Illumio CloudSecure – Step by Step Lab Guide

Hello! Welcome to the Illumio CloudSecure lab guide. Here we will provide you with a step-by-step overview of Illumio CloudSecure features from deployment to policy writing.

Objectives

Objective 1: Visibility into Cloud Resources and their Traffic Flows

Objective 2: Create Segmentation Policies for Applications

Objective 3: Create Segmentation Policies for the Organization

At the end of the lab, you'll be able to:

- Visualize your cloud assets and how they communicate with each other in the cloud.
- Write segmentation policies to prevent lateral movement and reduce the attack surface within your cloud assets.

Let's get started!

Prerequisite

1. An AWS account to run a CloudFormation template with resources.

Please refer to the GitHub link for detailed instructions on running the CloudFormation template required for the lab –

https://github.com/illumio-shield/CloudSecure-AWS-Demo-Template/blob/main/README.md

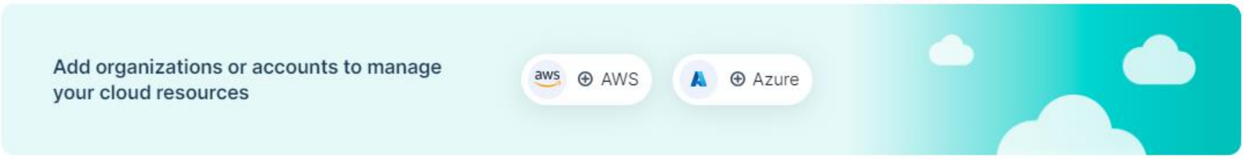
2. Illumio Free Trial

If you have not already signed up for the Illumio Free Trial, please sign up for the Free Trial using the link below.

https://console.illum.io/#/signup

3. Onboarding assets and Flow Logs

Login to your Illumio Unified Console. The first time you login, the page displays a message that you need to add your cloud accounts to CloudSecure.



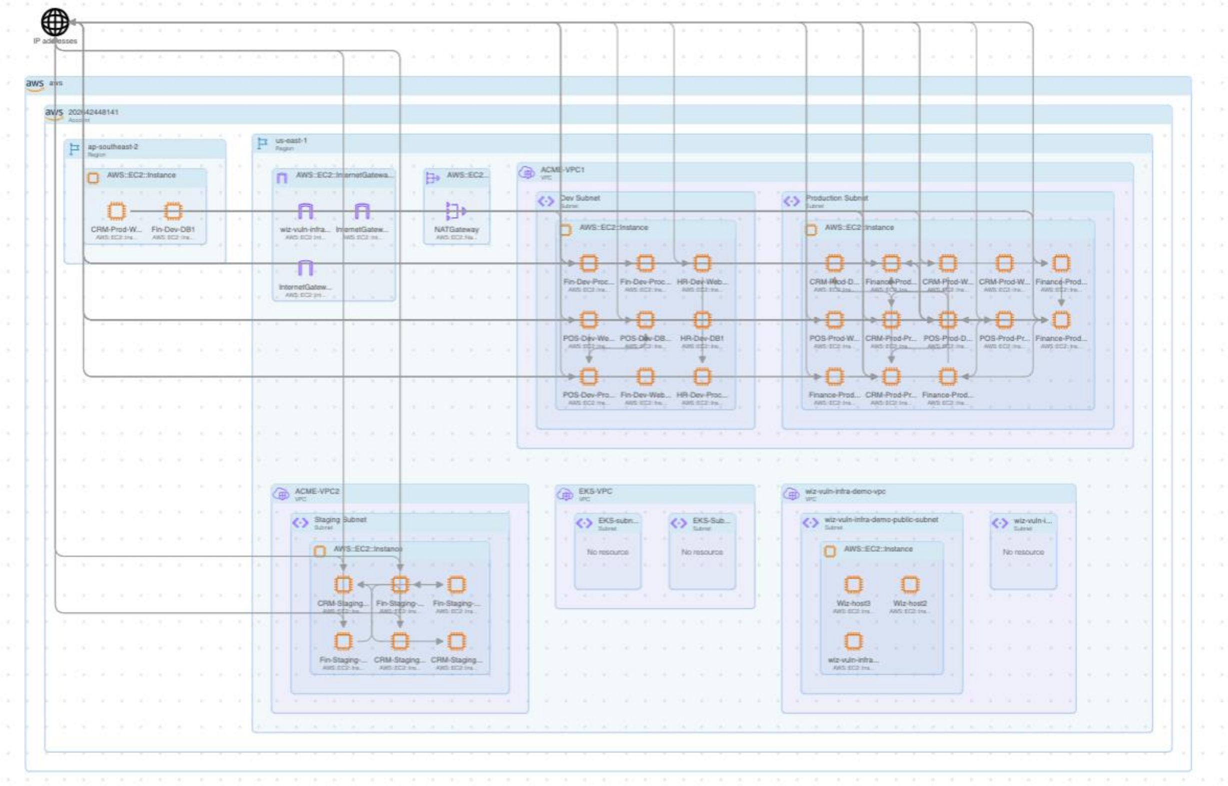
Add organizations or accounts to manage your cloud resources

