

 README.md

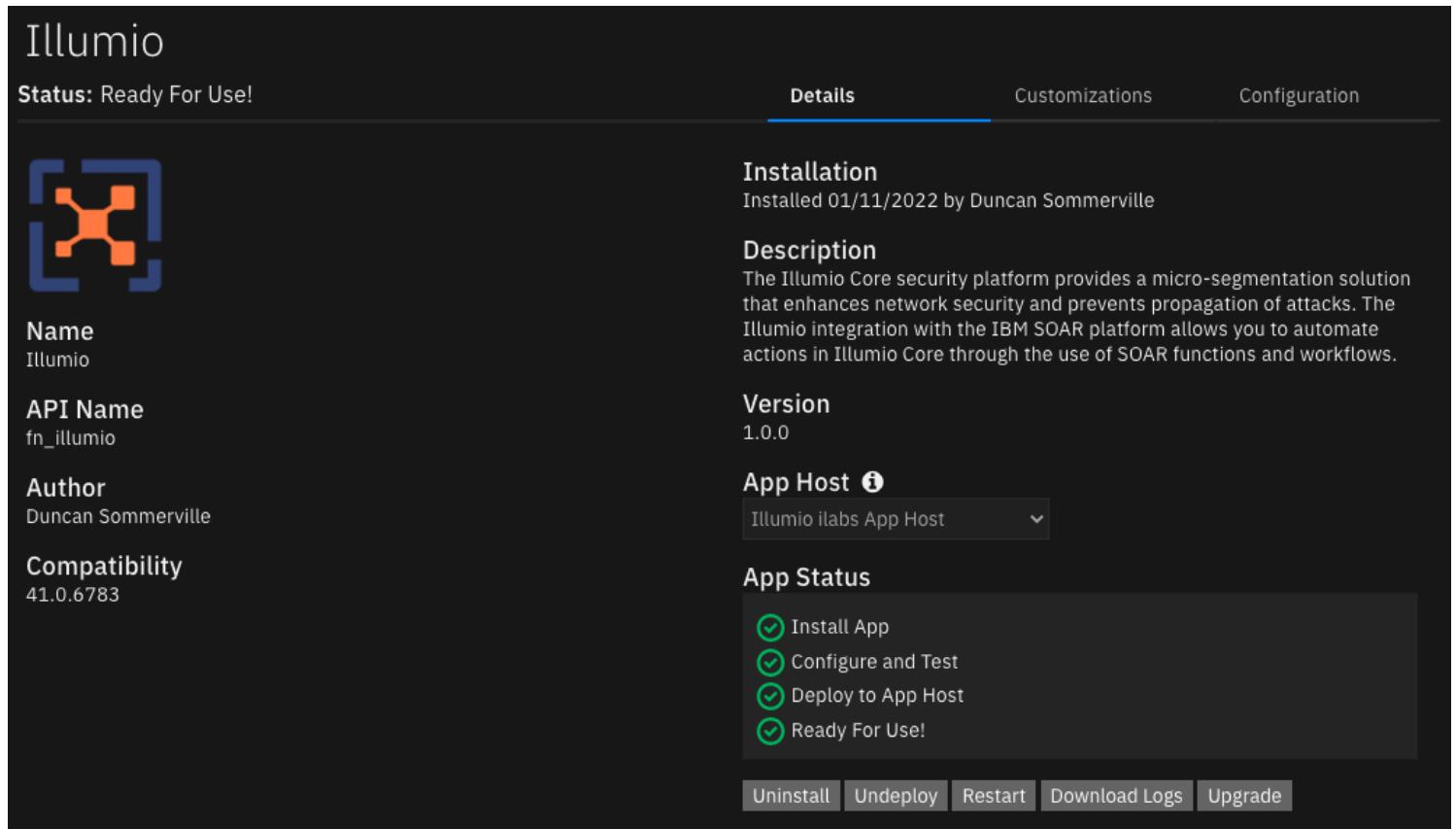
Illumio

Release Notes

| Version | Date | Notes |
|---------|---------|--|
| 1.0.0 | 02/2022 | Initial Release. Block port workflow and related actions |

Overview

Illumio Core Integration for IBM SOAR



The screenshot shows the Illumio Core integration app details page in the IBM SOAR platform. The top navigation bar includes tabs for **Details**, **Customizations**, and **Configuration**. The status is shown as "Ready For Use!". The app icon is a blue square with an orange 'X' shape. The app name is "Illumio". The API name is "fn_illumio". The author is "Duncan Sommerville". The compatibility version is "41.0.6783". The installation status is "Installed 01/11/2022 by Duncan Sommerville". The description states: "The Illumio Core security platform provides a micro-segmentation solution that enhances network security and prevents propagation of attacks. The Illumio integration with the IBM SOAR platform allows you to automate actions in Illumio Core through the use of SOAR functions and workflows." The version is "1.0.0". The app host is set to "Illumio ilabs App Host". The app status indicates that all steps (Install App, Configure and Test, Deploy to App Host, Ready For Use!) are completed successfully. At the bottom, there are buttons for Uninstall, Undeploy, Restart, Download Logs, and Upgrade.

The Illumio Core security platform provides a micro-segmentation solution that enhances network security and prevents propagation of attacks. The Illumio integration with the IBM SOAR platform allows you to automate actions in the Illumio Core Policy Compute Engine using SOAR functions and workflows.

You can find additional documentation for your version of Illumio Core through the [Illumio Support Portal](#).

The actions in this integration perform changes to the Illumio Policy Compute Engine that may impact the flow of traffic between workloads in your network. Please exercise caution when running functions and workflows to avoid service interruption.

Key Features

The following functions are currently implemented:

- Create an Enforcement Boundary
- Create a Rule Set
 - Create a Rule
- Create a Virtual Service
 - Bind Workloads to a Virtual Service
- Get an IP List by name
- Get one or more Workloads
- Provision policy objects
- Run a traffic analysis query
- Update the enforcement modes of one or more Workloads

Additionally, the integration provides the following workflow actions:

- Block traffic on a specified port and protocol across all Workloads

| Functions | | New Function |
|---|---|------------------------------|
| Name | Description | |
| Illumio: Update Workload Enforcement Mode | Update the Enforcement Mode for one or more workloads. | |
| Illumio: Run Traffic Analysis | Run an Explorer query to get a traffic analysis report based on the provided inputs. The query checks all sources and destinations for traffic on a given port/protocol. Returns up to 100,000 results. | |
| Illumio: Provision Objects | Provision draft policy changes for the given security policy objects. | |
| Illumio: Get Workloads | Get multiple workloads based on the given search criteria. | |
| Illumio: Get IP List | Get an IP List object by name. | |
| Illumio: Get Workload | Get a workload by HREF. | |
| Illumio: Create Enforcement Boundary | Create an enforcement boundary with an ingress service using the given port/protocol. | |
| Illumio: Create Virtual Service | Create a Virtual Service. | |
| Illumio: Create Ruleset | Create a ruleset security policy object. | |
| Illumio: Create Rule | Create a policy rule within a given ruleset. | |
| Illumio: Create Service Binding | Bind one or more workloads to an active virtual service. The virtual service must be created in draft and then provisioned for the call to work. | |

These functions are covered in more detail in the User Guide.

Requirements

This app supports the IBM Resilient SOAR Platform and the IBM Cloud Pak for Security.

Resilient platform

The Resilient platform supports two app deployment mechanisms, App Host and integration server.

If deploying to a Resilient platform with an App Host, the requirements are:

- Resilient platform >= 41.0.6783 .
- The app is in a container-based format (available from the AppExchange as a zip file).

If deploying to a Resilient platform with an integration server, the requirements are:

- Resilient platform >= 41.0.6783 .
- The app is in the older integration format (available from the AppExchange as a zip file which contains a tar.gz file).
- Integration server is running resilient-circuits>=42.0.0 .
- If using an API key account, make sure the account provides the following minimum permissions:

| Name | Permissions |
|----------|-------------|
| Org Data | Read |
| Function | Read |

The following Resilient platform guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Knowledge Center at ibm.biz/resilient-docs. On this web page, select your Resilient platform version. On the follow-on page, you can find the *App Host Deployment Guide* or *Integration Server Guide* by expanding **Resilient Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= 1.4.
- Cloud Pak is configured with an App Host.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

The following Cloud Pak guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security Knowledge Center table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Knowledge Center at ibm.biz/cp4s-docs. From this web page, select your IBM Cloud Pak for Security version. From the version-specific Knowledge Center page, select Case Management and Orchestration & Automation.

Illumio Core platform

The app supports Illumio Core >= 21.2.0. The app and the *illumio* python library it depends on rely on the Illumio Core REST API.

