

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



AI Powered Security with Hypershield

Jeroen Wittock - TME
DEVNET-1568

CISCO *Live!*

#CiscoLiveAPJC



Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

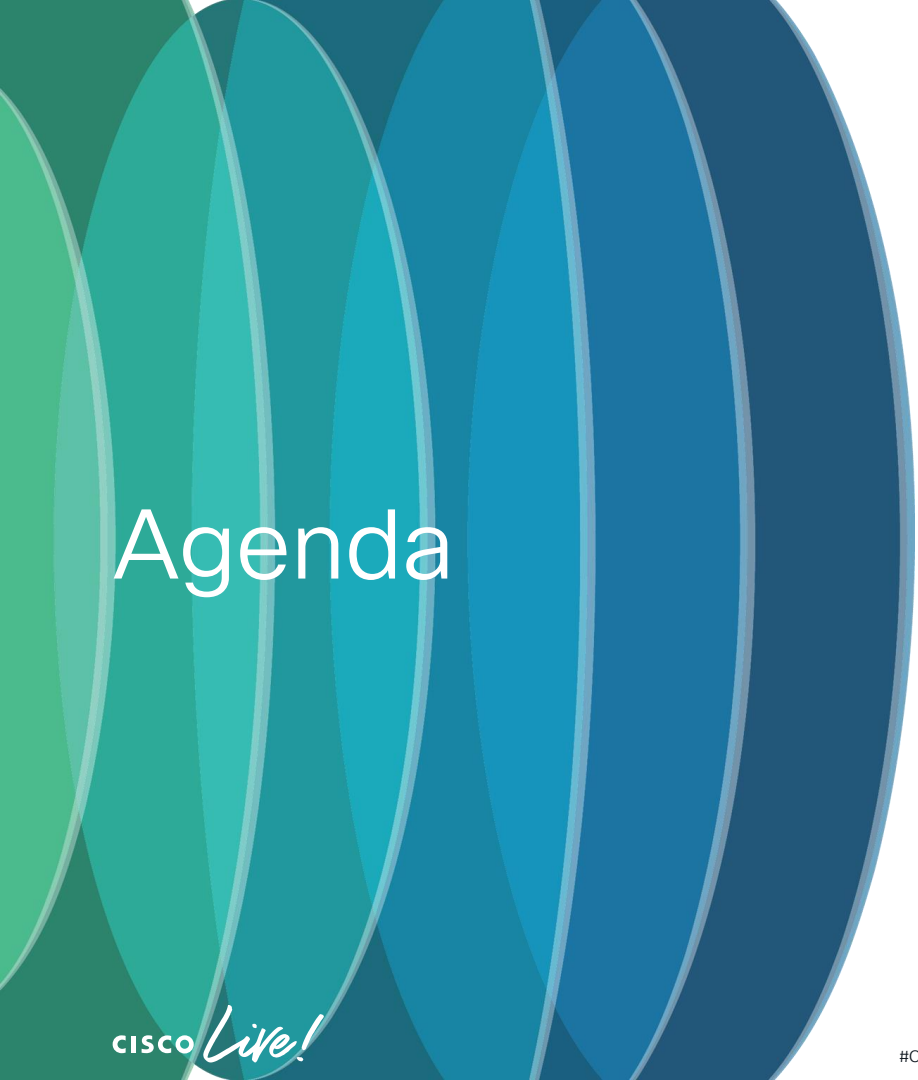
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-1568>



