

Workload Security

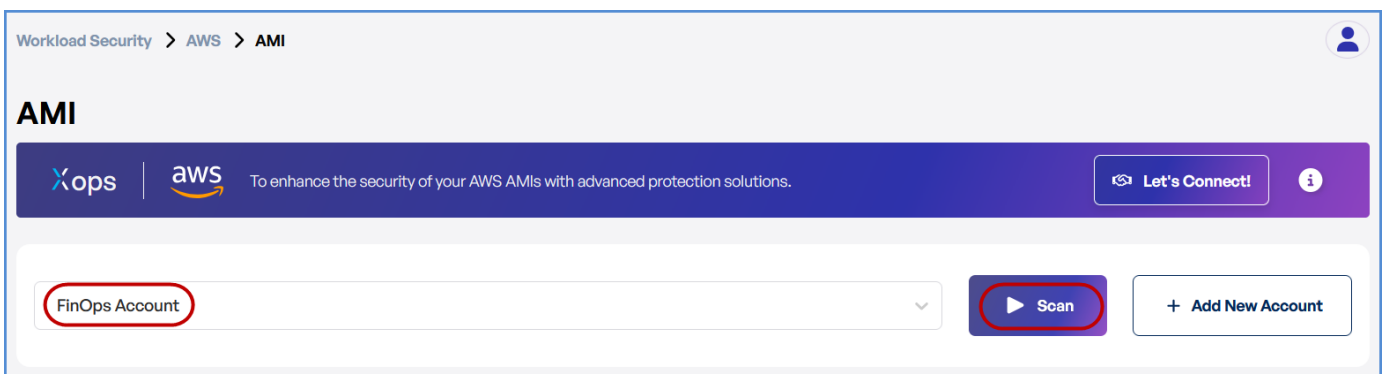
Techniques for protecting workloads deployed across multiple cloud platforms by leveraging security scans for container images and machine images in AWS and Azure.

Scan in Workload Security - AWS (AMI & ECR)

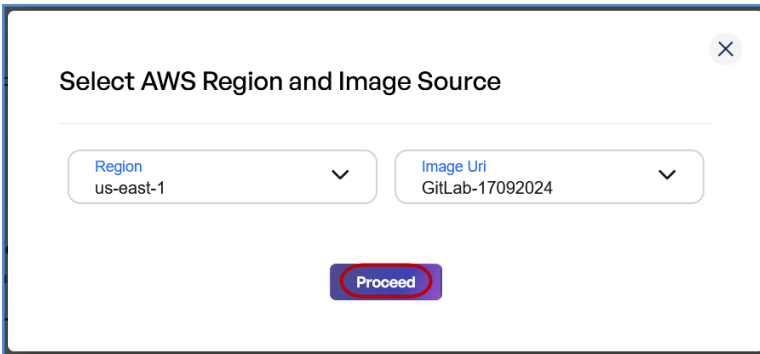
- **Log in to the Platform**
 - Access the platform and sign in using your credentials.
- **Navigate to Cloud Ops**
 - Locate the Side Navigation Bar on the left-hand side of the screen.
 - Click on the **Workload Security** tab to access its features.



- **Verify AWS Account**
 - Ensure that an AWS account has already been added to the platform.
 - If no account is available, click on **+ Add New Account..**
- **Select a Scan Type**
 - Choose from the following scan options:
 - **AMI (Amazon Machine Image)** scan for VM security.
 - **ECR (Elastic Container Registry)** scan for container images.
- **Initiate the Scan**
 - Select the target AWS account.
 - Click **Scan** to open a new input form.



- Choose the **Region** from the drop down list.
- Provide the **Image URI** (enabled after Region selection).
- Click **Proceed** to start the scan.