Proxy Server

The app **does** support a proxy server. Proxy settings can be specified in the app configuration file as detailed in the installation section below.

Python Environment

Python >= 3.6 is supported. Additional package dependencies may exist for each of these packages:

- `resilient-circuits>=42.0.0`
- `illumio>=0.7.2`

The *illumio* python library is provided as a wheel package and distributed as-is within the app integration binary and source releases under the `/lib` subdirectory.

For app host installations, the Dockerfile in the app distribution will automatically install the *illumio* library from `/lib`.

For integration server installations, the provided *illumio* wheel must be installed before installing the `fn_illumio` package:

```
# from the fn_illumio root
$ pip install ./lib/illumio*.whl
$ pip install .
```

Installation

Install

- To install or uninstall an App or Integration on the *Resilient platform*, see the documentation at ibm.biz/resilient-docs.
- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at ibm.biz/cp4s-docs and follow the instructions above to navigate to Orchestration and Automation.

App Configuration

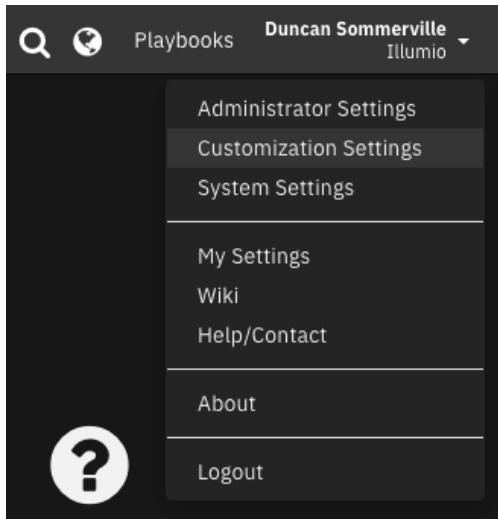
The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

```
[fn_illumio]
illumio_pce_domain_name = <PCE_DOMAIN_NAME>
illumio_pce_port = 443
illumio_pce_org_id = 1
illumio_pce_api_key = <PCE_API_KEY>
illumio_pce_api_secret = <PCE_API_SECRET>
# Optional proxy settings
#http_proxy=http://proxy:80
#https_proxy=https://proxy:80
```

| Config | Required | Example | Description |
|-------------------------|----------|-----------------------|---|
| illumio_pce_domain_name | Yes | example.pce.com | <i>The fully-qualified domain name of the Illumio Policy Compute Engine to connect to</i> |
| illumio_pce_port | Yes | 443 | <i>The port the Illumio Policy Compute Engine is listening on</i> |
| illumio_pce_org_id | Yes | 1 | <i>The organization ID to connect to on the Illumio Policy Compute Engine</i> |
| illumio_pce_api_key | Yes | api_1a1a2233b45c678d9 | <i>The Illumio Policy Compute Engine API key username</i> |
| illumio_pce_api_secret | Yes | 0a1bc2d3ef... | <i>The Illumio Policy Compute Engine API key secret</i> |
| http_proxy | No | http://proxy:80 | <i>HTTP proxy configuration</i> |
| https_proxy | No | https://proxy:80 | <i>HTTPS proxy configuration</i> |

Custom Layouts

The provided functions and workflows populate custom Data Tables that require a custom incident layout. To configure a new tab to display the tables, navigate to the **Customization Settings** page from the menu as shown:



From the Layouts tab (the default), select the **Incident Tabs** menu to bring up the default Incident tab layout.

A screenshot of the "Customization Settings" page. At the top, there are tabs for "Layouts" (which is underlined and highlighted in blue), "Rules", "Scripts", "Workflows", and "Functions". Below this is a sidebar with a "New Incident Wizard" button and a "Incident Tabs" dropdown menu. The "Incident Tabs" menu is expanded, showing "Manage Tabs" with a checkmark, and a list of tabs: "Summary Section", "Tasks", "Details", "Breach", and "Notes", each with a right-pointing arrow indicating they can be edited.

To add a custom tab, click the + icon at the end of the tab list. This will bring up a dialog box. Name the tab and click **Add**:

A screenshot of a modal dialog box titled "Add a Tab". It contains a "Tab Text" input field with the value "Illumio" and a red asterisk indicating it is required. Below this are three radio buttons for "Tab Visible": "Yes" (selected), "No", and "Conditional". At the bottom of the dialog are two buttons: "Cancel" and "Add", with "Add" being highlighted in blue.

Click the **Save** button to save your changes. Select your new custom tab from the tab list on the left of the screen to edit the layout:

The screenshot shows the 'Incident: Manage Tabs' interface. On the left, there is a sidebar with a list of tabs: 'New Incident Wizard', 'Incident Tabs', 'Manage Tabs', 'Summary Section', 'Tasks', 'Details', 'Breach', 'Notes', 'Members', 'News Feed', 'Attachments', 'Stats', 'Timeline', 'Artifacts', 'Email', and 'Illumio'. The 'Illumio' tab is currently selected. On the right, the main area displays the 'Incident: Manage Tabs' interface with four tabs: 'Tasks', 'Details', 'Email', and 'Illumio'. The 'Illumio' tab is highlighted with a blue border. Below the tabs, there are fields for 'Tab Text' (containing 'Illumio') and 'Tab Visible' (with a checked radio button). A 'Save' button is located at the bottom right.

Drag the Data Tables over from the right-hand side to add them to your custom tab layout:

The screenshot shows the 'Incident: Illumio' tab configuration interface. On the left, there is a sidebar with a list of tabs: 'New Incident Wizard', 'Incident Tabs', 'Manage Tabs', 'Summary Section', 'Tasks', 'Details', 'Breach', 'Notes', 'Members', 'News Feed', 'Attachments', 'Stats', 'Timeline', and 'Artifacts'. The 'Illumio' tab is currently selected. In the center, there is a text input field containing 'Traffic Flows'. On the right, there are two panels: 'Fields' and 'Data Tables'. The 'Fields' panel contains a list of fields: 'Address', 'Alberta Health Risk Assessment', 'Assessed Liability', 'City', 'Country/Region', 'Created By', 'Criminal Activity', 'Customizations Field (internal)', and 'Data Encrypted'. The 'Data Tables' panel contains a list of tables: 'Traffic Flows'. A 'Save' button is located at the top right of the interface.

Click the **Save** button to save your changes. The new tab should now appear on each Incident page.

If needed, you can configure conditions for when the tab will be visible, restricting it to only certain Incidents. This customization is beyond the scope of this document.

User Guide: fn_illumio_v1.0.0

Functions

New Function

| Name | Description | |
|---|---|-------|
| Illumio: Update Workload Enforcement Mode | Update the Enforcement Mode for one or more workloads. | trash |
| Illumio: Run Traffic Analysis | Run an Explorer query to get a traffic analysis report based on the provided inputs. The query checks all sources and destinations for traffic on a given port/protocol. Returns up to 100,000 results. | trash |
| Illumio: Provision Objects | Provision draft policy changes for the given security policy objects. | trash |
| Illumio: Get Workloads | Get multiple workloads based on the given search criteria. | trash |
| Illumio: Get IP List | Get an IP List object by name. | trash |
| Illumio: Get Workload | Get a workload by HREF. | trash |
| Illumio: Create Enforcement Boundary | Create an enforcement boundary with an ingress service using the given port/protocol. | trash |
| Illumio: Create Virtual Service | Create a Virtual Service. | trash |
| Illumio: Create Ruleset | Create a ruleset security policy object. | trash |
| Illumio: Create Rule | Create a policy rule within a given ruleset. | trash |
| Illumio: Create Service Binding | Bind one or more workloads to an active virtual service. The virtual service must be created in draft and then provisioned for the call to work. | trash |

Function - Illumio: Create Enforcement Boundary

Create an enforcement boundary with an ingress service using the given port/protocol.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_create_enforcement_boundary

| | |
|-----------------------|---|
| Name * | Illumio: Create Enforcement Boundary |
| API Name * | illumio_create_enforcement_boundary |
| Message Destination * | Illumio Message Queue |
| Description | Create an enforcement boundary with an ingress service using the given port/protocol. |

Inputs

| | |
|--|---|
| illumio_port | x |
| illumio_protocol | x |
| illumio_enforcement_boundary_name | x |
| illumio_enforcement_boundary_consumers | x |
| illumio_enforcement_boundary_providers | x |

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|--|--------|----------|-------------|--|
| illumio_enforcement_boundary_consumers | text | Yes | ams | Comma-separated list of HREFs of entities to be used as consumers for the rule, or "ams" for all workloads |
| illumio_enforcement_boundary_name | text | Yes | EB-IBM-SOAR | Enforcement boundary name |
| illumio_enforcement_boundary_providers | text | Yes | ams | Comma-separated list of HREFs of entities to be used as providers for the rule, or "ams" for all workloads |
| illumio_port | number | Yes | 8080 | Port number |
| illumio_protocol | select | Yes | - | Communication protocol |

