Background: This example demonstrates how Prisma Cloud can be used to alert on suspicious network traffic, and how to analyze networks in the Prisma Cloud console.

In this activity, you will:

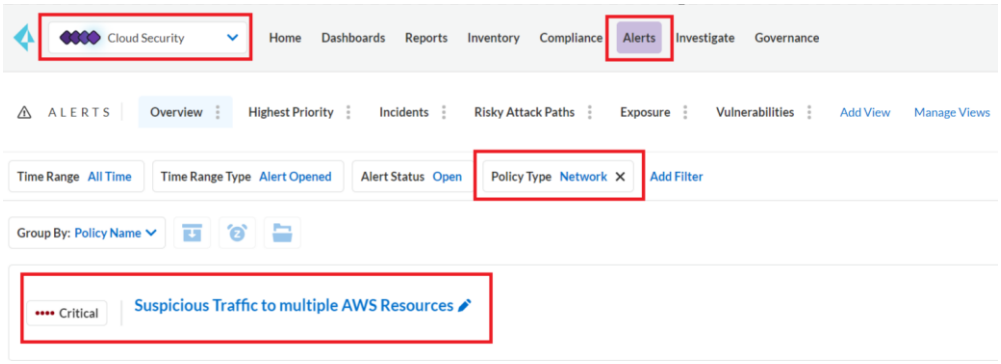
- View a Network Alert for suspicious activity.
- Analyze the Network Visualization to trace resources that may have been impacted.
- View the traffic that is reaching your cloud workloads.
- Examine Vulnerabilities that have been detected on your cloud Workload to understand the risk posture.
- View Alert on risky AWS IAM Permissions.
- Analyze the current resource configuration settings.
- Analyze the change history for the IAM configuration settings (show how the resource got to its current state).
- View how Prisma Cloud remediation commands can be leveraged to remediate security findings.

Note: This is a standalone activity and is not dependent on other activities.

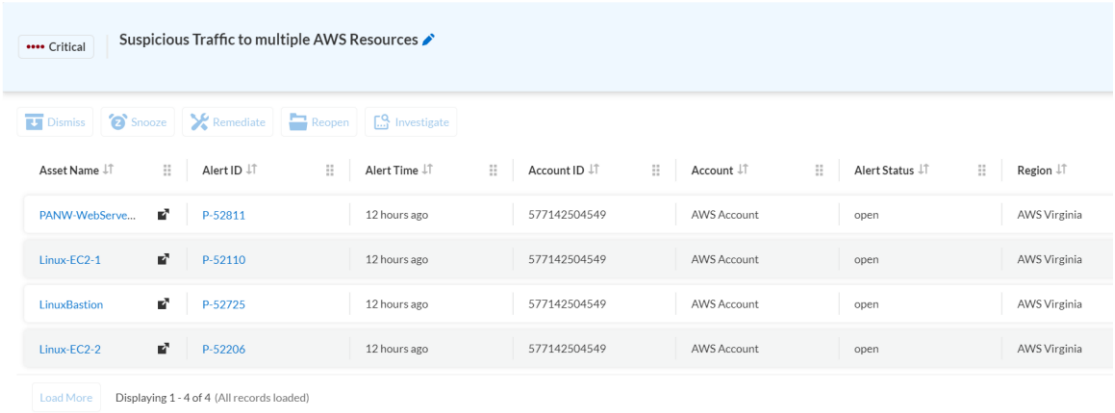
---------- **Task 1: Examine a Network Alert** ----------

Step 1. In the Prisma Cloud Enterprise Edition console, click the **Alerts** tab and then **Overview**.
Step 2. Select the **Reset Filters** icon on the top right corner of the screen to reset all filters and set the **Time Range** to **All Time**.
Step 3. Click on the **Add Filter** icon and select the following options and look for the alert **Suspicious Traffic to Multiple AWS Resources**:

a) Alert Status = **Open**
b) Policy Type = **Network**
c) Cloud Account = **AWS UTD Account**

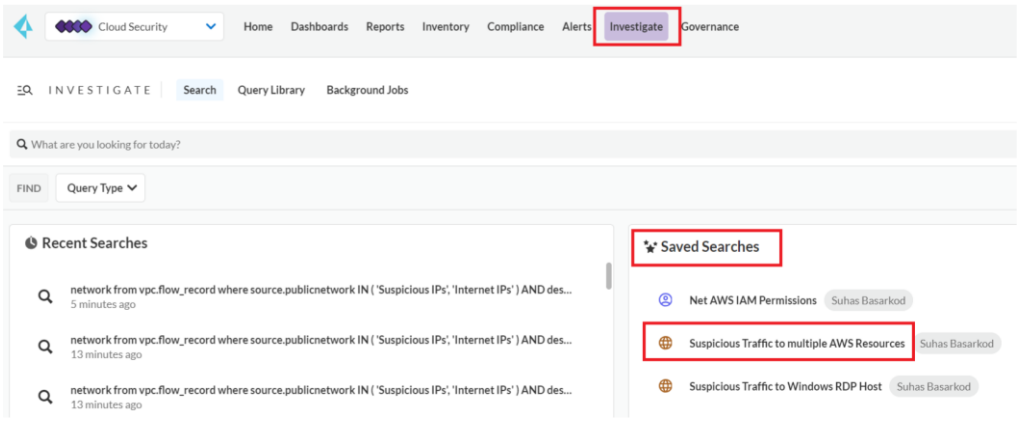


Step 4. Here you can see a list of resources causing this alert to fire.

