// Custom parser for Google Workspace Audit logs

{

attributes: {

"dataSource.category": "security",

"dataSource.name": "Google Workspace",

"dataSource.vendor": "Google"

},

patterns: {

keyPattern: "[^\"]+",

valuePattern: "[^\"]+",

valuePattern2: "[^\\}]+"

},

formats: [

{

format: ".\*\"events\": \\[$events=json{parse=dottedJson}$",

}, {

format: ".\*\"name\": \"$\_=keyPattern$\", \"value\": \"$\_=valuePattern$\"",

repeat: true

}, {

format: ".\*\"name\": \"$\_=keyPattern$\", \"boolValue\": $\_=valuePattern2$",

repeat: true

}, {

format: "${parse=dottedJson}$",

repeat: true,

rewrites: [

{

input: "id.time",

output: "timestamp",

match: "(\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}\\.\\d+Z)",

replace: "$1"

}

]

}

]

}