Select AWS Region and Image Source

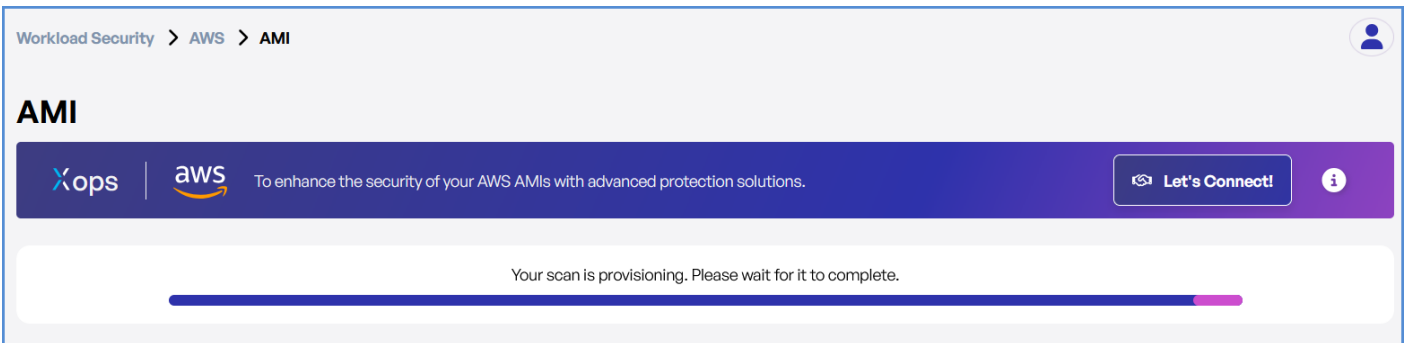
Region
us-east-1

Image Uri
GitLab-17092024

Proceed

- **Monitor and Review Results**

- Monitor scan progress, and upon completion, a report will be generated then open it.



Workload Security > AWS > AMI

AMI

Xops | aws To enhance the security of your AWS AMIs with advanced protection solutions. Let's Connect!

Your scan is provisioning. Please wait for it to complete.

- Upon completion, review results highlighting:
 - Security risks
 - Vulnerabilities
 - Compliance issues

Workload Security > AWS > AMI

AMI report

GitLab-17092024 AMI Thu, January 16, 2025 07:53:43 UTC

Total Vulnerabilities

609

Critical 15
 High 111
 Medium 304
 Low 179
 Informational 0

CVE ID	Description	References	Affects
CVE-2016-1585	Show	View	apparmor >
CVE-2016-1585	Show	View	libapparmor1 >
CVE-2022-36227	Show	View	libarchive13 >
CVE-2024-12084	Show	View	rsync >

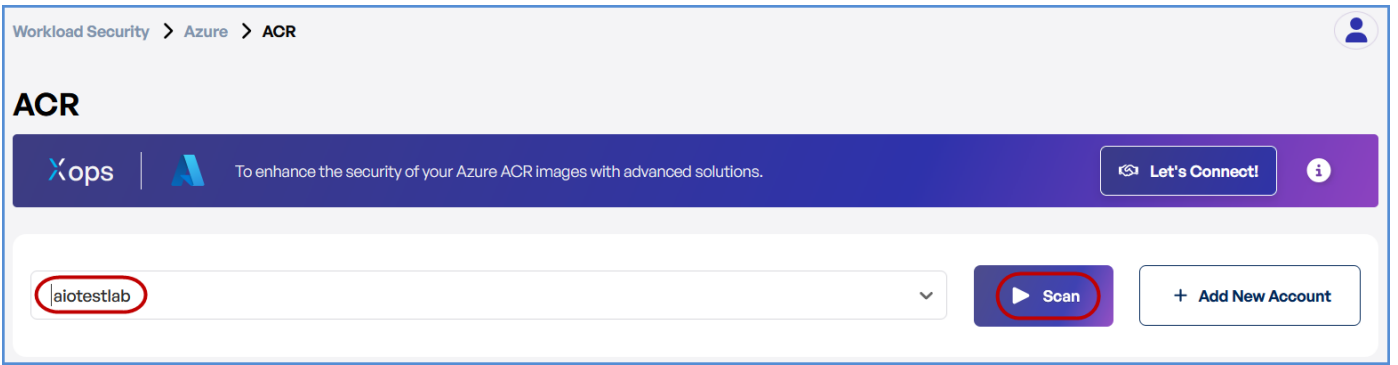
1 to 4 of 15 Page 1 of 4

Scan in Workload Security - Azure (ACR)

