

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

Ship securely: Automated security testing for developers

Alvin Delagon (he/him)

Developer Specialist Senior Solutions
Architect, DevAx
Amazon Web Services

Anitha Deenadayalan (she/her)

Developer Specialist Senior Solutions
Architect, DevAx
Amazon Web Services

Agenda

Shift left – security overview

Automated security testing

Additional security tools and processes

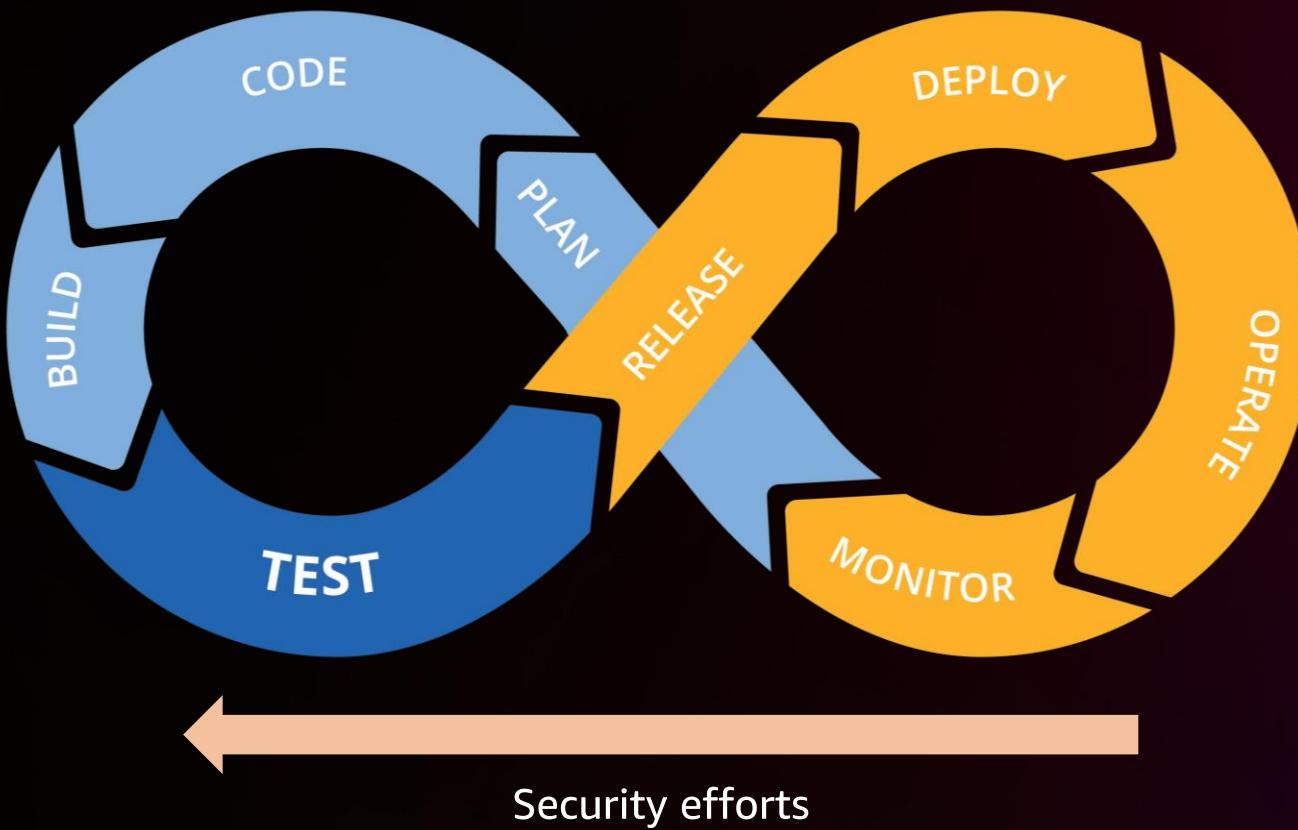
Cultural aspects

Workshop

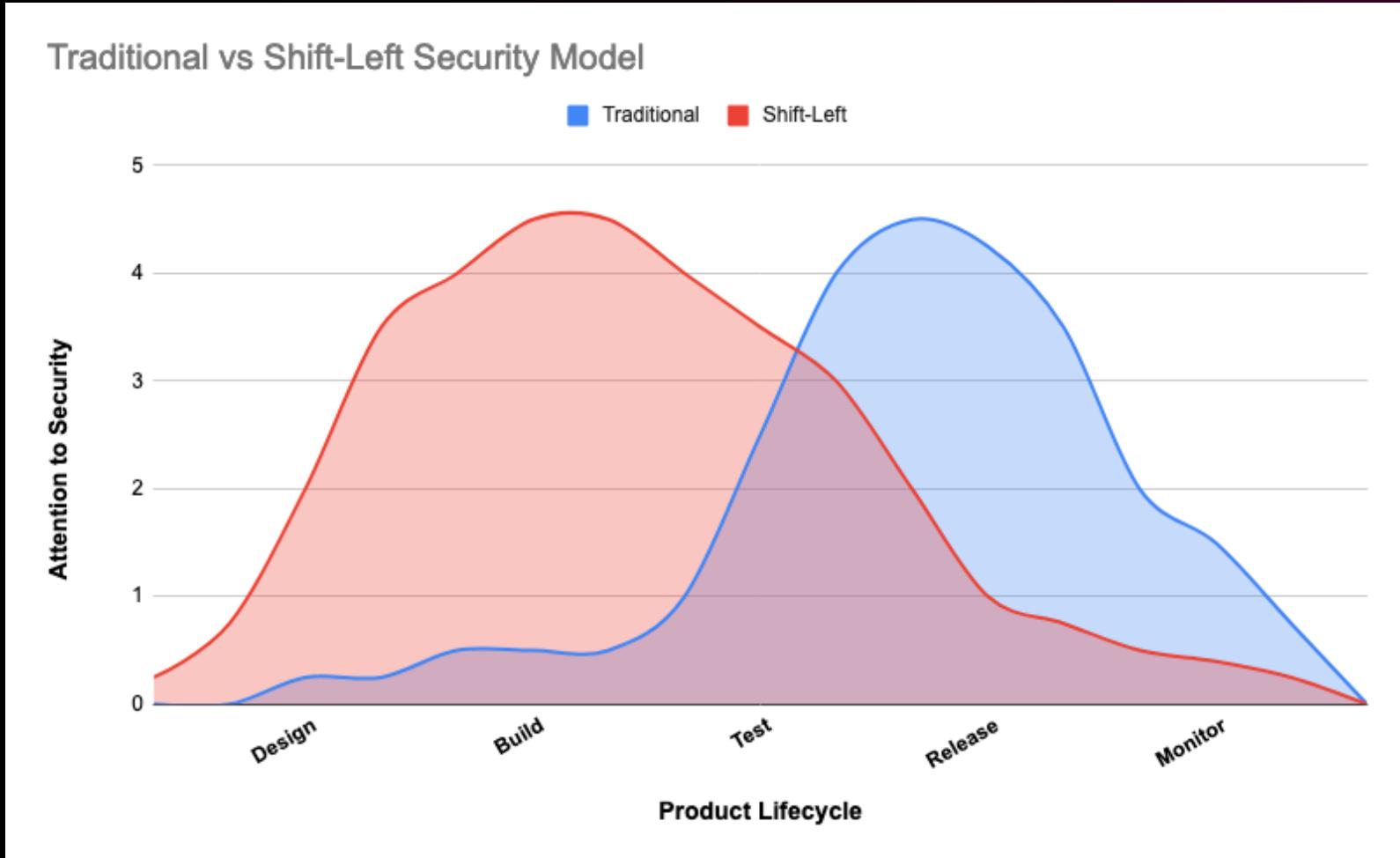
Takeaways

Shift left: Security

Move attention to security to the **earliest** possible point in the software development lifecycle



Attention to security



Does this mean more work for developers?

Investment in order to sleep better

Cheaper to fix security issues earlier¹

Faster time to market, less turnaround time

Most of it can be automated

[1] Error Cost Escalation through the Project Lifecycle –
<https://ntrs.nasa.gov/citations/20100036670>



Automated security testing

Are we writing code securely?

