Detect, investigate, and respond to security incidents

TONY SUAREZ
Solutions Architect
WWPS SLG
Amazon Web Services

Agenda

Common challenges customers face

Amazon Web Services (AWS) services that can help

Review goals and objectives of the workshop

Let’s get building

Common challenges customers face

Developers want to build fast

Developers don't want a lot of resistance

Security is everyone's job

Mistakes happen, fix it quickly

AWS helps customers go fast and be secure

AWS Trusted Advisor

About AWS Trusted Advisor

HOME OF AWS BEST PRACTICES

AWS services

AWS technical field experts

Your AWS account team

Auto-detected checks

Security

Fault tolerance

Performance

Cost optimization

Service quotas

Manual recommendations

Alerts on deviation and good standing

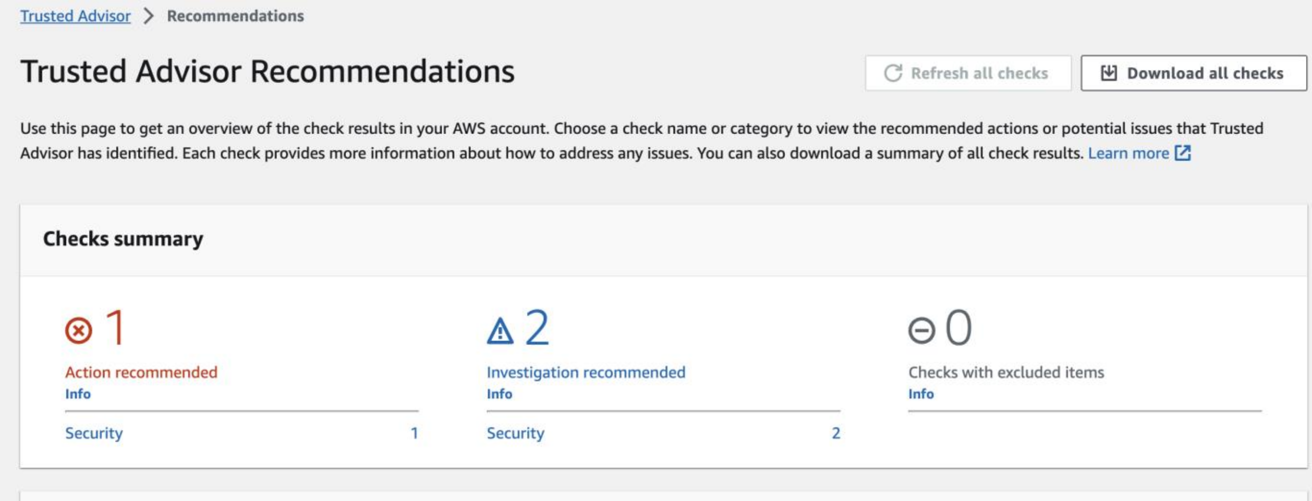
Multi-account/ AWS Organizations views

Prioritized and custom guidance

Closed-loop feedback tracking

AWS Trusted Advisor – Core checks and recommendations (available at no cost)

- Amazon S3 bucket permissions
- Security groups – specific ports Unrestricted
- AWS IAM use
- MFA on root account
- Amazon Elastic Block Store (EBS) public snapshots
- Amazon RDS public snapshots
- Service limits



Trusted Advisor Recommendations

Use this page to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. Learn more

