### 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

#### 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

#### Long DNS Requests
query.domain MATCHES '.{150,}' GROUP BY query.domain

#### HUNT EXAMPLES

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

### Field Primitives

<table>
<thead>
<tr>
<th>TYPE</th>
<th>SYNTAX</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>8.8.8.8, '10.0.0.8/8', '192.168.1.1'</td>
<td>ip, src.ip, answer.ip</td>
</tr>
<tr>
<td>Timestamp</td>
<td>'t'2017-02-08T17:49:10.017Z'</td>
<td>timestamp, pe_compile_time</td>
</tr>
<tr>
<td>String</td>
<td>'www.google.com'</td>
<td>domain, user_agent</td>
</tr>
<tr>
<td>Integer</td>
<td>1234</td>
<td>total_pkts, total_ip_bytes</td>
</tr>
<tr>
<td>Float</td>
<td>1.234</td>
<td>duration, geo_distance</td>
</tr>
<tr>
<td>Boolean</td>
<td>true, false</td>
<td>src.internal, has_export_table</td>
</tr>
</tbody>
</table>

### Source and Destination

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>src.ip</td>
<td>IP address associated with the traffic</td>
</tr>
<tr>
<td>dst.ip</td>
<td>Port associated with the traffic</td>
</tr>
<tr>
<td>src.ip_bytes</td>
<td>Bytes transferred from the provided endpoint</td>
</tr>
<tr>
<td>dst.ip_bytes</td>
<td>Bytes transferred from the provided endpoint</td>
</tr>
<tr>
<td>src.pkts</td>
<td>Packets transferred from the provided endpoint</td>
</tr>
<tr>
<td>dst.pkts</td>
<td>Packets transferred from the provided endpoint</td>
</tr>
<tr>
<td>src.internal</td>
<td>Boolean value defining whether the provided endpoint belongs to the customer IP space</td>
</tr>
<tr>
<td>dst.internal</td>
<td></td>
</tr>
<tr>
<td>src.asn</td>
<td>Registration information such as AS number and registered organization</td>
</tr>
<tr>
<td>dst.asn</td>
<td></td>
</tr>
<tr>
<td>src.geo</td>
<td>Geolocation information such as city and country</td>
</tr>
<tr>
<td>dst.geo</td>
<td></td>
</tr>
</tbody>
</table>

### Property Comparisons

**Equal or Not Equal:**
- dst.port = 80
- event_type == "http"
- domain == "www.google.com"
- http:referrer = null
- ftp:dst.geo.country != 'US'
- total_ip_bytes <> 0
- http:host.ip != null

**Less/Greater than (or equal to):**
- timestamp > 't"2017-01-01T00:00:00Z"
- status_code < 500
- duration <= 3600
- duration <= 1 hour
- src.ip_bytes >= 1000000
- bytes >= 1gb

**Set:**
- dst.ip IN ("8.8.8.8", "8.8.4.4")
- http:method NOT IN ("GET", "POST", "CONNECT")

### Nested Field Queries

<table>
<thead>
<tr>
<th>QUERY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>intel.feed = 'Alexa Top Domains' AND intel.severity = 'high'</td>
<td>Filters on aggregated values on all intel objects</td>
</tr>
<tr>
<td>intel {feed = 'Alexa Top Domains' AND severity = 'high'}</td>
<td>Filter on individual objects of intel field</td>
</tr>
</tbody>
</table>

Note that scoped syntax, (i.e., using braces ({ })) only works for nested fields.

### List of Nested Fields
- answers
- files
- http.headers.proxied_client_ips
- intel
- path
- san_dns
- san_ip
to
uri.params

### Property Comparisons

### Equal or Not Equal:
- dst.port = 80
- event_type == "http"
- domain == "www.google.com"
- http:referrer = null
- ftp:dst.geo.country != 'US'
- total_ip_bytes <> 0
- http:host.ip != null

### Less/Greater than (or equal to):
- timestamp > 't"2017-01-01T00:00:00Z"
- status_code < 500
- duration <= 3600
- duration <= 1 hour
- src.ip_bytes >= 1000000
- bytes >= 1gb

### Set:
- 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/\(0-9\)\}..""
Structural Components

+ ( )
+ AND
+ OR

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

httpuri.uri LIKE '%.php?a=%&cd%&cr=%' OR uri.uri LIKE

(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 5.3%' OR user_agent LIKE '%Windows 2000%' OR user_agent LIKE '%Windows NT 4.3%')

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:

SEARCH

Bulk Add Indicators
From a List
Copy to Clipboard
From Text

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

ADD INDICATORS TO SEARCH

Note: Indicators must be comma or new line separated.

ip   8.8.8.8 x

domain   www.google.com x

Copy Defanged Indicators
Add Indicators
Cancel

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 > 100000000 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)