STATIC APPLICATION SECURITY TESTING (SAST)

SAST tools catch bugs and vulnerabilities in your application, with thousands of automated static code analysis rules



Amazon CodeGuru



Checkmarx



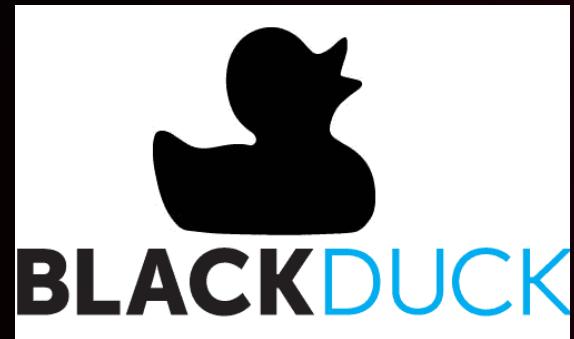
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How about code written by others?

SOFTWARE COMPOSITION ANALYSIS (SCA)

Most modern applications are composed of code written by others²

SCA tools check your dependencies for any vulnerabilities using a known database

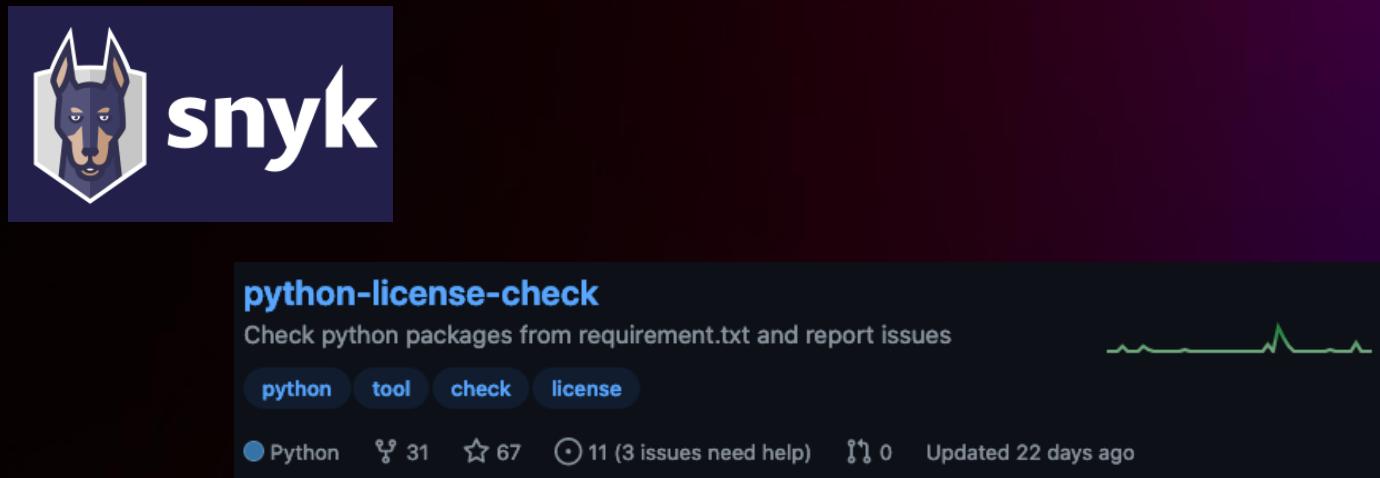
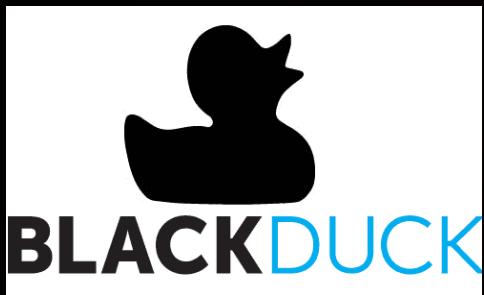


[2] Veracode State of Security Report – <https://www.veracode.com/state-of-software-security-report>

Are we protecting our intellectual property?

LICENSE CHECKING

Copyleft licenses such as **GNU General Public License** require you to distribute your application under the same license



Are our security controls working?