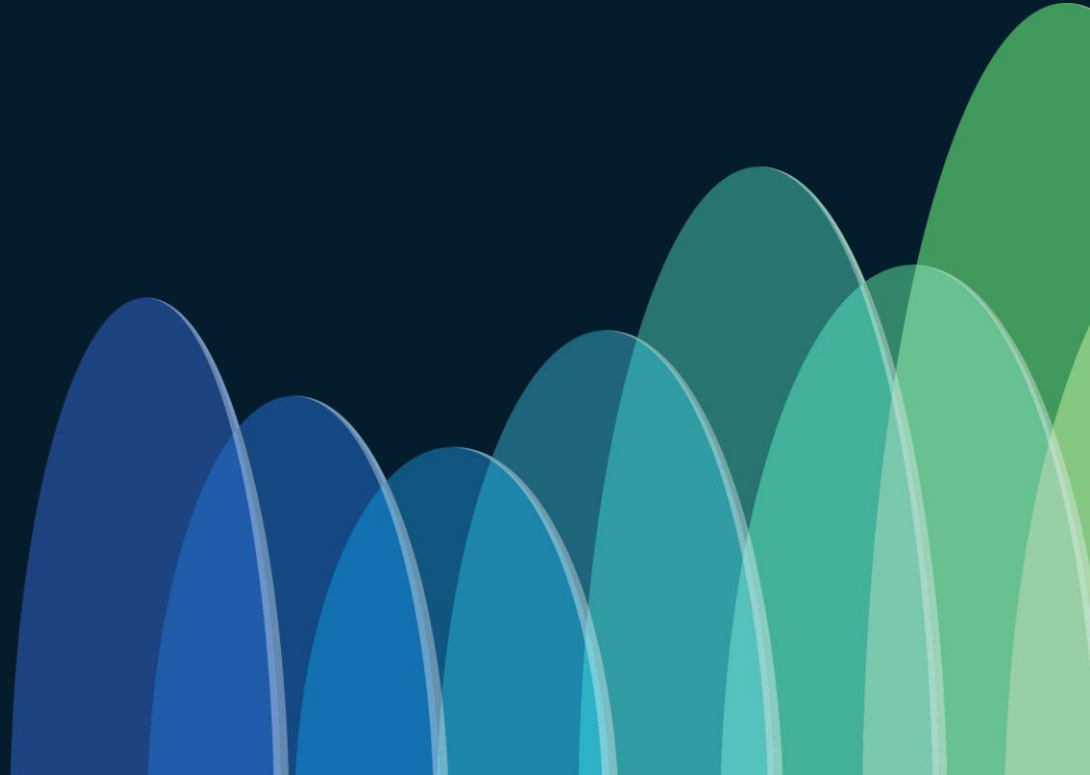


Agenda

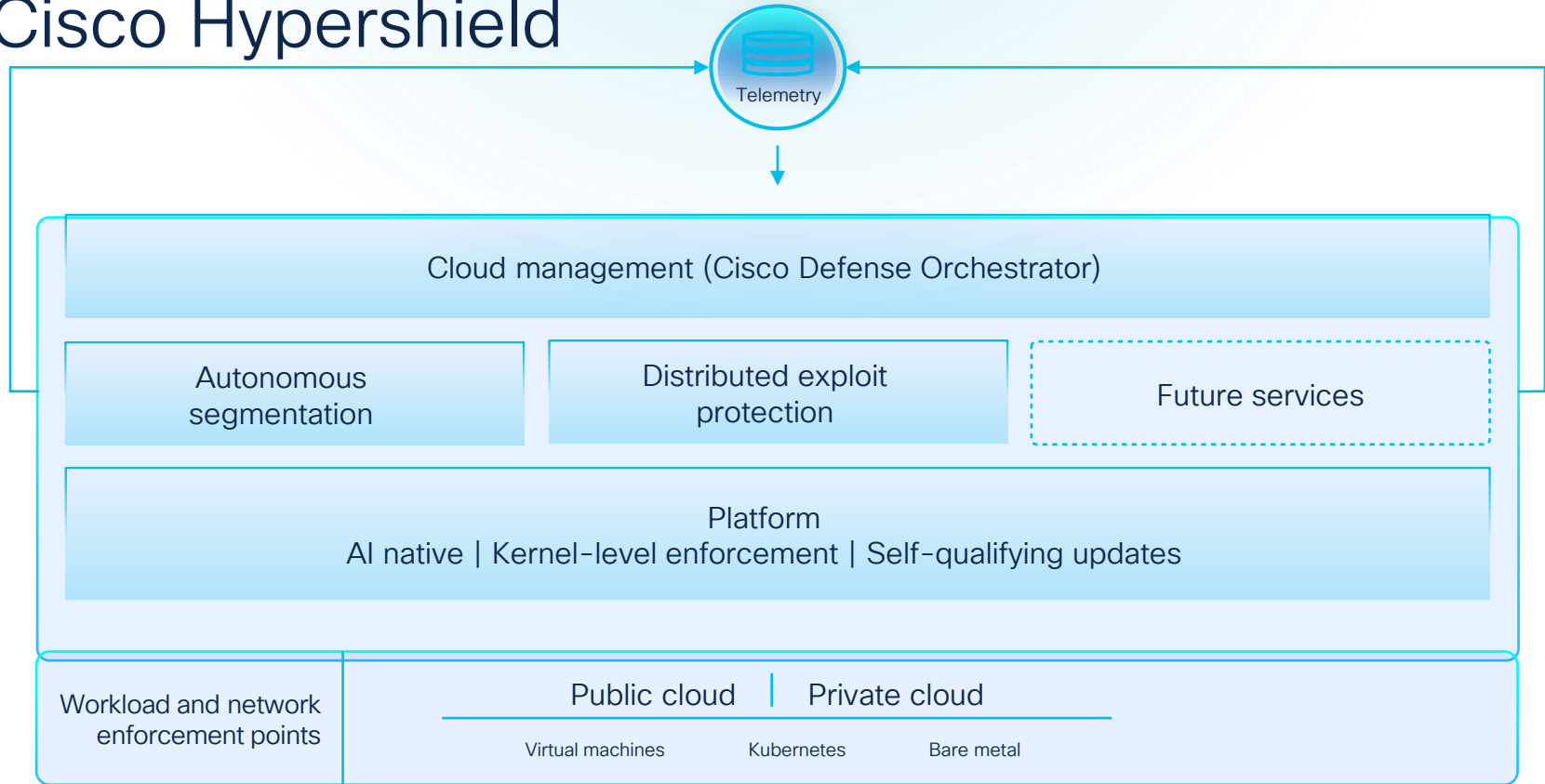
- Introducing hypershield
- Visibility and shields
- Creating policy

