POST \_xpack/watcher/watch/\_execute

{

"watch": {

"trigger": {

"schedule": {

"daily": {

"at": {

"hour": 5,

"minute": 0

}

}

}

},

"input": {

"search": {

"request": {

"indices": [

"bb-hbss-audit\*"

],

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"starttime": {

"gt": "now-1y"

}

}

},

{

"exists": {

"field": "username"

}

},

{

"term": {

"cmdname.keyword": {

"value": "Logon Attempt"

}

}

},

{

"term": {

"message": {

"value": "successful"

}

}

}

]

}

},

"size": 0,

"aggs": {

"by\_user": {

"terms": {

"field": "username.keyword",

"size": 1000000

},

"aggs": {

"inactive\_periods": {

"scripted\_metric": {

"init\_script": "params.\_agg.logins = []",

"map\_script": "params.\_agg.logins.add(doc.starttime.value)",

"reduce\_script": "def login\_times = [];for (agg in params.\_aggs){for (times in agg.values()) {for (time in times) {login\_times.add(time);}}}Collections.sort(login\_times);def period\_ms = 30L \* 24 \* 60 \* 60 \* 1000;def inactive\_periods = [];def t1 = login\_times.get(login\_times.size()-1);def t2 = System.currentTimeMillis();def inactive\_duration = t2 - t1;if (inactive\_duration > period\_ms) {def start = new Date(t1);def end = new Date(t2);def duration = Duration.ofMillis(inactive\_duration);inactive\_periods.add(['login': start, 'next\_login': end, 'duration\_iso8601': duration]);} return ['hits': inactive\_periods.size(), 'periods': inactive\_periods];"

}

}

}

}

}

}

}

}

},

"condition": {

"script": "for (b in ctx.payload.aggregations.by\_user.buckets) {if (b.inactive\_periods.value.hits > 0) {return true;}}return false;"

},

"transform" : {

"script" : "def output = []; for (b in ctx.payload.aggregations.by\_user.buckets){ if (b.inactive\_periods.value.hits == 0) { continue; } output.add( b.key);} Collections.sort(output); return output;"

},

"actions": {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

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

}},

"send\_email" : {

"email" : {

"to" : ["ian.t.robertson.ctr@mail.mil"], "subject" : "DAILY INACTIVE USER REPORT",

"body": "The following users are currently in a state of inactivity. The period of inactivity is defined as greater than or equal to 30 days from today:\n\nUsing the HBSS Audit Dataset.\n\nUSERNAME \n\n {{#ctx.payload.\_value}} \t {{.}} \n\n{{/ctx.payload.\_value}}"

}

}}

}

}

PUT \_xpack/watcher/watch/inactive-users

{

"metadata": {

"title" : "List of Inactive Users",

"description": "The following list of users have been identified as not having logged on the system within the past 30 days. Using a window of 1 year."

},

"trigger": {

"schedule": {

"daily": {

"at": {

"hour": 5,

"minute": 0

}

}

}

},

"input": {

"search": {

"request": {

"indices": [

"bb-hbss-audit\*"

],

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"starttime": {

"gt": "now-1y"

}

}

},

{

"exists": {

"field": "username"

}

},

{

"term": {

"cmdname.keyword": {

"value": "Logon Attempt"

}

}

},

{

"term": {

"message": {

"value": "successful"

}

}

}

]

}

},

"size": 0,

"aggs": {

"by\_user": {

"terms": {

"field": "username.keyword",

"size": 1000000

},

"aggs": {

"inactive\_periods": {

"scripted\_metric": {

"init\_script": "params.\_agg.logins = []",

"map\_script": "params.\_agg.logins.add(doc.starttime.value)",

"reduce\_script": "def login\_times = [];for (agg in params.\_aggs){for (times in agg.values()) {for (time in times) {login\_times.add(time);}}}Collections.sort(login\_times);def period\_ms = 30L \* 24 \* 60 \* 60 \* 1000;def inactive\_periods = [];def t1 = login\_times.get(login\_times.size()-1);def t2 = System.currentTimeMillis();def inactive\_duration = t2 - t1;if (inactive\_duration > period\_ms) {def start = new Date(t1);def end = new Date(t2);def duration = Duration.ofMillis(inactive\_duration);inactive\_periods.add(['login': start, 'next\_login': end, 'duration\_iso8601': duration]);}return ['hits': inactive\_periods.size(), 'periods': inactive\_periods];"

}

}

}

}

}

}

}

}

},

"condition": {

"script": "for (b in ctx.payload.aggregations.by\_user.buckets) {if (b.inactive\_periods.value.hits > 0) {return true;}}return false;"

},

"transform" : {

"script" : "def output = []; for (b in ctx.payload.aggregations.by\_user.buckets){ if (b.inactive\_periods.value.hits == 0) { continue; } output.add( b.key);} Collections.sort(output); return output;"

},

"actions": {

"send\_email" : {

"email" : {

"to" : ["ian.t.robertson.ctr@mail.mil", "david.d.jaccard.ctr@mail.mil", "kenneth.d.renard.ctr@mail.mil", "james.s.herron.ctr@mail.mil", "akhilomen.o.oniha.civ@mail.mil", "daniel.f.baggeroer.ctr@mail.mil", "jason.m.rogowski.ctr@mail.mil", "john.e.shaffer.ctr@mail.mil", "cesar.e.pie.ctr@mail.mil","michael.b.bost.ctr@mail.mil", "mario.barboza.civ@mail.mil", "carlos.j.mateo.ctr@mail.mil", "jesse.d.kurrus.ctr@mail.mil", "usarmy.adelphi.7-sig-cmd.list.cndsp-watch@mail.mil", "phillip.l.tucker.ctr@mail.mil", "stephen.r.neyens.ctr@mail.mil"],

"subject" : "DAILY INACTIVE USER REPORT",

"body": "The following users are currently in a state of inactivity. The period of inactivity is defined as greater than or equal to 30 days from today:\n\nUsing the HBSS Audit Dataset.\n\nUSERNAME \n\n {{#ctx.payload.\_value}} \t {{.}} \n\n{{/ctx.payload.\_value}}"

}

}}

}