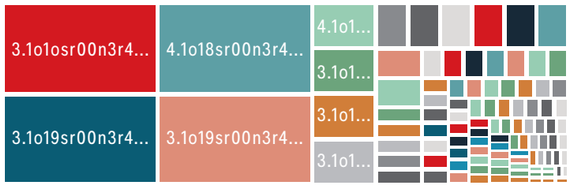
HUNT EXAMPLES

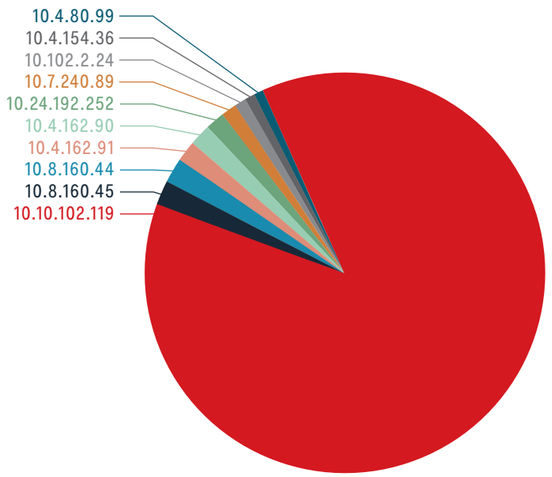
LONG DNS REQUESTS

```
query.domain MATCHES '.{150,}' GROUP BY
query.domain
```



HTTP POST TO IP ADDRESS

```
http:host.ip != null AND method = 'POST'
AND dst.internal = false GROUP BY
http:host.ip
```



POSSIBLE WEBSHELL COMMAND EXECUTION

```
src.internal = false AND ((uri.uri LIKE
'%whoami%') OR (uri.uri LIKE '%netstat%')
OR (uri.uri LIKE '%ifconfig%') OR (uri.uri
LIKE '%ipconfig%')) AND status_code = 200
GROUP BY uri.uri
```

uri.uri	count
/whoami	24
/whoami?r=http://p.alocdn.com/c/3843/i/COOKIE_UID/p.gif	19
/users/610/visitors/whoami	5
/live/boost/netstate/_ate.track.config_resp	2
/quiz-actions/a2536d84-7385-4003-82af-96f7ead2d71c/answers?apiAccount=...	2

Gigamon® | INSIGHT

IQL Quick Reference Guide

NEED HELP?

Contact your Technical Account Manager for assistance, or email **ce@gigamon.com.**

DOWNLOAD A COPY

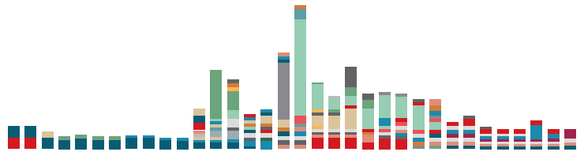
Gigamon Insight Portal > Help > Documentation > IQL Quick Reference Guide or gigamon.com/insight-iql-guide.

07.24.2019

NETWORK SECURITY POSTURE EXAMPLES

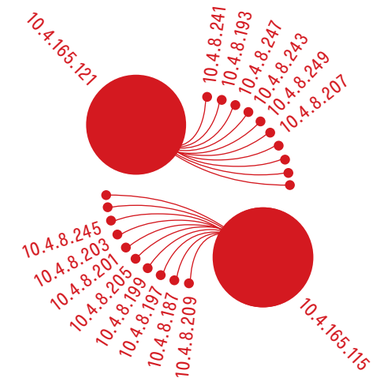
CLOUD STORAGE USE OVER TIME

```
http:host MATCHES
'.*(dropbox.com|\.box.com).*' GROUP BY
HOUR(timestamp), src.ip
```