Introducing Hypershield

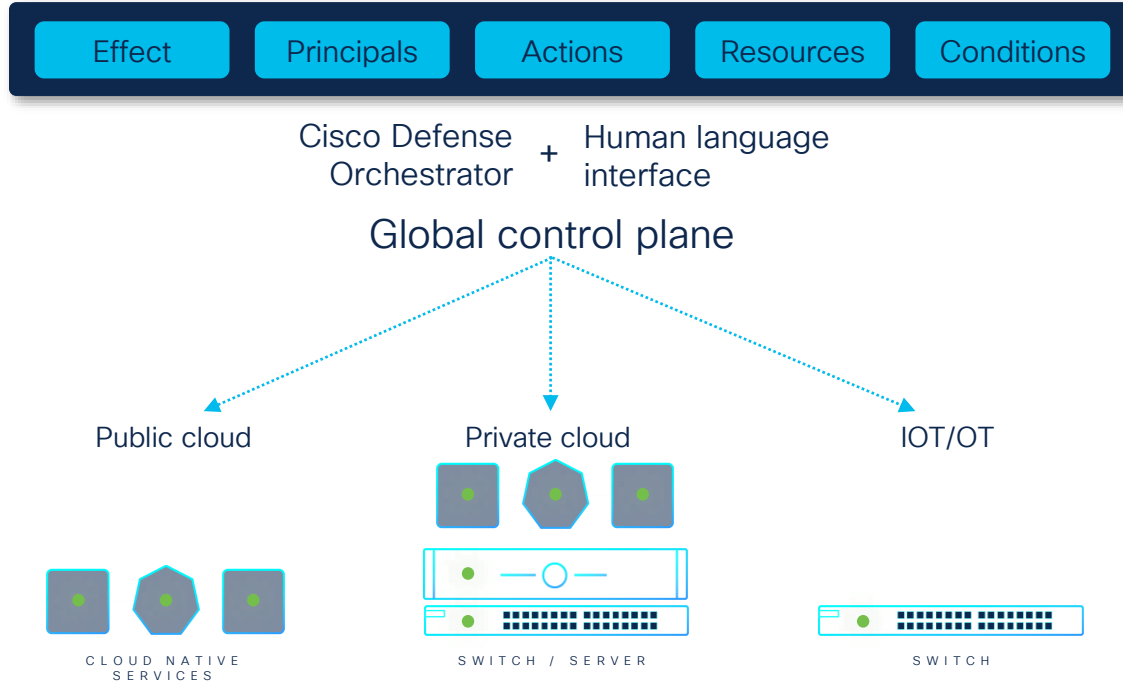
CISCO *Live!*



Cisco Hypershield



Manage globally, enforce locally



● Enforcement point

cisco *Live!*

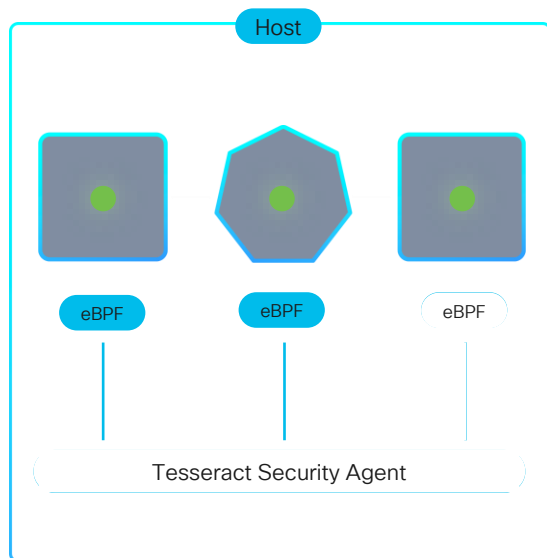
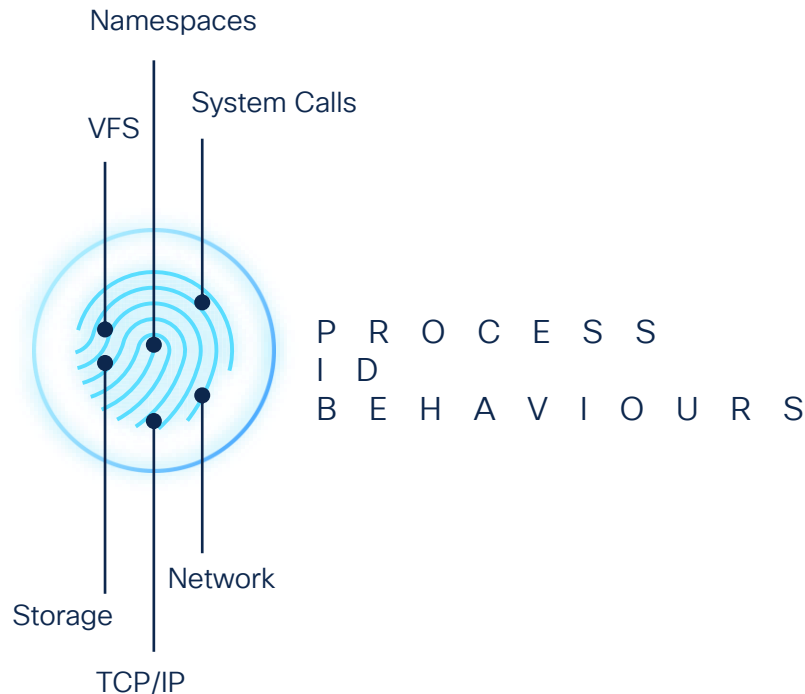
Includes

- Unified management
- Single global policy
- Intelligent placement of rules
- Integrations with cloud/app/infra metadata

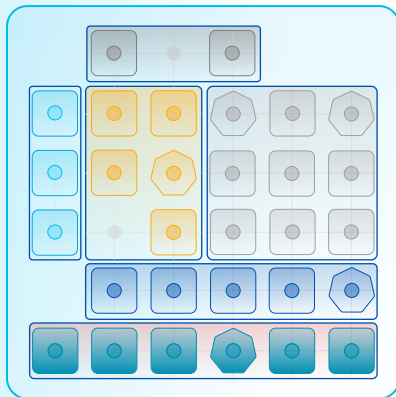
Environments

- Kubernetes
- Cloud – private/public
- On-prem

Deep visibility and enforcement in the workload

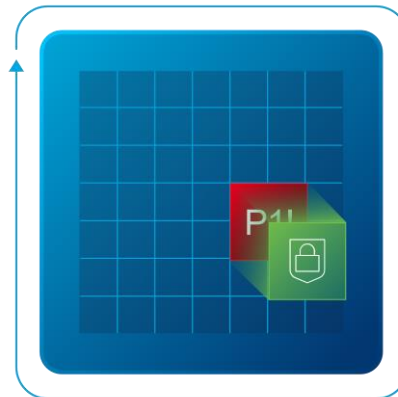


Cisco Hypershield use cases



Autonomous segmentation

- Deep understanding of app behaviour
- Comprehensive inputs for policy creation
- Constantly adapting to changing apps



Distributed exploit protection

- Mitigate known and unknown vulnerabilities
- Surgical compensating controls
- Protection within minutes, while app keeps running

System recommendations tested against live production traffic

Getting Started



2

OK

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public Confidential

Grab the example code

<https://github.com/CiscoDevNet/hypershield>

```
JWITTOCK-M-M4X7:Coding jwittock$ git clone git@github.com:CiscoDevNet/hypershield.git
Cloning into 'hypershield'...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 7 (delta 0), reused 6 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (7/7), 8.75 KiB | 4.37 MiB/s, done.
```

Add the CDO token to config.json

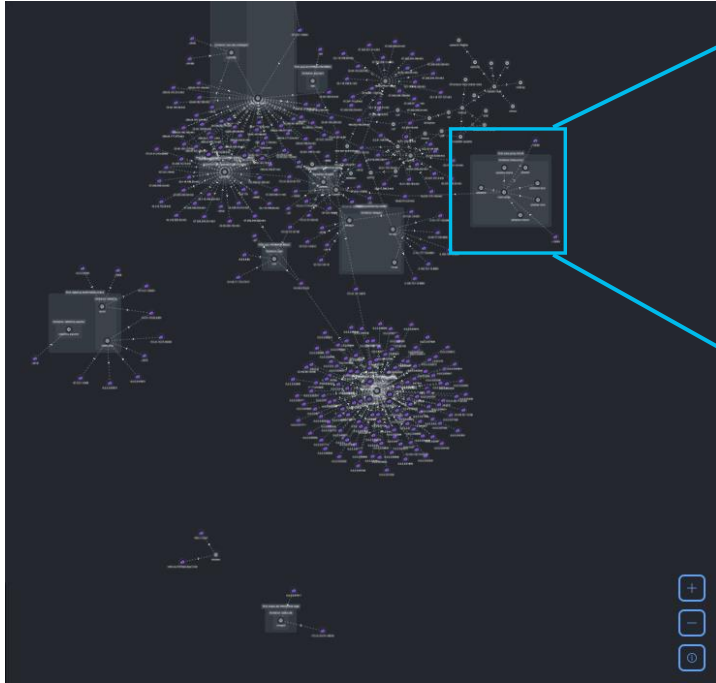
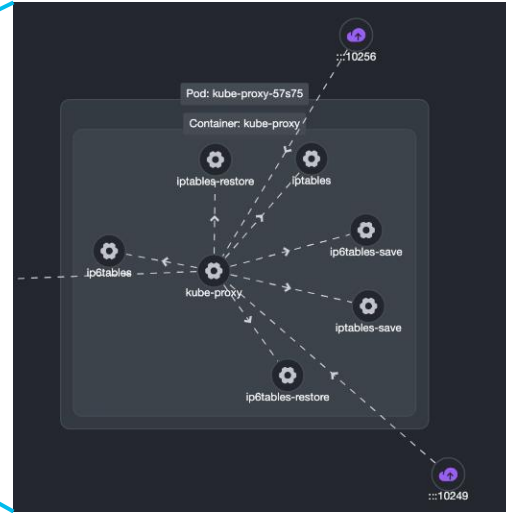
```
1 {
2   "CDO_TOKEN": "YOUR_TOKEN_HERE"
3 }
```