Checks summary

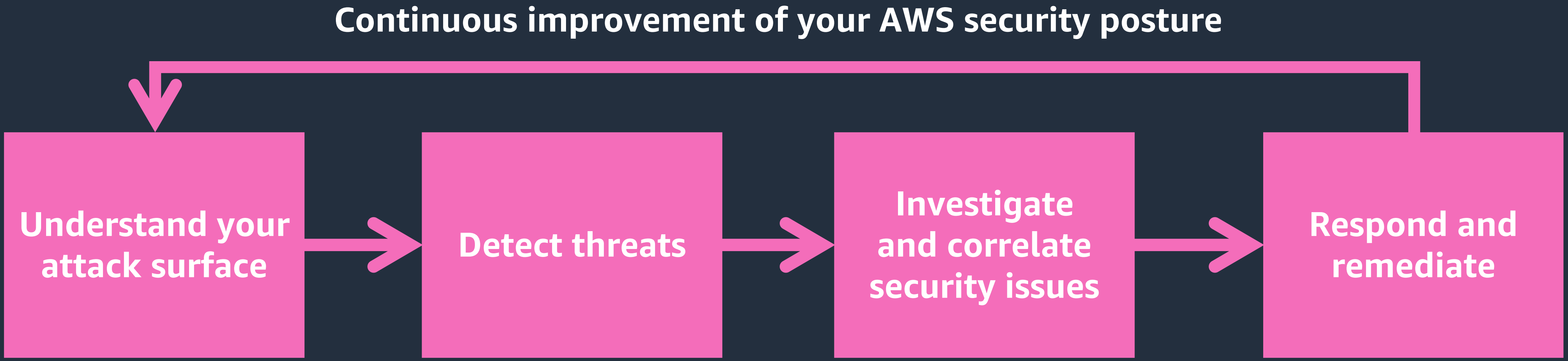
⊗ 1
Action recommended
Info
Security 1

⚠ 2
Investigation recommended
Info
Security 2

⊖ 0
Checks with excluded items
Info

AWS security services

Continuous security monitoring for AWS


Continuous improvement of your AWS security posture
Understand your attack surface
Detect threats
Investigate and correlate security issues
Respond and remediate

AWS security, identity, and compliance solutions

Identity and Access Management

- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager
- Amazon Verified Permissions

Detective controls

- AWS Security Hub
- Amazon GuardDuty
- Amazon Security Lake
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF
- Amazon VPC
- AWS PrivateLink
- AWS Systems Manager
- AWS Verified Access

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Private CA
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Amazon Detective
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery

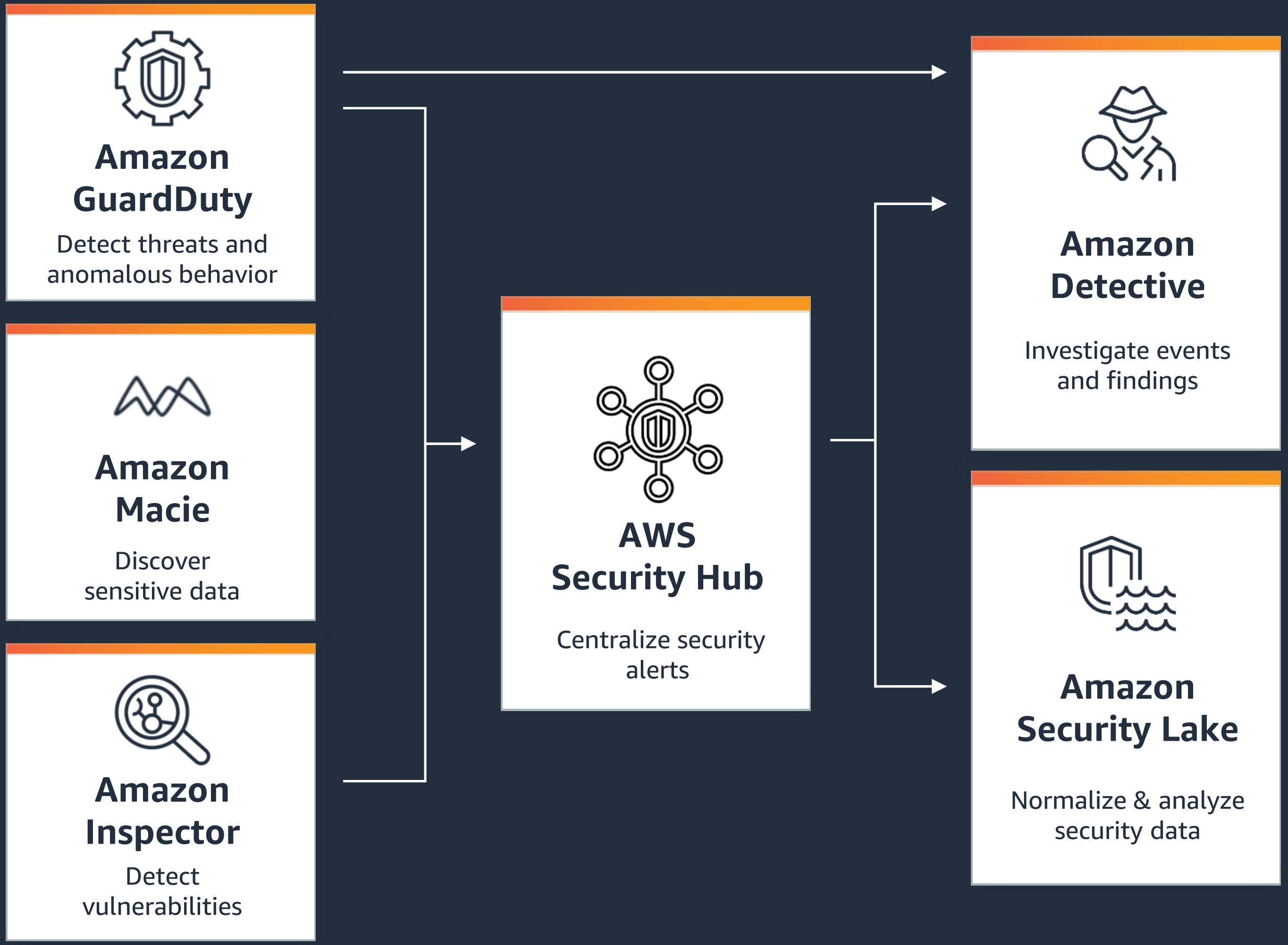
Compliance

- AWS Artifact
- AWS Audit Manager

Threat detection, monitoring, and response

Security monitoring and threat detection

Integrated with AWS workloads in an AWS account, along with identities and network activity



Amazon GuardDuty

Detect threats and anomalous behavior

Amazon Macie

Discover sensitive data

Amazon Inspector

Detect vulnerabilities

AWS Security Hub

Centralize security alerts

Amazon Detective

Investigate events and findings

Amazon Security Lake

Normalize & analyze security data

What is Amazon GuardDuty?

Amazon GuardDuty is a threat detection service that uses **machine learning**, anomaly detection, and **integrated threat intelligence** to identify and prioritize potential threats

One-step activation

Continuous monitoring of AWS accounts and resources

Global coverage with regional results

Detect known and unknown threats

Enterprise-wide consolidation and management

Your tasks today

Three modules – as you progress, it gets deeper into the AWS services

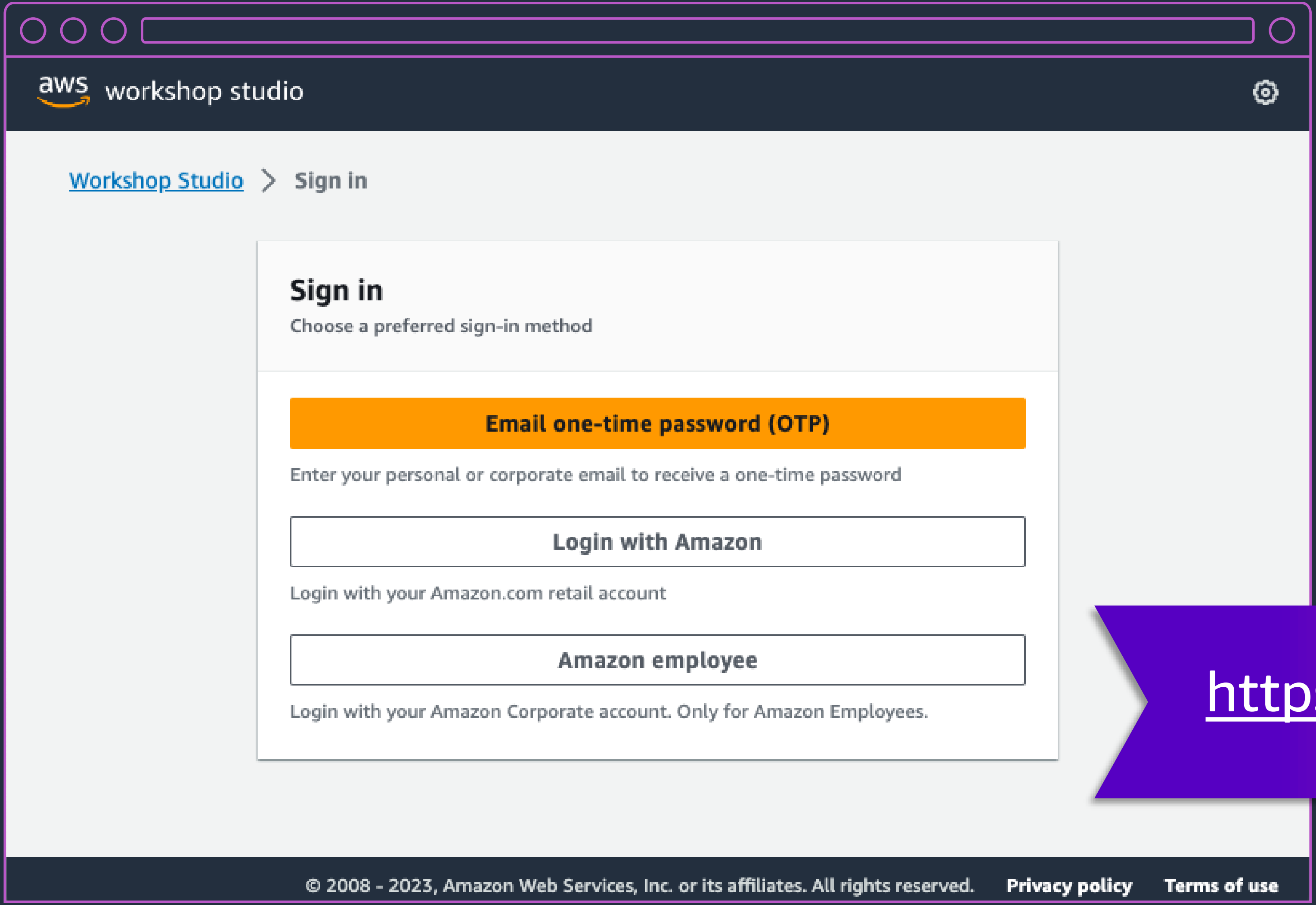
By default, common instructions are hidden but you can expand sections as needed