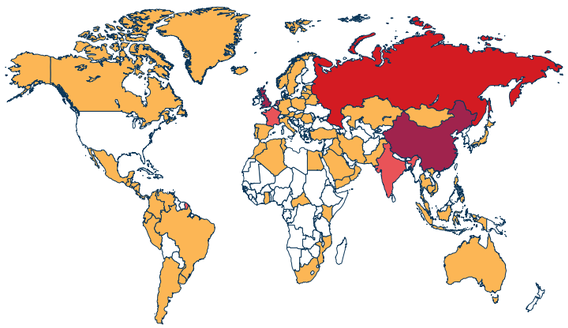
DEPRECATED SSL VERSIONS

```
ssl:version MATCHES 'SSLv[2,3]|TLSv10' AND
dst.internal = true AND src.internal =
false GROUP BY dst.ip, src.ip
```



OUTBOUND SSH SESSIONS

```
src.internal = true AND dst.internal =
false AND ssh:auth_success = true AND
dst.asn.isp NOT IN ( 'Amazon',
'Amazon.com', 'GitHub, Inc.', 'GitHub')
GROUP BY dst.geo.country, dst.asn.org
```



EVENTS AND PROPERTIES

EVENT TYPES

- Flow
- DNS
- HTTP
- SMTP
- X509
- Kerberos
- PE
- RDP
- SSH
- DHCP
- Software
- SSL
- Suricata
- SMB_FILE
- SMB_MAPPING
- NTLM
- TUNNEL
- FTP
- DCE-RPC

FIELD PRIMITIVES

Type	Syntax	Examples
IP	`8.8.8.8, '10.0.0.0/8', "192.168.1.1"`	`ip, src.ip, answer.ip`
Timestamp	`t'2017-02-08T17:49:10.017Z'`	`timestamp pe_compile_time`
String	`'www.google.com' "curl-agent"`	`domain user_agent`
Integer	`1234`	`total_pkts total_ip_bytes`
Float	`1.234`	`duration geo_distance`
Boolean	`true false`	`src.internal has_export_table`

SOURCE AND DESTINATION

Property	Description
`src.ip dst.ip`	IP address associated with the traffic
`src.port dst.port`	Port associated with the traffic
`src.ip_bytes dst.ip_bytes`	Bytes transferred from the provided endpoint src.ip_bytes ==> uploaded
`src.pkts dst.pkts`	Packets transferred from the provided endpoint
`src.internal dst.internal`	Boolean value defining whether the provided endpoint belongs to the customer IP space
`src.asn dst.asn`	Registration information such as AS number and registered organization
`src.geo dst.geo`	Geolocation information such as city and country

PROPERTY COMPARISONS

EQUAL OR NOT EQUAL: = == != <>

Exact field match

```
dst.port = 80
event_type == "http"
domain == "www.google.com"
http:referrer = null
```

(Records with no referrer)

```
ftp:dst.geo.country != 'US'
total_ip_bytes <> 0
http:host.ip != null
```

(HTTP records accessed by IP)

LESS/GREATER THAN (or equal to): < > <= >=

Filter on comparative size

```
timestamp > t"2017-01-01T00:00:00Z"
status_code < 500
duration <= 3600
duration <= 1 hour
src.ip_bytes >= 1000000
bytes >= 1gb
```

SET: IN

Exact match of multiple values

```
dst.ip IN ('8.8.8.8', '8.8.4.4')
http:method NOT IN ('GET', 'POST',
'CONNECT')
```

FUZZY: LIKE

Wildcards using SQL-like notation
% - 0 to many characters
_ - One character

```
rdp:cookie LIKE "_"
http:user_agent NOT LIKE 'Mozilla%'
ssh:cipher LIKE '%RC4%'
http:host.domain LIKE '%paypal%.%.com
```

REGEX: MATCHES

Lucene Regex support

```
ssl:version MATCHES 'SSLv[2,3]|TLSv10'
user_agent NOT MATCHES '.*Chrome\/6[0-9]\..*'
query.domain MATCHES '[a-zA-Z0-9]{16}\.onion((\.
([a-zA-Z]+|([xX][nN]--[a-zA-Z0-9]+)))+)?'
```