You can follow the instructions from the Illumio Documentation provided in the link below, to onboard your AWS account onto CloudSecure.

https://docs.illumio.com/cloudsecure/Content/Guides/cloudsecure-usage/onboard-accounts/onboard-aws-account.htm

Once you have onboarded your AWS account, you will now be able to see the resources within the Cloud Map.

Navigate to **Explore → Map**



Note: It may take 10-15 mins to show the data with flows in the cloud map.

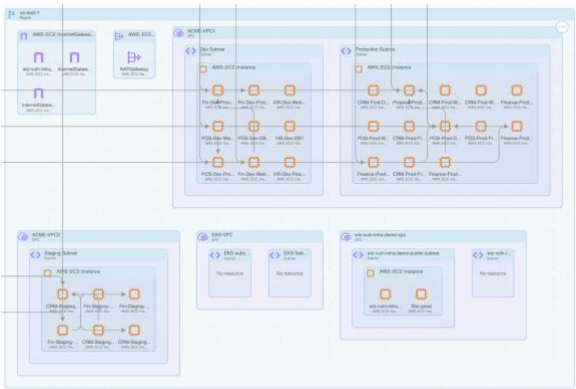
Objective 1: Exploring Map and Traffic

In this section, we will discuss and show how Illumio can help identify your various cloud assets and how they communicate between each other.

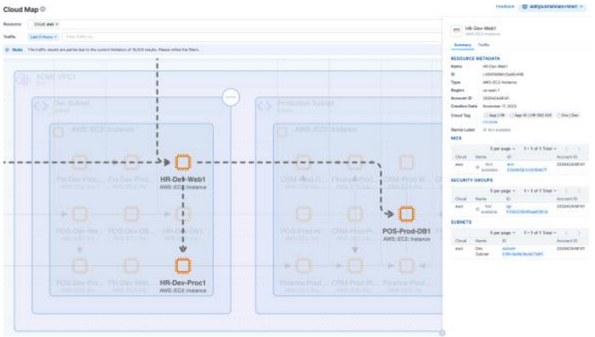
1. In the resource filter, select “aws”. You will now see a map with the lines

The cloud map provides you with a hierarchical view of all your cloud resources, starting with the cloud account, regions, VPC’s, subnets and resources.

Let’s zoom into the region, we have the CloudFormation template deployed. In our scenario, we have deployed the template in the US-East-1 region.



2. Click on the region, you have installed the CloudFormation template above and zoom in
3. Here you can view and analyze the various cloud resources.
   a. Click on “HR-Dev-Web1” EC2 instance.
   b. It will show you that this server has communication to “HR-Dev-Proc1”, “POS-Prod-DB1” and other sources within the internet.



      i. Explore through the summary and traffic tabs.

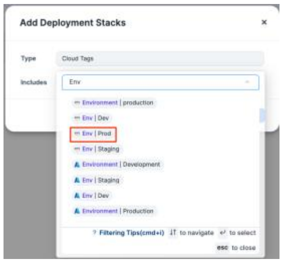
Congratulations!! You have completed Objective 1 of Illumio CloudSecure Experience.

Objective 2: Create Segmentation Policies for Application

CloudSecure makes it simple to group applications together. You can define applications by simply utilizing the existing cloud tags associated with the assets. Defining applications helps visualizing and writing segmentation policies.

