POST /\_xpack/watcher/watch/\_execute?pretty

{

"watch" : {

"trigger": {

"schedule": {

"interval": "24h"

}

},

"input": {

"search": {

"request": {

"indices": [

"pipeline-windows-\*"

],

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"@timestamp": {

"gt": "now-7d"

}

}

},

{

"exists": {

"field": "Username"

}

}

],

"must\_not" : [

{

"term" : {

"SecurityID" : "S-1-5-21" }

},

{

"term" : {

"SubjectDomainName" : "NAE"

}

}]

}

},

"size": 0,

"aggs": {

"by\_user": {

"terms": {

"field": "Username",

"size": 1000000

},

"aggs" : {

"events" : {

"terms" : {

"field" : "EventID"

}

}

}}

}}}

}

},

"condition": {

"compare": {

"ctx.payload.hits.total": {

"gt": 0

}

}

},

"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", "lewis.e.brooks.civ@mail.mil", "john.e.shaffer.ctr@mail.mil", "greg.a.weaver3.civ@mail.mil", "tracy.d.braun.civ@mail.mil", "cesar.e.pie.ctr@mail.mil", "curtis.b.arnold.civ@mail.mil", "matthew.c.ryan.ctr@mail.mil", "aaron.m.pratt.ctr@mail.mil", "antonio.r.fields.ctr@mail.mil", "richard.a.dietz.ctr@mail.mil", "michael.b.bost.ctr@mail.mil", "mario.barboza.civ@mail.mil", "carlos.j.mateo.ctr@mail.mil", "michael.b.devaughn.ctr@mail.mil", "jesse.d.kurrus.ctr@mail.mil", "jason.w.schaum.ctr@mail.mil", "lee.c.trossbach.ctr@mail.mil", "phillip.l.tucker.ctr@mail.mil", "stephen.r.neyens.ctr@mail.mil"], "subject" : "Who's Watching You?",

"body": "Description: This is an overall look at a test instance of how we are analyzing user activities on our Windows Domain. Below is an aggregation of Windows User accounts combined with the Windows Event ID for executables and sorted by number of occurrences within the last 7 days based upon a limited dataset.\n\n{{#ctx.payload.aggregations.by\_user.buckets}}{{key}} : \n {{#events.buckets}} \n \t {{key}} : # of executions {{doc\_count}} \n{{/events.buckets}}\n {{/ctx.payload.aggregations.by\_user.buckets}}"

}

}

}

}

}