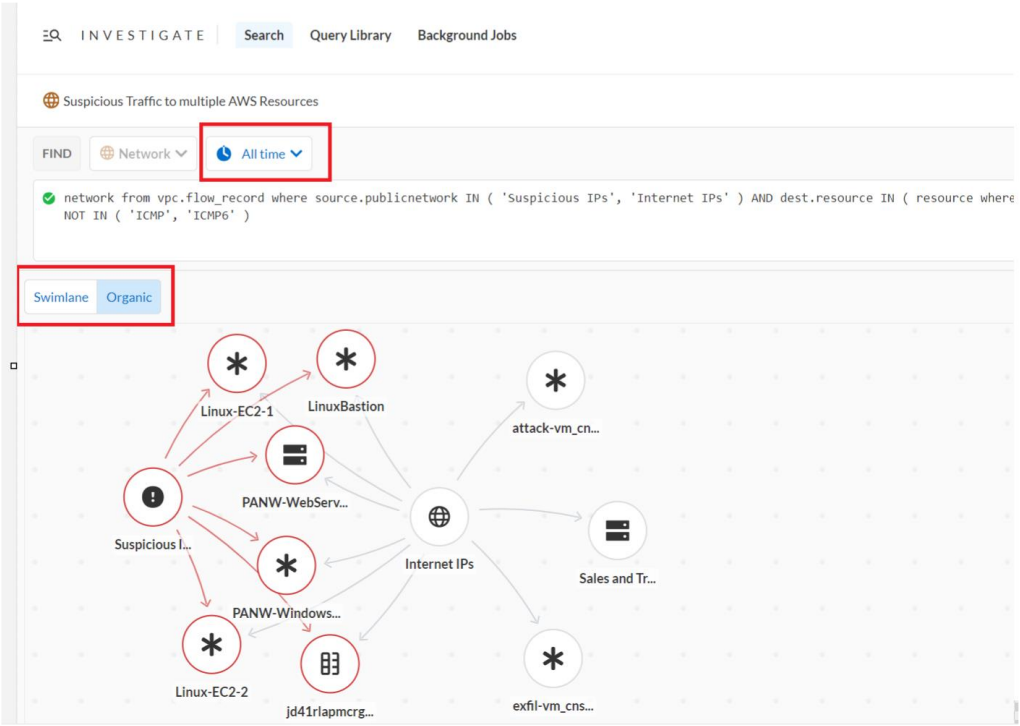


---------- Task 2: Examine the Traffic from Suspicious IPs ----------

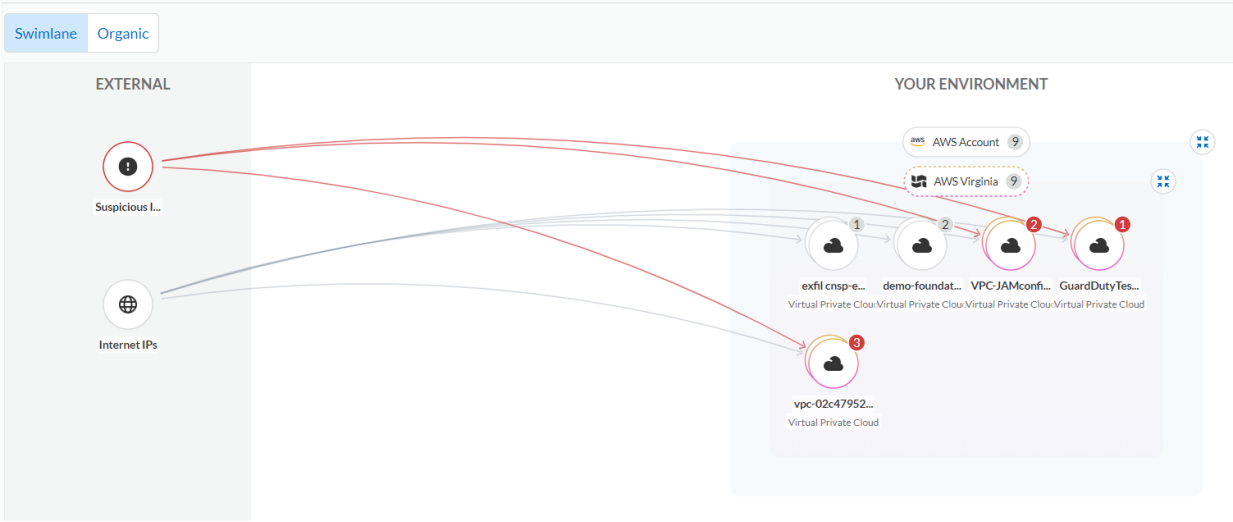
Step 1. Head over to the **Investigate** window. For your convenience, we have already created a query to list out the resources for the previous alert. To use that, within the **Saved Searches**, select **Suspicious Traffic to multiple AWS Resources**



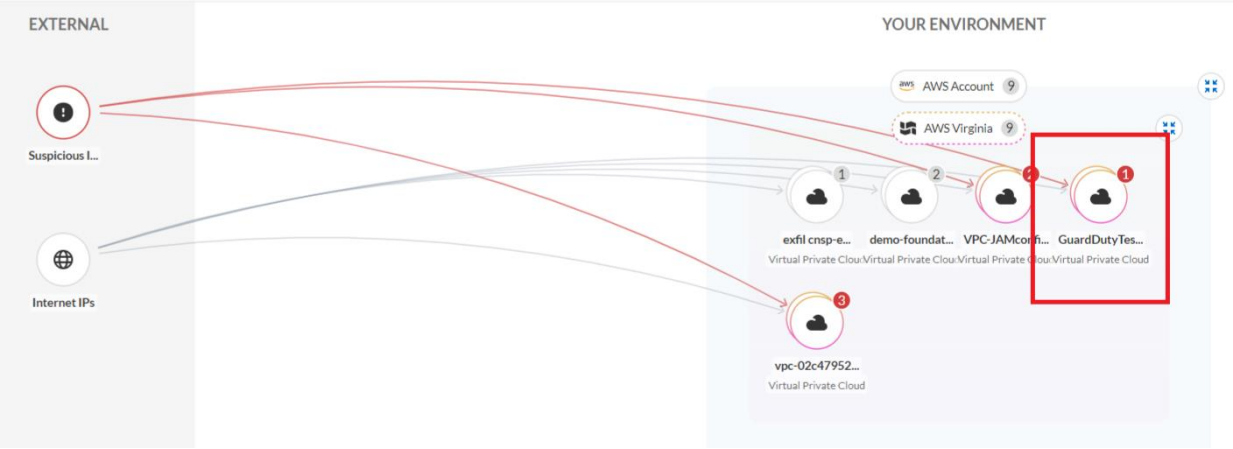
Step 2. Make sure to set the time window to **All Time.** Your graph may look a little different as the cloud environment is very dynamic. This shows all the resources that are taking traffic from Suspicious IPs, which are flagged by Prisma Cloud.