Create Deployments - A deployment stack essentially correlates with the stages that organizations use to manage their development lifecycle and defines the boundaries of their app deployment. The most common deployments would be "Dev", "Prod" and "Staging".

a. Under Application Discovery, click on "Deployments." → Click "Add"
b. Environment = Production
c. Add Cloud tags → "Env | Prod"



Add Deployment Stacks ×

Type: Cloud Tags

Includes: Env

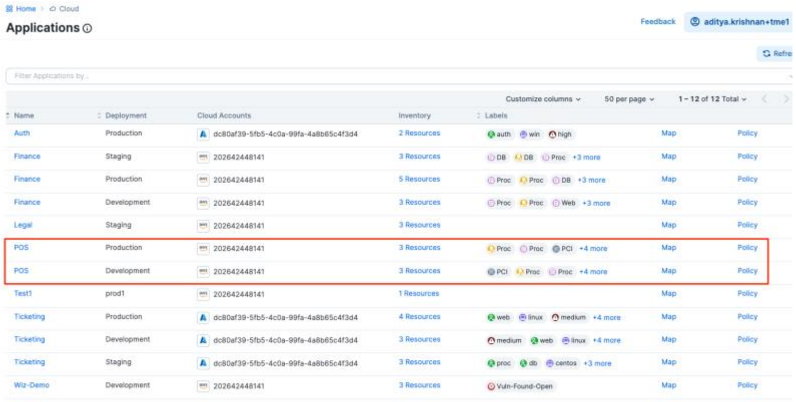
- Environment | production
- Env | Dev
- Env | Prod
- Env | Staging
- Environment | Development
- Env | Staging
- Env | Dev
- Environment | Production

d. Save the deployment.

Similarly, add the Dev and Staging deployments.

2. **Cloud Tag to label mapping** – This is a important feature within CloudSecure that allows users to associate additional labels with the application, allowing for more granularity when writing policies.
   a. Click "Tag to Label Mapping" in the left-hand side menu bar.
   b. "Add Mapping" → Filter by a Cloud Account → Select "Role" Cloud key tag
3. **Create an Application Definition** –
   a. Under "Application Discovery", click on "Application Definitions" → Click "Add"
   b. Select Cloud Account → Select Cloud tag "App | POS"
   c. Save the Application Definition

Click on "Applications" on the left-hand side menu. CloudSecure has automatically discovered the Finance Application in the "Dev", "Prod" and Staging deployments.



Name	Deployment	Cloud Accounts	Inventory	Labels		
Auth	Production	dc80af39-5fb5-4c0a-99fa-4a8b65c4f3d4	2 Resources	auth win high	Map	Policy
Finance	Staging	202642448141	3 Resources	DB DB Proc +3 more	Map	Policy
Finance	Production	202642448141	5 Resources	Proc Proc DB +3 more	Map	Policy
Finance	Development	202642448141	3 Resources	Proc Proc Web +3 more	Map	Policy
Legal	Staging	202642448141	3 Resources		Map	Policy
POS	Production	202642448141	3 Resources	Proc Proc PCI +4 more	Map	Policy
POS	Development	202642448141	3 Resources	PCI Proc Proc +4 more	Map	Policy
Test1	prod1	202642448141	1 Resources		Map	Policy
Ticketing	Production	dc80af39-5fb5-4c0a-99fa-4a8b65c4f3d4	4 Resources	web linux medium +4 more	Map	Policy
Ticketing	Development	dc80af39-5fb5-4c0a-99fa-4a8b65c4f3d4	3 Resources	medium web linux +4 more	Map	Policy
Ticketing	Staging	dc80af39-5fb5-4c0a-99fa-4a8b65c4f3d4	3 Resources	proc db centos +3 more	Map	Policy
Wiz-Demo	Development	202642448141	3 Resources	Vuln-Found-Open	Map	Policy

