All Event Classes

Name	Type	ID	Description
Account Change Audit	account_change_audit	3000	Account Audit events report when specific user account management tasks are performed, such as a user account is created, changed, deleted, renamed, disabled, enabled, locked out or unlocked.
Admin Group Info splunk_dev	admin_group_info	99902003	Group Info events report information about administrative groups.
Application Lifecycle splunk_dev	application_lifecycle	99904000	Application Lifecycle events report installation, removal, start, stop, and heartbeat of an application or service.
Application Log splunk_dev	application_log	99904001	Application Log events report status information about an application or service.
Authentication Audit	authentication_audit	3001	Authentication Audit events report authentication session activities such as user attempts a logon or logoff, successfully or otherwise.
Authorization Audit	authorization_audit	3002	Authorization Audit events report special privileges or groups assigned to a session.
BitLocker splunk_dev	bit_locker	99904002	BitLocker events report volume encryption and decryption activity.
CPU Usage splunk_dev	cpu_usage	99905000	CPU Usage events report service or application CPU usage statistics.
Clipboard Content Protection splunk_dev	clipboard_content_protection	99901000	Clipboard Content Protection events report the detection and resolution of clipboard content policy violations.
Command Activity splunk_dev	command_activity	99904004	Command Activity events report the state and status of commands.
Compliance splunk_dev	compliance	99901001	Compliance events report the results of a compliance and remediation checks.
Compliance Scan splunk_dev	compliance_scan	99901002	Compliance Scan events report the start, completion, and overall result of the scan. Detailed results are reported in individual compliance events.
Email Content Protection splunk_dev	email_content_protection	99901003	Email Content Protection events report the detection and resolution of email content policy violations.
Email Delivery Activity splunk_dev	email_delivery_activity	99901000	Email Delivery events report the delivery status of emails.
Email Delivery Alert splunk_dev	email_delivery_alert	99902000	Email Delivery Alert events report the detections and resolutions of email malicious activity.
Email File Activity splunk_dev	email_file_activity	99901001	Email File Activity events report non-threatening files within emails.
Email File Alert splunk_dev	email_file_alert	99902001	Email File Alert events report the detections and resolutions of malware within email file attachments.

Email URL Activity splunk_dev	email_url_activity	99901002	Email URL Activity events report non-threatening URLs within an email.
Email URL Alert splunk_dev	email_url_alert	99902002	Email URL Alert events report the detections and resolutions of URL malware within emails.
Endpoint Authentication Alert	endpoint_authentication_alert	2000	Endpoint Authentication Alert events report the detections and resolutions of authentication session malicious activity.
Endpoint Boot Record Alert	endpoint_boot_record_alert	2001	Endpoint Boot Record Alert events report the detections and resolutions of boot record malicious access.
Endpoint DNS Activity	endpoint_dns_activity	1002	Endpoint DNS Activity events report DNS queries and answers initiated by an application running on an endpoint.
Endpoint DNS Alert	endpoint_dns_alert	2002	Endpoint DNS Alert events report the detections and resolutions of malicious DNS queries.
Endpoint File Access Activity	endpoint_file_access_activity	1001	Endpoint File Access Activity events report when a network share object was checked to see whether client can be granted desired access on a file.
Endpoint File Activity	endpoint_file_activity	1004	Endpoint File Activity events report when a process performs an action on a file.
Endpoint File Alert	endpoint_file_alert	2004	Endpoint File Alert events report the detections and resolutions of file malicious activity.
Endpoint Folder Activity	endpoint_folder_activity	1005	Endpoint Folder Activity events report when a process performs an action on a folder.
Endpoint HTTP Activity	endpoint_http_activity	1006	Endpoint HTTP Activity events report HTTP connection and traffic caused by processes running on devices.
Endpoint HTTP Alert	endpoint_http_alert	2005	Endpoint HTTP Alert events report the detections of malware in the network HTTP traffic.
Endpoint Kernel Activity	endpoint_kernel_activity	1008	Endpoint Kernel Activity events report when an process creates, reads, or deletes a kernel resource.
Endpoint Kernel Alert	endpoint_kernel_alert	2007	Endpoint Kernel Alert events report the detections and resolutions of kernel resource malicious access.
Endpoint Memory Activity	endpoint_memory_activity	1009	Endpoint Memory Activity events report when a process performs internal memory allocation, modification, or other manipulation activities - such as a buffer overflow or turning off data execution protection (DEP) - that are not typical for a process.
Endpoint Memory Alert	endpoint_memory_alert	2008	Endpoint Memory Alert events report the detections and resolutions of malicious memory access.
Endpoint Module Activity	endpoint_module_activity	1010	Endpoint Module Activity events report when a process loads or unloads a module.

