String	Public Key Certificate Object	The certificate subject organizational unit.
Subject Organization splunk_dev	subject_organization	String	Public Key Certificate Object	The certificate subject organization.
Subject State splunk_dev	subject_state	String	Public Key Certificate Object	The certificate subject state.
Subject Street splunk_dev	subject_street	String	Public Key Certificate Object	The certificate subject street.
Subnet	subnet	Subnet	Device Object, Network Object	The subnet mask.
Subnet UID	subnet_uid	String	Device Object, Endpoint Object, Network Endpoint Object, Virtual Machine Object	The unique identifier of a virtual subnet.
Suffix splunk	suffix	String	User Entity Object	The suffix of a person. For example: `M.D.` or `Ph.D.`.
System	is_system	Boolean	File Object, Kernel Resource Object, Registry Key Object, Registry Value Object	The indication of whether the object is part of the operating system.
System CPU splunk_dev	cpu_system	Long	CPU Usage Event	System CPU.

System Call	system_call	String	Kernel Resource Object	The system call that was invoked.
TCP Flags	tcp_flags	Integer	Network Connection Information Object	The network connection TCP header flags (i.e., control bits).
TLS	tls	Transport Layer Security (TLS)	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Network Activity Event, Network Alert Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The Transport Layer Security (TLS) attributes.
TTL	ttl	Integer	DNS Answer Object	The time interval that the resource record may be cached. Zero value means that the resource record can only be used for the transaction in progress, and should not be cached.
Tactics	tactics	String Array	Attack Object	The a list of tactic ID's that are associated with the attack technique, as defined by ATT&CK Matrix^{TM}.
Technique ID	technique_uid	String	Attack Object	The unique identifier of the attack technique, as defined by ATT&CK Matrix^{TM}. For example: `T1189`.
Technique Name	technique_name	String	Attack Object	The name of the attack technique, as defined by ATT&CK Matrix^{TM}. For example: `Drive-by Compromise`.
Thread ID	tid	Integer	Process Object	The Identifier of the thread associated with the event, as returned by the operating system.
Time	time	Timestamp	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access	The event time set by the logging system using information from the raw event data (event_time).

			Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Finding Report Event, Folder Info Event, Folder Remediation Event, Incident Closure Event, Incident Creation Event, Incident Update Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update	

			Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Time Zone	timezone	Integer	Account Change Audit Event, Admin Group Info Event, Application Lifecycle Event, Application Log Event, Authentication Audit Event, Authorization Audit Event, BitLocker Event, CPU Usage Event, Clipboard Content Protection Event, Command Activity Event, Compliance Event, Compliance Scan Event, Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event, Email File Activity Event, Email File Alert Event, Email URL Activity Event, Email URL Alert Event, Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event, Entity Audit Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder Remediation Event, Information Protection Event, Instant Message Content Protection Event, Job Info Event, Job Remediation Event, Kernel Object Info Event, Kernel Remediation Event, License Count Event, License Lifecycle Event, Memory Usage Event, Module Info Event, Module Remediation Event, Network Activity Event, Network Alert Event, Network Connection Info Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event, Network Policy	The number of minutes that the reported event `time` is ahead or behind UTC. A number in the range -1,080 to +1,080.

			Violation Event, Network Remediation Event, Networks Info Event, Peripheral Device Info Event, Policy Change Event, Policy Override Audit Event, Prefetch Info Event, Print/FAX Content Protection Event, Process Info Event, Process Remediation Event, Public Key Certificate Lifecycle Event, Registration Event, Registry Key Info Event, Registry Key Remediation Event, Registry Value Info Event, Registry Value Remediation Event, Scan Event, Service Info Event, Service Remediation Event, Startup Application Info Event, Startup Application Remediation Event, Status Event, Throughput Event, Unscannable File Event, Unsuccessful Discovery Event, Unsuccessful Remediation Event, Update Event, Update Available Event, User Info Event, User Session Info Event, User Session Remediation Event, Windows Event Event	
Title splunk	title	String	User Entity Object	The job title of the person.
To splunk_dev	to	Email Address Array	Email Object	The email header To values, as defined by RFC 5322.
Total splunk_dev	total	Integer	License Count Event, Scan Event	The total number of items. See specific usage.
Total Bytes	bytes	Long	Network Traffic Object	The total number of bytes (in and out).
Total Packets	packets	Long	Network Traffic Object	The total number of packets (in and out).
Traffic	traffic	Network Traffic	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Network Activity Event, Network Alert Event, Network DNS Activity Event, Network DNS Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The network traffic refers to the amount of data moving across a network at a given point of time. Intended to be used alongside Network Connection.
Traffic Path	traffic_path	String	Network Connection Information Object	The boundary of the connection. For cloud connections, this translates to the traffic-path (same VPC, through IGW, etc.). For traditional networks, this is described as Local, Internal, or External.
Traffic Path ID	traffic_path_id	Integer	Network Connection Information Object	The boundary of the connection. For cloud connections, this translates to the traffic-path (same VPC, through IGW, etc.). For

