# Фильтр трафика по протоколам

app\_proto == «name\_protocol»

## Пример1:

app\_proto == «encrypted» — выведет зашифрованный трафик за указанный период

app\_proto not in ("encrypted", http, smb) — выведет весть трафик кроме encrypted, и протоколов http, smb

app\_proto == "zabbix" — выведет трафик zabbix

Далее смотрим Атаки Сессии для детального просмотра

## Пример2 (транспортный протокол):

proto == "icmp" — выведет весь трафик транспортного протокола icmp

proto not in ("icmp") — выведет весь трафик, исключая транспортный протокол icmp

## Пример 3

alert.cls == "Unknown Traffic"

Фильтр неизвестного трафика

## Пример4 (прикладной протокол):

app\_proto == "ldap"

# Фильтрация по уровню опасности

alert.pr == «level\_dangerouse»

Пример:

alert.pr == 2 — выведет все события с уровнем опасности 2 за указанный период

# Фильтрация по ip адресам атакуемого

alert.victim.ip == «IP атакуемого»

## Пример:

alert.victim.ip == 10.75.5.175 — вывод всех атак на ip адрес

alert.victim.ip not in ("10.75.5.175") — вывод всех атак на все IP, кроме 10.75.5.175

# Фильтрация по по IP адресам атакующего

alert.attacker.ip == «IP address»

## Пример:

alert.attacker.ip == 10.78.7.41 — выведет весь трафик с атакующего IP адреса

# Фильтрация по login

credentials.login == "указать логин"

## Пример:

credentials.login == "admin" — выведет все вводы логина «admin»

credentials.login == "admin" && credentials.valid == false — выведет все вводы логина «admin» с неуспешной идентификацией

host.ip == 10.78.133.73 && host.ip == 10.78.199.201 && credentials.login — выведет все данные по логинам между двумя хостами

host.ip == 10.78.133.73 && host.ip == 10.78.199.201 && credentials.login && credentials.password — добавит пароли

credentials.login && credentials.valid == "true" – выведет все удачные авторизации

# Фильтр по типу шифрования

Признак использования небезопасного типа шифрования 'RC4\_HMAC\_MD5':

kerberos.rsp.ticket.etype == "KRB\_ETYPE\_RC4\_HMAC"

# Фильтрация по подсети

src.ip == <ip/24>

Пример:

src.ip == 10.75.228.0/24 — выведет все IP из подсети 10.75.228.0/24