EQL Help Guide

Basic Structure

Event Type	Modifier	Event Schema	Boolean	"Value"
process	where		==	
security	false		!=	
file	with		<=	
registry	and		>=	
network	true		>	
image_load	until		<	
dns	or			
	join by			

Examples

file	where	file_name	==	"cmd.exe"
process	where	process_name	==	"cmd.exe"
	and	timestamp_utc	>	"2018-11-26"

process

All OS

- authentication_id
- command_line
- event_type_full
- exit_code
- process_path
- md5
- original_file_name
- parent_process_path
- parent_process_name
- serial_event_id
- pid
- ppid
- sha256
- timestamp
- sha1
- timestamp_utc
- unique_ppid
- unique_pid
- process_name

Windows

- event_subtype_full
  - already_running
  - creation_event
  - still_running
  - termination_event
- opcode
- package_name
- signature_signer
- signature_status
- user_domain
- user_name
- user_sid

Linux

- event_subtype_full
  - already_running
  - exec_event
  - fork_event
  - gid_change
  - session_id_change
  - still_running
  - termination_event
  - uid_change
- effective_gid
- effective_group_name
- exit_code_full
- opcode
- real_guid
- real_group_name
- real_uid
- real_user_name
- session_id
- tid

Mac

- event_subtype_full
  - already_running
  - exec_event
  - fork_event
  - gid_change
  - session_id_change
  - still_running
  - termination_event
  - uid_change
- effective_gid
- effective_group_name
- exit_code_full
- opcode
- real_guid
- real_group_name
- real_uid
- real_user_name
- session_id
- tid

file

All OS

- event_type_full
- file_attributes
- file_name
- file_path
- old_file_name
- old_file_path
- opcode
- pid
- process_name
- process_path
- serial_event_id
- share_mode
- timestamp
- timestamp_utc
- unique_pid
- zone_id

windows

- event_subtype_full
  - file_create_event
  - file_modify_event
  - file_delete_event
  - file_rename_event
  - file_overwrite_event
- create_disposition
- desired_access
- create_options
- user_domain

linux

- event_subtype_full
  - file_create_event
  - file_modify_event
  - file_delete_event
  - file_rename_event
  - file_overwrite_event
- effective_gid
- effective_group_name
- effective_uid
- effective_user_name
- real_gid
- real_group_name
- real_uid
- real_user_name

mac

- event_subtype_full
  - file_create_event
  - file_modify_event
  - file_delete_event
  - file_rename_event
  - file_overwrite_event
- effective_gid
- effective_group_name
- effective_uid
- effective_user_name
- real_gid
- real_group_name
- real_uid
- real_user_name

network

All OS

- connection_id
- destination_address
- destination_port
- event_id
- event_type_full
- in_bytes
- in_packet_court
- opcode
- out_bytes
- out_packet_court
- partial_flow
- pid
- process_name
- process_path
- protocol
- serial_event_id
- source_address
- source_port
- task
- timestamp
- timestamp_utc
- total_in_bytes
- total_out_bytes
- unique_pid

Windows

- event_subtype_full
  - ipv4_connection_attempt_event
  - ipv4_connection_accept_event
  - ipv4_disconnect_recieved_event
  - ipv6_reconnect_attempt_event
  - ipv6_connection_attempt_event
  - ipv6_connection_accept_event
  - ipv6_disconnect_recieved_event
  - ipv6_reconnect_attempt_event
  - ipv4_http_request_event
  - ipv6_http_request_event
- user_domain
- user_name
- user_sid

Linux

- event_subtype_full
  - ipv4_connection_attempt_event
  - ipv4_connection_accept_event
  - ipv4_disconnect_recieved_event
  - ipv6_reconnect_attempt_event
  - ipv6_connection_attempt_event
  - ipv6_connection_accept_event
  - ipv6_disconnect_recieved_event
  - ipv6_reconnect_attempt_event
  - ipv4_http_request_event
  - ipv6_http_request_event
- effective_gid
- effective_group_name
- effective_uid
- effective_user_name
- real_gid
- real_group_name
- real_uid
- real_user_name

Mac

- event_subtype_full
  - ipv4_connection_attempt_event
  - ipv4_connection_accept_event
  - ipv4_disconnect_recieved_event
  - ipv6_reconnect_attempt_event
  - ipv6_connection_attempt_event
  - ipv6_connection_accept_event
  - ipv6_disconnect_recieved_event
  - ipv6_reconnect_attempt_event
  - ipv4_http_request_event
  - ipv6_http_request_event
- effective_gid
- effective_group_name
- effective_uid
- effective_user_name
- real_gid
- real_group_name
- real_uid
- real_user_name

security

Windows

- event_subtype_full
  - admin_logon
  - explicit_user_logon
  - user_logoff
  - user_logon
  - user_logon_failed
  - workstation_unlocked
  - workstation_locked
- channel_name
- computer_name
- event_id
- event_message
- event_type_full
- ip_address
- logon_type
- opcode
- pid
- privilege_list
- process_name
- process_path
- provider_guid
- provider_name
- serial_event_id
- subject_domain_name
- subject_logon_id
- subject_user_name
- subject_user_sid
- system_pid
- system_process_name
- system_thread_id
- target_domain_name
- target_logon_id
- target_user_name
- task
- timestamp
- timestamp_utc
- unique_pid

image load

Windows

- event_subtype_full
  - driver_load_event
  - image_load_event
- event_type_full
- image_name
- image_path
- md5
- opcode
- pid
- process_name
- process_path
- serial_event_id
- sha256
- timestamp_utc
- unique_pid
- user_domain
- user_sid

dns

Windows

- event_subtype_full
  - lookup_failure
  - request_event
- event_type_full
- opcode
- pid
- process_name
- process_path
- query_name
- query_options
- query_results
- query_status
- query_type
- serial_event_id
- timestamp
- timestamp_utc
- unique_pid