No need to rush finishing all modules, the core objective is to learn and understand

If you need us, raise your hand or just call upon us

Let’s build …

Step 1: Sign in using your preferred method



Workshop Studio > Sign in

Sign in

Choose a preferred sign-in method

Enter your personal or corporate email to receive a one-time password

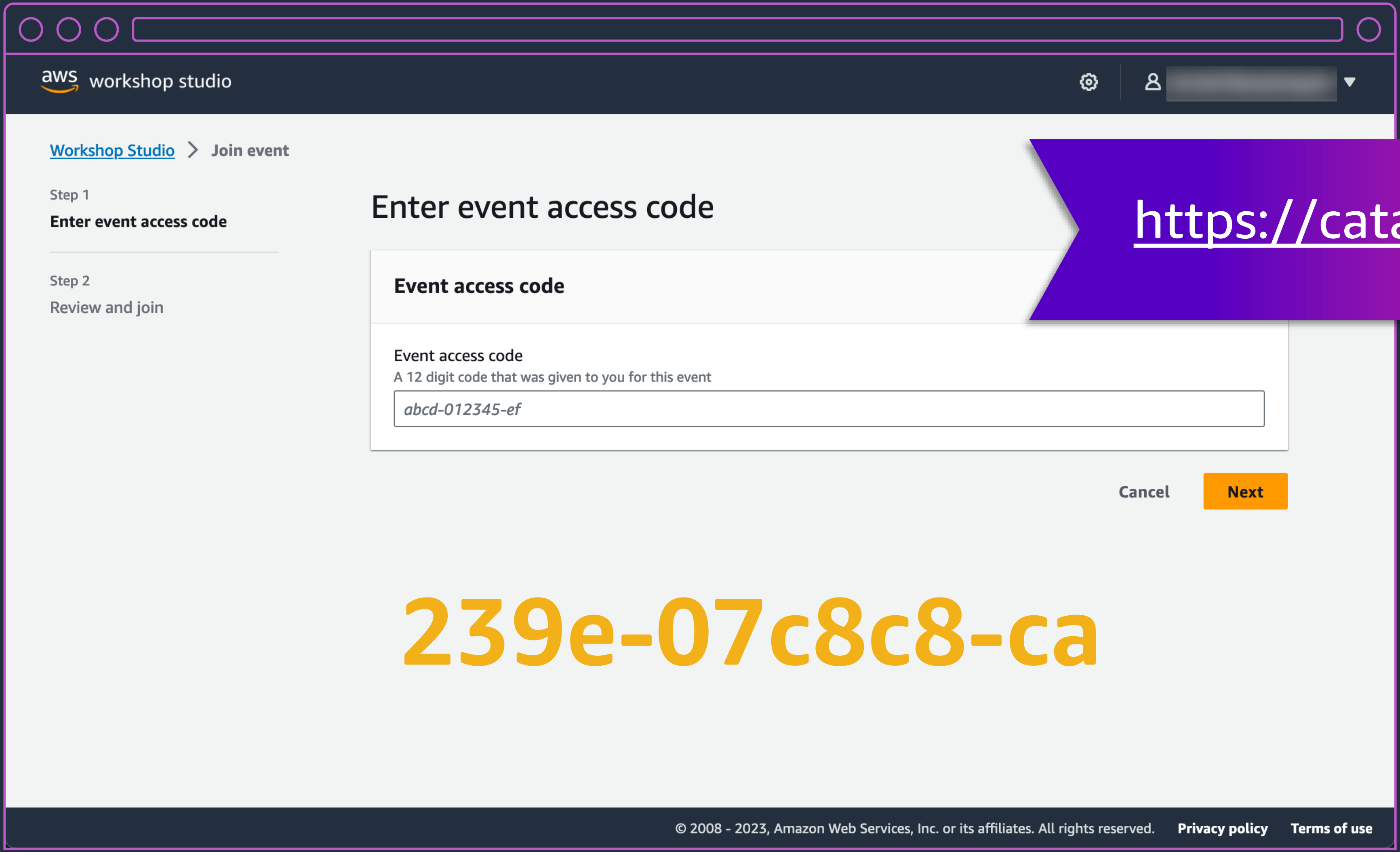
Login with your Amazon.com retail account

