

Resilient Integration with GRR

This package contains one function that allows you to search for your GRR Agents using IP, Host or User.

Customization Settings

LayoutsRulesScriptsWorkflowsFunctionsMessage DestinationsPhases & TasksIncident TypesBreachArtifacts

Workflows / Example: GRR Search by IP

Cancel

Save & Close

Save

Name *

Example: GRR Search by IP

API Name *

example_grr_search_by_ip

Description

An example Workflow using the GRR Search Function to get a GRR Agent's information using their IP Address.

Object Type *

Artifact

Creator

Res Admin

Last Modified

10/19/2018 04:00

Last Modified By

Orchestration Engine

Associated Rules

GRR Search by IP



app.config Settings:

```
[fn_grr_search]
grr_server=http://127.0.0.1:8000
grr_user=user
grr_pwd=password
#Can be True/False
verify_cert=False
```

Function Inputs:

| Function Name | Type | Required | Example |
|------------------|--------|----------|--------------|
| grr_search_value | String | Yes | "127.0.0.1" |
| grr_search_type | Select | Yes | host/ip/user |

Function Output:

```
results = {
    'grr_search_type': u'ip',
    'grr_search_value': u'127.0.0.1',
    'success': True
}
```

```
'agents': [  
  {  
    u'age': u'1538997200410715',  
    u'agentInfo': {  
      u'buildTime': u'2018-06-28 09:10:40',  
      u'clientDescription': u'grr linux amd64',  
      u'clientName': u'grr',  
      u'clientVersion': 3232  
    },  
    u'clientId': u'C.ddc30808cf5d06d3',  
    u'firstSeenAt': u'1538497879090708',  
    u'fleetspeakEnabled': False,  
    u'hardwareInfo': {  
      u'biosReleaseDate': u'05/19/2017',  
      u'biosRevision': u'4.6',  
      u'biosRomSize': u'64 kB',  
      u'biosVendor': u'Phoenix Technologies LTD',  
      u'biosVersion': u'6.00',  
      u'serialNumber': u'VMware-56 4d f0 c8... 77 7e 65',  
      u'systemFamily': u'Not Specified',  
      u'systemManufacturer': u'VMware',  
      u'systemProductName': u'VMware Virtual Platform',  
      u'systemSkuNumber': u'Not Specified',  
      u'systemUuid': u'xxxx'  
    },  
    u'interfaces': [{...}, {...}, {...}, {...}, {...}, {...},  
    {...}, {...}],  
    u'knowledgeBase': {  
      u'fqdn': u'localhost.localdomain',  
      u'os': u'Linux',  
      u'osMajorVersion': 7,  
      u'osMinorVersion': 5,  
      u'osRelease': u'RedHat'  
    },  
    u'lastBootedAt': u'1538996573000000',  
    u'lastClock': u'1539009155388036',  
    u'lastSeenAt': u'1539009155394278',  
    u'memorySize': u'8653881344',  
    u'osInfo': {  
      u'fqdn': u'localhost.localdomain',  
      u'kernel': u'3.10.0-862.14.4.el7.x86_64',  
      u'machine': u'x86_64',  
      u'release': u'RedHat',  
      u'system': u'Linux',  
      u'version': u'7.5'  
    },  
    u'urn': u'aff4:/C.ddc30808cf5d06d3',  
    u'volumes': [  
      {  
        u'actualAvailableAllocationUnits': u'21684382',  
        u'bytesPerSector': u'4096',  
        u'sectorsPerAllocationUnit': u'1',  
        u'totalAllocationUnits': u'24093702',  
        u'unixvolume': {u'mountPoint': u'/'}
```

```

    }
  ]
}

```

Pre-Process Script:

This example sets the search value **to the value of the Incident's Artifact**.

```

# Set the grr_search_value
inputs.grr_search_value = artifact.value

```

Post-Process Script:

This example loops the found agents and **adds Notes to the Incident**.

```

if results.success:
    # Loop all found agents
    for agent in results["agents"]:

        note_text = """"<i style="color:#00af08">GRR Agent Found:</i>
            <br><b>System Product Name:</b> {0}
            <br><b>System UUID:</b> {1}
            <br><b>System Manufacturer:</b> {2}
            <br><b>Release:</b> {3}
            <br><b>Machine:</b> {4}
            <br><b>Version:</b> {5}""".format(agent["hardwareInfo"]
["systemProductName"],
                                     agent["hardwareInfo"]
["systemUuid"],
                                     agent["hardwareInfo"]
["systemManufacturer"],
                                     agent["osInfo"]["release"],
                                     agent["osInfo"]["machine"],
                                     agent["osInfo"]["version"])

        incident.addNote(helper.createRichText(note_text))

    else:
        note_text = "{0} system not found in
GRR".format(results.grr_search_value)
        incident.addNote(helper.createPlainText(note_text))

```

Rules

| Rule Name | Object Type | Workflow Triggered | Conditions |
|-----------|-------------|--------------------|------------|
|-----------|-------------|--------------------|------------|

| Rule Name | Object Type | Workflow Triggered | Conditions |
|------------------|-------------|---------------------------|-----------------------------|
| GRR Search by IP | Artifact | Example: GRR Search by IP | Type is equal to IP Address |