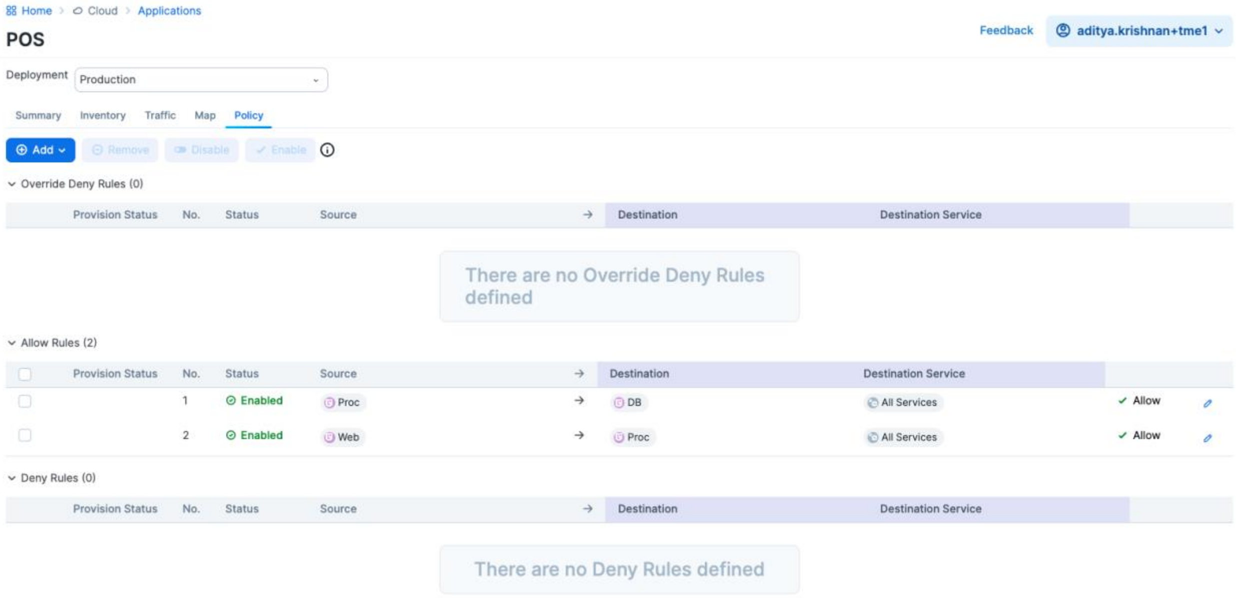
Now, you can write policies to your AWS security groups using simple labels that you have defined.

1. Click on “POS” in the Production environment.
2. You can view through the summary, inventory, traffic and map tabs

Note: The POS application is a 3-tier application with Web-Frontend, Proc-Middleware and DB-Backend

Here, we are going to create a policy to only allow the instances to talk on the above ports and block all other ports.

3. Click on “Policy”.
4. Let us create 2 allow rules –
   a. Allow traffic from Web → Proc on All Services
   b. Allow traffic from Proc to Database on All Services
5. Provision the rules



POS

Deployment: Production

Override Deny Rules (0)

Provision Status	No.	Status	Source	→	Destination	Destination Service

There are no Override Deny Rules defined

Allow Rules (2)

□	Provision Status	No.	Status	Source	→	Destination	Destination Service		
□		1	Enabled	Proc	→	DB	All Services	✓ Allow	
□		2	Enabled	Web	→	Proc	All Services	✓ Allow	

Deny Rules (0)

Provision Status	No.	Status	Source	→	Destination	Destination Service

There are no Deny Rules defined

Now, you can verify the policies written in the Security groups of your AWS console.

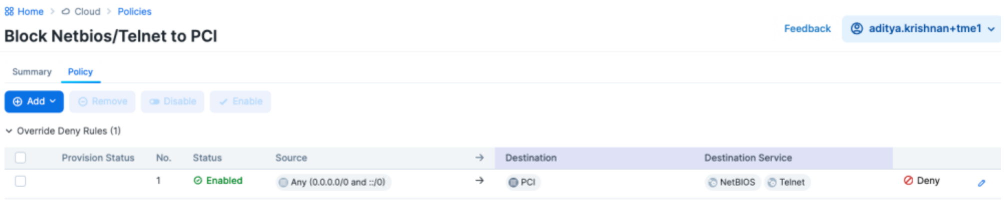
Congratulations!! You have completed Objective 2 of Illumio CloudSecure Experience.

Objective 3: Create Segmentation Policies for the Organization

Organizational policies are guardrail policies that are applied across your entire infrastructure. These could address the mandates set by corporate security to restrict certain traffic flows from propagating within your environment. The most common example is to block high risk ports within the entire organization such as Telnet, FTP, SMB, and RDP.

To create meaningful label-based policies, we can convert existing cloud tags to Illumio labels. These labels in turn can be used to write label-based policies within Illumio. In this scenario, we would like to ensure that our PCEI compliant systems are blocked from being accessed on RDP or Telnet.