Login with your Amazon Corporate account. Only for Amazon Employees.

© 2008 - 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy policy Terms of use

https://catalog.workshops.aws/join

Step 2: Enter the event access code



aws workshop studio [redacted]

Workshop Studio > Join event

Step 1
Enter event access code

Step 2
Review and join

Enter event access code

Event access code

Event access code
A 12 digit code that was given to you for this event

abcd-012345-ef

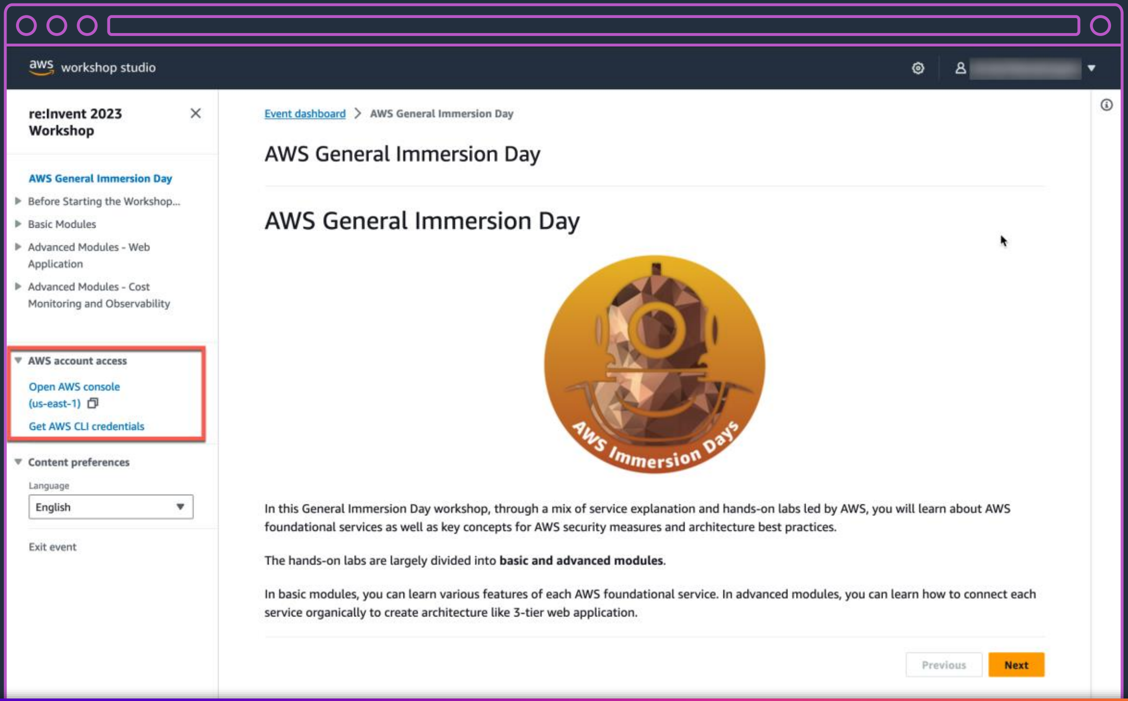
Cancel **Next**

Privacy policy **Terms of use**

https://catalog.workshops.aws/join

239e-07c8c8-ca

Step 3: Access AWS account



aws workshop studio [redacted]

re:Invent 2023 Workshop

AWS General Immersion Day
- Before Starting the Workshop...
- Basic Modules
- Advanced Modules - Web Application
- Advanced Modules - Cost Monitoring and Observability

AWS account access

Open AWS console (us-east-1)

