

Background: This activity demonstrates how Prisma Cloud alerts on attacks on cloud resources and how you can leverage the Prisma Cloud data correlation to analyze the attacks in more detail and remediate them. **In this activity, you will:**

- View Alerts on risky SQL, Code injection, and other attacks.
- Analyze the attack paths and the resources involved in them.
- View how Prisma Cloud can be leveraged to remediate and block the attacks.

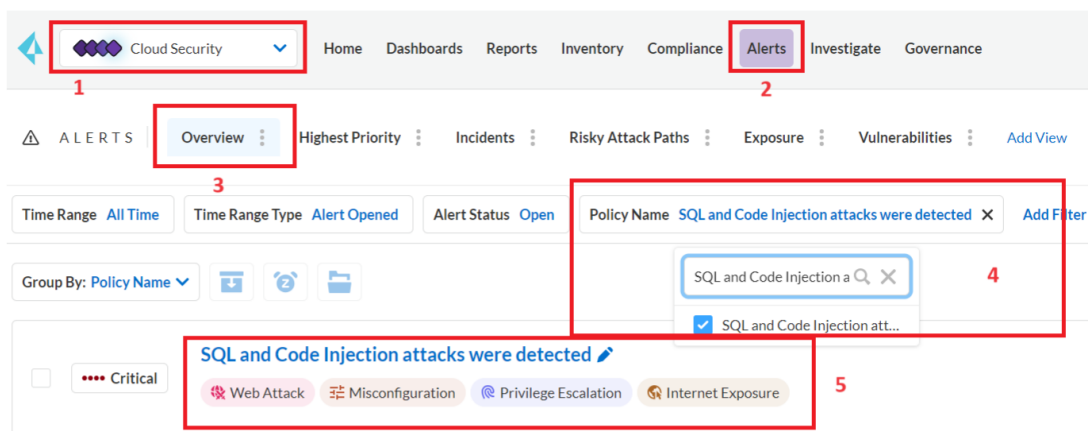
Note: This is a standalone activity and is not dependent on other activities.

----- Task 1: Investigate Attacks on Cloud Resources -----

Step 1. Navigate to **Prisma Cloud Enterprise Edition > Cloud Security > Alerts > Overview**.

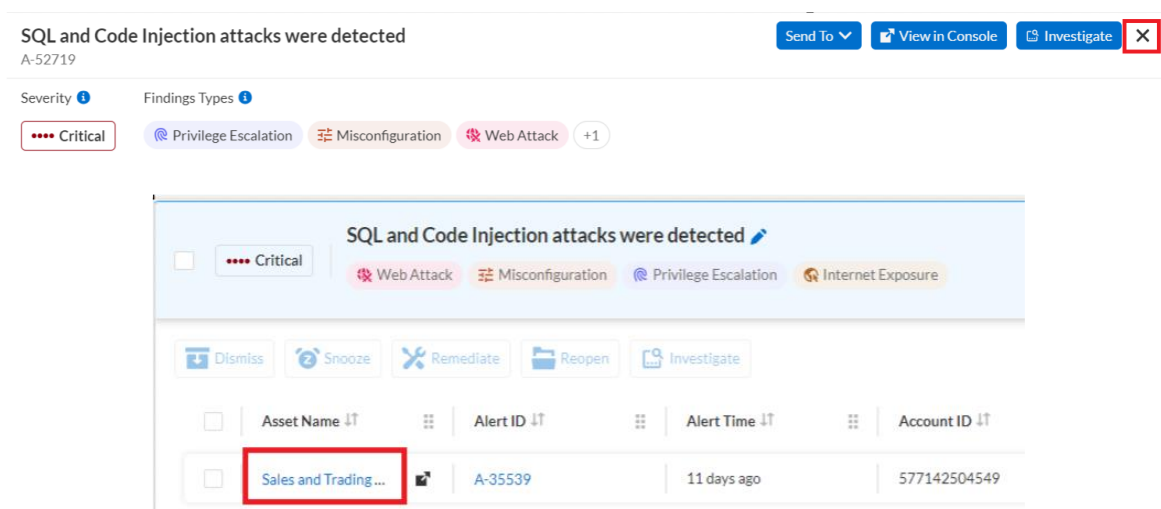
Step 2. Set the following filters (you can add additional filters by clicking on the **Add Filter** button):

- Time Range = **All Time**
- Policy Name = **SQL and Code Injection attacks were detected**



Notes: **SQL and Code Injection attacks were detected** is a custom search policy and Alert rule that was created for the lab by leveraging out-of-the-box Prisma Cloud policies. This is done for ease of use and convenience of lab experience.