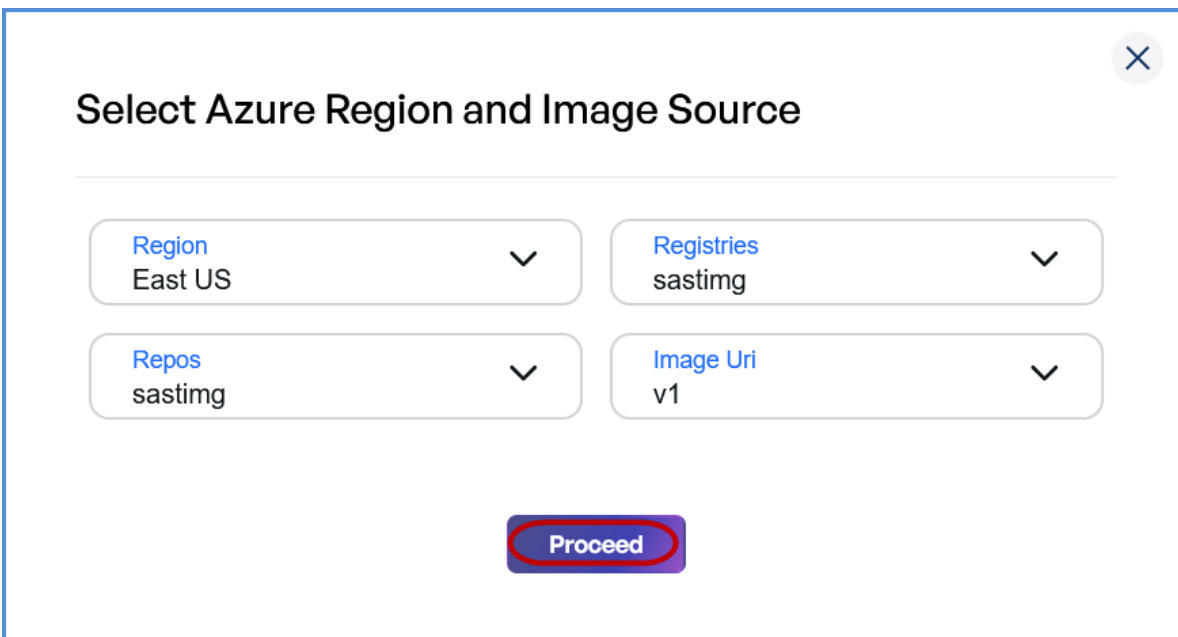
- **Log in to the Platform**
 - Access the platform and sign in using your credentials.
- **Navigate to Cloud Ops**
 - Locate the Side Navigation Bar on the left-hand side of the screen.
 - Click on the **Workload Security** tab to access its features.



- **Verify Azure Account**
 - Ensure that an Azure account has already been added to the platform.
 - If no account is available, click on **+ Add New Account..**
- **Choose ACR Scan Option**
 - Select **ACR (Azure Container Registry) Scan.**
- **Initiate the Scan**
 - Select the target Azure account.
 - Click **Scan** to open a new input form.

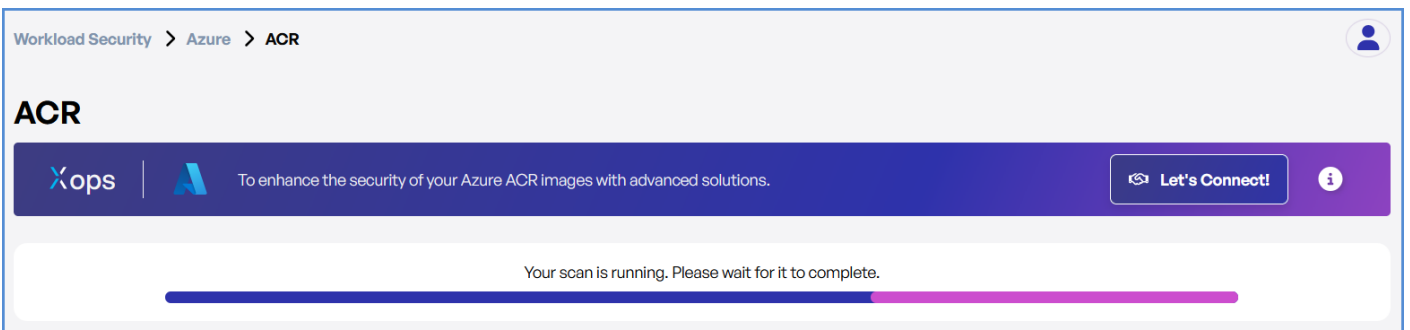


- Choose the **Region** from the drop down list.
- Select the **Registry** (enabled after Region selection).
- Choose the **Repository** (enabled after Registry selection).
- Provide the **Image URI** (enabled after Repository selection).
- Click **Proceed** to start the scan.