▼ Outputs:

```

results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "href": "/orgs/1/sec_policy/active/enforcement_boundaries/1019",
        "name": "EB-IBM-SOAR-3389-TCP",
        "created_at": "2022-01-07T16:17:25.515Z",
        "updated_at": "2022-01-07T16:17:25.526Z",
        "created_by": {
            "href": "/users/464"
        },
        "updated_by": {
            "href": "/users/464"
        },
        "caps": [
            "write",
            "provision"
        ],
        "ingress_services": [
            {
                "port": 3389,
                "proto": 6
            }
        ],
        "providers": [
            {
                "actors": "ams"
            }
        ],
        "consumers": [
            {
                "ip_list": {
                    "href": "/orgs/1/sec_policy/active/ip_lists/1334"
                }
            }
        ]
    },
    "raw": None,
    "inputs": {
        "illumio_protocol": "TCP",
        "illumio_enforcement_boundary_providers": "ams",
        "illumio_enforcement_boundary_name": "EB-IBM-SOAR-3389-TCP",
    }
}

```

```

        "illumio_port": 3389,
        "illumio_enforcement_boundary_consumers": "/orgs/1/sec_policy/active/ip_lists/1334"
    },
    "metrics": {
        "version": "1.0",
        "package": "fn-illumio",
        "package_version": "1.0.0",
        "host": "C02G82JEMD6R",
        "execution_time_ms": 604,
        "timestamp": "2022-01-07 11:41:47"
    }
}

```

▼ Example Pre-Process Script:

```

port = rule.properties.illumio_port
protocol = rule.properties.illumio_protocol

inputs.illumio_port = port
inputs.illumio_protocol = protocol
inputs.illumio_enforcement_boundary_name = "EB-IBM-SOAR-{0}-{1}".format(str(port), protocol)
inputs.illumio_enforcement_boundary_consumers = workflow.properties.any_ip_list.content['href']

```

▼ Example Post-Process Script:

None

Function - Illumio: Create Virtual Service

Create a Virtual Service.

The screenshot shows the Fn SOAR platform's customization settings for a function named 'Illumio: Create Virtual Service'. The interface includes tabs for Layouts, Rules, Scripts, Workflows, Functions (which is selected), Message Destinations, Phases & Tasks, Incident Types, Breach, and Artifact Types. Below the tabs, there are input fields for Name, API Name, Message Destination, and Description. The 'Name' field contains 'Illumio: Create Virtual Service', 'API Name' contains 'illumio_create_virtual_service', 'Message Destination' is set to 'Illumio Message Queue', and the 'Description' field contains 'Create a Virtual Service.' In the 'Inputs' section, three inputs are listed: 'illumio_port', 'illumio_protocol', and 'illumio_virtual_service_name'. Each input has a delete icon ('x') to its right.

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|------------------------------|--------|----------|-------------|--|
| illumio_port | number | Yes | 8080 | Port number |
| illumio_protocol | select | Yes | - | Communication protocol. TCP and UDP are supported |
| illumio_virtual_service_name | text | Yes | VS-IBM-SOAR | Virtual service name. If no value is set, use the value SOAR-{port}-{protocol} |

▼ Outputs:

```

results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "href": "/orgs/1/sec_policy/draft/virtual_services/575f43f4-3f99-4bb0-8a6f-9e2da7a9fb2",
        "name": "VS-IBM-SOAR-3389-TCP",
        "created_at": "2022-01-07T15:23:17.885Z",
        "updated_at": "2022-01-07T15:23:17.897Z",
        "update_type": "create",
        "created_by": {
            "href": "/users/464"
        },
        "updated_by": {
            "href": "/users/464"
        },
        "caps": [
            "write",
            "provision",
            "delete"
        ],
        "apply_to": "host_only",
        "service_ports": [
            {
                "port": 3389,
                "proto": 6
            }
        ],
        "ip_overrides": []
    },
    "raw": None,
    "inputs": {
        "illumio_protocol": "TCP",
        "illumio_port": 3389,
        "illumio_virtual_service_name": "VS-IBM-SOAR-3389-TCP"
    },
    "metrics": {
        "version": "1.0",
        "package": "fn-illumio",
        "package_version": "1.0.0",
        "host": "C02G82JEMD6R",
        "execution_time_ms": 658,
        "timestamp": "2022-01-07 10:23:17"
    }
}

```

▼ Example Pre-Process Script:

```

port = rule.properties.illumio_port
protocol = rule.properties.illumio_protocol

```

```

inputs.illumio_port = port
inputs.illumio_protocol = protocol
inputs.illumio_virtual_service_name = "VS-IBM-SOAR-{0}-{1}".format(str(port), protocol)

```

▼ Example Post-Process Script:

None

Function - Illumio: Create Service Binding

Bind one or more workloads to an active virtual service. The virtual service must be created in draft and then provisioned for the call to work.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_create_service_binding

| | |
|-----------------------|--|
| Name * | Illumio: Create Service Binding |
| API Name * | illumio_create_service_binding |
| Message Destination * | Illumio Message Queue |
| Description | Bind one or more workloads to an active virtual service. The virtual service must be created in draft and then provisioned for the call to work. |

Inputs

- illumio_virtual_service_href
- illumio_workload_hrefs

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|------------------------------|------|----------|---------|--|
| illumio_virtual_service_href | text | Yes | - | Virtual Service object reference key |
| illumio_workload_hrefs | text | Yes | - | Comma-separated string of workload HREF values |

▼ Outputs:

```

results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "service_bindings": [
            {
                "href": "/orgs/1/service_bindings/c7098f30-8460-4873-a06c-8df87dc1ba1d"
            },
            {
                "href": "/orgs/1/service_bindings/ef302a43-0e59-4288-a4aa-1196369d1f29"
            }
        ]
    }
}

```

```

},
{
  "href": "/orgs/1/service_bindings/0fe5b79a-0b0d-4281-89db-d8a7867aaf61"
}
],
"errors": []
},
"raw": None,
"inputs": {
  "illumio_workload_hrefs": "/orgs/1/workloads/32e366cc-bd18-44aa-a637-9a6e761e268e,/orgs/1/workloads/...",
  "illumio_virtual_service_href": "/orgs/1/sec_policy/active/virtual_services/..."
},
"metrics": {
  "version": "1.0",
  "package": "fn-illumio",
  "package_version": "1.0.0",
  "host": "C02G82JEMD6R",
  "execution_time_ms": 469,
  "timestamp": "2022-01-07 10:23:22"
}
}
}

```

▼ Example Pre-Process Script:

```
inputs.illumio_virtual_service_href = workflow.properties.virtual_service_active_href['href']
inputs.illumio_workload_hrefs = ','.join(workflow.properties.traffic_flow_workloads['hrefs'])
```

▼ Example Post-Process Script:

None

Function - Illumio: Create Ruleset

Create a ruleset security policy object.

Customization Settings

Functions / illumio_create_ruleset

| | |
|-----------------------|--|
| Name * | Illumio: Create Ruleset |
| API Name * | illumio_create_ruleset |
| Message Destination * | Illumio Message Queue |
| Description | Create a ruleset security policy object. |

Inputs

illumio_ruleset_name

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|----------------------|------|----------|-------------|----------------------|
| illumio_ruleset_name | text | Yes | RS-IBM-SOAR | Ruleset display name |

▼ Outputs:

```
results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "href": "/orgs/1/sec_policy/draft/rule_sets/11110",
        "name": "RS-IBM-SOAR-3389-TCP",
        "created_at": "2022-01-07T15:23:25.411Z",
        "updated_at": "2022-01-07T15:23:25.411Z",
        "update_type": "create",
        "created_by": {
            "href": "/users/464"
        },
        "updated_by": {
            "href": "/users/464"
        },
        "caps": [
            "write",
            "provision"
        ],
        "enabled": True,
        "scopes": [
            []
        ]
    },
    "raw": None,
    "inputs": {
        "illumio_ruleset_name": "RS-IBM-SOAR-3389-TCP"
    },
    "metrics": {
        "version": "1.0",
        "package": "fn-illumio",
        "package_version": "1.0.0",
        "host": "C02G82JEMD6R",
        "execution_time_ms": 780,
        "timestamp": "2022-01-07 10:23:25"
    }
}
```

▼ Example Pre-Process Script:

```
port = rule.properties.illumio_port
protocol = rule.properties.illumio_protocol

inputs.illumio_ruleset_name = "RS-IBM-SOAR-{0}-{1}".format(str(port), protocol)
```

▼ Example Post-Process Script:

None

Function - Illumio: Create Rule

Create a policy rule within a given ruleset.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_create_rule

Name * Illumio: Create Rule

API Name * illumio_create_rule

Message Destination * Illumio Message Queue

Description Create a policy rule within a given ruleset.