Step 4. Click on the **SQL and Code Injection attacks were detected** result and click on the **Sales and Trading cnsnp-app4** under the **Asset Name** column.



Step 5. This should bring up details about this instance and contain more findings and information about the attacks. The **Overview** tab contains the overview of this VM. Clicking on the **Attack Path** will reveal how the attack occurred and the resources involved in it.

Sales and Trading cnsp-eu
EC2 Instance [View Config](#) ✦ ✕

Findings Types ⓘ

Web Attack Privilege Escalation Misconfiguration High Privileged Role Internet Exposure +1 more

Overview **Attack Paths** Audit Trail Alerts (25) Findings Vulnerabilities (230) Package Info IAM Details Relationships Ob

A-52629 Remote code execution (RCE) risk due to a publicly exposed AWS EC2 instance with Spring4Shell vulnerability

A-52629 Remote code execution (RCE) risk due to a publicly exposed AWS EC2 instance with Spring4Shell vulnerability
This policy identifies AWS EC2 instances which have Spring4Shell vulnerabilities and are publicly exposed. The Spring4Shell vulnerability allows att...

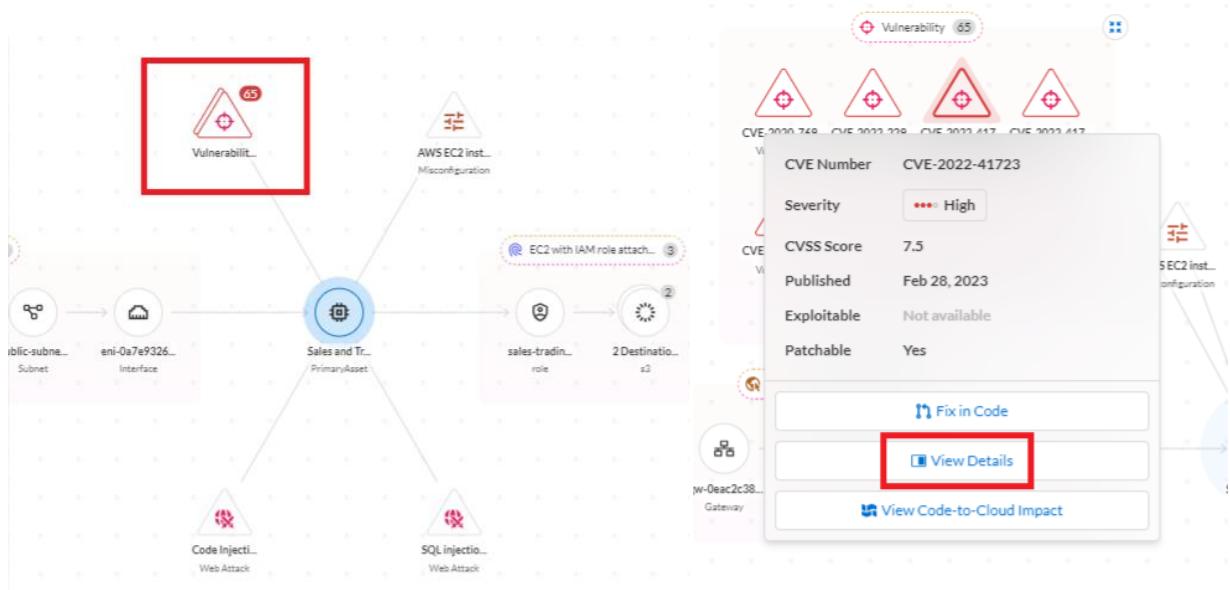
A-52719 SQL and Code Injection attacks were detected

A-52719 SQL and Code Injection attacks were detected

The diagram illustrates the attack path for finding A-52719. It shows a sequence of resources: Internet Gateway (igw-0eac2c38...) → VPC (demo-foundat...) → Subnet (public-subne...) → Interface (eni-0a7e9326...) → Sales and Trading EC2 instance (PrimaryAsset). The EC2 instance is associated with several findings: Vulnerability (65), AWS EC2 instance Misconfiguration, Code Injection (Web Attack), and SQL Injection (Web Attack). It also has IAM roles attached: sales-trading role and prisma-cloud s3. A group of findings labeled 'EC2 with IAM role attach...' (3) is also shown.

