Qradar

- Ignore when another rule matches
- Qradar expiring whitelist
- Qradar global whitelist
- Reference Maps

Ignore when another rule matches

When a building block or rule matches it's specific fields, do not fire matched events

```
and NOT when a subset of at least this number of these rules, in order, from the
same|different source IP to the same destination IP, over this many seconds
```

Qradar expiring whitelist

Use AQL filter query

```
username LIKE 'testUser' and LONG(DATEFORMAT(starttime, 'yyyyMMdd')) < 20190429
```

Qradar global whitelist

Use Routing Rules with **forwarding > bypass correlation**

For IP ranges, use Network Hierarchy.

Reference Maps

[http://www.siem.su/docs/ibm/Technical_remarks/Reference_Data_Collections_Technical_Note.pdf]