And Verify: `python3 check-token.py`

```
JWITTOCK-M-M4X7:example_scripts jwittock$ python3 check-token.py
Tenant Name: CDO_hypershield-tme
Tenant UID: 6a32347a-a9db-430f-8dc7-e210c1274252
User Name: jwittock-api@CDO_hypershield-tme
User UID: 562757d1-70cd-4597-87a3-341216b3fce8
User Roles: [<UserRole.ROLE_SUPER_ADMIN: 'ROLE_SUPER_ADMIN'>]
User Expires: 2092-11-09 23:25:47+00:00
```

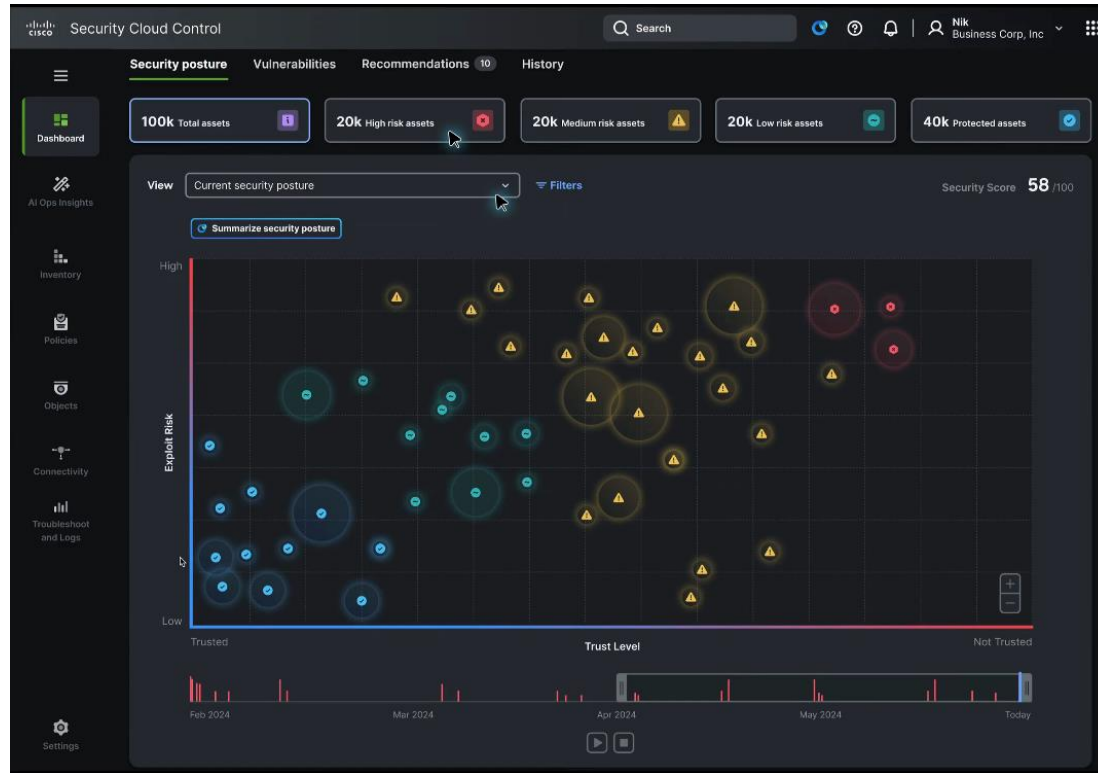
Visibility and Shields

Visibility: today



Coming soon:
enhanced searching and filtering

Visibility: soon



Visibility through the API

- Collecting a graph requires the UID of the agent.
- So list the available agents and their UID's:

python3 list_agents.py

```
Listing agents in tenant:
Name: kubernetes_ip-10-0-3-215.us-east-2.compute.internal
Id: fb4b0f62-6606-48d0-a54a-d84921fd7371
-----
Name: kubernetes_ip-10-0-1-125.us-east-2.compute.internal
Id: f763ac2f-35b8-4bf6-ae03-c1559e778235
-----
Name: node1.ocpcluster.ocp-cloud.com
Id: 7c330125-33bb-4709-bb96-2451b8fd5d47
-----
Name: node3.ocpcluster.ocp-cloud.com
Id: 37472303-860b-400c-bd54-5d96908fdc37
-----
Name: node2.ocpcluster.ocp-cloud.com
Id: baebf018-7cd0-46cd-b6b3-e8d3b2a31d61
-----
```

Visibility through the API

- Now collect the graph from the agent:

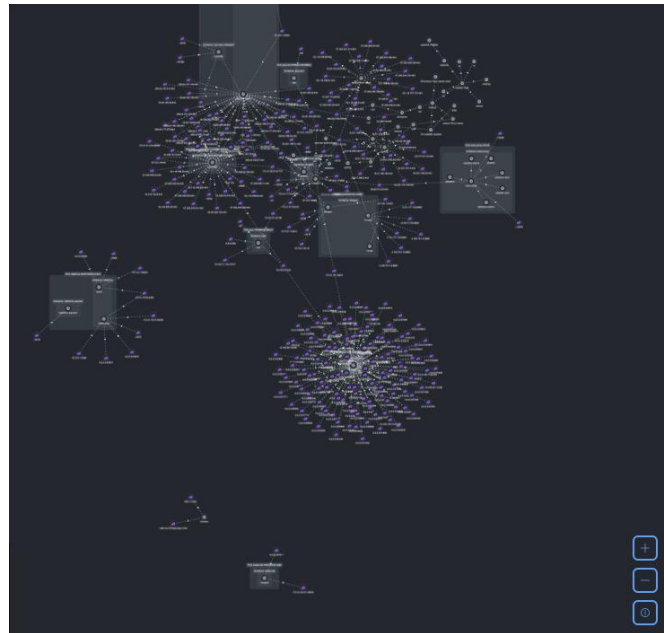
```
python3 get_agent_graph.py 7c330125-33bb-4709-bb96-2451b8fd5d47
```

- This will create a file called:

```
graph_ 7c330125-33bb-4709-bb96-2451b8fd5d47.json
```

CISCO *Live!*

11



Shields: today

Cisco Hypershield

Q Type 'Ctrl' + '/' to search

cisco-daf-ea-demo
jwitlock@cisco.com

Overview

Quick actions ▾

Summary Vulnerabilities

Q Search

Status	Name	CVSS v3 ①	Assets affected	Mitigation	
Exploitable - shield deployment failed	CVE-HS-TEST	9.5 Critical	1	Exploitable - shield deployment failed	...