Step 6. Within the graph, you can see the traffic flow and the complete attack path. The traffic enters through the **Internet Gateway** and hits the **Sales and Trading EC2** instance. This instance has an IAM role **sales-trading-admin-role-cnsp-app4** attached to it, which has **wildcard access to the S3 bucket** and also access to the **prisma-cloud-pcds-bucket** S3 Bucket. As this instance is vulnerable to **SQL and Code injection attacks**, the attacker can potentially perform a **Data exfiltration** from the S3 bucket through the compromised host. This is represented by the Attack Path.

Step 7. Within the graph, clicking on the **Vulnerabilities** icon and clicking on any **Vulnerability** will provide more information about the vulnerability. On the selected Vulnerability, clicking on **View Details** will open an additional findings sidebar.



CVE-2022-41723

Remediate Send To X

CVSS 7.5 Impacted Stages Code Deploy Run Severity High Risk Factors +2 More

Overview Assets

Details

cve	CVE-2022-41723
Description	A maliciously crafted HTTP/2 stream could cause excessive CPU consumption in the HPACK decoder, sufficient to cause a denial of service from a small number of small requests.
Package Name	golang-1.15
Fix Version	
Impacted Version	[*]
Published Date	Feb 28, 2023
Cpu Arch	

Step 8. Clicking on **Assets** will show more information about the affected assets. Once done, close the **CVE Sidecar**.

CVE-2022-41723

Remediate Send To X

CVSS 7.5 Impacted Stages Code Deploy Run Severity High Risk Factors +2 More

Overview Assets

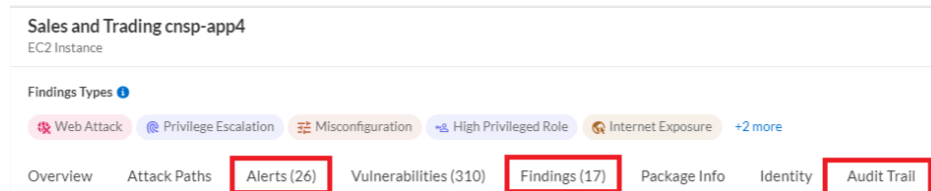
Risk Factor Select

1 Packages	Associated Repositories Count 1	Fix Impact 8% of all Code Vulnerabilities Across 1 Associated Repositories	Actions	
4 Hosts	Associated Host VM images Count 0	Fix Impact 33% of all Runtime Hosts	Actions	

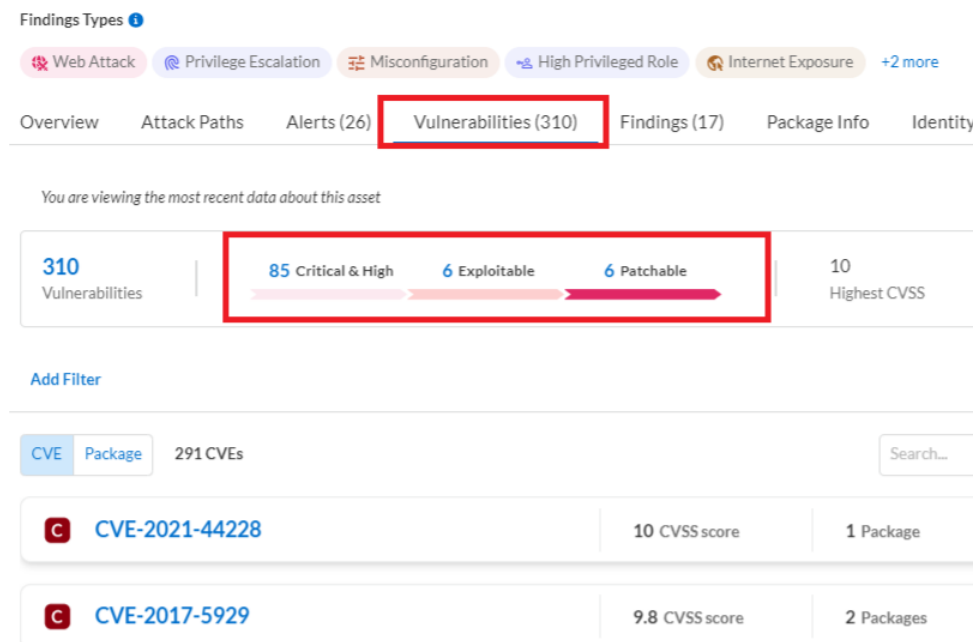
Step 9. Clicking on **Audit Trail** will show more information about what changes occurred at the resource level and the timeline.