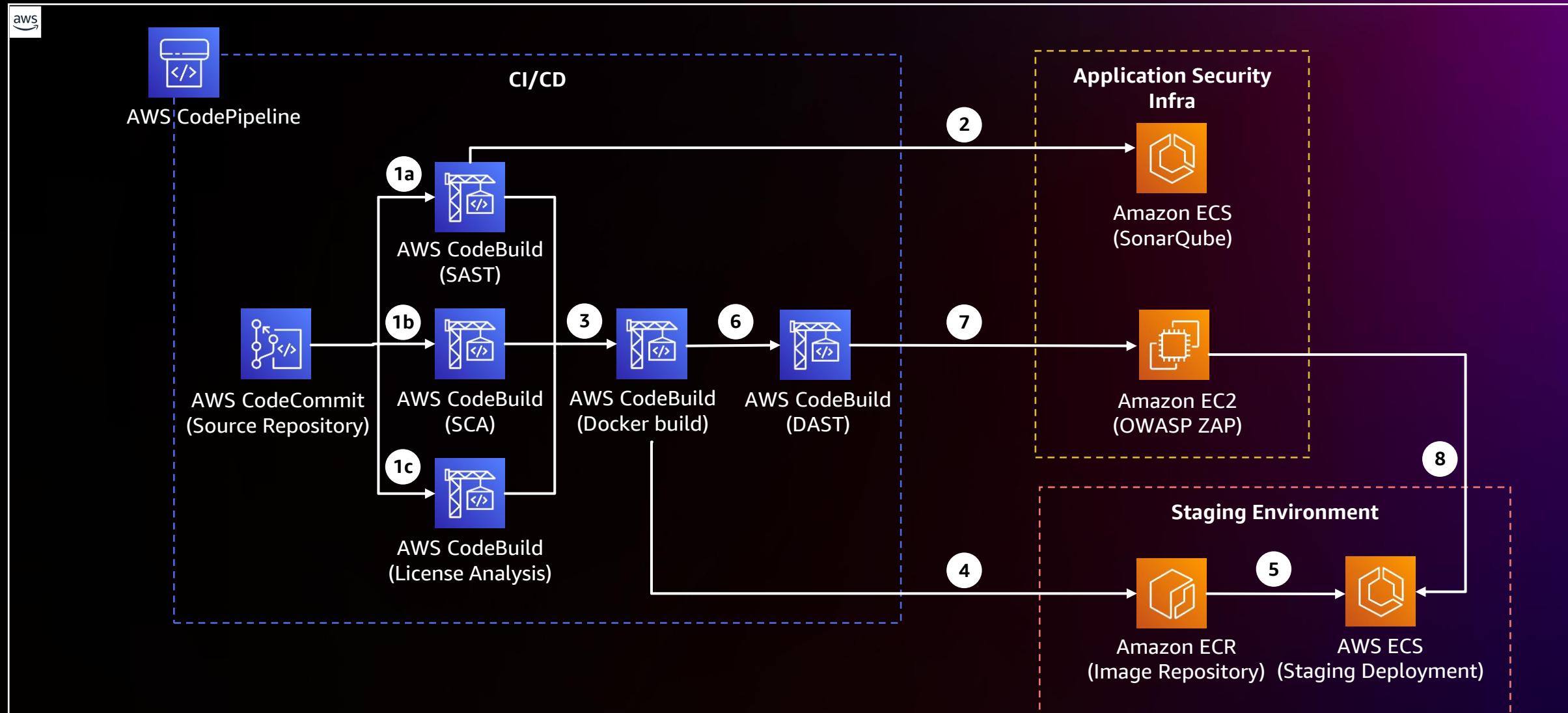
DYNAMIC APPLICATION SECURITY TESTING (DAST)

DAST tests the security posture of your application during **runtime**

This is used in tandem with other AppSec tools in order to validate your security controls



Automated security testing



Additional security tools & processes

Security before writing code

THREAT MODELING

Helps to identify **security requirements** prior to development^{3,4}

Threat ID	Asset	Entry point	Attack summary	Technique
TR-01	User account	Login page	Being able to hijack someone's account and conduct malicious activities	Brute-force attacks, password dumps, session hijacking, phishing
Threat ID	Preventive/Corrective controls			
TR-01	<ul style="list-style-type: none">• Multi-factor authentication• Password lifecycle and rules• Secure generation of session IDs• Session lifecycle• Secure storage of session cookies• Regular security reminders to customers			