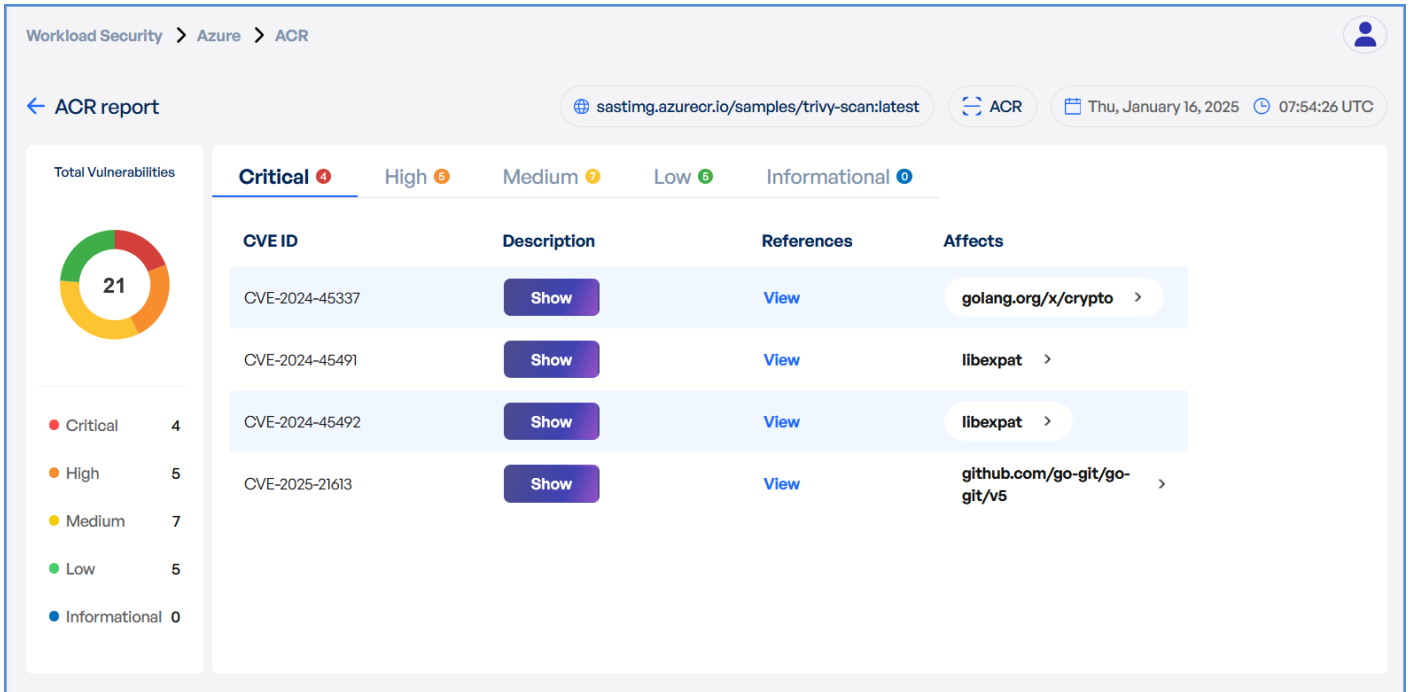
• Monitor and Review Results

- Monitor scan progress, and upon completion, a report will be generated then open it.



- Upon completion, review results highlighting:
 - Security risks
 - Vulnerabilities

o Compliance issues



Note:

- For accessing historic reports or addressing scan failures, refer to the [Report History Page](#) for further details and View error.

Revision #13

Created 1 February 2025 09:09:35 by Axiom IO

Updated 19 September 2025 17:57:37 by Axiom IO