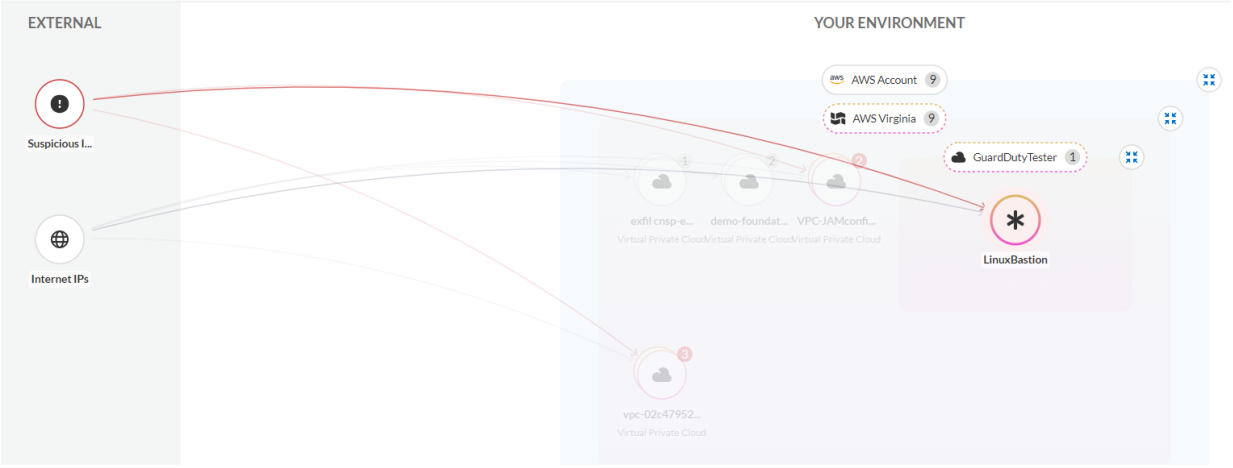
Step 3. Toggle between **Swimlane** and **Organic** for different visualizations of the traffic.



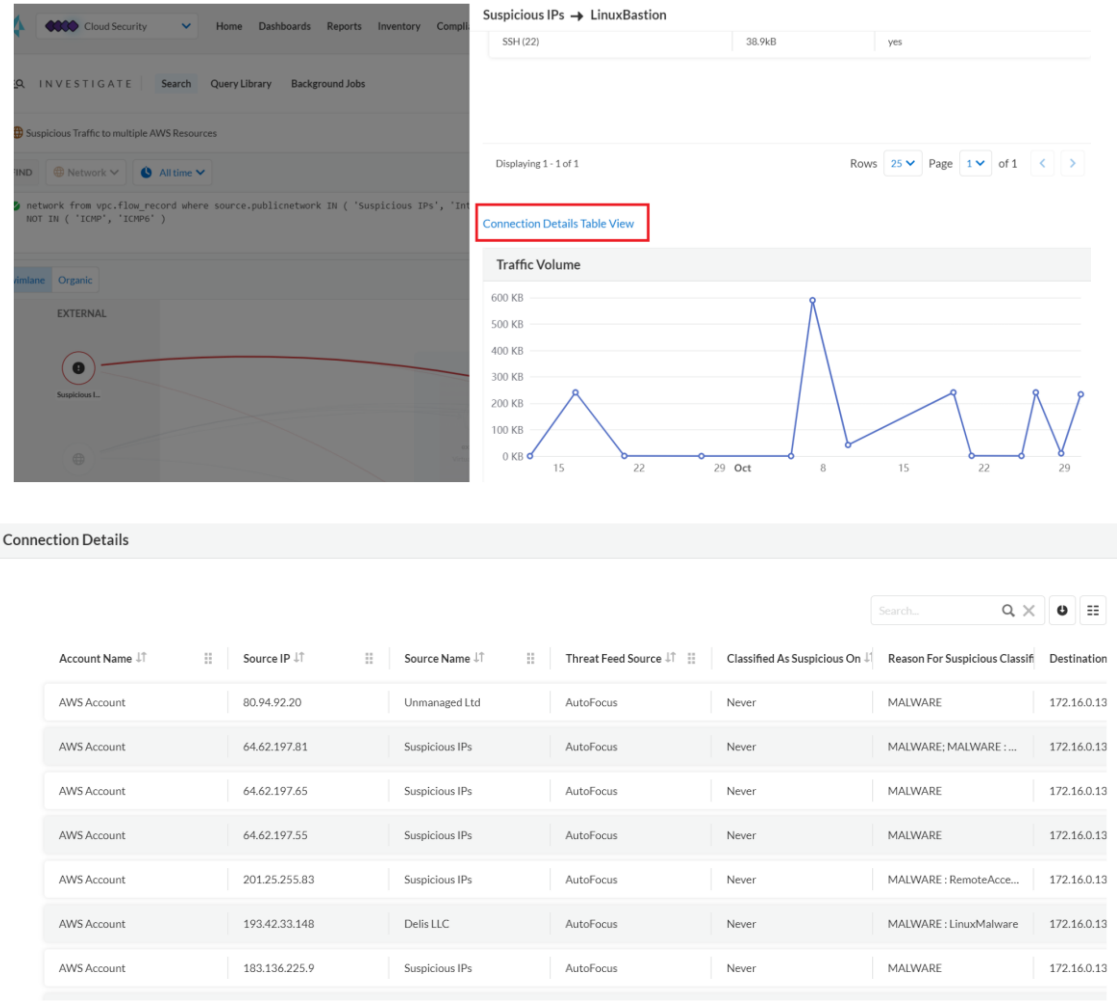
Step 4. For the rest of the flow, we will stick with **Swimlane** visualization. Clicking on the **GuardDuty Tester** VPC will expand it and reveal **LinuxBastion** host



