All Objects

Name	Type	Referenced By	Description
Attack	attack	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	The attack object describes the technique and associated tactics related to an attack.
Cloud	cloud	Event Origin Object	The Cloud object describes a cloud service or resource. It refers to compute, storage, networking, security, or other services that are accessed over the internet, which are hosted at a remote data center and managed by a cloud services provider.
Cloud Service	service	Cloud Object	The information pertaining to the cloud service.
Common Vulnerability Scoring System V2	cvssv2	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 Vulnerability Scoring System V2 object describes the base metrics as defined by the National Institute of Standards and Technology (NIST). See Common Vulnerability Scoring System for more information.
Container	container	Event Origin Object	The Container object describes a specific container, which is a source of events. A Docker container is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
DNS Answer	dns_answer	Endpoint DNS Activity Event, Endpoint DNS Alert Event, Network DNS Activity Event, Network DNS Alert Event	The Domain Name System (DNS) answer object.
DNS 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 object.
Device	device	Event Origin Object	Addressable device where events occurred.

Device Entity splunk	device_entity	Finding Report Event	A device of the environment that supports information-related activities. Devices should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.
Digital Signature	digital_signature	File Object	The digital signature of a file or application.
Email splunk_dev	email	Email Content Protection Event, Email Delivery Activity Event, Email Delivery Alert Event	The Email object describes the email metadata such as sender, recipients, and direction.
Email Authentication splunk_dev	email_auth	Email Delivery Activity Event, Email Delivery Alert Event	The Email Authentication object describes the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) attributes of an email.
Endpoint	endpoint		The endpoint object describes an addressable entity that has name and IP address.
Enrichment	enrichment	Base Event	The enrichment object describes inline enrichment data for attributes of interest within the event.
Event Origin	event_origin	Base Event	The event origin is where the event was created.
Event Source	event_source		The event source object describes the collection context of the event. Events that originate from a monitored logging facility contain a data source object.
Extended User	user_ex		The extended/enriched user object.
Feature	feature	Event Origin Object	The feature object describes a feature of a software product.
File	file	Email File Activity Event, Email File Alert Event, Endpoint File Access Activity Event, Endpoint File Activity Event, Endpoint File Alert Event, Endpoint Folder Activity Event, Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, File Content Protection Event, File Info Event, File Remediation Event, Folder Info Event, Folder 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 object describes files, folders, links and mounts, including the reputation information, if applicable.
Finding splunk	finding	Finding Report Event	The finding object describes the results of detections or analytics.

Fingerprint	fingerprint	Digital Signature Object, File Object	The fingerprint object describes the algorithm and value of digital fingerprint. A fingerprint is a short sequence of bytes used to identify a longer public key or file content.
Geo Location	location	Device Object, Device Entity Object, Endpoint Object, Network Object, Network Endpoint Object, User Entity Object	The location object describes a geographical location, usually associated with an IP address.
Group	group	Admin Group Info Event Device Object, Device Entity Object, Extended User Object, Policy Object, User Object, User Entity Object, Virtual Machine Object	The group object associated with an entity such as policy or rule.
HTTP Header	http_header	HTTP Request Object	The HTTP Header Object
HTTP Request	http_request	Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The HTTP Request Object details a request made to a web server.
HTTP Response	http_response	Endpoint HTTP Activity Event, Endpoint HTTP Alert Event, Network HTTP Activity Event, Network HTTP Alert Event	The HTTP Response Object details a response from a web server to a requester.
Image	image	Container Object, Virtual Machine Object	The Image object describes a specific Virtual Machine or Container image.
Job	job	Endpoint Scheduled Job Activity Event, Job Info Event, Job Remediation Event	The job object describes the name, command line and state of a scheduled job or task.
Kernel Resource	kernel	Endpoint Kernel Activity Event, Endpoint Kernel Alert Event, Kernel Object Info Event, Kernel Remediation Event	The kernel resource object describes the name and type of a kernel resource.
License Information splunk_dev	license_info	License Count Event, License Lifecycle Event	The license information object describes the type, number, and expiry of a license.
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	The malware object describes the classification of known malicious software, which is intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, etc.