BUILDING COMPLEX QUERIES

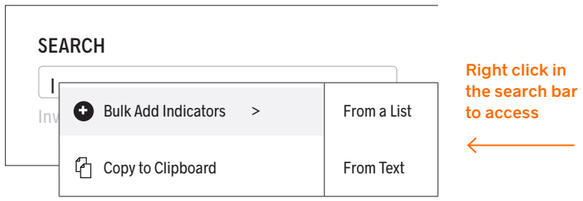
STRUCTURAL COMPONENTS

- ( )
- AND
- OR

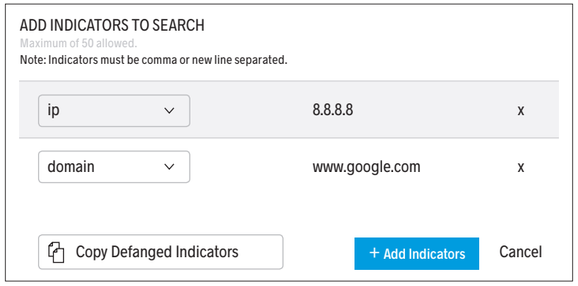
```
server_name MATCHES 'www\..*\.com' AND
subject MATCHES 'CN=www\..*\.net' AND
issuer MATCHES 'CN=www\..*\.com'

http:uri.uri LIKE '%.php?a=%&cd%&cr=%' OR
uri.uri LIKE '%/?f=%&a=%&cd=%&cr=%&ir='

(http:user_agent='hola_get' OR
http:host='client.hola.org') AND
src.internal = true

src.internal = true AND (user_agent LIKE
'%Windows_XP%' OR user_agent LIKE
'%Windows 2003%' OR user_agent LIKE
'%Windows NT 5.%' OR user_agent LIKE
'%Windows 2000%' OR user_agent LIKE
'%Windows NT 4.%')
```

BULK INDICATOR PARSING

Quickly search across your environment for multiple indicators by pasting an unformatted text blob (or list of indicators) into the bulk indicator search feature.
From the search tab, right click on the search bar to import from a list or text blob:



Gigamon Insight will parse the contents for IoCs (IPs, domains, hashes, etc.), remove common defanging techniques and generate a query to run in your environment.



AGGREGATIONS

Aggregate up to two fields using `GROUP BY`. Returns top 100 aggregate values of $field1 and top 10 of `$field2`. Modify counts using limit. Maximum of 10,000 aggregates.

Unique Value Counting

```
src.internal = true AND dst.internal = false AND
service = 'dns' GROUP BY dst.ip

src.internal = true AND http:host MATCHES
'.*(gotomypc.com|logmein.com)' GROUP BY src.ip
LIMIT 20, http:host LIMIT 4

src.internal = true AND dst.internal = false AND
service = 'http' GROUP BY src.ip LIMIT 10000
```

Aggregate Functions

SUM

Sum of integer or float field

```
src.internal = true AND src.ip_bytes >
1000000000 AND dst.ip_bytes < 500000000 AND dst.
internal = false GROUP BY dst.asn.org, SUM(src.
ip_bytes)

src.internal = true AND dst.asn.asn_org =
'Amazon.com, Inc.' GROUP BY src.ip, SUM(total_ip_
bytes)
```

MIN/MAX

Min/Max value of integer, float, timestamp field

```
http:host.domain = 'lumtest.com' AND
uri.uri = '/myip.json' AND
referrer.host.domain = null GROUP BY
src.ip, MIN(timestamp)

service = 'ssh' AND src.internal = true
AND dst.internal = false GROUP BY src.ip,
MAX(duration)
```

MINUTE/HOUR/DAY

X-duration buckets of events based on any timestamp field

```
src.internal = true AND dst.internal =
false AND flow:service != null GROUP BY
HOUR(timestamp), service

dst.asn.asn_org = 'Dropbox, Inc.' GROUP BY
DAY(timestamp), SUM(total_ip_bytes)

intel.indicator != null AND
dst.asn.asn_org IN ('Hosting Solution
Ltd.','Digital Ocean, Inc.','Choopa, LLC')
GROUP BY dst.ip, HOUR(timestamp)
```