Shields: soon

Security Cloud Control

Search

Overview

Security posture Vulnerabilities **Recommendations 10** History

Dashboard

AI Ops Insights

Inventory

Policies

Objects

Connectivity

Troubleshoot and Logs

Search All types

Recommendation	Number of actions	Security score impact	Action	Assigned to
> Remediate vulnerabilities from CVE-2024-21626	2	+ 32	Deploy View	Nik
> Autonomous segmentation available for 1 application	2	+ 27	Review	Nik

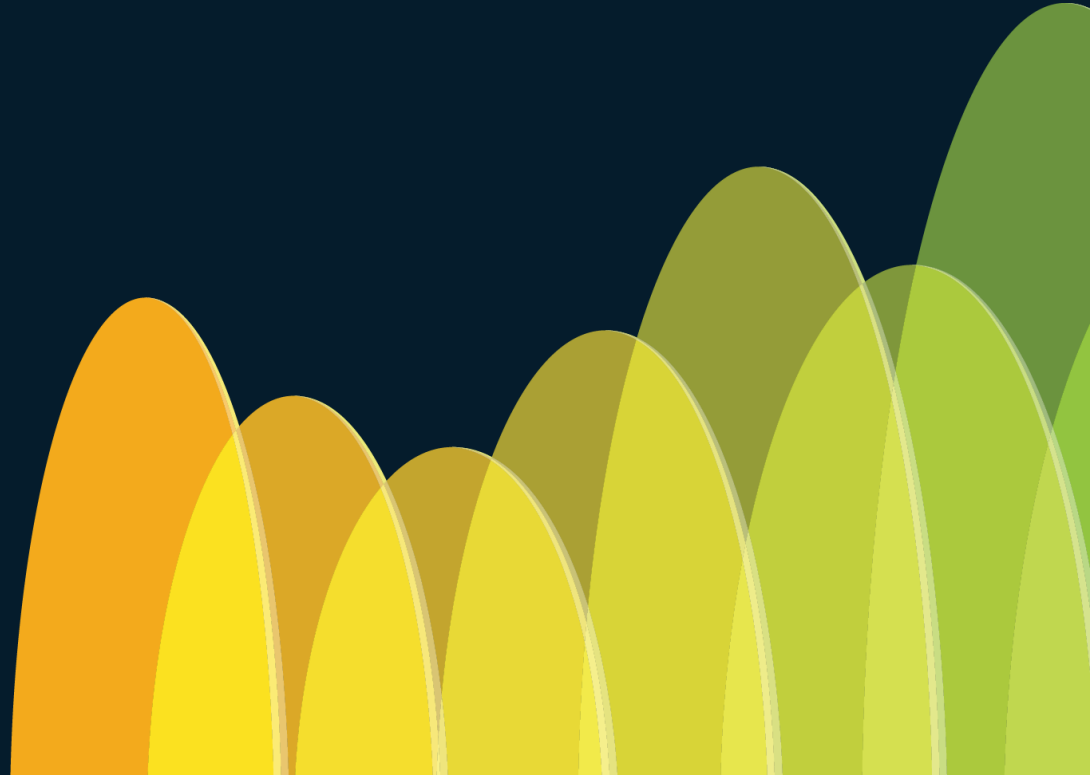
Policy group **Policy changes** **Object changes** **Created by** **Created on** **Status** **Confidence Score**

Finance App group	3 added 1 edited	—	Hypershield	May 19 2024 07:21	Testing Completed	95%
-------------------	------------------	---	-------------	-------------------	-------------------	-----

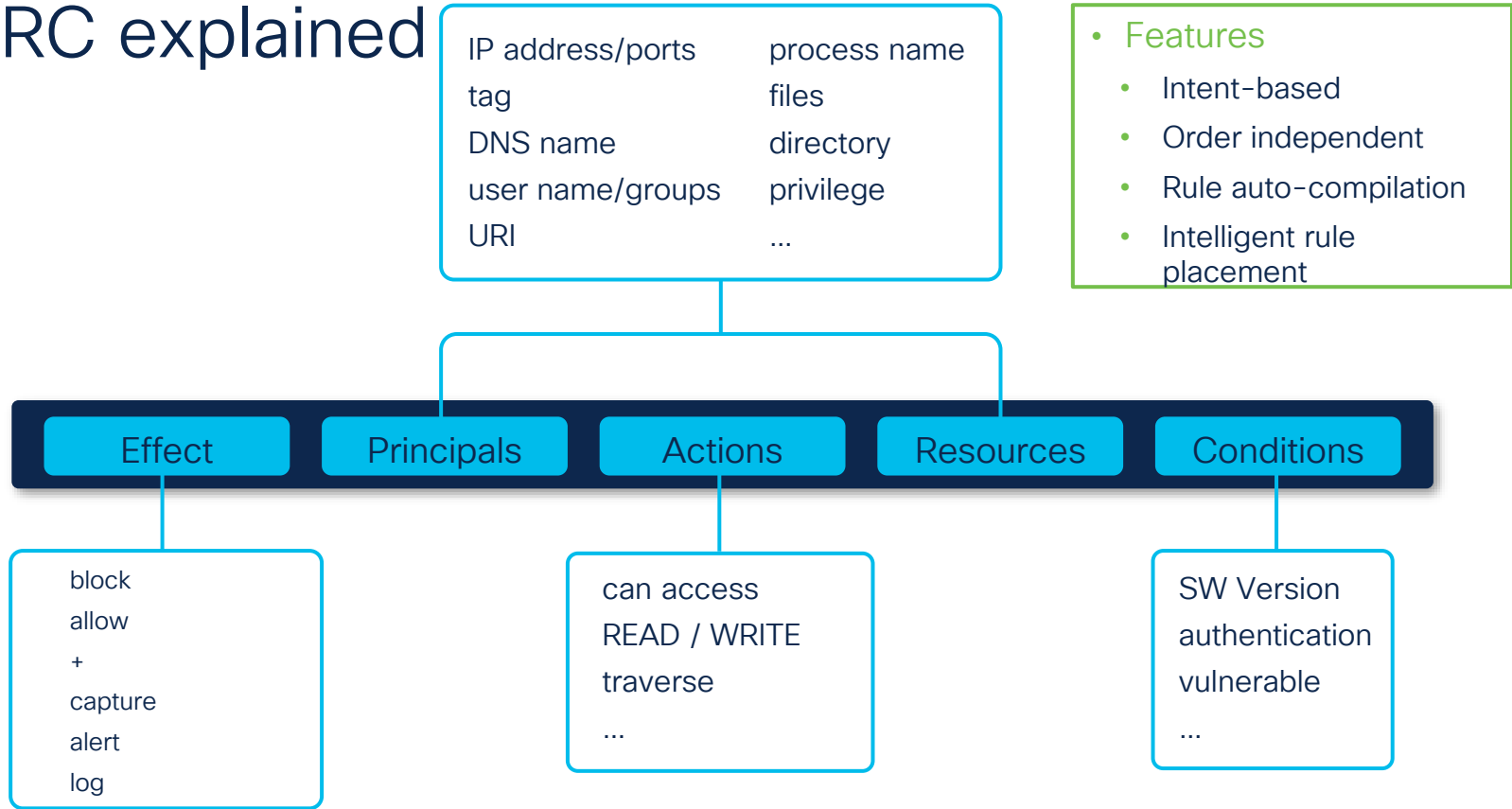
Explain why this recommendation is needed Show the effects of the recommendation