1. **Tag to Label Mapping**
   a. Click "Tag to Label Mapping" in the left-hand side menu bar
   b. "Add Mapping" → Filter by a Cloud Account → Select "Compliance" Cloud key tag
2. **Write organizational Policies**
   a. Click "Policies" on the left hand side menu
   b. Under Organizational Policies, click "Add"
   c. Name the policy "Block Netbios/Telnet to PCI"
   d. Create an "Override Deny Rule" to block "Any" to "PCI" on "Netbios and Telnet"

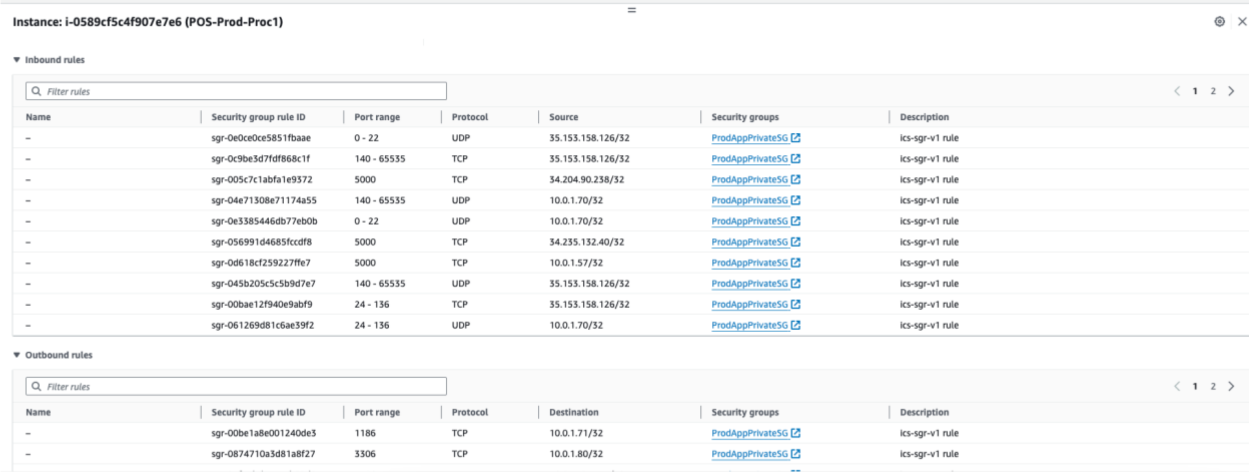


Block Netbios/Telnet to PCI

Override Deny Rules (1)

	Provision Status	No.	Status	Source	→	Destination	Destination Service		
□		1	Enabled	Any (0.0.0.0/0 and ::/0)	→	PCI	NetBIOS Telnet	Deny	

The POS application that was created in the previous section is a PCI compliant application with Compliance labels of "PCI". If you now go to the AWS security group rules for POS application, you will notice that all traffic ports will be included except "NetBios" and "Telnet".



Instance: i-0589cf5c4f907e7e6 (POS-Prod-Proc1)

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-0e0ce0ce5851fbaae	0 - 22	UDP	35.153.158.126/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-0c9be3d7fdf868c1f	140 - 65535	TCP	35.153.158.126/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-005c7c1abfa1e9372	5000	TCP	34.204.90.238/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-04e71308e71174a55	140 - 65535	UDP	10.0.1.70/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-0e3385446db77eb0b	0 - 22	UDP	10.0.1.70/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-056991d4685fccdf8	5000	TCP	34.235.132.40/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-0d618cf259227ffe7	5000	TCP	10.0.1.57/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-045b205c5c5b9d7e7	140 - 65535	UDP	35.153.158.126/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-00bae12f940e9abf9	24 - 136	TCP	35.153.158.126/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-061269d81c6ae39f2	24 - 136	UDP	10.0.1.70/32	ProdAppPrivateSG	ics-sgr-v1 rule

Outbound rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
–	sgr-00be1a8e001240de3	1186	TCP	10.0.1.71/32	ProdAppPrivateSG	ics-sgr-v1 rule
–	sgr-0874710a3d81a8f27	3306	TCP	10.0.1.80/32	ProdAppPrivateSG	ics-sgr-v1 rule

Congratulations!! You have now completed Objective 3 of Illumio CloudSecure Experience.

Recap

During this hands-on lab, you were able to successfully:

- Understand how applications in the cloud communicate with each other utilizing the Cloud map and Traffic View. No other segmentation technology, be it CNAPP or CSPM, delivers such powerful visibility of cloud assets and traffic data.
- Reduce attack surface and protect high value assets using simple application segmentation policies.
- Prevent Lateral movement within the entire cloud estate by creating organizational policies.

You have now put Zero Trust Segmentation in place in minutes versus the tedium of writing and configuring security groups and NACL rules for segmentation.