Splunk Function/Stage	Splunk Query Example	Resulting XQL Query Example
avg	index=xdr_data | stats avg(dst_association_strength)	datamodel dataset in (xdr_data) | comp avg(dst_association_strength)
now	where _time>=relative_time(now(), "-70m@m")	filter _time >= now() - 70m
/	eval delta = round(volume/previous_avg, 2)	alter delta = round(divide(volume, previous_avg)), 2)
CIDR	All_Traffic.src IN (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)	xdm.source.ipv4 incidr "10.0.0.0/8" or xdm.source.ipv4 incidr "172.16.0.0/12" or xdm.source.ipv4 incidr "192.168.0.0/16"
_time >= now() - 70m	_time >= now() - 70m	filter timestamp_diff(_time,current_time(),"MINUTE") >= 70
bin	index = xdr_data | bin _time span=5m	datamodel dataset in (xdr_data) | bin _time span=5m

coalesce	index= xdr_data | eval product_or_vendor_not_null=coalesce(_product, _vendor)	datamodel dataset in (xdr_data) | alter product_or_vendor_not_null = coalesce(_product, _vendor)
count	index=xdr_data | stats count(_product) BY _time	datamodel dataset in (xdr_data) | comp count(_product) by _time
ctime	index=xdr_data | convert ctime(field) as field	datamodel dataset in (xdr_data) | alter field = format_timestamp("%m/%d/%Y %H:%M:%S", to_timestamp(field))
earliest	index = xdr_data earliest=24d	datamodel dataset in (xdr_data) | filter _time >= to_timestamp(add(to_epoch(current_time()),2073600000))
eval	index=xdr_data | eval field = "test"	datamodel dataset in (xdr_data) | alter field = "test"
fillnull	index=xdr_data | fillnull value = "missing ipv6" agent_ip_addresses_v6	datamodel dataset in (xdr_data) | replacenull agent_ip_addresses_v6 = "missing ipv6"

floor	index=xdr_data | eval floor_test = floor(1.9)	datamodel dataset in (xdr_data) | alter floor_test = floor(1.9)
iplocation	index=xdr_data | inputlookup append=true my_lookup.csv	datamodel dataset in (xdr_data) | union (dataset=my_lookup | limit 1000000000)
iplocation	index = xdr_data | inputlookup agent_ip_addresses	datamodel dataset in (xdr_data) | iploc agent_ip_addresses loc_continent AS Continent, loc_country AS Country, loc_region AS Region, loc_city AS City, loc_latlon AS lon
isnotnull	index=xdr_data | eval x = isnotnull(agent_hostname)	datamodel dataset in (xdr_data)\n | alter x = if(agent_hostname != null, true, false)
isnull	index=xdr_data | eval x = isnull(agent_hostname)	datamodel dataset in (xdr_data)\n | alter x = if(agent_hostname = null, true, false)

json_extract	index= xdr_data | eval London=json_extract(dfe_labels,"dfe_labels{0}")	datamodel dataset in (xdr_data) | alter London = dfe_labels -> dfe_labels[0]{}
join	join agent_hostname [index = xdr_data]	join type=left conflict_strategy=right (datamodel dataset in (xdr_data)) as inner agent_hostname = inner.agent_hostname
latest	index = xdr_data latest=-24d	datamodel dataset in (xdr_data) |filter _time <= to_timestamp(add(to_epoch(date_floor(current_time(),"d")),-2073600000))
len	index = xdr_data | where uri != null | eval length = len(agent_ip_address)	datamodel dataset in (xdr_data) | filter agent_ip_addresses != null | alter agent_ip_address_length = len(agent_ip_addresses)
ltrim(<str>,<trim_chars>)	index=xdr_data | eval trimed_agent=ltrim("agent_hostname", "agent_")	datamodel dataset in (xdr_data) | alter trimed_agent = ltrim("agent_hostname", "agent_")

lower	index = xdr_data | eval field = lower("TEST")	datamodel dataset in (xdr_data) | alter field = lowercase("TEST")
max	index =xdr_data | stats max(action_file_size) by _product	datamodel dataset in (xdr_data) | comp max(action_file_size) by _product
md5	index=xdr_data | eval md5_test = md5("test")	datamodel dataset in (xdr_data) | alter md5_test = md5("test")
median	index = xdr_data | stats median(actor_process_file_size) by _time	datamodel dataset in (xdr_data) | comp median(actor_process_file_size) by _time
min	index =xdr_data | stats min(action_file_size) by _product	datamodel dataset in (xdr_data) | comp min(action_file_size) by _product
mvcount	index = xdr_data | where http_data != null | eval http_data_array_lengt	datamodel dataset in (xdr_data) | filter http_data != null | alter http_data_array_length = array_length(http_data)

	h = mvcount(http_data)	
mvdedup	index = xdr_data | eval s=mvdedup(action_app_id_transitions)	datamodel dataset in (xdr_data) | alter s = arraydistinct(action_app_id_transitions)
mvexpand	index = xdr_data | mvexpand dfe_labels limit = 100	datamodel dataset in (xdr_data) | arrayexpand dfe_labels limit 100
mvfilter	index = xdr_data | eval x = mvfilter(isnull(dfe_labels))	datamodel dataset in (xdr_data) | alter x = arrayfilter(dfe_labels, if("@element" = null, true, false) = true)
mvindex	index=xdr_data | eval field = mvindex(action_app_id_transitions, 0)	datamodel dataset in (xdr_data) | alter field = arrayindex(action_app_id_transitions, 0)
mvjoin	index=xdr_data | eval n=mvjoin(action_app_id_transitions, ";")	datamodel dataset in (xdr_data) | alter n = arraystring(action_app_id_transitions, ";")

