**/////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*DAILY USER REPORT**

PUT /\_watcher/watch/daily-user-report

{

"trigger": {

"schedule": {

"daily": {

"at": {

"hour": 5,

"minute": 0

}

}

}

},

"input": {

"search": {

"request": {

"indices": [

"pipeline-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": {"file":"reduce-inactiveusers"}

}

}

}

}

}

}

}

}

},

"condition": {

"script": {

"file": "condition"

}

},

"transform": {

"script": {

"file": "transform-inactiveusers"

}

},

"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"], "subject" : "DAILY USER REPORT (Alpha)",

"body": "The following users are currently in an inactive state for the past 30 Days or more:\n\n{{ctx.payload}}\n"

}

}

}

}

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INACTIVE USERS (SLIDING WINDOW)**

POST \_xpack/watcher/watch/\_execute

{

"watch": {

"trigger": {

"schedule": {

"monthly" : { "on" : 1, "at" : "noon" }

}

},

"input": {

"search": {

"request": {

"indices": [

"pipeline-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": {"file":"reduce-inactive-slidingwindow"}

}

}

}

}

}

}

}

}

},

"condition": {

"script": {

"file": "condition"

}

},

"transform": {

"script": {

"file": "transform-inactiveusers"

}

},

"actions": {

"send\_email" : {

"email" : {

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

"subject" : "MONTHLY USER REPORT: All 30-Day Inactive Users List",

"body": "The following users had periods of inactivity greater than 30 days within the past year:\n\n{{ctx.payload}}\n\n"

}

}

}

}

}

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INACTIVE USER MATCH**

PUT /\_watcher/watch/inactive-users

{

"trigger": {

"schedule": {

"interval": "1h"

}

},

"input" : {

"search" : {

"request" : {

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

"body" : {

"query": {

"bool": {

"must": [

{

"exists": {

"field": "username"

}

},

{

"term": {

"cmdname.keyword": {

"value": "Logon Attempt"

}

}

},

{

"term": {

"message": {

"value": "successful"

}

}

}

]

}

},

"size": 0,

"aggs": {

"by\_user": {

"terms": {

"field": "username.keyword",

"min\_doc\_count": 0,

"size": 1000000

},

"aggs": {

"by\_date": {

"date\_histogram": {

"field": "starttime",

"interval": "30d",

"min\_doc\_count": 0,

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

"extended\_bounds": {

"min": "now-12M",

"max": "now"

}

}

}

}

}

}

}

}

}

},

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "INACTIVE USER ACTIVITY ALERT"

}},

"send\_email" : {

"email" : {

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

"subject" : "30-Day Inactive Users",

"body": "USERNAME \t # Logins \n\n {{#ctx.payload.aggregations.by\_user.buckets}}{{key}}: {{doc\_count}}\n{{/ctx.payload.aggregations.by\_user.buckets}}"

}

},

"my-webhook": {

"webhook" : {

"method" : "POST",

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

"port" : 9612,

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

}}}}

**//////////////////////VERSION 2 with SCRIPTING**

PUT /\_watcher/watch/inactive-users

{

"trigger": {

"schedule" : {

"daily" : {

"at" : {

"hour" : 22,

"minute" : 51

}

}

}

},

"input" : {

"search" : {

"request" : {

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

"body" : {

"query": {

"bool": {

"must": [

{

"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": {

"by\_date": {

"date\_histogram": {

"field": "starttime",

"interval": "30d",

"min\_doc\_count": 0,

"extended\_bounds": {

"min": "now-12M",

"max": "now"

}

}

}

}

}

},

"function\_score": {

"script\_score": {

"script": {

"lang": "painless",

"inline": "int foo = 1;int foo2 = 3; return foo+foo2;"

}

} }}

}

}

},

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "INACTIVE USER ACTIVITY ALERT @ MIDNIGHT"

}},

"send\_email" : {

"email" : {

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

"subject" : "Testing HBSS signal",

"body": "HBSS USER MATCH DETECTED. MIDNIGHT RUN. TESTING BODY."