Endpoint Module Alert	endpoint_module_alert	2009	Endpoint Module Alert events report the detections and resolutions of module malicious activity.
Endpoint Network Activity	endpoint_network_activity	1011	Endpoint Network Activity events report network connection and traffic caused by processes running on endpoints.
Endpoint Network Alert	endpoint_network_alert	2010	Endpoint Network Alert events report the detections and resolutions of malicious endpoint network activity.
Endpoint Peripheral Activity	endpoint_peripheral_activity	1013	Endpoint Peripheral Activity events report peripheral device activity.
Endpoint Peripheral Device Alert	endpoint_peripheral_alert	2012	Endpoint Peripheral Device Alert events report the detections and resolutions of peripheral device activity.
Endpoint Process Activity	endpoint_process_activity	1014	Endpoint Process Activity events report when a process launches, injects, opens or terminates another process, successful or otherwise.
Endpoint Process Alert	endpoint_process_alert	2013	Endpoint Process Alert events report the detections and resolutions of process malicious activity.
Endpoint Registry Key Activity	endpoint_registry_key_activity	1015	Endpoint Registry Key Activity events report when a process performs an action on a Windows registry key.
Endpoint Registry Key Alert	endpoint_registry_key_alert	2014	Endpoint Registry Key Alert events report the detections and resolutions of registry key malicious access.
Endpoint Registry Value Activity	endpoint_registry_value_activity	1016	Endpoint Registry Value Activity events reports when a process performs an action on a Windows registry value.
Endpoint Registry Value Alert	endpoint_registry_value_alert	2015	Endpoint Registry Value Alert events report the detections and resolutions of registry value malicious access.
Endpoint Resource Activity	endpoint_resource_activity	1017	Endpoint Resource Activity events report when a process accesses an OS managed resource/object, successful or otherwise.
Endpoint Scheduled Job Activity	endpoint_scheduled_job_activity	1018	Endpoint Scheduled Job Activity events report activities related to scheduled jobs or tasks.
Entity Audit	entity_audit	3003	Entity Audit events report activity by a managed client, a micro service, or a user at a management console. The activity can be a create, update, and delete operation on a managed entity.
File Content Protection splunk_dev	file_content_protection	99901004	File Content Protection events report the detection and resolution of file content policy violations.
File Info splunk_dev	file_info	99902001	File Info events report information about files that are present on the system.
File Remediation splunk_dev	file_remediation_result	99903000	File Remediation events report file remediation activity.
Finding Report splunk	finding_report	101000	Finding events report the results of detections or analytics.

Folder Info splunk_dev	folder_info	99902002	Folder Info events report information about folders that are present on the system.
Folder Remediation splunk_dev	folder_remediation_result	99903001	Folder Remediation events report folder remediation activity.
Incident Associate splunk	incident_associate	101001	Incident Associate events report when a new event is associated with an existing incident.
Incident Closure splunk	incident_close	101002	Incident closure events report when an incident has been closed.
Incident Creation splunk	incident_create	101003	Incident creation events report the creation of an incident.
Incident Update splunk	incident_update	101004	Incident updates events report when an incident has been updated.
Information Protection splunk_dev	information_protection	99901008	Information Protection events report the detection and resolution of content policy violations.
Instant Message Content Protection splunk_dev	im_content_protection	99901005	Instant Message Content Protection events report the detection and resolution of instant message content policy violations.
Job Info splunk_dev	job_info	99902004	Job Info events report information about scheduled jobs.
Job Remediation splunk_dev	job_remediation_result	99903002	Job Remediation events report job remediation activity.
Kernel Object Info splunk_dev	kernel_object_info	99902005	Kernel Object Info events report information about kernel resources.
Kernel Remediation splunk_dev	kernel_remediation_result	99903003	Kernel Remediation events report kernel resource remediation activity.
License Count splunk_dev	license_count	99904005	License Count events report aggregate license counts.
License Lifecycle splunk_dev	license_lifecycle	99904006	License Lifecycle events report the installation, update, expiration, and removal of a license.
Memory Usage splunk_dev	mem_usage	99905001	Memory Usage events report service or application memory usage statistics.
Module Info splunk_dev	module_info	99902006	Module Info events report information about loaded modules.
Module Remediation splunk_dev	module_remediation_result	99903004	Module Remediation events report module remediation activity.
Network Activity	network_activity	1012	Network Activity events report network connection and traffic activity.
Network Alert	network_alert	2011	Network Alert events report the detections and resolutions of network threats.
Network Connection Info splunk_dev	network_connection_info	99902007	Network Connection Info events report information about active network connections.

