MQL Demo Searches

Identifying Classes of Data in your Environment

has(class) | groupby [metaclass,class]

Pivoting on Intel Hits

class=intel_hit type=4 intelwhitelisted=false intel_context.observable_threat_actors=apt1 | table [meta_ts,intelmatchclass,intel_context.observable_threat_actors,intel_context.observable_labels]

Subsearch

srcipv4:(metaclass=connection dstcountrycode:ru) srcisp:private* has(username) | groupby [username]

Hunting Network Logons

class:ms_windows_event eventid=4624 logontypeid=3 !username:/\$/

Regex on URI

class=bro_http uri:/\b(?<=https?:\/\/)(?!www\.paypal\.com\/)\S{0,40}pa?y\S{0,2}al(?!\S*\.com\/)/

FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.082019

Searches from Slides

Searches

Freeform search (Raw data): google.com
Exact match: domain=google.com
Partial match: domain:google.com
Exclusion: !domain:google.com
Exclusion: NOT domain:google.com

Array

domain:[google.com,Microsoft.com,yahoo.com]
domain:&[google.com,cache]

Aliases

~ipv4=215.18.25.33
~port=445

Regex

Search-only
Prefix: username:sm*
Suffix: uri:*index.php
In search, *use other fields to limit results:*
PCRE: useragent:/^\(\)\s+\{/

Lists

Create lists using CONFIGURE > Lists.

domain:$google_clients

Range Pair

dstport:<20,124>

Network

CIDR Range:
class:bro_http srcipv4:10.0.0.0/8
| groupby srcipv4
Private IP address space:
class:bro_http
!dstisp:"private ip address lan"

Nested Object

detect_rulematches.rulename:"fireeye nx alert [malware-object]"

Subsearch

srcipv4:(rawmsg:Trojan) dstipv4:(intelmatchvalue in class:intel_hit intelmatchfield:srcipv4) !class:intel_hit

Directives

Time

domain: dstcountrycode=ru start:"24 hours ago" end:"1 hour ago"
domain: dstcountrycode=ru start:201805300100

Page Size

srcipv4=215.18.25.33 {page_size:50}

Transforms

Sort

tcp | sort < srcport
tcp | sort < [srcport,dstport]
tcp | sort < dstport | sort > dstport

Groupby

class:bro_http | groupby useragent
class:bro_http | groupby useragent 100
class:bro_http | groupby < useragent 10
class:bro_http | groupby useragent 100 50
class:bro_http | groupby [dstport,dstcountrycode]
class:bro_http | groupby < dstport

Table

class=bro_http | table[meta_ts,srcipv4,dstipv4,dstport,domain] | sort < domain

Histogram

Dash-board only.

class=fireeye_nx {limit:0} | histogram meta_ts hour

FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.082019