PUT /\_watcher/watch/user-30day-login

{

"metadata": {

"watch" : "user 30 day login activity"

},

"trigger": {

"schedule": {

"interval": "1m"}},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-hbss-audit-\*" ],

"body" : {

"query":{

"bool" : {

"must" : { "match" : { "cmdname.keyword" : "Logon Attempt" }}

}},

"size": 0,

"aggs":{

"by\_user":{

"terms":{

"field":"username.keyword",

"min\_doc\_count": 0,

"order" : { "\_count" : "asc" },

"size":10000

} ,

"aggs": {

"by\_date": {

"date\_histogram": {

"field": "starttime",

"interval": "30d",

"order" : { "\_count" : "asc" },

"min\_doc\_count": 0,

"extended\_bounds": {

"min": "now-3M",

"max": "now"

}

}

},

"categories": {

"terms": {

"field": "\_count"

}

},

"min\_bucket\_selector": {

"bucket\_selector": {

"buckets\_path": {

"count": "categories.\_bucket\_count"

},

"script": {

"inline": "params.count != 0"

}

}

}

}

}

} } }}},

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "USER 30 DAY LOGIN ACTIVITY ALERT"

}},

"my-webhook": {

"webhook" : {

"method" : "POST",

"host" : "bigbrother3.arl.army.mil",

"port" : 9612,

"body" : "{{ctx.id}}"

}},

"send\_email" : {

"email" : {

"to" : "ian.t.robertson.ctr@mail.mil",

"subject" : "Testing USER signal",

"body": "{{ctx.payload.aggregations}} "

}

}

}}