Inputs

illumio_ruleset_href
illumio_rule_consumers
illumio_rule_providers
illumio_rule_resolve_consumers_as
illumio_rule_resolve_providers_as

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|-----------------------------------|-------------|----------|---------|---|
| illumio_rule_consumers | text | Yes | - | Comma-separated list of HREFs of entities to be used as consumers |
| illumio_rule_providers | text | Yes | - | Comma-separated list of HREFs of entities to be used as providers |
| illumio_rule_resolve_consumers_as | multiselect | Yes | - | Consumer objects the rule should apply to |
| illumio_rule_resolve_providers_as | multiselect | Yes | - | Provider objects the rule should apply to |
| illumio_ruleset_href | text | Yes | - | Ruleset object reference key |

▼ Outputs:

```
results = {
    "version": 2.0,
    "success": True,
    "content": {
        "href": "/orgs/1/sec_policy/draft/rule_sets/11110/sec_rules/18665",
        "created_at": "2022-01-07T16:41:42.244Z",
        "updated_at": "2022-01-07T16:41:42.255Z",
        "update_type": "create",
        "created_by": {
            "href": "/users/464"
        },
        "updated_by": {
            "href": "/users/464"
        }
}
```

```

},
"ingress_services": [],
"providers": [
    {
        "virtual_service": {
            "href": "/orgs/1/sec_policy/draft/virtual_services/575f43f4-3f99-4bb0-8a6f-9e2da7a9fdb2"
        }
    }
],
"consumers": [
    {
        "ip_list": {
            "href": "/orgs/1/sec_policy/draft/ip_lists/1334"
        }
    }
],
"enabled": True,
"resolve_labels_as": {
    "providers": [
        "virtual_services"
    ],
    "consumers": [
        "workloads"
    ]
},
"sec_connect": False,
"stateless": False,
"machine_auth": False,
"unscoped_consumers": False,
"network_type": "brn"
},
"raw": None,
"inputs": {
    "illumio_rule_resolve_consumers_as": [
        "workloads"
    ],
    "illumio_rule_consumers": "/orgs/1/sec_policy/active/ip_lists/1334",
    "illumio_ruleset_href": "/orgs/1/sec_policy/draft/rule_sets/11110",
    "illumio_rule_resolve_providers_as": [
        "virtual_services"
    ],
    "illumio_rule_providers": "/orgs/1/sec_policy/active/virtual_services/575f43f4-3f99-4bb0-8a6f-9e2da7a9fdb2"
},
"metrics": {
    "version": "1.0",
    "package": "fn-illumio",
    "package_version": "1.0.0",
    "host": "C02G82JEMD6R",
    "execution_time_ms": 457,
    "timestamp": "2022-01-07 11:41:42"
}
}

```

▼ Example Pre-Process Script:

```

inputs.illumio_ruleset_href = workflow.properties.ruleset.content['href']
inputs.illumio_rule_consumers = workflow.properties.any_ip_list.content['href']
inputs.illumio_rule_providers = workflow.properties.virtual_service_active_href['href']

```

▼ Example Post-Process Script:

None

Function - Illumio: Get IP List

Get an IP List object by name.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_get_ip_list

Name * Illumio: Get IP List

API Name * [? illumio_get_ip_list](#)

Message Destination * [Illumio Message Queue](#)

Description Get an IP List object by name.

Inputs

illumio_ip_list_name

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|----------------------|------|----------|--------------------------|--|
| illumio_ip_list_name | text | Yes | Any (0.0.0.0/0 and ::/0) | IP List object name. Accepts partial matches |

▼ Outputs:

```
results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "href": "/orgs/1/sec_policy/active/ip_lists/1334",
        "name": "Any (0.0.0.0/0 and ::/0)",
        "created_at": "2021-09-13T15:03:07.000Z",
        "updated_at": "2021-09-13T15:03:07.015Z",
        "created_by": {"href": "/users/0"},
        "updated_by": {"href": "/users/0"},
        "ip_ranges": [
            {"from_ip": "0.0.0.0/0", "exclusion": False},
            {"from_ip": "::/0", "exclusion": False}
        ]
    },
    "raw": None,
    "inputs": {
        "illumio_ip_list_name": "Any (0.0.0.0/0 and ::/0)"
    },
    "metrics": {
        "version": "1.0",
        "package": "fn-illumio",
        "package_version": "1.0.0",
        "host": "C02G82JEMD6R",
        "execution_time_ms": 811,
        "timestamp": "2022-01-07 10:22:52"
    }
}
```

```
    }  
}
```

▼ Example Pre-Process Script:

None

▼ Example Post-Process Script:

None

Function - Illumio: Get Workload

Get a workload by HREF.

The screenshot shows the 'Customization Settings' interface with the 'Functions' tab selected. A function named 'Illumio: Get Workload' is displayed with the following details:

- Name ***: Illumio: Get Workload
- API Name ***: illumio_get_workload
- Message Destination ***: Illumio Message Queue
- Description**: Get a workload by HREF.

In the 'Inputs' section, there is a single input field containing 'illumio_workload_href'.

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|-----------------------|------|----------|---------|-------------------------------|
| illumio_workload_href | text | Yes | - | Workload object reference key |

▼ Outputs:

```
results = {  
    "version": 2.0,  
    "success": True,  
    "reason": None,  
    "content": {  
        "href": "/orgs/1/workloads/3d14ec61-edaf-452e-b1b9-b7308652c0f6",  
        "created_at": "2021-09-13T16:01:07.735779Z",  
        "updated_at": "2021-12-16T16:47:04.458647Z",  
        "created_by": {  
            "href": "/orgs/1/agents/17456"  
        },  
        "updated_by": {  
        }  
    }  
}
```

```
        "href": "/orgs/1/agents/17456"
    },
    "caps": [
        "write"
    ],
    "hostname": "user-4",
    "public_ip": "66.124.202.19",
    "interfaces": [
        {
            "name": "eth0",
            "address": "fe80::402:ffff:feef:5a4d",
            "cidr_block": 64,
            "network": {
                "href": "/orgs/1/networks/9977853d-639e-4af0-a505-9e0fd419ce06"
            },
            "network_detection_mode": "link_local",
            "loopback": False
        },
        {
            "name": "eth0",
            "address": "10.1.0.46",
            "cidr_block": 24,
            "default_gateway_address": "10.1.0.1",
            "network": {
                "href": "/orgs/1/networks/a9dd8b22-3108-4c64-911b-ac1b2eb5919e"
            },
            "network_detection_mode": "single_private_brn",
            "loopback": False
        },
        {
            "name": "eth0.public",
            "address": "66.124.202.19",
            "cidr_block": 32,
            "network": {
                "href": "/orgs/1/networks/a9dd8b22-3108-4c64-911b-ac1b2eb5919e"
            },
            "network_detection_mode": "manual",
            "loopback": False
        }
    ],
    "service_provider": "example.com",
    "data_center": "us-west.example.com",
    "data_center_zone": "us-west",
    "os_id": "ubuntu-x86_64-xenial",
    "os_detail": "5.4.0-1038-aws #40-Ubuntu SMP Fri Feb 5 23:50:40 UTC 2021 (Ubuntu 20.04.2 LTS)",
    "online": True,
    "deleted": False,
    "ignored_interface_names": [],
    "containers_inherit_host_policy": False,
    "blocked_connection_action": "drop",
    "labels": [
        {
            "href": "/orgs/1/labels/15420"
        },
        {
            "href": "/orgs/1/labels/15431"
        },
        {
            "href": "/orgs/1/labels/15430"
        },
        {
            "href": "/orgs/1/labels/15411"
        }
    ],
    "agent": {
```

```

    "href": "/orgs/1/agents/17456",
    "config": {
        "mode": "illuminated",
        "log_traffic": False,
        "visibility_level": "flow_summary"
    },
    "status": {
        "status": "active",
        "uid": "us-west+i-0ab12cd3e4fg5678h",
        "instance_id": "i-0ab12cd3e4fg5678h",
        "last_heartbeat_on": "2022-01-07T16:14:31.378648Z",
        "uptime_seconds": 10025687,
        "agent_version": "21.2.0-7831",
        "managed_since": "2021-09-13T16:01:07.772006Z",
        "fw_config_current": False,
        "firewall_rule_count": 0,
        "security_policy_refresh_at": "2022-01-03T20:54:34.809195Z",
        "security_policy_applied_at": "2022-01-03T20:54:34.809195Z",
        "security_policy_received_at": "2022-01-03T20:54:34.809195Z",
        "agent_health_errors": {
            "errors": [],
            "warnings": []
        },
        "security_policy_sync_state": "syncing"
    },
    "unpair_allowed": True,
    "type": "Host"
},
"ven": {
    "href": "/orgs/1/vens/3d14ec61-edaf-452e-b1b9-b7308652c0f6"
},
"enforcement_mode": "visibility_only",
"visibility_level": "flow_summary"
},
"raw": None,
"inputs": {
    "illumio_workload_href": "/orgs/1/workloads/3d14ec61-edaf-452e-b1b9-b7308652c0f6"
},
"metrics": {
    "version": "1.0",
    "package": "fn-illumio",
    "package_version": "1.0.0",
    "host": "C02G82JEMD6R",
    "execution_time_ms": 486,
    "timestamp": "2022-01-07 10:27:31"
}
}