> Autonomous segmentation available for 2 zones	1	+ 16	Review	Nik
> Autonomous segmentation available for 32 workloads	1	+ 5	Review	Nik
> Autonomous segmentation available for 32 workloads	2	+ 3	Review	Nik
> Autonomous segmentation available for 5 applications	2	+ 2	Review	Nik
> Review 2 unusual behaviors	2	+ 1	Review	Nik
> Review 1 unusual behavior	2	+ 1	Review	Nik
> Clean up policies	2	+ 1	Deploy View	Nik
> Install Tesseract Security Agents on 14 workloads	2	+ 1	Install View	Nik

Creating Policy



PARC explained



AI recommends policy

✓ Distributed Exploit Shield | runc-exec...

✓ Verified

REMEDIATION 1

Recommended

The Distributed Exploit Shield blocks new container processes with a current working directory of "/" in the host namespace.

Reason

Remediates vulnerability **CVE-2024-21626**

Effect

Block and alert

Principal

/usr/local/sbin/runc

Action

sys_execve

Resource

*

Condition

when principal.version <= 1.1.11 or unknown and action.cwd = "host_ns:/"

Deployed by 8,734 other customers

Deploy

View 3 alternative remediations

Archive

Effect

Block and alert

Principals

File path / executable

Actions

Execute permit

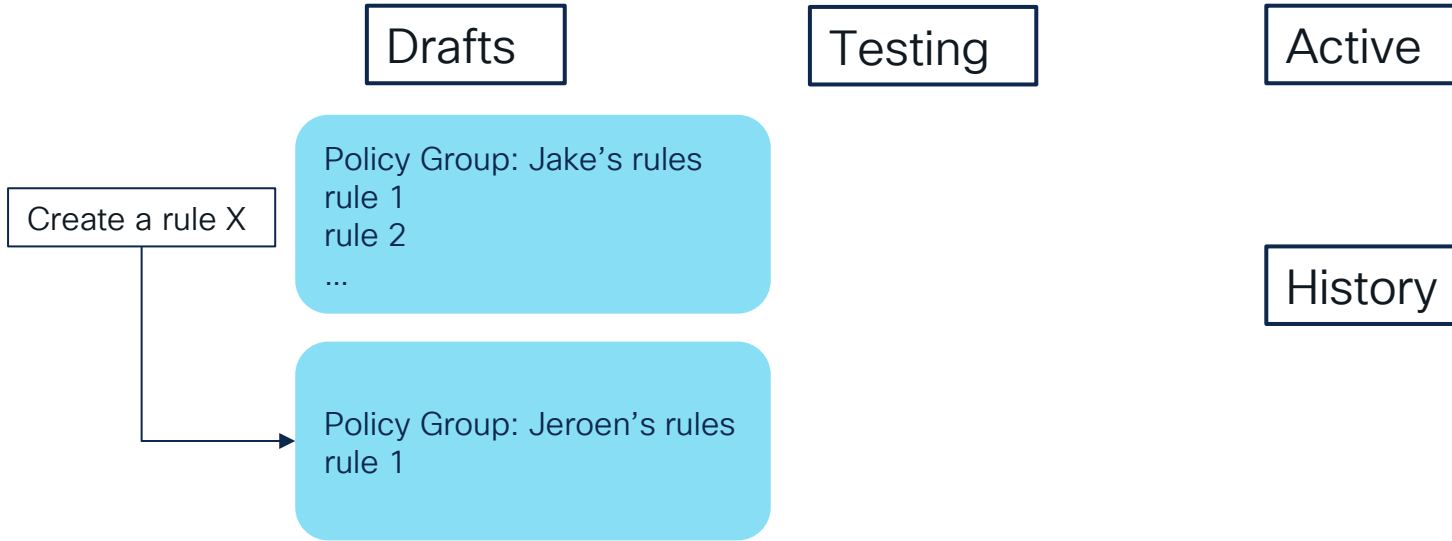
Resources

* (act on any resource)