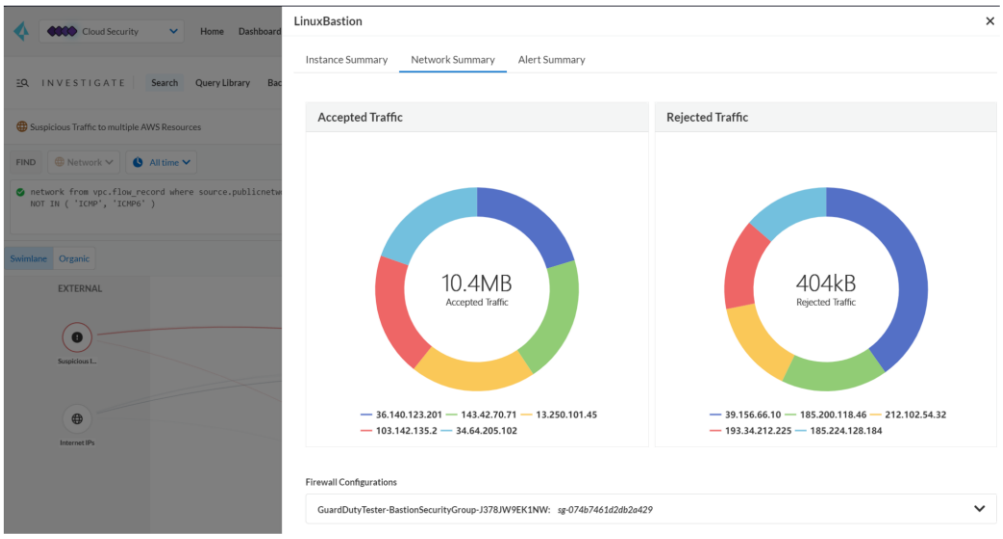
Step 5. Hover your mouse and click on the line connecting **Suspicious IP** and **Linux Bastion**



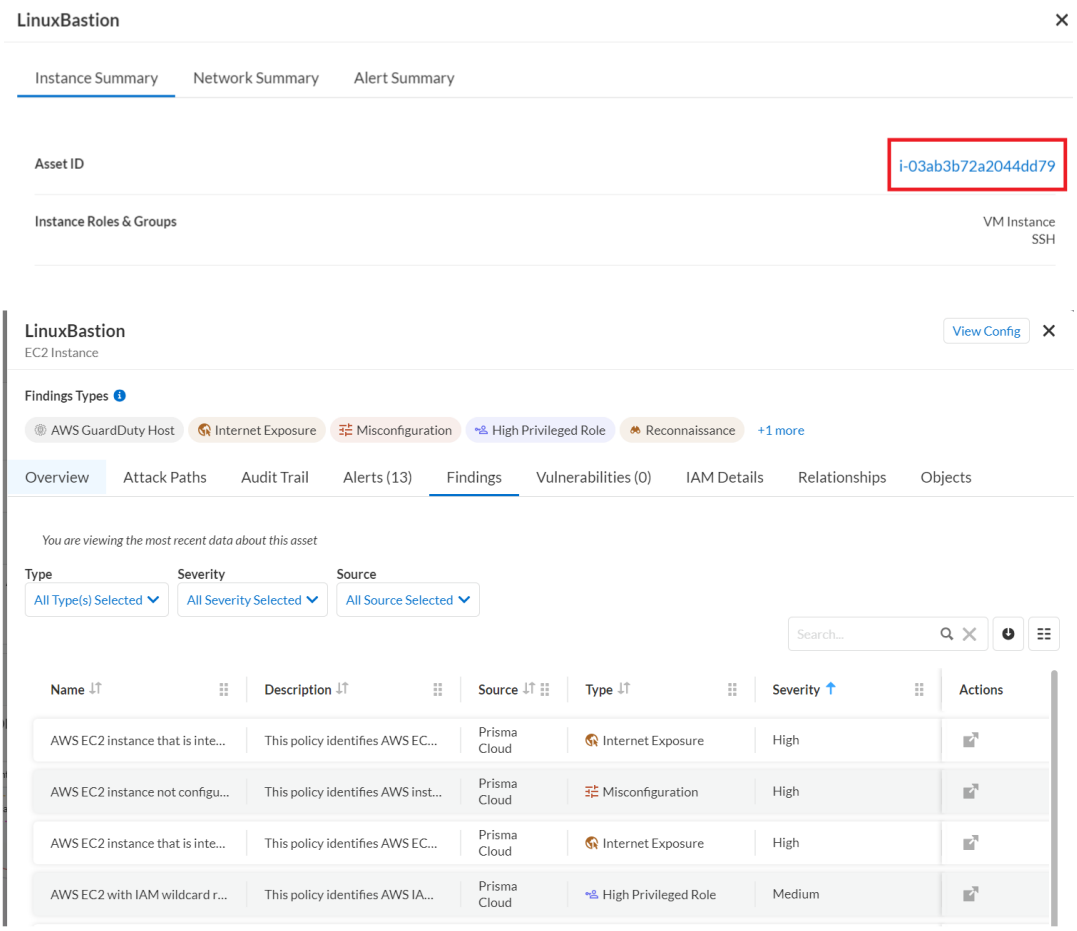
Step 6. This will open a sidecar. Click on the **Connection Details Table view** to see the breakdown of the traffic flow between **suspicious IPs** and the **LinuxBastion** host



Step 7. Close the **Connection Details** window and the **Suspicious IPs > LinuxBastion** window.
Step 8. Click on the **LinuxBastion** host and this will open another window that provides the network summary of that VM.



Step 9. Click on the **LinuxBastion** VM, and under the **Instance Summary,** click the value corresponding to **Asset ID** to investigate further the VM. Go to the **Findings** tab at the top of the page to get details.