				traditional networks, this is described as Local, Internal, or External.
Trusted splunk_dev	num_trusted	Integer	Scan Event	The number of trusted items.
Trusted Device	is_trusted	Boolean	Device Object	The event occurred on a trusted device.
Type	type	String	Compliance Event, Compliance Scan Event, Scan Event, Update Event, Update Available Event DNS Answer Object, DNS Query Object, Device Object, Device Entity Object, Enrichment Object, Event Source Object, Extended User Object, File Object, Finding Object, Group Object, Kernel Resource Object, License Information Object, Managed Entity Object, Module Object, Network Object, Network Information Object, OS Object, Observable Object, Policy Object, Printer Object, Registry Value Object, Resource Object, Rule Object, TLS Extension Object, User Object, Virtual Machine Object	The type of an object or value. See specific usage.
Type ID	type_id	Integer	Compliance Event, Compliance Scan Event, Scan Event Device Object, Device Entity Object, Event Source Object, Extended User Object, File Object, Finding Object, Kernel Resource Object, License Information Object, Network Object, Network Information Object, OS Object, Observable Object, Policy Object, TLS Extension Object, User Object	The type identifier of an object. See specific usage.
Type IDs splunk_dev	type_ids	Integer Array	OS Service Object, Startup Application Object	The service type identifiers.
Types splunk_dev	types	String	OS Service Object, Startup Application Object	The service types.
URL	url	Uniform Resource Locator (URL)	Email URL Activity Event, Email URL Alert Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The URL object that pertains to the event or object. See specific usage.
URL Category IDs	category_ids	Integer Array	Uniform Resource Locator (URL) Object	An array of URL category identifies.
URL Text	text	String	Uniform Resource Locator (URL) Object	The URL. For example: `http://www.example.com/download/trou`

				`ble.exe`.
UUID	uuid	String	Extended User Object, User Object	The universally unique identifier. See specific usage.
Unique ID	uid	String	Compliance Scan Event, Scan Event Cloud Service Object, Container Object, Device Object, Device Entity Object, Endpoint Object, Extended User Object, Feature Object, File Object, Finding Object, Group Object, HTTP Request Object, Image Object, License Information Object, Malware Object, Managed Entity Object, Metadata Object, Network Object, Network Connection Information Object, Network Endpoint Object, Peripheral Device Object, Policy Object, Process Object, Product Object, Resource Object, Rule Object, Session Object, User Object, User Entity Object, Virtual Machine Object	The unique identifier. See specific usage.
Unmapped Data	unmapped	Object	Base Event	The attributes that are not mapped to the event schema. The names and values of those attributes are specific to the event source.
Used splunk_dev	is_used	Boolean	SMTP Transport Layer Security Object	The indication of whether the TLS is used when sending email.
Used splunk_dev	used	Integer	License Count Event	The number of items used.
User	user	User	Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job	The user that pertains to the event or object.

			Activity Event, User Info Event Job Object	
User Accounts splunk	accounts	User Array	User Entity Object	The user accounts associated with the person.
User CPU splunk_dev	cpu_user	Long	CPU Usage Event	User CPU.
User Credential ID	credential_uid	String	Extended User Object, Session Object, User Object	The unique identifier of the user's credential. For example, AWS Access Key ID.
User Entities splunk	user_entities	User Entity Array	Finding Report Event	The users that are identified in reported the events.
User Present	is_user_present	Boolean	Endpoint Authentication Alert Event, Endpoint Boot Record Alert Event, Endpoint DNS Activity Event, Endpoint DNS Alert Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Endpoint Memory Activity Event, Endpoint Memory Alert Event, Endpoint Module Activity Event, Endpoint Module Alert Event, Endpoint Network Activity Event, Endpoint Network Alert Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Endpoint Process Activity Event, Endpoint Process Alert Event, Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Endpoint Resource Activity Event, Endpoint Scheduled Job Activity Event	The indication of whether the user was logged on at event generation time.
User Result	user_result	User	Account Change Audit Event	The result of the user account change. It should contain the new values of the changed attributes.
VLAN	vlan_uid	String	Device Object, Endpoint Object, Network Endpoint Object	The Virtual LAN identifier.
VPC UID	vpc_uid	String	Device Object, Endpoint Object, Network Endpoint Object, Virtual Machine Object	The unique identifier of the Virtual Private Cloud (VPC).
Valid splunk_dev	is_valid	Boolean	Public Key Certificate Object	The indication of whether the certificate is valid.

Value	value	String	Enrichment Object, Fingerprint Object, HTTP Header Object, Observable Object	The value that pertains to the object. See specific usage.
Vendor	vendor	String	Peripheral Device Object	The vendor that pertains to the object. See specific usage.
Version	version	String	Cloud Service Object, Feature Object, File Object, Managed Entity Object, Metadata Object, OS Object, Policy Object, Product Object, Public Key Certificate Object, Rule Object, SMTP Transport Layer Security Object, Transport Layer Security (TLS) Object	The version that pertains to the event or object. See specific usage.
Violations splunk_dev	num_violations	Integer	Clipboard Content Protection Event, Email Content Protection Event, File Content Protection Event, Information Protection Event, Instant Message Content Protection Event, Print/FAX Content Protection Event	The number of times the policy or rule was violated.
Volume UID splunk_dev	volume_uid	String	BitLocker Event	The unique identifier of the volume.
X-Forwarded-For	x_forwarded_for	IP Address Array	HTTP Request Object	The X-Forwarded-For header identifying the originating IP address(es) of a client connecting to a web server through an HTTP proxy or a load balancer.