

```

{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "AutomationRuleDisplayName": {
      "metadata": {
        "description": "AutomationRuleDisplayName"
      },
      "defaultValue": "CMT-ReOpen-Closed-Email-Automation-Rule",
      "type": "String"
    },
    "workspace": {
      "type": "String",
      "metadata": {
        "description": "Log Analytics Workspace Name"
      }
    }
  },
  "resources": [
    {
      "name": "8794d879-97c8-4dac-a704-f7700ae8cd32",
      "type": "Microsoft.Operationallnsights/workspaces/providers/automationRules",
      "properties": {
        "displayName": "[parameters('AutomationRuleDisplayName')]",
        "order": 101,
        "triggeringLogic": {
          "isEnabled": false,
          "triggersOn": "Incidents",
          "triggersWhen": "Updated",
          "conditions": [
            {
              "conditionType": "Property",
              "conditionProperties": {
                "propertyName": "IncidentTitle",
                "operator": "Contains",
                "propertyValues": [
                  "Email reported by",
                  "Email messages containing ",
                  "Admin triggered manual investigation of email involving one user"
                ]
              }
            },
            {
              "conditionType": "Property",
              "conditionProperties": {
                "propertyName": "IncidentLabel",
                "operator": "NotEquals",
                "propertyValues": [
                  "Redirected"
                ]
              }
            },
            {
              "conditionType": "Property",
              "conditionProperties": {

```

```

        "propertyName": "IncidentUpdatedBySource",
        "operator": "Equals",
        "propertyValues": [
            "M365Defender"
        ]
    },
    {
        "conditionType": "PropertyChanged",
        "conditionProperties": {
            "propertyName": "IncidentStatus",
            "changeType": "ChangedTo",
            "operator": "Equals",
            "propertyValues": [
                "Closed"
            ]
        }
    }
],
},
"actions": [
    {
        "order": 1,
        "actionType": "ModifyProperties",
        "actionConfiguration": {
            "severity": null,
            "status": "Active",
            "classification": null,
            "classificationReason": null,
            "classificationComment": null,
            "owner": null,
            "labels": null
        }
    }
],
},
"apiVersion": "2019-01-01-preview",
"scope": "[concat('Microsoft.Operationallnsights/workspaces/', parameters('workspace'))]"
}
]
}

```