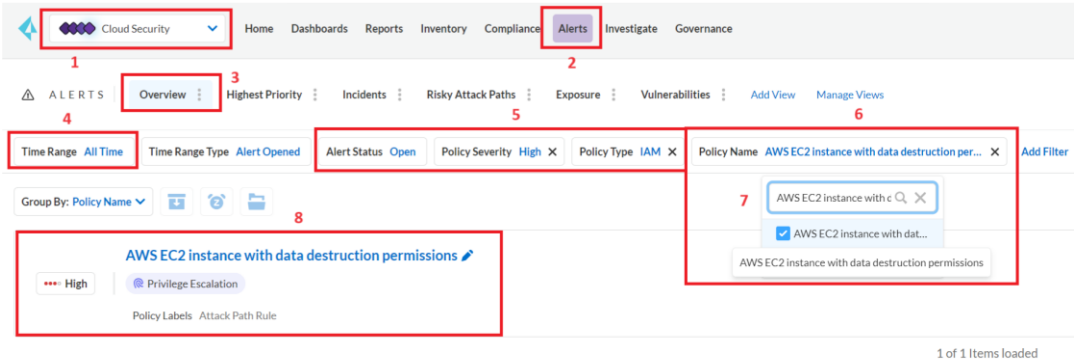


---------- Task 3: Investigate Risky AWS EC2 IAM Permissions ----------

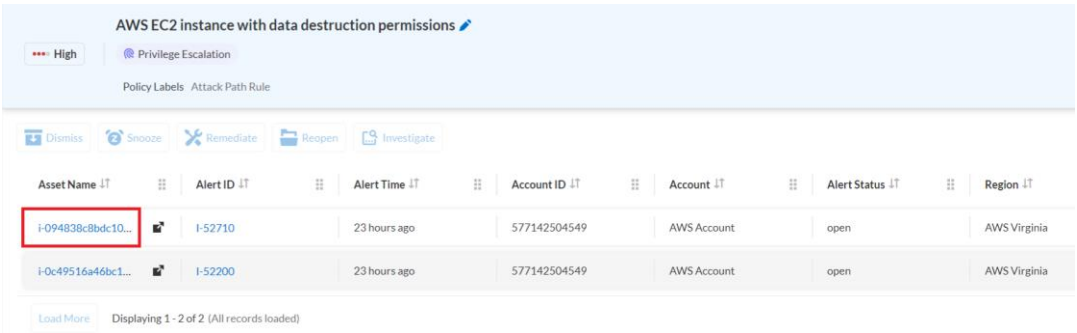
Step 1. Navigate to **Prisma Cloud Enterprise Edition console > Cloud Security > Alerts** > **Overview**.
Step 2. Select the **Reset Filters** icon on the top right corner of the screen to reset all filters. Use **Add Filter** option to add the specified filters below
Step 3. In the filter options, select the following:

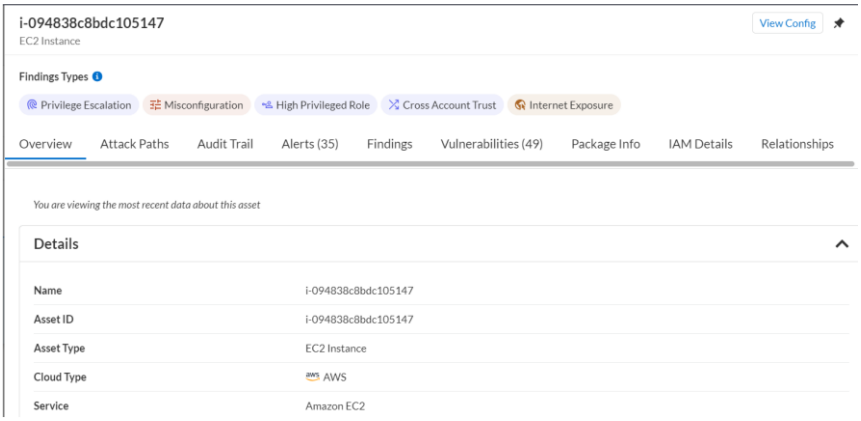
a) Time Range **= All Time**
b) Alert Status = **Open**
c) Policy Severity = **High**
d) Policy Type = **IAM**
e) Policy Name = **AWS EC2 instance with data destruction permissions**

Step 4. Navigate to **Prisma Cloud Enterprise Edition console > Cloud Security > Alerts > Overview.**



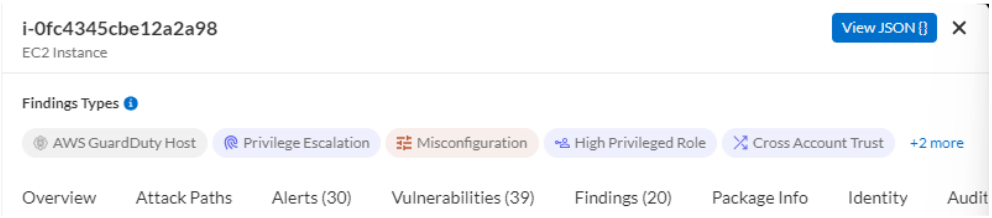
Step 5. Click on the **AWS EC2 instance with data destruction permissions** and Click on the value under the **Asset Name** column to view more information about the resource.





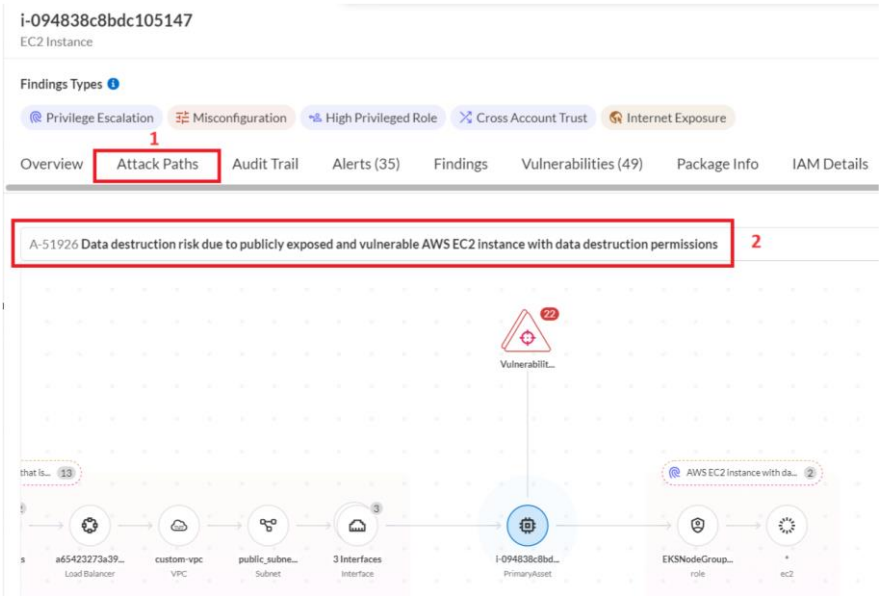
Step 6. In the Resource sidecar, click on the below options to explore further.

a) Clicking on **View JSON** will bring up the configuration of the selected resource.

