Illumio CloudSecure – Step by Step Lab Guide for Azure Deployments

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**

*“You can only protect what you see”.* Visibility into cloud resources and traffic flows are crucial for ensuring robust security measures are in place.

**Objective 2: Create Segmentation Policies for Applications**

Application policies are written to control traffic flows destined for specific applications. As different teams within your organization may own different applications, this allows for security policy to be applied at a granular level, based on individual needs.

**Objective 3: Create Segmentation Policies for the Organization**

Organization Policies are rulesets that can be broadly applied across your infrastructure, perhaps to meet various security compliance guidelines across various applications. Denying protocols like RDP, NetBIOS, Telnet etc. may be mandated by corporate security teams, and this provides for an easy way to apply these policies across your cloud assets.

**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 and organizational policies to prevent lateral movement and reduce the attack surface within your cloud assets.

Let’s get started!

# Prerequisite

1. An Azure subscription with Owner permissions is needed in order to run a PowerShell script that will load your environment with resources.

Please refer to the GitHub link for detailed instructions on running the Bicep template required for the lab – This can be used to populate a new Azure Resource Group with workloads and traffic flows to quickly try out CloudSecure.

<https://github.com/stauffer-jeff/CloudSecure-Azure-Demo-Template>

Note: After running the template in your Azure environment, you will need to enable NSG flow logs from the resources created and send their traffic to a storage account within your subscription. (basic blob storage is fine. Version 2)

1. 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>

1. 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.

A screenshot of a phone

Description automatically generated

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

<https://docs.illumio.com/cloudsecure/Content/Guides/cloudsecure-usage/get-started/onboard-azure-subscription.htm>

Once you have onboarded your Azure subscription, 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. The cloud map provides you with a hierarchical view of all your cloud resources, starting with the cloud subscription, regions, virtual networks, subnets and resources. Clicking on the “+” sign in the corner of each region will expand that icon to display resources found in the next layer down. Try expanding the region in which you deployed the Bicep template to reveal virtual networks, subnets, and individual resources that were created.

A screenshot of a cloud map

Description automatically generated

## 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 “azure”. You will now see a map with traffic lines overlayed upon resources

A screenshot of a computer

Description automatically generated

1. Here you can view and analyze the various cloud resources. Hover your mouse over any workload to get an animated view of flow lines from that resources’ perspective.

A screenshot of a cloud map

Description automatically generated

Also by clicking on a resource, a side panel will open up to provide further details about that resource, as well as a traffic flow table.

A screenshot of a computer

Description automatically generated

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

## Objective 2: Create Deployments and Application Definitions

CloudSecure makes it simple to organize resources into specific applications and the various instances where they are deployed. You can define applications by simply utilizing the existing cloud tags or other metadata associated with those assets. There are 2 steps involved:

1. **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”.
   1. Under Application Discovery, click on “Deployments.” 🡪 Click “Add”
   2. Environment = Production
   3. Add Cloud tags 🡪 “Env | Prod” . This defines the “boundary” of what resources are part of your “Production” deployment.

A screenshot of a cloud tag

Description automatically generated

* 1. Save the deployment.

Similarly, add the Dev and Staging deployments.

1. **Create an Application Definition** –
   1. Under “Application Discovery”, click on “Application Definitions” 🡪 Click “Add”
   2. Give the Application a name of “Ticketing”
   3. Click on “Add Resources Using Cloud Metadata”
   4. Under “Filter by Cloud Accounts” select your Azure subscription
   5. Under “Select Cloud Tags” select the Azure tag of “App|Ticketing”. Click on “Add to Selection” to move this tag over to the right of the screen. This defines the “boundary” of what resources are part of your “Ticketing” Application.
   6. Click Confirm Selection
   7. Save this Application Definition.