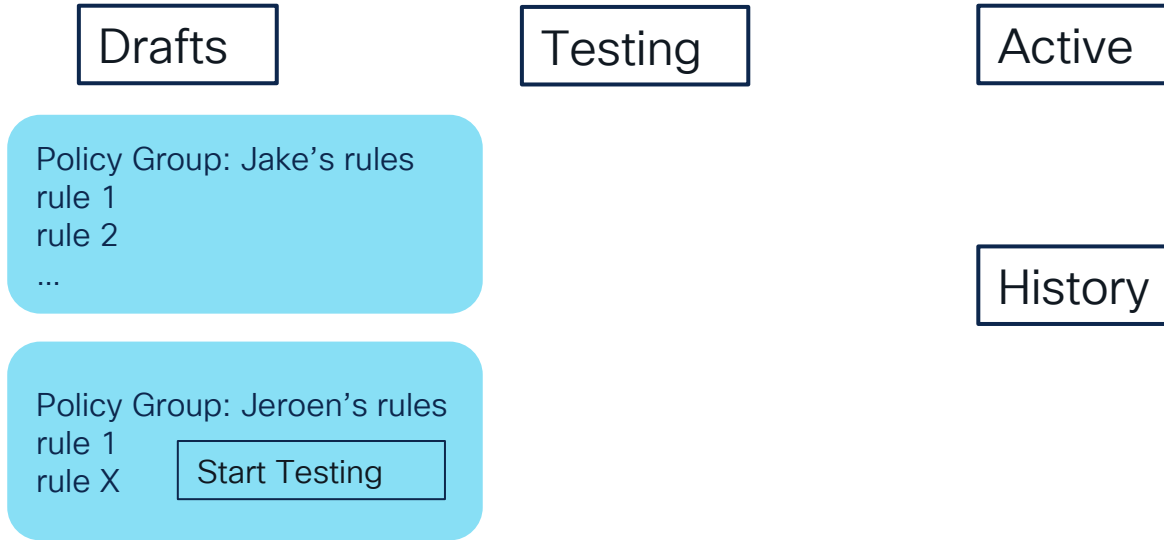
Conditions

Minimum version and namespace

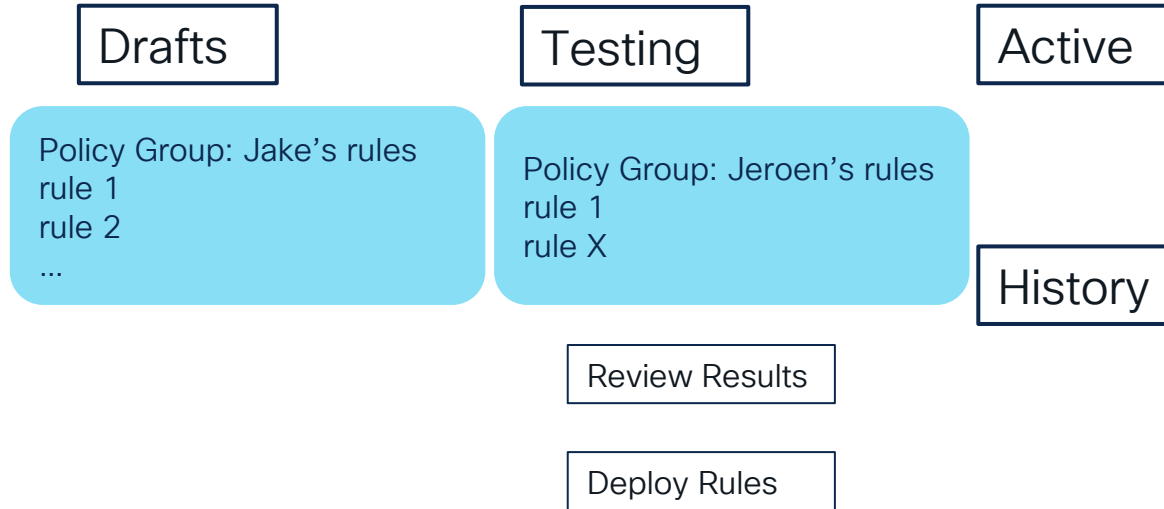
A day in the life of a policy rule



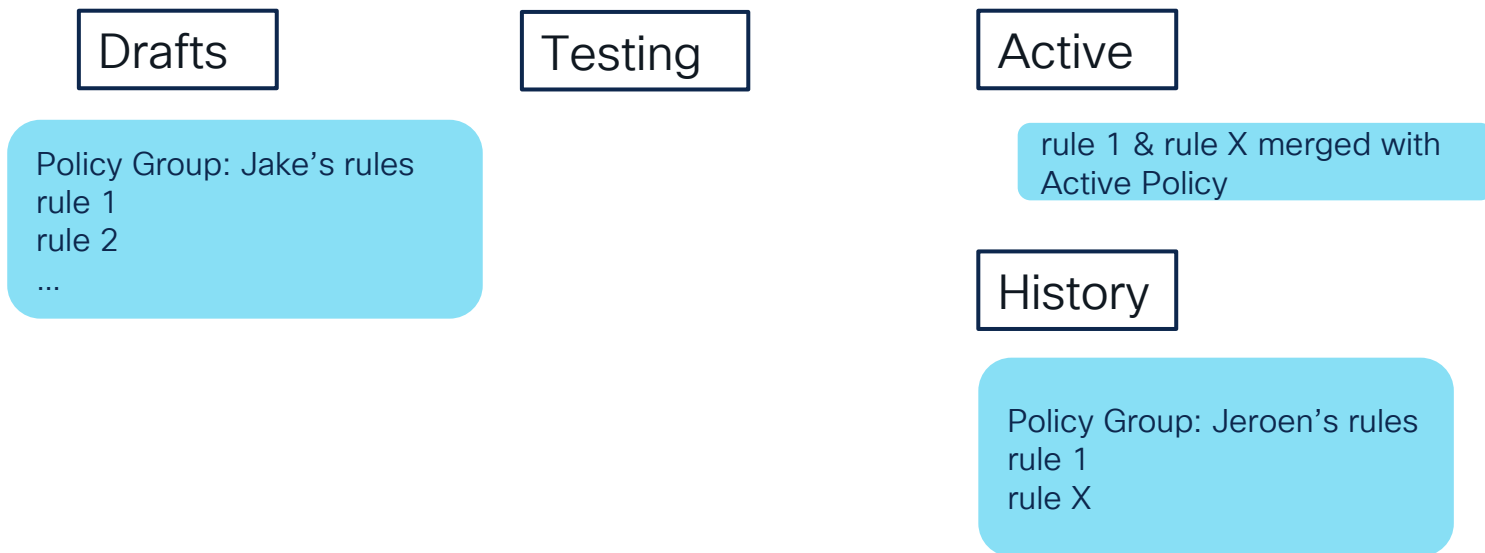
A day in the life of a policy rule



A day in the life of a policy rule



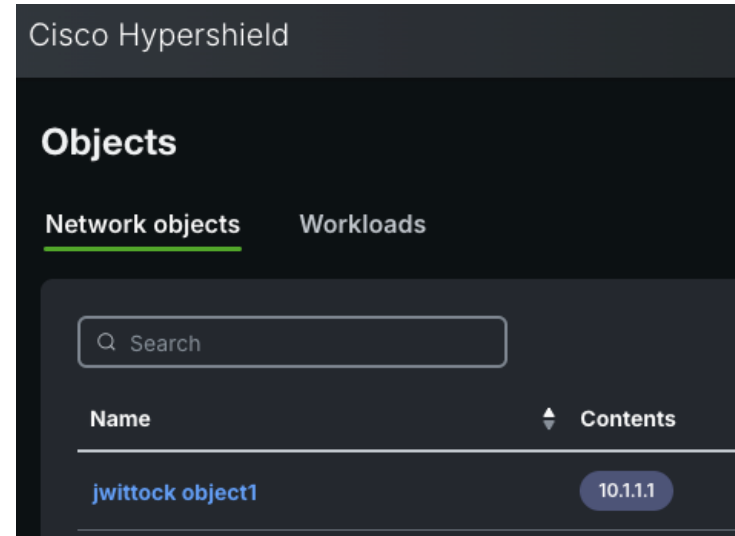
A day in the life of a policy rule



Create principal and resource objects

- python3 create_object.py

```
JWITTOCK-M-M4X7:example_scripts jwittock$ python3 create_object.py
{
  "id": "de3ea176-12f9-4e32-8a38-33e61bb207de",
  "tenantId": "6a32347a-a9db-430f-8dc7-e210c1274252",
  "name": "jwittock object1",
  "description": "",
  "objectType": "DAF_NETWORK_OBJECT",
  "contents": [
    {
      "sgt": [],
      "vlan": [],
      "@type": "DAF_NETWORK_CONTENT",
      "addresses": [
        {
          "ips": [
            "10.1.1.1"
          ],
          "port": "",
          "awsTags": [],
          "vCenterTags": []
        }
      ]
    }
  ],
  "createdBy": "jwittock-api@CDO_hypershield-tme",
  "updatedBy": "jwittock-api@CDO_hypershield-tme",
  "updatedAt": "2024-10-25T12:31:51.238Z",
  "createdAt": "2024-10-25T12:31:51.238Z",
  "referenceId": null
}
```



Create policy group

- python3 create_policy-group.py

```
[JWITTOCK-M-M4X7:example_scripts jwittock$ python3 create_policy-group.py
{
  "id": "201783bb-1d2e-483e-a7ed-ef25dbaf5142",
  "tenantId": "6a32347a-a9db-430f-8dc7-e210c1274252",
  "name": "jwittock CLAPJ24 policy group",
  "description": "Add your description",
  "createdBy": "jwittock-api@CDO_hypershield-tme",
  "updatedBy": "jwittock-api@CDO_hypershield-tme",
  "status": "OPEN",
  "type": "FIREWALL",
  "diffCounts": {
    "addPolicy": 0,
    "editPolicy": 0,
    "deletePolicy": 0,
    "editObject": 0,
    "deleteObject": 0
  },
  "updatedAt": "2024-10-25T12:42:02.838Z",
  "createdAt": "2024-10-25T12:42:02.838Z",
  "referenceId": null,
  "enforcement": null,
  "fwAgentCount": null
}
Policy-group id is: "201783bb-1d2e-483e-a7ed-ef25dbaf5142"
```

Cisco Hypershield

Policies

Active

Drafts

History



Policy group completed testing

[sock_shop](#)

Q Search

Status

Name

Policy changes

Draft

[jwittock CLAPJ24 policy group](#)

-

Create policy

- python3 create_policy.py

```
JWITTOCK-M-M4X7:example_scripts jwittock$ python3 create_policy.py
{