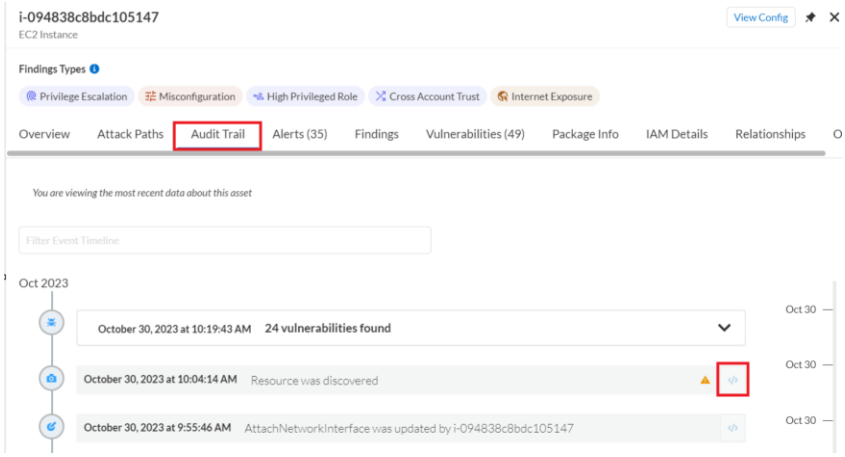


b) Clicking on **Overview** will provide an overview of the resource. After reviewing, close the pop-up or click **Done**.

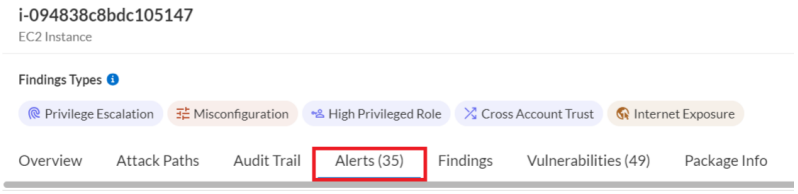
c) Clicking on **Attack Paths** will bring up the attack path graph and highlight where the selected resource fits in the path. Further clicking on the various items within the graph will show relevant information and configuration of the selected item



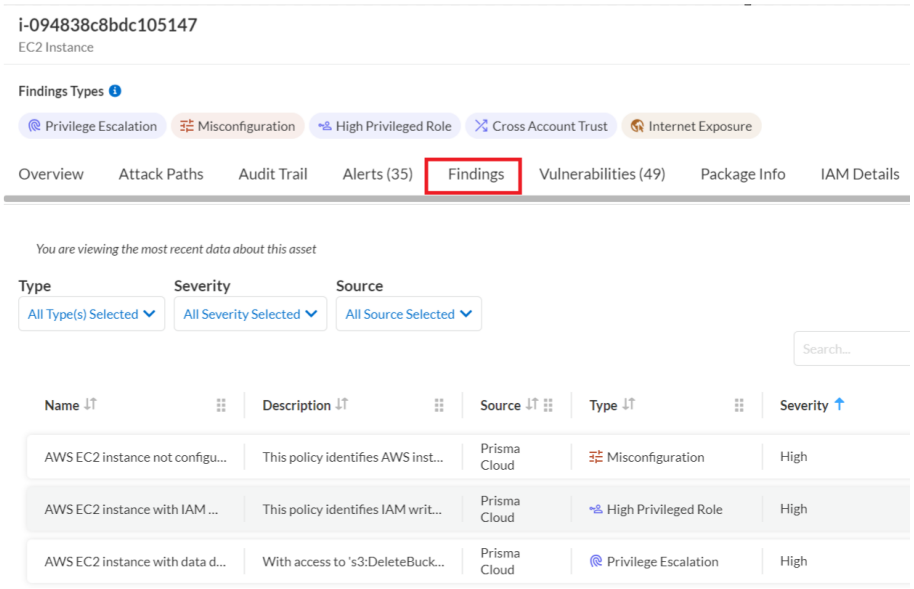
d) Clicking on the **Audit Trail** will open up the Audit trail for this resource where you will be able to see the timeline of the configuration changes made on the resource from the time it was discovered by Prisma Cloud. This is continuously monitored by Prisma Cloud and any changes to the configuration are recorded. Click on the **</>** to view the resource configuration



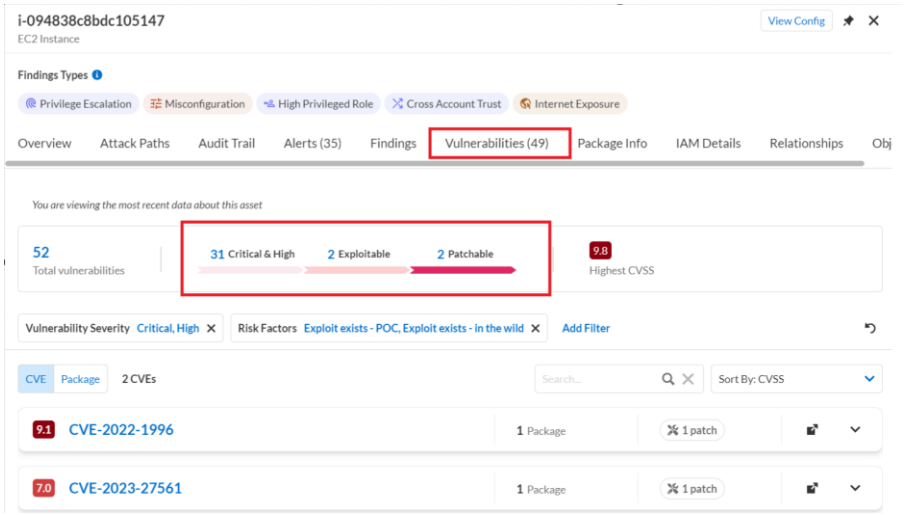
e) Clicking on **Alerts** will show the various alerts that are open for this specific resource.



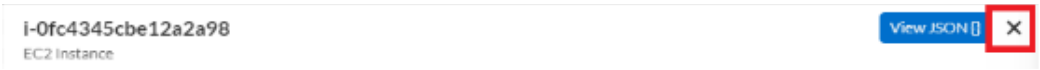
f) Clicking on **Findings** will show the various findings about the selected resource and the severity of those findings.