```

▼ Example Pre-Process Script:

None

▼ Example Post-Process Script:

None

Function - Illumio: Get Workloads

Get multiple workloads based on the given search criteria.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_get_workloads

Name * Illumio: Get Workloads

API Name * illumio_get_workloads

Message Destination * Illumio Message Queue

Description Get multiple workloads based on the given search criteria.

Inputs

illumio_workload_name
illumio_workload_hostname
illumio_workload_ip_address
illumio_workload_online
illumio_workload_managed
illumio_workload_labels
illumio_workload_enforcement_mode

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|-----------------------------------|---------|----------|-----------|--|
| illumio_workload_enforcement_mode | select | No | - | Search for workloads based on enforcement mode. |
| illumio_workload_hostname | text | No | - | The hostname of the workload to search for. |
| illumio_workload_ip_address | text | No | 127.0.0.1 | The IP address of the workload to search for. Supports partial matches. |
| illumio_workload_labels | text | No | - | Search for workloads based on a comma-separated list of Label HREFs. |
| illumio_workload_managed | boolean | No | - | If set, returns only managed workloads if true, or unmanaged workloads if false. |
| illumio_workload_name | text | No | - | The name of the workload(s) to search for. Supports partial matches. |
| illumio_workload_online | boolean | No | - | If set, returns only online workloads if true or offline workloads if false. |

▼ Outputs:

```

results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "workloads": [
            {
                "href": "/orgs/1/workloads/3d14ec61-edaf-452e-b1b9-b7308652c0f6",
                "created_at": "2021-09-13T16:01:07.735779Z",
                "updated_at": "2021-12-16T16:47:04.458647Z",
                "created_by": {
                    "href": "/orgs/1/agents/17456"
                },
                "updated_by": {
                    "href": "/orgs/1/agents/17456"
                },
                "caps": [
                    "write"
                ],
                "hostname": "user-4",
                "public_ip": "66.124.202.19",
                "interfaces": [
                    {
                        "name": "eth0",
                        "address": "fe80::402:ffff:feef:5a4d",
                        "cidr_block": 64,
                        "network": {
                            "href": "/orgs/1/networks/9977853d-639e-4afd-a505-9e0fd419ce06"
                        },
                        "network_detection_mode": "link_local",
                        "loopback": False
                    },
                    {
                        "name": "eth0",
                        "address": "10.1.0.46",
                        "cidr_block": 24,
                        "default_gateway_address": "10.1.0.1",
                        "network": {
                            "href": "/orgs/1/networks/a9dd8b22-3108-4c64-911b-ac1b2eb5919e"
                        },
                        "network_detection_mode": "single_private_brn",
                        "loopback": False
                    },
                    {
                        "name": "eth0.public",
                        "address": "66.124.202.19",
                        "cidr_block": 32,
                        "network": {
                            "href": "/orgs/1/networks/a9dd8b22-3108-4c64-911b-ac1b2eb5919e"
                        },
                        "network_detection_mode": "manual",
                        "loopback": False
                    }
                ],
                "service_provider": "example.com",
                "data_center": "us-west.example.com",
                "data_center_zone": "us-west",
                "os_id": "ubuntu-x86_64-xenial",
                "os_detail": "5.4.0-1038-aws #40-Ubuntu SMP Fri Feb 5 23:50:40 UTC 2021 (Ubuntu 20.04.2 LTS)",
                "online": True,
                "deleted": False,
                "ignored_interface_names": [],
                "containers_inherit_host_policy": False,
                "blocked_connection_action": "drop",
            }
        ]
    }
}

```

```
"labels": [
    {
        "href": "/orgs/1/labels/15420"
    },
    {
        "href": "/orgs/1/labels/15431"
    },
    {
        "href": "/orgs/1/labels/15430"
    },
    {
        "href": "/orgs/1/labels/15411"
    }
],
"agent": {
    "href": "/orgs/1/agents/17456",
    "config": {
        "mode": "illuminated",
        "log_traffic": False,
        "visibility_level": "flow_summary"
    },
    "status": {
        "status": "active",
        "uid": "us-west+i-0ab12cd3e4fg5678h",
        "instance_id": "i-0ab12cd3e4fg5678h",
        "last_heartbeat_on": "2022-01-07T16:14:31.378648Z",
        "uptime_seconds": 10025687,
        "agent_version": "21.2.0-7831",
        "managed_since": "2021-09-13T16:01:07.772006Z",
        "fw_config_current": False,
        "firewall_rule_count": 0,
        "security_policy_refresh_at": "2022-01-03T20:54:34.809195Z",
        "security_policy_applied_at": "2022-01-03T20:54:34.809195Z",
        "security_policy_received_at": "2022-01-03T20:54:34.809195Z",
        "agent_health_errors": {
            "errors": [],
            "warnings": []
        },
        "security_policy_sync_state": "syncing"
    },
    "unpair_allowed": True,
    "type": "Host"
},
"ven": {
    "href": "/orgs/1/vens/3d14ec61-edaf-452e-b1b9-b7308652c0f6"
},
"enforcement_mode": "visibility_only",
"visibility_level": "flow_summary"
},
{
    "href": "/orgs/1/workloads/1fd97272-1497-47b8-95c9-6f530dbe0749",
    "created_at": "2021-09-13T16:00:39.951135Z",
    "updated_at": "2021-12-16T16:47:04.465816Z",
    "created_by": {
        "href": "/orgs/1/agents/17423"
    },
    "updated_by": {
        "href": "/orgs/1/agents/17423"
    },
    "caps": [
        "write"
    ],
    "hostname": "dev-db-2",
    "public_ip": "66.124.202.19",
    "interfaces": [

```

```
{
    "name": "eth0",
    "address": "fe80::45a:d8ff:fea9:54b1",
    "cidr_block": 64,
    "network": {
        "href": "/orgs/1/networks/9977853d-639e-4af8-a505-9e0fd419ce06"
    },
    "network_detection_mode": "link_local",
    "loopback": False
},
{
    "name": "eth0",
    "address": "10.1.0.82",
    "cidr_block": 24,
    "default_gateway_address": "10.1.0.1",
    "network": {
        "href": "/orgs/1/networks/a9dd8b22-3108-4c64-911b-ac1b2eb5919e"
    },
    "network_detection_mode": "single_private_brn",
    "loopback": False
},
{
    "name": "eth0.public",
    "address": "66.124.202.19",
    "cidr_block": 32,
    "network": {
        "href": "/orgs/1/networks/a9dd8b22-3108-4c64-911b-ac1b2eb5919e"
    },
    "network_detection_mode": "manual",
    "loopback": False
}
],
"service_provider": "example.com",
"data_center": "us-west.example.com",
"data_center_zone": "us-west",
"os_id": "ubuntu-x86_64-xenial",
"os_detail": "5.4.0-1038-aws #40-Ubuntu SMP Fri Feb 5 23:50:40 UTC 2021 (Ubuntu 20.04.2 LTS)",
"online": True,
"deleted": False,
"ignored_interface_names": [],
"containers_inherit_host_policy": False,
"blocked_connection_action": "drop",
"labels": [
    {
        "href": "/orgs/1/labels/15427"
    },
    {
        "href": "/orgs/1/labels/15426"
    },
    {
        "href": "/orgs/1/labels/15418"
    },
    {
        "href": "/orgs/1/labels/15422"
    }
],
"agent": {
    "href": "/orgs/1/agents/17423",
    "config": {
        "mode": "illuminated",
        "log_traffic": False,
        "visibility_level": "flow_summary"
    },
    "status": {
        "status": "active",
        "last_update": "2021-02-05T23:50:40Z"
    }
}
```

```

        "uid": "us-west+i-0e65e2aec3677d51e",
        "instance_id": "i-0e65e2aec3677d51e",
        "last_heartbeat_on": "2022-01-07T16:15:17.913215Z",
        "uptime_seconds": 10025636,
        "agent_version": "21.2.0-7831",
        "managed_since": "2021-09-13T16:00:39.974839Z",
        "fw_config_current": False,
        "firewall_rule_count": 0,
        "security_policy_refresh_at": "2022-01-03T20:55:54.361991Z",
        "security_policy_applied_at": "2022-01-03T20:55:54.361991Z",
        "security_policy_received_at": "2022-01-03T20:55:54.361991Z",
        "agent_health_errors": {
            "errors": [],
            "warnings": []
        },
        "security_policy_sync_state": "syncing"
    },
    "unpair_allowed": True,
    "type": "Host"
},
"ven": {
    "href": "/orgs/1/vens/1fd97272-1497-47b8-95c9-6f530dbe0749"
},
"enforcement_mode": "visibility_only",
"visibility_level": "flow_summary"
}
]
},
"raw": None,
"inputs": {
    "illumio_workload_enforcement_mode": "visibility_only",
    "illumio_workload_managed": True
},
"metrics": {
    "version": "1.0",
    "package": "fn-illumio",
    "package_version": "1.0.0",
    "host": "C02G82JEMD6R",
    "execution_time_ms": 534,
    "timestamp": "2022-01-07 11:41:53"
}
}