Get AWS CLI credentials

Content preferences

Language

English

Exit event

Event dashboard > AWS General Immersion Day

AWS General Immersion Day

AWS General Immersion Day

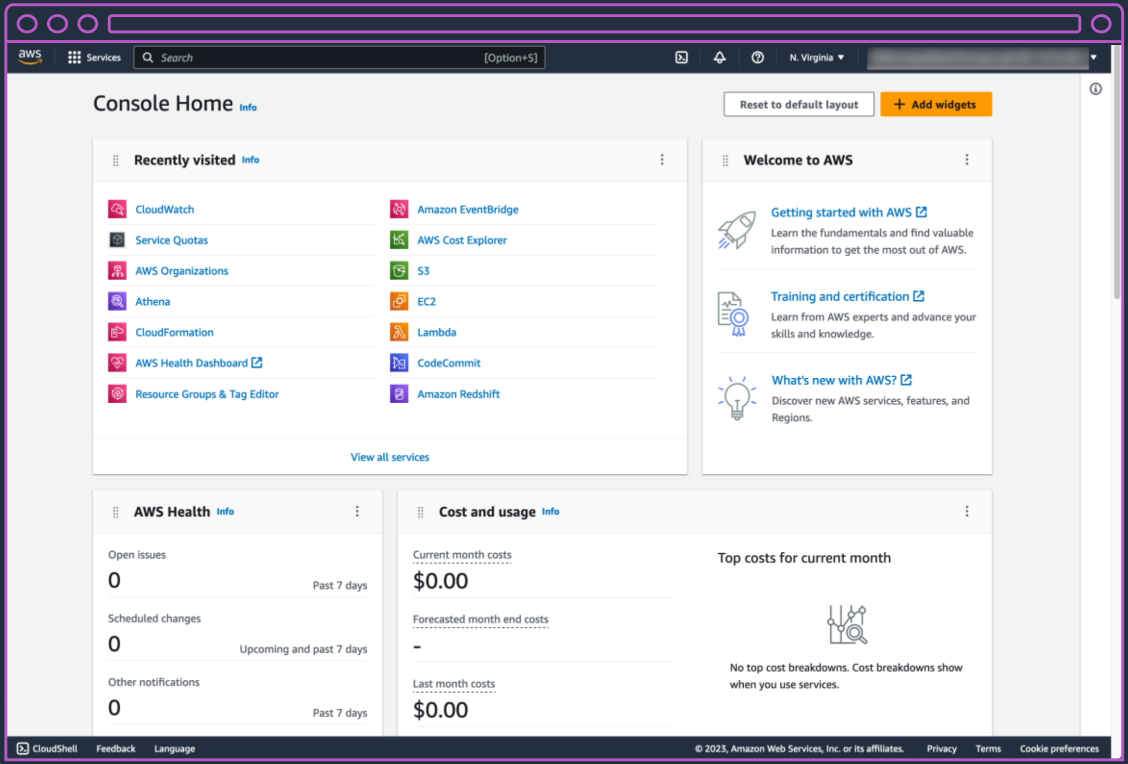
AWS Immersion Days

In this General Immersion Day workshop, through a mix of service explanation and hands-on labs led by AWS, you will learn about AWS foundational services as well as key concepts for AWS security measures and architecture best practices.

The hands-on labs are largely divided into **basic and advanced modules**.

In basic modules, you can learn various features of each AWS foundational service. In advanced modules, you can learn how to connect each service organically to create architecture like 3-tier web application.

Previous Next



[redacted]

Console Home Info

Reset to default layout | + Add widgets

Recently visited Info

CloudWatch	Amazon EventBridge
Service Quotas	AWS Cost Explorer
AWS Organizations	S3
Athena	EC2
CloudFormation	Lambda
AWS Health Dashboard	CodeCommit
Resource Groups & Tag Editor	Amazon Redshift

View all services

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

AWS Health Info

Open issues
0 Past 7 days

Scheduled changes
0 Upcoming and past 7 days

Other notifications
0 Past 7 days

Cost and usage Info

Current month costs
$0.00

Forecasted month end costs
-

Last month costs
$0.00

Top costs for current month

No top cost breakdowns. Cost breakdowns show when you use services.

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Access the AWS Management Console or generate AWS CLI credentials as needed

Please Provide Your Feedback

Step 1: Select Security, Governance and Resilience
Step 2: Select Detect, investigate and respond to security scenarios

Thank you!

Tony Suarez
suarito@amazon.com

Kain Leo
leokai@amazon.com