Click on “Application Definitions” on the left-hand side menu. CloudSecure will now automatically scan your onboarded cloud accounts and discover any resources that mean your definition for “Ticketing Application”, and divide them into the “Dev”, “Prod” and Staging deployments you defined. This will require approval before these groupings can be used for writing security policy. (approval is needed in the future if new resources or are discovered before they can be added to these deployments as well)

A screenshot of a computer

Description automatically generated

* 1. Click on “View Details” to see the various deployments where CloudSecure has discovered resources for this Application. Approve each deployment in order to begin to write security policy for each instance.

A screenshot of a computer

Description automatically generated

At this point, CloudSecure has discovered what assets are part of the Ticketing application as well as the various deployments where those assets are deployed. Now you can write security policy that is specific to this application, and differentiate policy between production, staging, and dev environments.

1. From the Applications menu item, click on “Ticketing” in the Production environment.
2. You can view through the summary, inventory, traffic and map tabs

Note: The Ticketing application is a 3-tier application with Web-Frontend, Proc-Middleware and DB-Backend. We can create some simple policies to allow/deny various protocols that will be applied to all resources within this application:

1. Click on Policy Tab, and selection the ‘Production’ deployment from the drop-down menu up top.
2. Create an Override Deny Rule to block all RDP traffic:
   1. Add🡪Add Override Deny Rule
   2. Source: Ticketing Application
   3. Dest: Ticketing Application
   4. Policy Services: RDP
3. Create an Allow Rule for SSH traffic:
   1. Add🡪Add Allow Rule
   2. Source: Ticketing Application
   3. Dest: Ticketing Application
   4. Policy Services: SSH
4. Save and Provision the rule
5. CloudSecure knows the list of inventory and their associated Network Security Groups that will need this policy applied, and will push these rules into the appropriate Azure NSG’s.

A screenshot of a computer

Description automatically generated

Now, you can verify the policies written in to your NSG’s in the Azure portal.

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

## Objective 3: Create Segmentation Policies for your Organization

1. **Cloud Tag to label mapping** – This is a critical feature within Cloudsecure that allows users to associate additional labels with the application, allowing for more granularity when writing policies. You can select from any existing cloud tags (or multiple tags) and map them to an Illumio label type. For example, you might want to create labels that describe the “role” this workload provides, the “location” of where its deployed, or even the “Cost Center” used for assigning ownership. In this example we’ll create a Compliance tag to label some production workloads as “PCI” assets.
   1. Click “Tag to Label Mapping” in the left-hand side menu bar
   2. Click “Add Mapping” 🡪 Filter by a Cloud Account (select Azure subscription)
   3. From “Select Cloud Tag Keys” select the Azure tag called Compliance, click on “Add to Selection.” The tag will move to the right side of the screen.
   4. Now we need to create a new Illumio Label Type to map this tag to. Click the pull-down menu under “Maps to Illumio Label Type” and there will be an option for “Create New Label Type”. Select an icon for this new label type, a Display Name of “Compliance” and a Key of “CP” (some screens will use the shortened key name.)
   5. The Mapping screen should look something like the following:

A screenshot of a computer

Description automatically generated

* 1. Click Confirm & Save.
  2. Now we can utilize this additional label in policy writing.

Organizational Policies are one way to create Security rulesets that can have very broad coverage in your environment, such as complying with corporate security mandates, or implementing “dev/prod” separation with a few clicks. For this section, we will create a policy that prohibits any NetBIOS, Telnet, or RDP traffic in your PCI environment. Let’s use the recently created label of Compliance to achieve this goal:

1. Go to the Policies tab
2. Select Organiation Policies
3. Click Add
4. Give it a name of “Block NetBIOS and Telnet”
5. Click Add, and create an Override Deny Rule
6. Source: Any (0.0.0.0/0)
7. Destination: PCI label
8. Policy Services: NetBIOS, Telnet.
9. Save and Provision
10. CloudSecure will push this policy to any workload that is labeled with the Compliance tag of ‘PCI’ to secure these resources from risky ports.

A screenshot of a computer

Description automatically generated

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