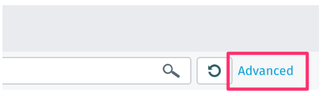
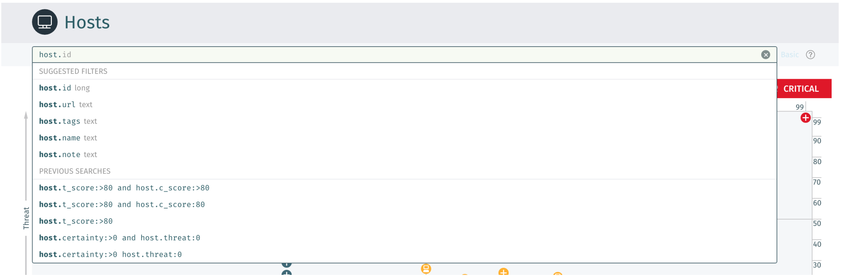
Advanced Search Reference Guide





Examples of a search term

SIMPLE	foobar	value	
	tags:foobar	filter:value	On **Hosts**, this will return hosts with this tag and hosts with detections with this tag
	host.tags:foobar	index.filter:value	On **Hosts**, this will return only hosts with this tag
COMPLEX	detection.grouped_details.uuid:abc	index.path.filter:value	

Values

Search for a simple value to return broad results:

Example	Meaning	Tip
414	Any value containing “414”	
admin	Any value containing “admin”	
“admin 1”	Any value which is exactly “admin 1”	Put quotes around a value to search for an exact match or for a value with embedded spaces.

Filter

Search for a value on a specific filter:

Example	Value Type	Meaning	Tip
tags:investigate	string	Tag containing “investigate”	Put quotes around a value to search for an exact match
dst_port:414	integer	Destination port is exactly “414”	Integer key/values are exact matches by default
is_key_asset:true	boolean	Object is a key asset	
src_ip:1.1.1.1	ip address	source IP address is exactly 1.1.1.1	IP key/values are exact matches by default

Deep Searches

Interesting nested values can be uncovered by a deep search.

For example, on **Hosts**, find a host with specific detections using “detection_summaries”:

Example	Meaning
host.detection_summaries.tags:investigate	Host containing a detection with tag containing “investigate”
host.detection_summaries.category:exfil	Host contaning exfil detections
host.detection_summaries.threat:>75	Host containing detections with a threat greater than 75

On **Detections**, find specific detection details by searching on “grouped_details”

Example	Meaning
detection.grouped_details.uuid:	Detection involving this UUID
detection.grouped_details.accounts:	Detection involving this account

These are not all the deep searches you can perform on hosts and detections. Look out for a link to a complete list of deep searches you can perform soon.

Operators and Special Characters

Boolean Operators

Combine multiple keys with boolean operators to create complex searches.

Example	Operator	Meaning
threat:>80 certainty:>80	AND (implicit)	Threat and certainty is greater than 80
threat:>80 AND certainty:>80	AND	Threat and certainty is greater than 80
threat:>80 OR certainty:>80	OR	Threat or certainty is greater than 80
NOT tags:admin	NOT	No tag containing “admin”.
(threat:>80 AND certainty:>80) OR (threat:>50 AND tags:investigate)	AND, OR	Either threat and certainty are greater than 80 or threat is greater than 50 and a tag contains “investigate”

Wildcard

Specify a wildcard (*) to find values that start with, end with or are between a value:

Example	Meaning
admin*	Starts with “admin”
“admin building”*	Starts with “admin building”
admin	Contains “admin”
”admin building”	Contains “admin building”
1.1.*.1	Starts with “1.1.” and ends with”.1”
“foo*bar foo”	Starts with “foo” and ends with “bar foo”
*admin	Ends with “admin”
*”admin building”	Ends with “admin building”

Integer and Date/Time Operators

Specify ranges for integer and date/time values:

Example	Operator	Meaning
threat:>80	>	Threat is greater than 80
last_seen:>=“2018-09-08T1300”	>=	Last seen is on or after September 8 2018, 13:00
threat:<80	<	Threat is less than 80
last_seen:<=2018-09-08T1300	<=	Last seen timestamp is on or before…
last_seen:[2018-09-08T1300 to 2018-09-10T1300]	[ ]	Last seen timestamp is on or between… September 8 13:00 to September 10 13:00