Network DNS Activity	network_dns_activity	1003	Network DNS Activity events report DNS queries and answers as seen on the network.
Network DNS Alert	network_dns_alert	2003	Network DNS Alert events report the detections and resolutions of malicious DNS queries.
Network HTTP Activity	network_http_activity	1007	Network HTTP Activity events report HTTP connection and traffic information.
Network HTTP Alert	network_http_alert	2006	Network HTTP Alert events report the detections of malware in the network HTTP connections and traffic.
Network Policy Violation splunk_dev	network_policy	99901006	Network Policy events report the detection and resolution of network policy violations.
Network Remediation splunk_dev	network_remediation_result	99903005	Network Remediation events report network remediation activity.
Networks Info splunk_dev	networks_info_info	99902008	Networks Info events report information about network adapters.
Peripheral Device Info splunk_dev	peripheral_device_info	99902009	Peripheral Device Info events report information about peripheral devices.
Policy Change splunk_dev	policy_change	99904007	Policy change events report when the endpoint applies a new policy.
Policy Override Audit splunk_dev	policy_audit	99903001	Reports user policy override activity at a management console or a managed client.
Prefetch Info splunk_dev	prefetch_info	99902010	Prefetch Info events report information about Windows prefetch files.
Print/FAX Content Protection splunk_dev	print_content_protection	99901007	Print/FAX Content Protection events report the detection and resolution of print/FAX content policy violations.
Process Info splunk_dev	process_info	99902011	Process Info events report information about running processes.
Process Remediation splunk_dev	process_remediation_result	99903006	Process Remediation events report process remediation activity.
Public Key Certificate Lifecycle splunk_dev	public_key_cert_lifecycle	99904003	The Public Key Certificate Lifecycle events report the installation, update, expiration, and removal of a public key certificate.
Registration splunk_dev	registration	99904008	Registration events report device or application registration with a management system.
Registry Key Info splunk_dev	registry_key_info	99902012	Registry Key Info events report information about Windows registry keys.
Registry Key Remediation splunk_dev	registry_key_remediation_result	99903007	Registry Key Remediation events report registry key remediation activity.
Registry Value Info splunk_dev	registry_value_info	99902013	Registry Value Info events report information about Windows registry values.

Registry Value Remediation splunk_dev	registry_value_remediation_result	99903008	Registry Value Remediation events report registry value remediation activity.
Scan splunk_dev	scan	99901009	Scan events report the start, completion, and results of a scan job. The scan event includes the number of items that were scanned and the number of detections that were resolved.
Service Info splunk_dev	service_info	99902014	Service Info events report information about running services.
Service Remediation splunk_dev	service_remediation_result	99903010	Service Remediation events report service remediation activity.
Startup Application Info splunk_dev	startup_app_info	99902016	Startup Application Info events report information about startup applications.
Startup Application Remediation splunk_dev	startup_app_remediation_result	99903012	Startup Application Remediation events report startup application remediation activity.
Status splunk_dev	status	99905002	Status events report the status of a component, for example a service, application or appliance. Report the status information in the message attribute, for example "Connection failure", "Low Disk", or "High CPU". If additional status information is required, include common extension status attributes such as status_detail, status_os, status_exception and status_stack_trace. If reporting status for a specific process, include the Process object.
Throughput splunk_dev	throughput	99905003	Throughput events report the processing rate of a service or application.
Unscannable File splunk_dev	unscannable_file	99901010	Unscannable File events report files that could not be scanned and the reasons why.
Unsuccessful Discovery splunk_dev	discovery_no_result	99902000	Unsuccessful Discovery events report unsuccessful attempts at Evidence of Compromise queries.
Unsuccessful Remediation splunk_dev	remediation_no_result	99903009	Unsuccessful Remediation events report unsuccessful remediation attempts.
Update splunk_dev	update	99904009	Update events report code, content, configuration, or policy updates that are made to an application or service.
Update Available splunk_dev	update_available	99904010	Update Available events report when code, content, configuration, or policy updates are available.
User Info splunk_dev	user_info	99902017	User Info events report information about users.
User Session Info splunk_dev	session_info	99902015	User Session Info events report information about existing user sessions.
User Session Remediation splunk_dev	session_remediation_result	99903011	User Session Remediation events report user session remediation results.

Windows Event	windows	1999	Windows activity event class represent a general purpose Microsoft Windows operating system event.