```

▼ Example Pre-Process Script:

None

▼ Example Post-Process Script:

```

workload_hrefs = [workload['href'] for workload in results.content['workloads']]
workflow.addProperty('workload_hrefs', {'hrefs': workload_hrefs})

```

Function - Illumio: Run Traffic Analysis

Run an Explorer query to get a traffic analysis report based on the provided inputs. The query checks all sources and destinations for traffic on a given port/protocol. Returns up to 100,000 results.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_run_traffic_analysis

Name * Illumio: Run Traffic Analysis

API Name * illumio_run_traffic_analysis

Message Destination * Illumio Message Queue

Description Run an Explorer query to get a traffic analysis report based on the provided inputs. The query checks all sources and destinations for traffic on a given port/protocol. Returns up to 100,000 results.

Inputs

illumio_port
illumio_protocol
illumio_traffic_analysis_start_time
illumio_traffic_analysis_end_time
illumio_traffic_analysis_policy_decisions

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|---|----------------|----------|---------|---|
| illumio_port | number | Yes | 8080 | Port number |
| illumio_protocol | select | Yes | - | Communication protocol |
| illumio_traffic_analysis_end_time | datetimepicker | Yes | - | End of the query time range |
| illumio_traffic_analysis_policy_decisions | multiselect | Yes | - | List of policy decisions to include in the search results |
| illumio_traffic_analysis_start_time | datetimepicker | Yes | - | Start of the query time range |

▼ Outputs:

```
results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "traffic_flows": [
            {
                "src": {
                    "ip": "198.204.226.234"
                },
                "dst": {
                    "ip": "10.1.100.43",
                    "workload": {

```

```
"href": "/orgs/1/workloads/9c8b69b9-c741-4689-b8c7-f8ebee0dbe8",
"hostname": "windows-jumpbox-1",
"os_type": "windows",
"labels": [
    {
        "href": "/orgs/1/labels/15415",
        "key": "app",
        "value": "A-ADMIN"
    },
    {
        "href": "/orgs/1/labels/15411",
        "key": "env",
        "value": "E-PROD"
    },
    {
        "href": "/orgs/1/labels/15412",
        "key": "loc",
        "value": "L-DALLAS"
    },
    {
        "href": "/orgs/1/labels/15416",
        "key": "role",
        "value": "R-JUMP-SRV"
    }
]
},
"service": {
    "port": 3389,
    "proto": 6,
    "process_name": "svchost.exe",
    "windows_service_name": "TermService",
    "user_name": "NETWORK SERVICE"
},
"num_connections": 1,
"state": "active",
"timestamp_range": {
    "first_detected": "2021-12-29T20:38:13Z",
    "last_detected": "2021-12-29T20:38:13Z"
},
"dst_bi": 0,
"dst_bo": 0,
"policy_decision": "potentially_blocked",
"flow_direction": "inbound"
},
{
    "src": {
        "ip": "27.124.5.118"
    },
    "dst": {
        "ip": "10.1.100.43",
        "workload": {
            "href": "/orgs/1/workloads/9c8b69b9-c741-4689-b8c7-f8ebee0dbe8",
            "hostname": "windows-jumpbox-1",
            "os_type": "windows",
            "labels": [
                {
                    "href": "/orgs/1/labels/15415",
                    "key": "app",
                    "value": "A-ADMIN"
                },
                {
                    "href": "/orgs/1/labels/15411",
                    "key": "env",
                    "value": "E-PROD"
                }
            ]
        }
    }
}
```

```

        },
        {
            "href": "/orgs/1/labels/15412",
            "key": "loc",
            "value": "L-DALLAS"
        },
        {
            "href": "/orgs/1/labels/15416",
            "key": "role",
            "value": "R-JUMP-SRV"
        }
    ]
}
},
"service": {
    "port": 3389,
    "proto": 6,
    "process_name": "svchost.exe",
    "windows_service_name": "TermService",
    "user_name": "NETWORK SERVICE"
},
"num_connections": 17,
"state": "timed out",
"timestamp_range": {
    "first_detected": "2021-12-25T13:49:29Z",
    "last_detected": "2021-12-25T13:49:29Z"
},
"dst_bi": 0,
"dst_bo": 0,
"policy_decision": "potentially_blocked",
"flow_direction": "inbound"
}
]
},
"raw": None,
"inputs": {
    "illumio_protocol": "TCP",
    "illumio_traffic_analysis_policy_decisions": ["potentially_blocked", "unknown"],
    "illumio_traffic_analysis_end_time": 1640926800000,
    "illumio_traffic_analysis_start_time": 1640322000000,
    "illumio_port": 3389
},
"metrics": {
    "version": "1.0",
    "package": "fn-illumio",
    "package_version": "1.0.0",
    "host": "C02G82JEMD6R",
    "execution_time_ms": 8923,
    "timestamp": "2022-01-07 10:23:10"
}
}
}

```

▼ Example Pre-Process Script:

```

from datetime import datetime, timezone, timedelta

inputs.illumio_port = rule.properties.illumio_port
inputs.illumio_protocol = rule.properties.illumio_protocol

start_time = rule.properties.illumio_block_port_traffic_analysis_start_time
end_time = rule.properties.illumio_block_port_traffic_analysis_end_time

inputs.illumio_traffic_analysis_start_time = start_time
inputs.illumio_traffic_analysis_end_time = end_time

```

▼ Example Post-Process Script:

```
flows = results.content['traffic_flows']
traffic_flow_workloads = set()

for flow in flows:
    if 'workload' in flow['dst'] and flow['dst']['workload']['href']:
        traffic_flow_workloads.add(flow['dst']['workload']['href'])

workflow.addProperty('traffic_flow_workloads', {'refs': list(traffic_flow_workloads)})
incident.addNote(
    helper.createRichText(
        u"<b>Illumio: Block Port</b> workflow: found <b>{0}</b> traffic flows".format(len(traffic_flow_workloads))
    )
)
```

Function - Illumio: Provision Objects

Provision draft policy changes for the given security policy objects.

Customization Settings

Functions / illumio_provision_objects

| | |
|-----------------------|---|
| Name * | Illumio: Provision Objects |
| API Name * | illumio_provision_objects |
| Message Destination * | Illumio Message Queue |
| Description | Provision draft policy changes for the given security policy objects. |

Inputs

illumio_policy_object_refs

▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|----------------------------|------|----------|---------|---|
| illumio_policy_object_refs | text | Yes | - | Comma-separated list of policy object HREFs |

▼ Outputs:

```
results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "provisioned_hrefs": [
            "/orgs/1/sec_policy/active/virtual_services/575f43f4-3f99-4bb0-8a6f-9e2da7a9fb2"
        ]
}
```

```

},
"raw": None,
"inputs": {
    "illumio_policy_object_refs": "/orgs/1/sec_policy/draft/virtual_services/..."
},
"metrics": {
    "version": "1.0",
    "package": "fn-illumio",
    "package_version": "1.0.0",
    "host": "C02G82JEMD6R",
    "execution_time_ms": 490,
    "timestamp": "2022-01-07 10:23:20"
}
}

```

▼ Example Pre-Process Script:

```
inputs.illumio_policy_object_refs = workflow.properties.virtual_service.content['href']
```

