Mandiant

INTEGRATIONS - FIELD DETAILS

Before submitting events to the Director for processing, they need to be translated into the data structure that the Director expects. This is a dictionary of key value pairs where the key names must correspond to valid fields for the event objects in Director.

The following sections provides details for the fields used and criteria requirements to match events to Job Actions.

Event Fields

Some integrations have field mappings sections that tells the platform which fields from the integration to match against. To improve event matching to Job Actions, it is best practice to populate as many of the fields as possible for each event. The following integrations have these field mapping sections: Azure Sentinel, Azure LogAnalytics, Elasticsearch, FireEye Helix, Graylog, LogRhythm Elasticsearch, Logzilla, and Securonix SNYPR. There are other integrations, such as Splunk and Splunk ES, that will require similar configuration in the integration itself.

Field Name	Description
computer	An optional field for the computer name used when matching Host CLI Actions. When present, this is checked against the hostname known for the Actor involved in the Action.
description	A human-friendly description or name of the event.
dest_ip	For network events, the destination IP Address of the event. This is an optional field, but if present it must be a string of at most 255 characters. It can be an IP address in dotted-quad format, a hostname, or an FQDN.
dest_port	For network events, the destination port of the event. This is an optional field that should have an integer between 0 and 65535 when populated.
email_recipient	For events created in response to email Actions, this could be the username or email address of the email sender.
email_sender	For events created in response to email Actions, this could be the username or email address of the email sender.
email_subject	For events created in response to email Actions, this could be the subject of the email that was sent.
filehashes	Optional field for events that contain one or more hashes of files. If present, it is used when matching Actions where the hashes of the file is involved. This can contain multiple hashes, separated by a pipe character |, such as when an event has an MD5 and a SHA256 value.

Field Name	Description
host	This is what is displayed as the event source in the Director UI. In most cases it would be the sensor/device that generated the event, but it could be something different based on the needs of a specific integration.
raw_event	Whenever possible, this would be the original raw event (eg, in the case of a SIEM, it might be the log line received over syslog). If that's not available, a JSON dump of the raw event fields is typically used.
sid	A short identifier of the type of event. This is strictly optional and is not displayed in the UI or used for matching an event to a Job Action.
src_ip	For network events, the source IP Address of the event. It can be an IP address in dotted-quad format, a hostname, or an FQDN.
src_port	For network events, the source port of the event. This is an optional field that should have an integer between 0 and 65535 when populated.
start_time	The timestamp for the event. This should be a string in ISO8601 format to avoid problems with timezone differences.
url	Optional field that currently isn't displayed in the UI anywhere. However, it is used for matching Malicious DNS Query Actions. If you run that type of Action, the field should be the domain name.
user	An optional field for events that contain a username, for example events from certain endpoint products might have this. This is not currently shown in the UI or used for matching Job Actions.

Network Action Matching Criteria

There are specific criteria an event must meet to match a Network Job Action. In the following table, the Match Type column contains the string the platform uses to indicate the match. These strings can be seen in an API response.

Match Type	Description
actor_address/time/file hash	This match type is only available for Job Actions that use a file from the File Library. • The start_time of the event is within the Job Action began_at and ended_at times • One of the IP addresses in the event matches an Actor IP Address from the Job Action • The filehashes field in the event matches one of the files used in the Job Action

Match Type	Description
actor_address/time/port	• The start_time of the event is within the Job Action began_at and ended_at times • One of the IP addresses in the event matches an Actor IP address from the Job Action • The src_port and dest_port fields in the event match the Job Action conversations
actor_address/time/single_port	This match type is often encountered when the Job Action ran through a proxy to an AWS Actor. • The start_time of the event is within the Job Action began_at and ended_at times • One of the IP addresses in the event matches an Actor IP Address from the Job Action • Either the src_port or dest_port field in the event matches a Job Action conversation
address/port	• The source and destination IP addresses of the event match conversations from the Job Action • The source and destination ports of the event match conversations from the Job Action
address/port/time	• The source and destination IP addresses of the event match conversations from the Job Action • Source and destination ports of the event match conversations from the Job Action • The start_time field for the event is within the Job Action began_at and ended_at times
address/time	• The source and destination IP addresses of the event match conversations from the Job Action • The start_time field for the event is within the Job Action began_at and ended_at times • The event is missing the src_port or dest_port fields
address/time/job_action_no_ports	• The source and destination IP addresses of the event match conversations from the Job Action • The start_time field for the event is within the Job Action began_at and ended_at times • There are no ports recorded for the Job Action conversations (eg, for ICMP traffic)
dns:time/domain	The Job Action is a Malicious DNS Query. • The start_time of the event is within the Job Action began_at and ended_at times • The url field for the event is the domain requested in the Job Action

Match Type	Description
email:address/time	The Job Action is an email Action • The email_subject field for the event is blank • The start_time of the event is within the Job Action began_at and ended_at times • The email_sender and email_recipient fields for the event are present and match the email addresses used in the Job Action
email:subject/uid	The Job Action is an email Action. • The email_subject for the event is present • The subject ontains the Job Action's unique email identifier string
port_scan:address/time/single_port	The Job Action is a port scan Action. • The start_time of the event is within the Job Action began_at and ended_at times • The source and destination IP addresses of the event match conversations from the Job Action • A single port from the event matches one from the Job Action

Host CLI Action Matching Criteria

Host CLI Actions have a specific set of criteria that an event must meet that is similar, but different from Network Job Actions. In the following table, the Match Type column contains the string the platform uses to indicate the match. These strings can be seen in an API response.

Match Type	Description
host_cli:host/time	• The start_time of the event is within the Job Action began_at and ended_at times and the host or computer field for the event matches an Actor IP address or hostname from the Job Action • For hostnames, this match is case-insensitive
host_cli:host/time/filehash	• The event filehashes field is present and matches a file used in the Action • The event time is between the Job Action began_at and ended_at times using the Filehash Match time skew on the Integration Settings page • The host or computer field for the event matches an Actor IP address or hostname from the Job Action
host_cli:ip/time	• The start_time of the event is within the Job Action began_at and ended_at times and the src_ip or dest_ip field of the event matches the Actor's management IP address • For Protected Host CLI Actions, this can also match on the management IP address of the Protected Theater involved in running the Action