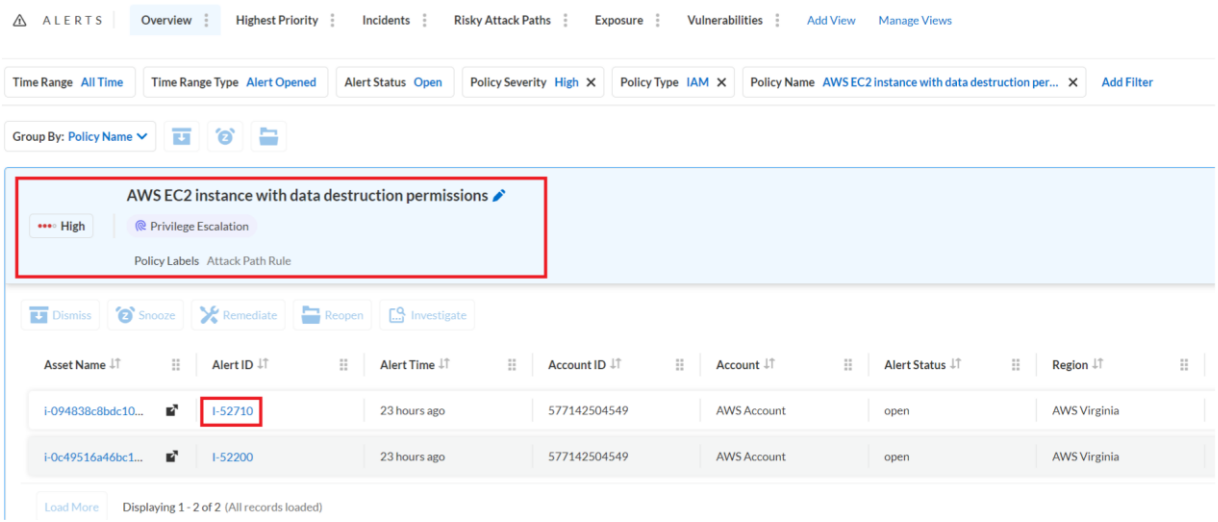
g) Clicking on the **Vulnerabilities** will show the various vulnerabilities that were detected for this resource. Further clicking on options such as **Critical & High**, **Exploitable** and **Patchable** will filter the results.

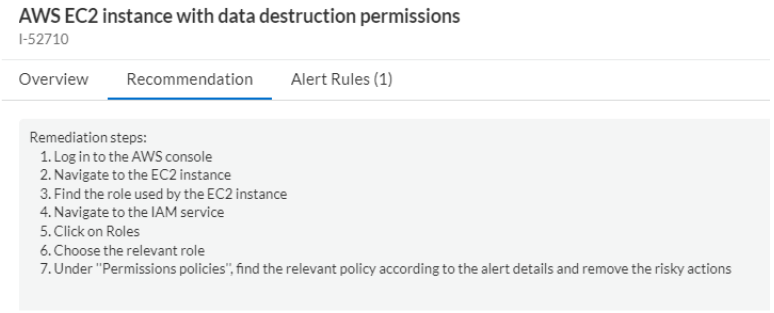


h) Feel free to explore the rest of the options and once done, close the window.



Step 7. Click on the **AWS EC2 instance with data destruction permissions** and click the corresponding value for the **Alert ID** to see the **Overview** and remediation **Recommendation**.

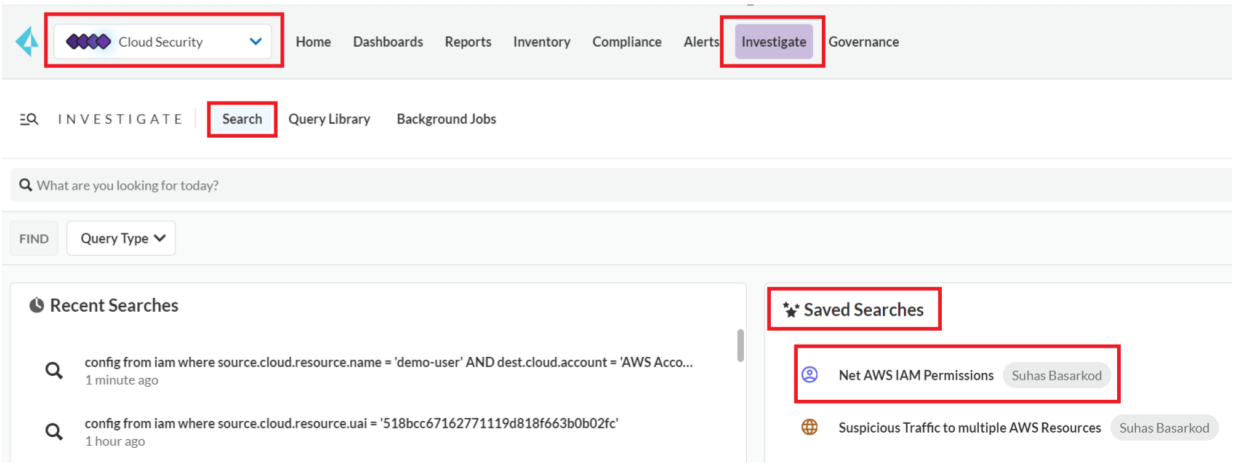




Step 8. Once done reviewing, close the window.