The **Alerts** tab will show all the alerts that are that this resource is currently involved in.

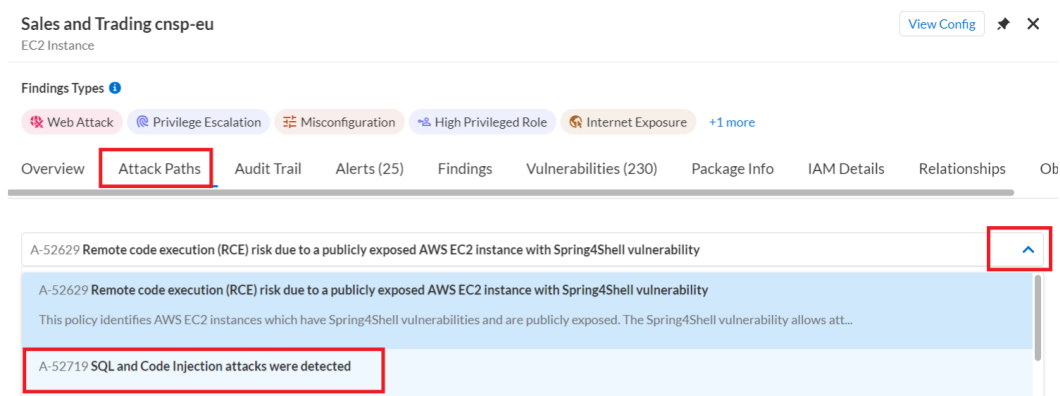
The **Findings** tab shows the findings for this specific resource.



Step 10. Within the **Sales and Trading cnsp-app4** VM sidecar, click on the **Vulnerabilities** tab to see all the Vulnerabilities that were detected for this VM. Further clicking on options such as **Critical & High**, **Exploitable** and **Patchable** will filter the results.



Step 11. Navigate back to the **Attack Path** graph (and make sure that the “**SQL and Code Injection attacks were detected**” alert is selected). Let’s further investigate the Attack Path in the graph and examine the blast radius.



Step 12. Within the graph, click on the S3 Bucket **prisma-cloud-pcdis-bucket** by clicking on it and clicking on **View Details**

The top part of the image shows an attack graph with a central node labeled 'Sales and Tr... PrimaryAsset'. It is connected to several other nodes: 'Vulnerability' (65), 'AWS EC2 inst... Misconfiguration', 'EC2 with IAM role attach... 3', 'Code Inject... Web Attack', and 'SQL Injectio... Web Attack'. A subgraph on the left shows 'public-subne... Subnet' connected to 'eni-0a7e9326... Interface', which is connected to the central node. A subgraph on the right shows 'sales-tradin... role' connected to 's3' (prisma-cloud-pcdis-bucket), which is highlighted with a red box. Below the graph, a 'View Details' button is highlighted with a red box. The bottom part of the image shows the details page for 'prisma-cloud-pcdis-bucket' S3 Bucket. The 'Findings Types' section shows 'Discovery' and 'Misconfiguration'. The 'Overview' tab is selected. The 'Details' section shows the Name 'prisma-cloud-pcdis-bucket' and Asset ID 'prisma-cloud-pcdis-bucket'.

prisma-cloud-pcdis-bucket	
S3 Bucket	
Findings Types	
Discovery	Misconfiguration
Overview Attack Paths Audit Trail Alerts (3) Findings (3) Vulnerabilities (0)	
You are viewing the most recent data about this asset	
Details	
Name	prisma-cloud-pcdis-bucket
Asset ID	prisma-cloud-pcdis-bucket

- a) Here you can see the S3 Bucket details. Head over to the **Alerts** tab in the S3 Bucket details and here you will see that there's an alert for this bucket- **Storage Asset with sensitive data found**. Do not click on the Policy Name as clicking on the Policy Name as you will be navigated to another page. Once done looking at Alerts, close the **Alert** window

prisma-cloud-pcbs-bucket
S3 Bucket

Findings Types

Discovery Misconfiguration

Overview Attack Paths Audit Trail Alerts (3) Findings Vulnerabilities (0) IAM Details Relationships

You are viewing the most recent data about this asset

Search...

