

Best Practices for MQL in Rules

Best Practices for MQL in Rules

- Use the Taxonomy - specify metaclass or class
- Do not use MQL search-only features(transforms, groupbys, freeform, partial matching searches, aliases)
- Escape spaces and keywords with quotes (single or double)
- Anchor regex searches
- Do not use too many distinguishers
- Do not use URI as a distinguisher
- Use Lists

Specify Class and Metaclass

All rules should contain **at least** one class or metaclass reference.

INDEX SEARCH ▾ dstipv4=12.34.56.78

Query

metaclass=http_proxy dstipv4=12.34.56.78

Number of events to
analyze in 24 hours

558.4M

13.2M



3

©2019 FireEye | Private & Confidential

Search-only MQL Features

- Freeform static search INDEX SEARCH ▾ metaclass=http_proxy index.php
- Prefix matching INDEX SEARCH ▾ metaclass=http_proxy domain:softtek*
- Transforms INDEX SEARCH ▾ metaclass=http_proxy index.php | groupby [domain]
- Subsearch INDEX SEARCH ▾ srcipv4:(metaclass=http_proxy index.php)
- Alias INDEX SEARCH ▾ ~ip4=192.168.171.20



4

©2019 FireEye | Private & Confidential

Regular Expressions in Rules

Update Freeform/Matching Searches to RegEx in Rules

Freeform static search

INDEX SEARCH ▾ metaclass=http_proxy index.php

Query

metaclass=http_proxy uri:/index\..php/

Prefix matching

INDEX SEARCH ▾ metaclass=http_proxy domain:softtek*

Query

metaclass=http_proxy domain:/^softtek.* /



5

©2019 FireEye | Private & Confidential

Balance Distinguishers

- Danger of creating too many alerts to act if there are too many distinguishers
- Avoid URI field as a distinguisher



6

©2019 FireEye | Private & Confidential

Use Lists

Replace

```
metaclass:[file_xfer,http_proxy]
md5:[12345678c534e304c5e529f64637c4a5,55bb
952454d714b12345678e17a5ac71,24c0101234567
89e50b1ac413ffadb195,4123456783653c3e81944
abc377d,742d48849e522eefc2fec99d12345678]
OR
domain:[\"foo0.com\", \"bar0.com\", \"foo1.com
\", \"foo0.net\", \"bar0.net\", \"foo1.net\",
\"bar1.net\", \"f002.net\"]
```

With

```
metaclass:[file_xfer,http_proxy]
md5:$list_of_evil_md5s OR
domain:$list_of_evil_domains
```

Consider using a list when...

1. You have a series of items that are referenced by multiple rules.
2. You have a series of more than 4-5 items.
3. You want to perform searches against a series of items, as well as write rules for those items.



7

©2019 FireEye | Private & Confidential