  "id": "201783bb-1d2e-483e-a7ed-ef25dbaf5142",
  "tenantId": "6a32347a-a9db-430f-8dc7-e210c1274252",
  "referenceId": null,
  "name": "jwittock CLAPJ24 policy group",
  "description": "Add your description",
  "createdBy": "jwittock-api@CDO_hypershield-tme",
  "updatedBy": "jwittock-api@CDO_hypershield-tme",
  "status": "OPEN",
  "type": "FIREWALL",
  "diffCounts": {
    "addPolicy": 1,
    "editPolicy": 0,
    "deletePolicy": 0,
    "editObject": 0,
    "deleteObject": 0
  },
  "enforcement": null,
  "fwAgentCount": null,
  "createdAt": "2024-10-25T12:42:02.838Z",
  "updatedAt": "2024-10-25T12:46:57.950Z"
}
```

← Policies

jwittock CLAPJ24 policy group

Add your description

Delete

Total changes	Updated by	Updated at	Created by	Created on
1	jwittock-api@CDO_hypershield-tme	25/10/2024, 14:46:57	jwittock-api@CDO_hypershield-tme	25/10/2024, 14:42:02

Staged changes

1

policy added

Policies

Objects

Operation	Policy name	Changed by	Changed on
Added	jwittock CLAPJ24 test		

Effect	Principal	Action	Resource	
After	✓ Permit and warn	jwittock object1	icmp	jwittock object2

Start testing on policy group

- python3 start_testing.py

```
JWITTOCK-M-MAX7:example_scripts jwittock$ python3 test.py
{
  "id": "201783bb-1d2e-483e-a7ed-ef25dbaf5142",
  "tenantId": "6a823a7a-a9db-430f-8dc7-e210c1274252",
  "referenceId": null,
  "name": "jwittock CLAPJ24 policy group",
  "description": "Add your description",
  "createdBy": "jwittock-api@CDO_hypershield-tme",
  "updatedBy": "jwittock-api@CDO_hypershield-tme",
  "status": "TESTING",
  "type": "FIREWALL",
  "diffCounts": {
    "addPolicy": 1,
    "editPolicy": 0,
    "deletePolicy": 0,
    "editObject": 0,
    "deleteObject": 0
  },
  "enforcement": {
    "policyGroupId": "201783bb-1d2e-483e-a7ed-ef25dbaf5142",
    "firewallEnforcement": {
      "permanentStoreHash": "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca95991b7852b855",
      "add": [
        "a306c6d9-6357-414c-a5ee-730d724bfcc5"
      ],
      "edit": [],
      "delete": [],
      "data": [
        {
          "id": "c62aacc1-9e6a-4b81-9a67-aca861211bc9"
```

Cisco Hypershield

← Policies

jwittock CLAPJ24 policy group

Add your description

Testing in Progress

Total changes	Updated by	Updated at
1	jwittock - api@CDO_hypershield - tme	25/10/2024, 15:04:30

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC