Logic App Kusto Query Telemetry

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Execute: [Web] [Desktop] [Web (Lens)] [Desktop (SAW)] https://processus.kusto.windows.net/process

```
WorkflowTriggers
| where TIMESTAMP >= datetime(2021-06-01T00:00)
| where subscriptionId has "1e4f30e0-ba75-4721-ad01-092454a46d8b"
| where resourceGroup has "essAstPrdWu2RgSecurity"
| where flowName has "ast-sentinel-prd-square1awsguarddutyalerts"
| where status != ""
| summarize count() by status
```

Execute: [Web] [Desktop] [Web (Lens)] [Desktop (SAW)] https://processus.kusto.windows.net/process

```
WorkflowActions
| where TIMESTAMP >= datetime(2021-06-01T00:00)
| where subscriptionId has "1e4f30e0-ba75-4721-ad01-092454a46d8b"
| where resourceGroup has "essAstPrdWu2RgSecurity"
| where flowName has "ast-sentinel-prd-square1awsguarddutyalerts"
| where status != ""
| summarize count() by status
```

EXAMPLE, gov: Execute: [Web] [Desktop] [Web (Lens)] [Desktop (SAW)] https://processff.kusto.usgovcloudapi.net/process

```
HttpIncomingRequests | where operationName == "POST/WORKFLOWS/TRIGGERS/PATHS/INVOKE" | where targetUri startswith "https://prod-21.usgovvirginia.logic.azure.us:443/workflows/3a6b8a89d0a346ac8b8ca011c53f1606/triggers/" | project TIMESTAMP,TaskName,operationName,httpStatusCode
```

```
TIMESTAMP TaskName operationName httpStatusCode 2021-06-29 18:01:49.5305371 HttpIncomingRequestStart POST/WORKFLOWS/TRIGGERS/PATHS/INVOKE -1 2021-06-29 18:01:49.6206852 HttpIncomingRequestEndWithSuccess POST/WORKFLOWS/TRIGGERS/PATHS/INVOKE 202 2021-07-08 19:49:52.5751350 HttpIncomingRequestStart POST/WORKFLOWS/TRIGGERS/PATHS/INVOKE -1 2021-07-08 19:49:52.7619729 HttpIncomingRequestEndWithSuccess POST/WORKFLOWS/TRIGGERS/PATHS/INVOKE 202
```