---------- Task 4: Investigate Over Permissive IAM Permissions ----------

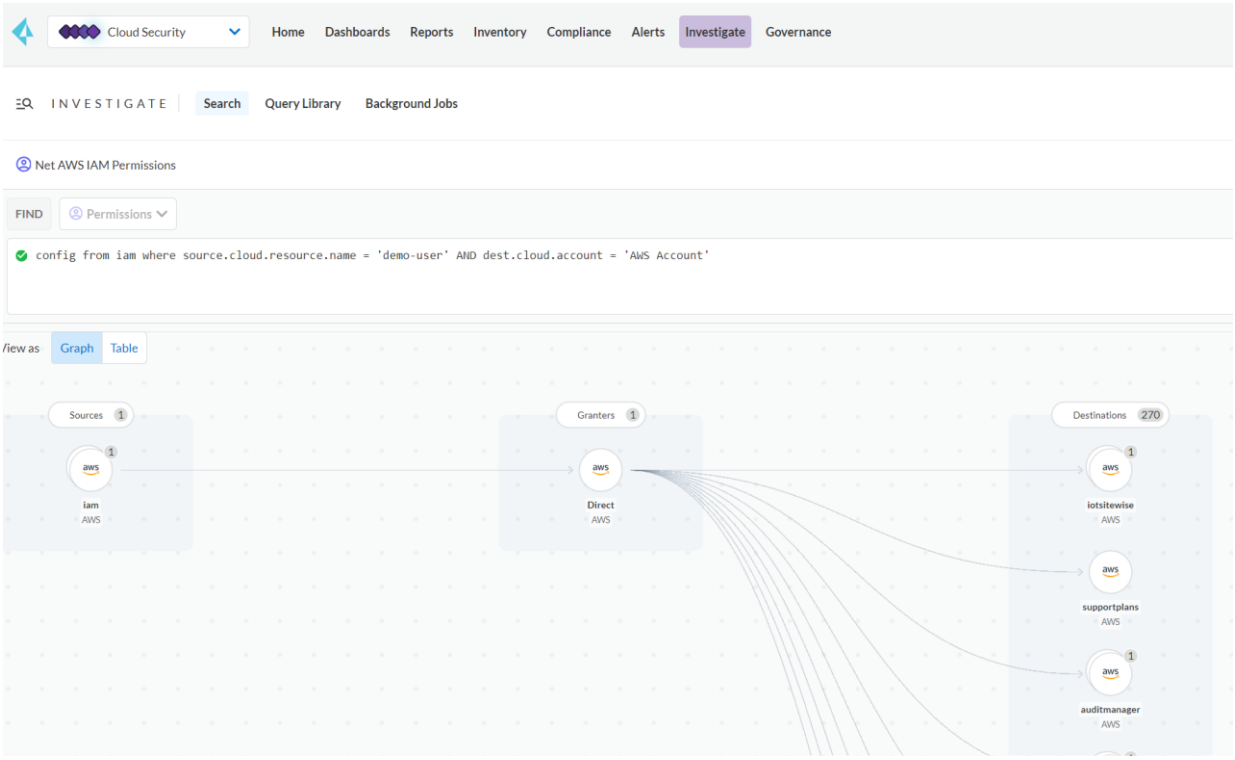
Step 1. In this task, we will find out, with a simple **RQL query**, the net effective permissions of an IAM user to demonstrate the effectiveness of IAM RQL queries in Prisma Cloud.
Step 2. Navigate to **Prisma Cloud** > **Cloud Security > Investigate** and select **Net AWS IAM Permissions** from **Saved Searches**



Step 3. The RQL query of the selected search query should look like the following:

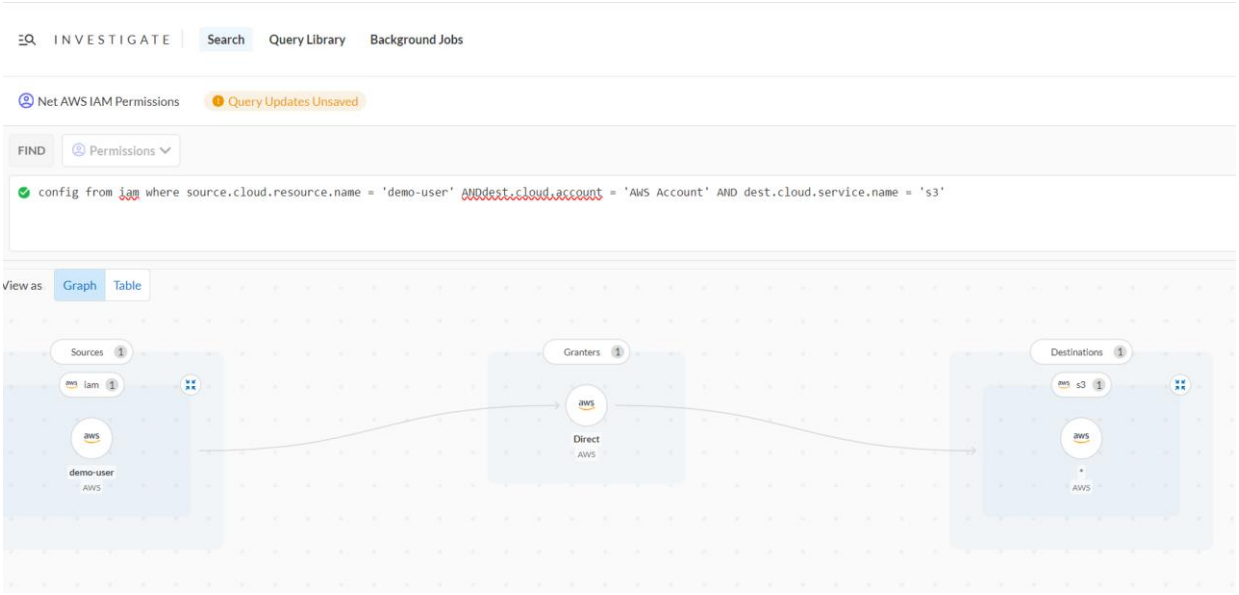
config from iam where source.cloud.resource.name = 'demo-user' AND dest.cloud.account = 'AWS UTD Account'

Step 4. Click on the **Graph** icon.



Step 5. This graph shows the permissions that the IAM user **demo-user** holds within the specified AWS Account. Feel free to explore the graph further.
Step 6. Within the **Destinations** column of the graph, to further narrow down the search to a specific AWS Service such as S3, update the query with the following

config from iam where source.cloud.resource.name = 'demo-user' AND dest.cloud.account = 'AWS UTD Account' AND dest.cloud.service.name = 's3'



Step 7. From the screenshot, you can see that there's a "*" (wildcard) permission assigned, which is not a best-practice implementation in a production environment.
Step 8. To investigate the permissions of the IAM role used by EKS Node in the previous task, use the below query and explore the **Graph/Table**

config from iam where dest.cloud.account = 'AWS UTD Account' AND grantedby.cloud.entity.name = 'EKSNodeGroupRole-cnsp-app4' AND source.cloud.service.name = 'ec2'