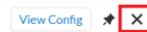
Severity	Alert Time	Policy Name	Alerts
Low	55 minutes ago	Storage Asset with sensitive data found	D-52427
Low	1 year ago	AWS S3 Object Versioning is disabled	P-713
Informational	1 year ago	AWS Access logging not enabled on S3 buckets	P-12

Step 13. Close the **S3 bucket** sidecar. Close the **Sales and Trading cnspp-app4** sidecar

prisma-cloud-pcbs-bucket
S3 Bucket



Sales and Trading cnspp-eu
EC2 Instance



Findings Types

Web Attack Privilege Escalation Misconfiguration High Privileged Role Internet Exposure +1 more

Step 14. In the **SQL and Code injection attacks were detected** Alert window, click on the value corresponding to the **Alert ID** column. In the next windows, click on the **Evidence** tab.

SQL and Code Injection attacks were detected					
Critical Web Attack Misconfiguration Privilege Escalation Internet Exposure					
Dismiss Snooze Remediate Reopen Investigate					
	Asset Name	Alert ID	Alert Time	Account ID	Account
<input type="checkbox"/>	Sales and Trading ...	A-52719	17 hours ago	577142504549	AWS Account

SQL and Code Injection attacks were detected

A-52719

Send To

View in Console

Investigate



Severity

Findings Types

Critical

Privilege Escalation

Misconfiguration

Web Attack

+1

Overview

Evidence

Alert Rules (2)

Graph

Table



Step 15. Click on the **SQL Injection** and click on **View Additional Finding Details**. You will now be directed to the **Prisma Cloud Runtime Security WaaS (Web Application and API Security)** console, which was responsible for detecting this attack. Here we will be able to see more information about the attack.

Finding Name	SQL injection payload detected in HTTP traffic
Finding Type	Web Attack
Severity	High
Description	This policy detects SQL Injection attacks. An SQL injection (SQLi) attack occurs when an attacker inserts an SQL query into the input fields of a web application. A successful attack can read...

[View Additional Finding Details](#)

Note: The below screenshot might look different in your case as some menus are collapsed to fit the screenshot on the page.

Step 16. Click on the **SQL Injection** number to bring up the **Aggregated WaaS Events** for that attack type.

Time	IP	Co...	HTTP Host	Path	Query	Eff...	Count
Nov 1, 2023 3:3...	172.20.1.53		172.20.1.164:...	/	id=' OR '1	Alert	1
Nov 1, 2023 3:1...	172.20.1.53		172.20.1.164:...	/	id=' OR '1	Alert	1
Nov 1, 2023 3:0...	172.20.1.53		172.20.1.164:...	/	id=' OR '1	Alert	1
Nov 1, 2023 2:1...	172.20.1.53		172.20.1.164:...	/	id=' OR '1	Alert	1

Step 17. As you can see, attacks are detected and the effect is set to **Alert**. This can be changed to **Prevent** to prevent the attacks. But we will **not be performing** that action in this lab but we will show how it can be achieved.

Step 18. If you scroll further down, you can see which rule is responsible for detecting the attacks and this would be **finance-eks-cluster-waas-policy**. Click on the rule and select **Yes** for the pop-up dialogue.

Rule name	Description (optional)
finance-eks-cluster-host-waas-policy	

Step 19. Click on the rule and click on the item under the App List

Rule name	Description (optional)
finance-eks-cluster-host-waas-policy	

Rule scope

■ Billing Click to edit scope

API endpoint discovery On

Automatically detect ports On

App list

Filter rule applications by keywords and attributes

Selected	App ID	HTTP host	TLS	GRPC	HT
<input type="checkbox"/>	app-BDCD	http://*/*	Disabled	Disabled	Dis

Step 20. Click on the **App Firewall** tab and you should see the **SQL Injection** and other items (Grayed out because the lab role is a read-only role and doesn't have permissions to change settings), which can be set to **Prevent** or **Ban** to prevent these attacks

Edit app-BDCD

App definition **App firewall** DoS protection Access control Bot protection Custom rules Advanced settings

Effect is applied by client IP

Firewall settings

Global effect Disable Alert Prevent Ban

Protection	Mode	Exceptions
SQL Injection	Disable Alert Prevent Ban	
Cross-Site Scripting (XSS)	Disable Alert Prevent Ban	
OS Command Injection	Disable Alert Prevent Ban	
Code Injection	Disable Alert Prevent Ban	