▼ Example Post-Process Script:

```

if results.content['provisioned_refs']:
    active_href = results.content['provisioned_refs'][0]
else:
    active_href = workflow.properties.virtual_service.content['href']

workflow.addProperty('virtual_service_active_href', {'href': active_href})
incident.addNote(
    helper.createRichText(
        u"<b>Illumio: Block Port</b> workflow: provisioned service with HREF <b>{0}</b>.".format(active_href)
    )
)

```

Function - Illumio: Update Workload Enforcement Mode

Update the Enforcement Mode for one or more workloads.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifact Ty

Functions / illumio_update_workload_enforcement_mode

Name * Illumio: Update Workload Enforcement Mode

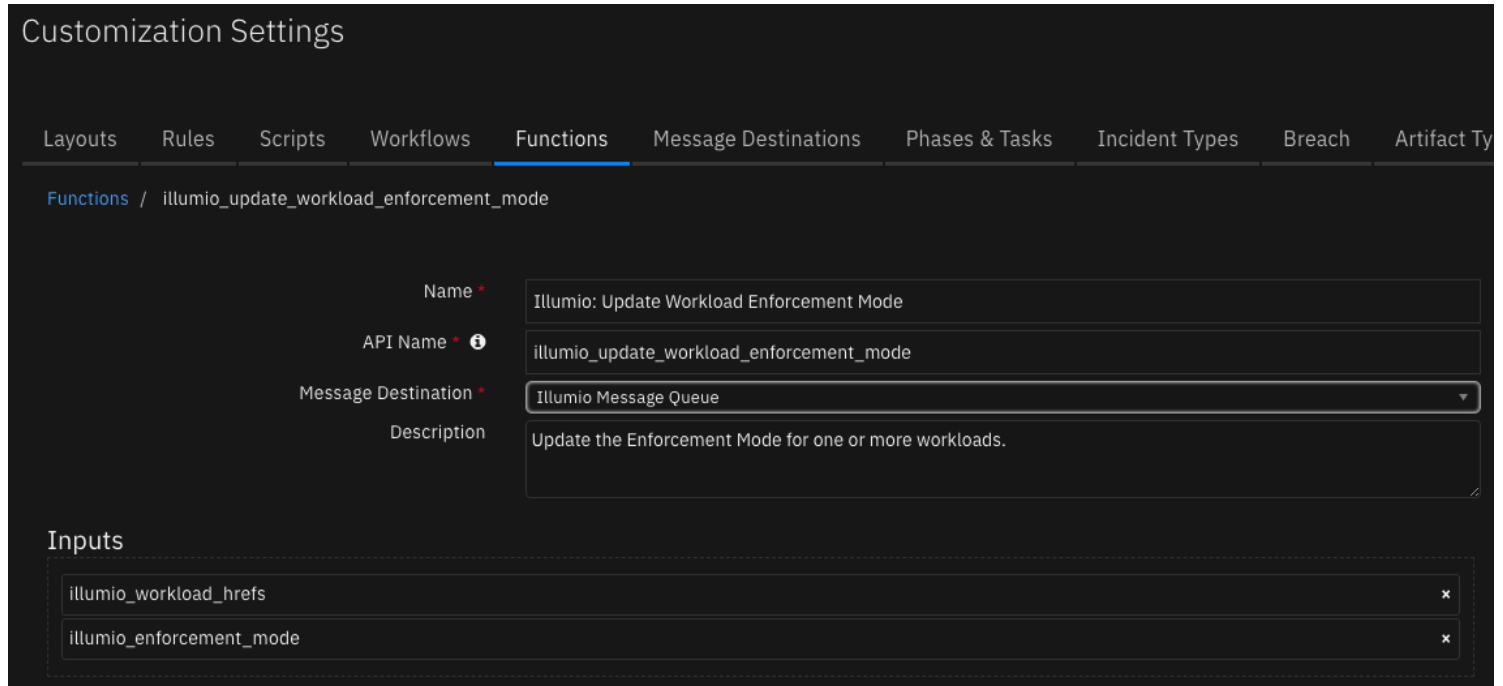
API Name * illumio_update_workload_enforcement_mode

Message Destination * Illumio Message Queue

Description Update the Enforcement Mode for one or more workloads.

Inputs

illumio_workload_hrefs
illumio_enforcement_mode



▼ Inputs:

| Name | Type | Required | Example | Tooltip |
|--------------------------|--------|----------|---------|--|
| illumio_enforcement_mode | select | Yes | - | Workload enforcement mode |
| illumio_workload_hrefs | text | Yes | - | Comma-separated string of workload HREF values |

▼ Outputs:

```
results = {
    "version": 2.0,
    "success": True,
    "reason": None,
    "content": {
        "errors": [],
        "workloads": [
            "/orgs/1/workloads/3d14ec61-edaf-452e-b1b9-b7308652c0f6",
            "/orgs/1/workloads/1fd97272-1497-47b8-95c9-6f530dbe0749"
        ]
    },
    "raw": None,
    "inputs": {
        "illumio_enforcement_mode": "selective",
        "illumio_workload_hrefs": "/orgs/1/workloads/3d14ec61-edaf-452e-b1b9-b7308652c0f6, ..."
    },
    "metrics": {
        "version": "1.0",
        "package": "fn-illumio",
        "package_version": "1.0.0",
        "host": "C02G82JEMD6R",
        "execution_time_ms": 1107,
        "timestamp": "2022-01-07 11:17:34"
    }
}
```

▼ Example Pre-Process Script:

```
inputs.illumio_workload_hrefs = ','.join(workflow.properties.workload_hrefs['hrefs'])
```

▼ Example Post-Process Script:

```
incident.addNote(  
    helper.createRichText(  
        u"<b>Illumio: Block Port</b> workflow: moved all Visibility Only workloads into Selective enforcement."  
    )  
)
```

Rule - Illumio: Block Port

This rule is used to trigger the Block Port workflow for a specified port and protocol.

The screenshot shows the configuration of a rule named 'Illumio: Block Port'. It includes fields for Display Name, Object Type (Incident), and Conditions (set to 'Malware'). The Activities section lists Ordered Activities (Port, Protocol, Update Enforcement, Create Allow List, Traffic Analysis Start Time, Traffic Analysis End Time) and Workflow Activities (Illumio: Block Port). The Layout section shows the same activity list. A note at the bottom states the action must be run manually from an incident of type Malware.

Rules / Illumio: Block Port

Display Name * Illumio: Block Port

Object Type Incident

Conditions Add conditions in which to invoke the rule. [Clear All](#)

Incident Type is equal to Malware

Activities

Ordered Activities will be invoked in the order specified below. They include: [Add Tasks](#), [Run Script](#), and [Set Field](#). [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Illumio: Block Port

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

▼ Hide Activity Fields

Layout

| | |
|-----------------------------|---|
| Port | x |
| Protocol | x |
| Update Enforcement | x |
| Create Allow List | x |
| Traffic Analysis Start Time | x |
| Traffic Analysis End Time | x |

The action must be run manually from an incident of type **Malware**.

Malware Sim SIM

Description

Test incident

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts Email

Edit

Basic Details

| | |
|--------------------------------------|----------------|
| Name <small>i</small> | Malware Sim |
| Description <small>i</small> | Test incident |
| Incident Type <small>i</small> | Malware |
| NIST Attack Vectors <small>i</small> | Other |

The Block Port rule can be triggered from the Actions dropdown menu at the upper-right of the incident page:

The screenshot shows the 'Actions' dropdown menu open, revealing options like 'Illumio: Block Port', 'Action Status', 'Workflow Status', 'Close Incident', and 'Delete Incident'. The 'Illumio: Block Port' option is highlighted.

The workflow requires values for the following form fields attached to the Block Port Rule:

| Field | Description |
|-----------------------------|--|
| Port | The port to block |
| Protocol | The traffic protocol to block |
| Update Enforcement | If yes, updates the enforcement mode of all workloads in Visibility Only mode to Selective enforcement |
| Create Allow List | If yes, creates policy objects and rules to allow traffic from the given traffic analysis timespan on the blocked port and protocol |
| Traffic Analysis Start Time | The beginning of the analysis period to find traffic flows that will be added to the allow list rule. If Create Allow List is set to No, these values are ignored |
| Traffic Analysis End Time | The end of the analysis period to find traffic flows that will be added to the allow list rule. If Create Allow List is set to No, these values are ignored |

Illumio: Block Port

| | |
|-------------------------------|--|
| Port * | <input type="text" value="8080"/> |
| Protocol * | <input type="text" value="TCP"/> |
| Update Enforcement * | <input type="text" value="Unknown"/> |
| Create Allow List * | <input type="text" value="Unknown"/> |
| Traffic Analysis Start Time * | <input type="text" value="MM/DD/YYYY HH:mm:ss Z"/> <input type="button" value="Calendar"/> |
| Traffic Analysis End Time * | <input type="text" value="MM/DD/YYYY HH:mm:ss Z"/> <input type="button" value="Calendar"/> |

| | |
|---------------------------------------|--|
| <input type="button" value="Cancel"/> | <input style="background-color: #0072BD; color: white; font-weight: bold; padding: 5px 10px; border-radius: 5px; border: none; font-size: 10pt; text-decoration: none; margin-left: 10px;" type="button" value="Execute"/> |
|---------------------------------------|--|

Rule - Illumio: Block Selected Port

This rule is used to trigger the Block Selected Port workflow from an Artifact of type **Port**. It can be triggered from the Actions menu of **Port** artifact in the Artifacts tab once it has been added to an incident. The incident can be of any type.