pow	index=xdr_data | eval pow_test = pow(2, 3)	datamodel dataset in (xdr_data) | alter pow_test = pow(2, 3)
relative_time(X,Y)	• index ="xdr_data" | where _time > relative_time(now(),"-7d@d") • index ="xdr_data" | where _time > relative_time(now(),"+7d@d")	• datamodel dataset in (xdr_data) | filter _time > to_timestamp(add(to_epoch(date_floor(current_time(),"d")),-604800000)) • datamodel dataset in (xdr_data)| filter _time > to_timestamp(add(to_epoch(date_floor(current_time(),"d")),604800000))
replace	index= xdr_data | eval description = replace(agent_hostname,"\(."NEW")	datamodel dataset in (xdr_data) | alter description = replace(agent_hostname, concat("\(", "NEW"))
rex	index=xdr_data action_local_ip!="0.0.0.0" | rex field=action_local_ip "(?<src_ip>\d+\.\d+\.\d+\.48)" | where src_ip != "" | table action_local_ip src_ip	datamodel dataset in (xdr_data) |filter (action_local_ip != "0.0.0.0" AND action_local_ip != null) | alter src_ip = arrayindex(regextract(action_local_ip, "(\d+\.\d+\.\d+\.48)"), 0) | filter src_ip != "" | fields action_local_ip, src_ip

round	index=xdr_data | eval round_num = round(3.5)	datamodel dataset in (xdr_data) | alter round_num = round(3.5)
rtrim	index=xdr_data | eval trimed_hostname=rtrim ("agent_hostname", "hostname")	datamodel dataset in (xdr_data) | alter trimed_hostname = rtrim("agent_hostname", "hostname")
search	index = xdr_data | eval ip="192.0.2.56" | search ip="192.0.2.0/24"	datamodel dataset in (xdr_data) | alter ip = "192.0.2.56" | filter incidr(ip,"192.0.2.0/24") = true
sha256	index = xdr_data | eval sha256_test = sha256("test")	datamodel dataset in (xdr_data) | alter sha256_test = sha256("test")
sort (ascending order)	index = xdr_data | sort action_file_size	datamodel dataset in (xdr_data) | sort asc action_file_size | limit 10000
sort (descending order)	index = xdr_data | sort -action_file_size	datamodel dataset in (xdr_data) | sort desc action_file_size | limit 10000

spath	index = xdr_data | spath output=myfield input=action_network_http path=headers.User-Agent	datamodel dataset in (xdr_data) | alter myfield = json_extract(action_network_http,"$.headers.User-Agent")
split	index = xdr_data | where mac != null | eval split_mac_address = split(mac, ":")	datamodel dataset in (xdr_data)\n | filter mac != null\n | alter split_mac_address = split(mac, ":")
stats	index=xdr_data | stats count(event_type) by _time	datamodel dataset in (xdr_data) | comp count(event_type) by _time
stats dc	index = xdr_data | stats dc(_product) BY _time	datamodel dataset in (xdr_data) | comp count_distinct(_product) by _time
strcat	index=xdr_data | strcat story_id "/" http_req_before_method comboIP	datamodel dataset in (xdr_data) | alter comboIP=concat(if(story_id!=null, story_id,""),"/",if(http_req_befo

		re_method!=null,http_req_before_method,""))
sum	index=xdr_data | where action_file_size != null | stats sum(action_file_size) by _time	datamodel dataset in (xdr_data) | filter action_file_size != null | comp sum(action_file_size) by _time
table	index = xdr_data | table _time, agent_hostname, agent_ip_addresses, _product	datamodel dataset in (xdr_data) | fields _time, agent_hostname, agent_ip_addresses, _product
tonumber	index=xdr_data | eval tonumber_test = tonumber("90210")	datamodel dataset in (xdr_data) | alter tonumber_test = to_number("90210")

top	The following Splunk functions can be translated to XQL: • limit index = xdr_data | where action_app_id_risk > 0 | top limit=20 action_app_id_risk • countfield index = xdr_data | top countfield=count_agent_hostname agent_hostname by _time • showcount index = xdr_data | where action_app_id_risk > 0 | top 3 showcount=t action_app_id_risk • showperc index = xdr_data | where action_app_id_risk > 0 | top 3 showperc=t	• limit datamodel dataset in (xdr_data) | filter action_app_id_risk > 0 | top 20 action_app_id_risk top_count as count, top_percent as percent • countfield datamodel dataset in (xdr_data) |top 10 agent_hostname by _time top_count as count_agent_hostname, top_percent as percent • showcount datamodel dataset in (xdr_data) | filter action_app_id_risk > 0 | top 3 action_app_id_risk top_count as count, top_percent as percent • showperc datamodel dataset in (xdr_data) | filter action_app_id_risk > 0 | top 3 action_app_id_risk top_count as count, top_percent as percent • percentfield datamodel dataset in (xdr_data) | top 10 agent_hostname by _time top_count as count, top_percent as agent_hostname_percentage

	action_app_id_risk • percentfield index = xdr_data | top percentfield=agent_hostname_percentage agent_hostname by _time	
upper	index=xdr_data | eval field = upper("test")	datamodel dataset in (xdr_data) | alter field = uppercase("test")
var	index=xdr_data | stats var (event_type) by _time	datamodel dataset in (xdr_data) | comp var(event_type) by _time