}

},

"my-webhook": {

"webhook" : {

"method" : "POST",

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

"port" : 9612,

"body" : "{{ctx.payload.aggregations.by\_user.buckets}}"

}}}}

**///////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*USER 30 DAY ORIGINAL SCRIPT**

curl -XPUT 'elastic:changeme@bigbrother3.arl.army.mil:9200/\_watcher/watch/user-30day-login' -d '

{

"metadata": {

"watch" : "user 30 day login activity"

},

"trigger": {

"schedule": {

"interval": "1m"}},

"input" : {

"search" : {

"request" : {

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

"body" : {

"query":{

"bool" : {

"must" : { "exists" : { "field" : "username" }} AND

"term" : {"cmdname": { "Logon Attempt"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-30d"}}}

}},

"size":0,

"aggs":{

"by\_user":{

"terms":{

"field":"username.keyword",

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

"size":100}

}}

} } } } } ,

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

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

}},

"my-webhook": {

"webhook" : {

"method" : "POST",

"host" : "bigbrother3",

"port" : 9612,

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

}}}}'

**//////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*VERSION 3 FROM 1/13/2017**

PUT /\_watcher/watch/inactive-users

{

"trigger": {

"schedule": {

"interval": "1h"

}

},

"input" : {

"search" : {

"request" : {

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

"body" : {

"query": {

"bool": {

"must": [

{

"range":

{"@timestamp": {

"gte": "now-12M",

"lte": "now"

}

}},

{

"exists": {

"field": "username"

}

},

{

"term": {

"cmdname.keyword": {

"value": "Logon Attempt"

}

}

},

{

"term": {

"message": {

"value": "successful"

}

}

}

]

}

},

"size": 0,

"aggs": {

"by\_user": {

"terms": {

"field": "username.keyword",

"min\_doc\_count": 0,

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

"size": 1000000

},

"aggs": {

"by\_date": {

"date\_histogram": {

"field": "starttime",

"interval": "30d",

"min\_doc\_count": 0,

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

"extended\_bounds": {

"min": "now-3M",

"max": "now"

}

}

}

}

}

}

}

}

}

},

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "INACTIVE USER ACTIVITY ALERT"

}},

"send\_email" : {

"email" : {

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

"subject" : "30-Day Inactive Users",

"body": "{{ctx.payload.aggregations.by\_user.buckets}}"

}

},

"my-webhook": {

"webhook" : {

"method" : "POST",

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

"port" : 9612,

"body" : "{{ctx.payload.aggregations.by\_user.buckets}}"

}}}}

**//////////////////////////WATCH EXE**

POST \_xpack/watcher/watch/\_execute

{

"watch": {

"trigger": {

"schedule": {

"daily": {

"at": {

"hour": 5,

"minute": 0

}

}

}

},

"input": {

"search": {

"request": {

"indices": [

"pipeline-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": {"file":"reduce-inactiveusers"}

}

}

}

}

}

}

}

}

},

"condition": {

"script": {

"file": "condition"

}

},

"transform": {

"script": {

"file": "transform-inactiveusers"

}

},

"actions": {

"send\_email" : {

"email" : {

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

"subject" : "TESTING (RAW Data): 30-Day Inactive Users List",

"body": "The following users had periods of inactivity greater than 30 days within the past year:\n\nThe payload is formatted into a dictionary containing user names mapped to an array of inactivity periods.\n{ \n\tuserX: { \n\t\tlogin: <date>,\n\t\t\tnext\_login: <date>,\n\t\t\tduration\_iso8601: <duration between logins in ISO 8601 format>\n\t}\n}\n\n{{ctx.payload}}\n\nDATA: \n\n{{#ctx.payload}}{{key}}: {{if(inactive\_periods != 0) {inactive\_periods} else{} }}\n{{/ctx.payload}}\n\n"

}

}

}

}

}