		Event, Network HTTP Alert Event	
Managed Entity	managed_entity	Entity Audit Event	The managed entity object describes the type and version of an object, such as a policy or configuration.
Metadata	metadata	Base Event	The metadata associated with the event.
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 object describes the load attributes of a module.
Network splunk	network		The network object describes a network identified by a subnet mask.
Network Connection Information	network_connection	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 object.
Network Endpoint	network_endpoint	Authentication Audit Event, Authorization 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 endpoint object describes source or destination of a network connection.
Network Information	network_info	Networks Info Event Device Object, Device Entity Object	The network information object describes the type, reputation, and associated addresses of a network interface.
Network 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	The network proxy object describes a network proxy.

		HTTP Alert Event	
Network 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 object describes network data traffic. Network traffic refers to the amount of data moving across a network at a given point of time.
OS	os	Device Object	The OS object describes an operating system, such as Linux or Windows.
OS Service splunk_dev	os_service	Service Info Event, Service Remediation Event	The service object describes an application that can be started automatically at system startup, or by operating system-defined services controls.
Object	object	Base Event File Object, Process Object	An unordered collection of additional attributes that are not defined by the schema.
Observable	observable	Base Event	The observable object is a pivot element that contains related information found in many places in the event.
Peripheral Device	peripheral_device	Endpoint Peripheral Activity Event, Endpoint Peripheral Device Alert Event, Peripheral Device Info Event	The peripheral device object describes the identity, vendor and model of a peripheral device.
Policy splunk_dev	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 describes the policy and rule that either triggered the event or the policy that was in effect when the event occurred. Policy attributes provide traceability to the operational state of the security product at the time that the event was captured, facilitating forensics, troubleshooting, and policy tuning/adjustments.
Printer splunk_dev	printer	Print/FAX Content Protection Event	The printer object.
Process	process	Account Change Audit Event, Application Log Event, Authentication Audit Event, 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	The process object describes a running instance of a launched program.

		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, Module Info Event, Network Connection Info Event, Process Info Event, Process Remediation Event, Status Event Process Object	
Product	product	Event Origin Object, File Object	The product object describes a software product.
Public Key Certificate splunk_dev	public_key_certificate	Public Key Certificate Lifecycle Event	The Public Key Certificate, or a digital certificate, is used to prove the ownership of a public key. The certificate includes information about its lifetime, about the identity of its owner (called the subject) and the digital signature of an entity that has verified the certificate's contents (called the issuer).
Registry Key	registry_key	Endpoint Registry Key Activity Event, Endpoint Registry Key Alert Event, Registry Key Info Event, Registry Key Remediation Event	The registry key object describes a Windows registry key.
Registry Value	registry_value	Endpoint Registry Value Activity Event, Endpoint Registry Value Alert Event, Registry Value Info Event, Registry Value Remediation Event	The registry value object describes a Windows registry value.
Resource	resource	Endpoint Resource Activity Event	The resource object describes a managed object.
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 rule object associated with a policy or event.
SMTP Transport Layer Security splunk_dev	smtp_tls	Email Object	The SMTP Transport Layer Security (TLS) object describes the security attributes used by the SMTP servers to send/receive the email.
Session	session		The Session detailed information.

Splunk Fields splunk	splunk		The Account object.
Startup Application splunk_dev	startup_app	Startup Application Info Event, Startup Application Remediation Event	The startup application object describes an application that has associated startup criteria and configuration.
TLS Extension	tls_extension		The Transport Layer Security (TLS) extension object.
Transport Layer Security (TLS)	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 negotiated TLS protocol used for secure communications over an establish network connection.
Uniform Resource Locator (URL)	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 Uniform Resource Locator (URL) object describes the path and reputation of a URL.
User	user	Account Change Audit Event, Admin Group Info Event, Authentication Audit Event, Authorization Audit Event, 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, Entity Audit Event, User Info Event Job Object, Process Object, User Entity Object	The user object describes the identity of a user.

User Entity splunk	user_entity	Finding Report Event	The user entity object represents a real user in an organizational network environment.
Virtual Machine splunk_dev	virtual_machine		The virtual machine object.