POST \_xpack/watcher/watch/\_execute

{

"watch": {

"metadata": {

"window\_period": "3d",

"last\_period":"24h"

},

"trigger": {

"schedule": {

"interval": "24h"

}

},

"input": {

"search": {

"request": {

"indices": "pipeline-auth\*",

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"@timestamp": {

"gte": "now-{{ctx.metadata.window\_period}}"

}}

}]}

},

"aggs": {

"periods": {

"filters": {

"filters": {

"history": {

"range": {

"@timestamp": {

"gte": "now-{{ctx.metadata.window\_period}}"

}

}

},

"last\_period": {

"range": {

"@timestamp": {

"gte": "now-{{ctx.metadata.last\_period}}"

}

}

}

}

},

"aggs": {

"hosts": {

"terms": {

"field": "client\_addr",

"size": 10000

}

}

}

}

},

"size": 0

}

}

}

},

"condition" : {

"script": "return ctx.payload.aggregations.periods.buckets.history.hosts.buckets.size() > ctx.payload.aggregations.periods.buckets.last\_period.hosts.buckets.size();"

},

"transform": {

"script": {

"file": "transform-last-known-time"

}

},

"actions": {

"send\_email" : {

"email" : {

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

"subject" : "Systems Reporting Status (Alpha)",

"body": "Pipeline Auth Logs\n@author: Ian Robertson\n\n The following systems have not reported logs in the last {{ctx.metadata.last\_period}} hours using a {{ctx.metadata.window\_period}} window.\nUSE CASE: Verify Systems Reporting, Systems connectivity, and/or Data Validation \nDo per each index type.\n\n {{#ctx.payload.\_value}}{{.}} \n \n {{/ctx.payload.\_value}}\n\nPayload: \n\n{{ctx.payload}}"

}

}

}

}

}