Rules / Illumio: Block Selected Port

| | |
|----------------|---|
| Display Name * | <input type="text" value="Illumio: Block Selected Port"/> |
| Object Type | Artifact |
| Conditions | Add conditions in which to invoke the rule. Clear All |

| | | |
|--|---|-----------------------------------|
| <input type="text" value="Type"/> <input type="button" value="▼"/> | <input type="text" value="is equal to"/> <input type="button" value="▼"/> | <input type="text" value="Port"/> |
|--|---|-----------------------------------|

Activities

| | |
|-----------|--|
| Ordered | Ordered Activities will be invoked in the order specified below. They include: <i>Add Tasks, Run Script, and Set Field</i> . Add New |
| Workflows | Workflow Activities are started after all Ordered Activities complete. |

| | |
|--------------|---|
| Destinations | Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started. |
|--------------|---|

[▼ Hide Activity Fields](#)

| | |
|--------|--|
| Layout | <div style="border: 1px dashed #ccc; padding: 5px; width: 150px; height: 150px; margin-bottom: 10px;"> <input type="text" value="Protocol"/> </div> <div style="border: 1px dashed #ccc; padding: 5px; width: 150px; height: 150px; margin-bottom: 10px;"> <input type="text" value="Update Enforcement"/> </div> <div style="border: 1px dashed #ccc; padding: 5px; width: 150px; height: 150px; margin-bottom: 10px;"> <input type="text" value="Create Allow List"/> </div> <div style="border: 1px dashed #ccc; padding: 5px; width: 150px; height: 150px; margin-bottom: 10px;"> <input type="text" value="Traffic Analysis Start Time"/> </div> <div style="border: 1px dashed #ccc; padding: 5px; width: 150px; height: 150px; margin-bottom: 10px;"> <input type="text" value="Traffic Analysis End Time"/> </div> |
|--------|--|

The Port field is not included in the form fields: the value is instead pulled from the Port Artifact. All remaining fields are identical to the **Block Port** Rule.

Workflow - Illumio: Block Port

API Name

`illumio_block_port`

Overview

The **Block Port** workflow can be used to block incoming traffic to all workloads on a specified port and protocol. This deny rule is configured in the Illumio Policy Compute Engine using an Enforcement Boundary.

Workflows / Illumio: Block Port

Name * Illumio: Block Port

API Name * illuminio_block_port

Description Block traffic on a given port and protocol throughout the network using an enforcement boundary. Optionally, legitimate traffic flows can be explicitly allowed based on a traffic analysis query.

Object Type * Incident

Creator Duncan Sommerville
Last Modified 12/20/2021 09:30
Last Modified By Duncan Sommerville
Associated Rules Illumio: Block Port

```

graph LR
    Start(( )) --> GetIPList[Ilumio: Get IP List]
    GetIPList --> AllowTraffic[Allow legitimate traffic]
    AllowTraffic --> RunTrafficAnalysis[Illumio: Run Traffic Analysis]
    RunTrafficAnalysis --> FindTraffic[Find traffic flows]
    FindTraffic --> CreateVirtualService[Ilumio: Create Virtual Service]
    CreateVirtualService --> ProvisionObjects1[Ilumio: Provision Objects]
    ProvisionObjects1 --> CreateServiceBinding[Ilumio: Create Service Binding]
    CreateServiceBinding --> CreateRuleSet[Ilumio: Create Rule Set]
    CreateRuleSet --> CreateRule[Ilumio: Create Rule]
    CreateRule --> ProvisionObjects2[Ilumio: Provision Objects]
    ProvisionObjects2 --> CreatePort[Ilumio: Create Port]
    CreatePort --> ProvisionObjects3[Ilumio: Provision Objects]
    ProvisionObjects3 --> ProvisionRuleSet[Provision the Ruleset]
    ProvisionRuleSet --> CreateEnforcementBoundary[Ilumio: Create Enforcement Boundary]
    CreateEnforcementBoundary --> ProvisionObjects4[Ilumio: Provision Objects]
    ProvisionObjects4 --> UpdateEnforcement[Update enforcement mode]
    UpdateEnforcement --> RebindWorkloads[Rebind workloads]
    RebindWorkloads --> UpdateWorkloadEnforcement[Ilumio: Update Workload Enforcement]
    UpdateWorkloadEnforcement --> End(( ))
  
```

The first conditional branch of the workflow checks whether a Traffic Analysis search should be performed for traffic within a given timespan. If so, a search is performed for any Potentially Blocked or Unknown traffic on the port and protocol to be blocked within that span of time. If any traffic flows are found, policy objects and rules are then created to make sure traffic is allowed and continues uninterrupted to the destination workloads found in the search.

Note: The Traffic Analysis timespan should not overlap with the breach - it is intended to find "good" traffic from before the attack to mitigate any interruption of legitimate services receiving traffic on the blocked port and protocol.

If you are uncertain when the breach began, err on the side of caution to avoid creating rules that may allow malicious traffic flows.

A Virtual Service is created for the blocked port and protocol to be used in the Rule that will allow traffic. Once the Virtual Service is provisioned, the destination workloads found in the traffic analysis are then bound to it.

A Ruleset and Rule are then created and provisioned to allow the traffic.

In all branches, an Enforcement Boundary is created to deny traffic on the specified port and protocol.

The second conditional branch checks if the Enforcement Mode should be updated for workloads currently in Visibility Only enforcement. If so, all workloads in Visibility Only mode will be changed to Selective enforcement.

Workflow - Illumio: Block Selected Port

API Name

illumio_block_selected_port

Overview

The **Block Selected Port** workflow clones the Block Port workflow and is used with the Block Selected Port Rule to trigger from Port-type Artifacts. Both workflows have the same functionality outside of where the blocked port value originates.

Data Table - Traffic Flows

Data table used to store traffic flow data returned from Explorer traffic analysis queries.

| Tasks | Details | Breach | Notes | Members | News Feed | Attachments | Stats | Timeline | Artifacts | Email | Illumio |
|--|------------|--------|-------|---------|----------------------|----------------------|---|----------|-----------|-------|--------------------------|
| | | | | | | | | | | | Edit |
| Traffic Flows | | | | | | | | | | | Search... 🔍 |
| Source IP ⓘ Destination IP ⓘ Port ⓘ Protocol ⓘ Flows ⓘ First Detected ⓘ Last Detected ⓘ Flow Details ⓘ | | | | | | | | | | | |
| 10.2.8.183 | 10.8.4.216 | 137 | TCP | 2 | 2022-01-08T06:27:19Z | 2022-01-08T06:27:19Z | Valid network traffic found by Block Port workflow. | | | | |
| 10.2.8.183 | 10.8.4.233 | 137 | TCP | 1 | 2022-01-08T05:55:08Z | 2022-01-08T05:55:08Z | Valid network traffic found by Block Port workflow. | | | | |

API Name

illumio_traffic_flows

Columns

| Field Name | API Name | Type | Placeholder | Required | Description |
|----------------|----------------|-----------|----------------------|----------|---|
| Source IP | source_ip | text | 127.0.0.1 | Yes | Source (consumer) IP address for the traffic flow. |
| Destination IP | destination_ip | text | 127.0.0.1 | Yes | Destination (provider) IP address for the traffic flow. |
| Port | port | number | 8080 | Yes | Traffic flow destination port. |
| Protocol | protocol | select | TCP | Yes | Traffic flow protocol. |
| Flows | flows | number | 0 | Yes | Flow count during detection period. |
| First Detected | first_detected | text | 2022-01-01T12:00:00Z | Yes | Timestamp at which the flow was initially detected. |
| Last Detected | last_detected | text | 2022-01-01T12:00:00Z | Yes | Timestamp at which the flow was last detected. |
| Flow Details | flow_details | rich text | | No | Any additional details about the traffic flow. |

Troubleshooting & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is a IBM Community provided App. Please search the Community (<https://ibm.biz/resilientcommunity>), or contact app-integrations@illumio.com for assistance.