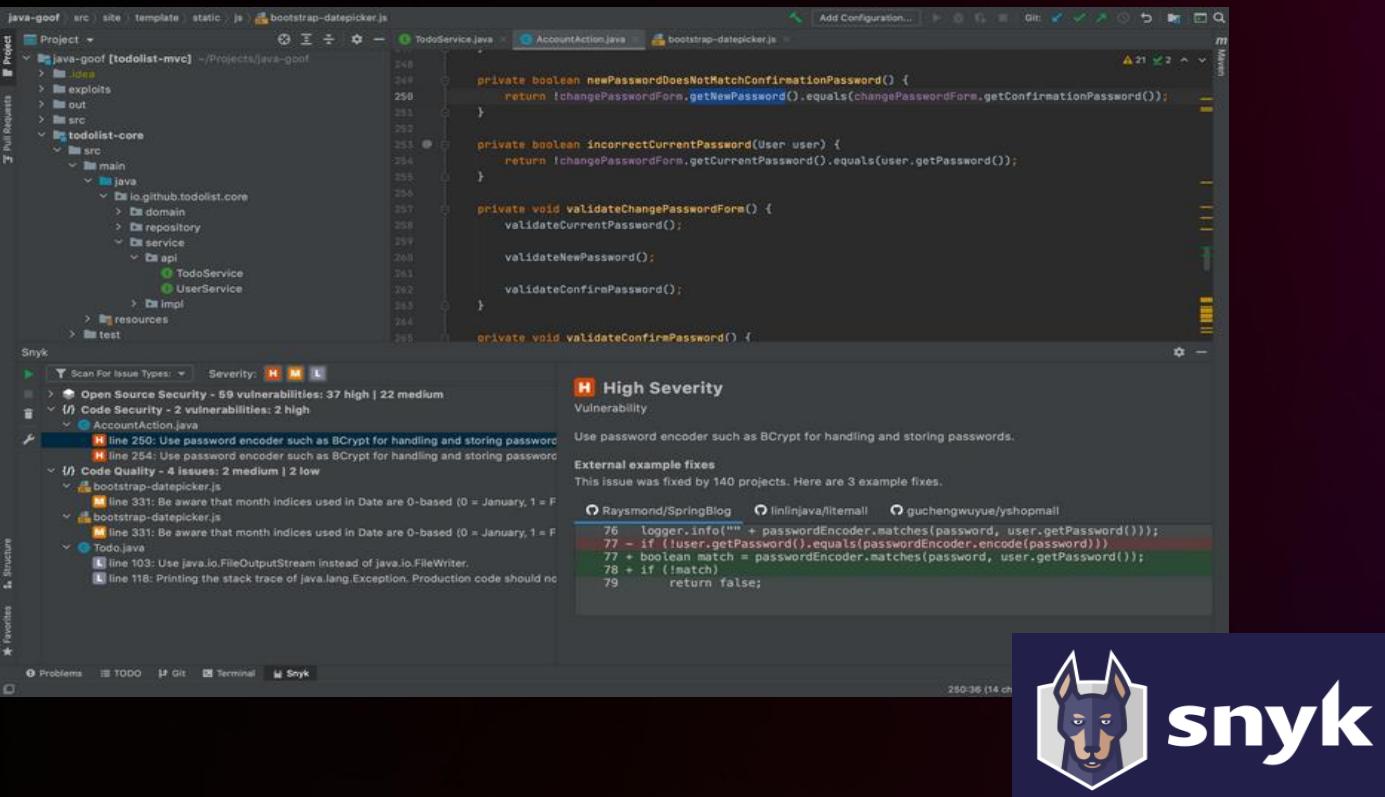
[3] How to approach threat modeling – <https://aws.amazon.com/blogs/security/how-to-approach-threat-modeling/>

[4] Threat modeling the right way for builders – <https://catalog.workshops.aws/threatmodel>

Security while writing code

IDE SECURITY EXTENSIONS

IDE extensions can provide quick and actionable security findings as you write your code



Security in source control

GIT HOOKS

Using Git hooks (pre-commit) allows you to trigger security scans automatically on your codebase to prevent accidental leakage of sensitive info such as AWS credentials and SSH keys



Security in configuration

SECRETS MANAGEMENT

Sensitive configurations such as database credentials are better stored somewhere else and accessed securely



AWS Secrets Manager



AWS Systems Manager



confidant

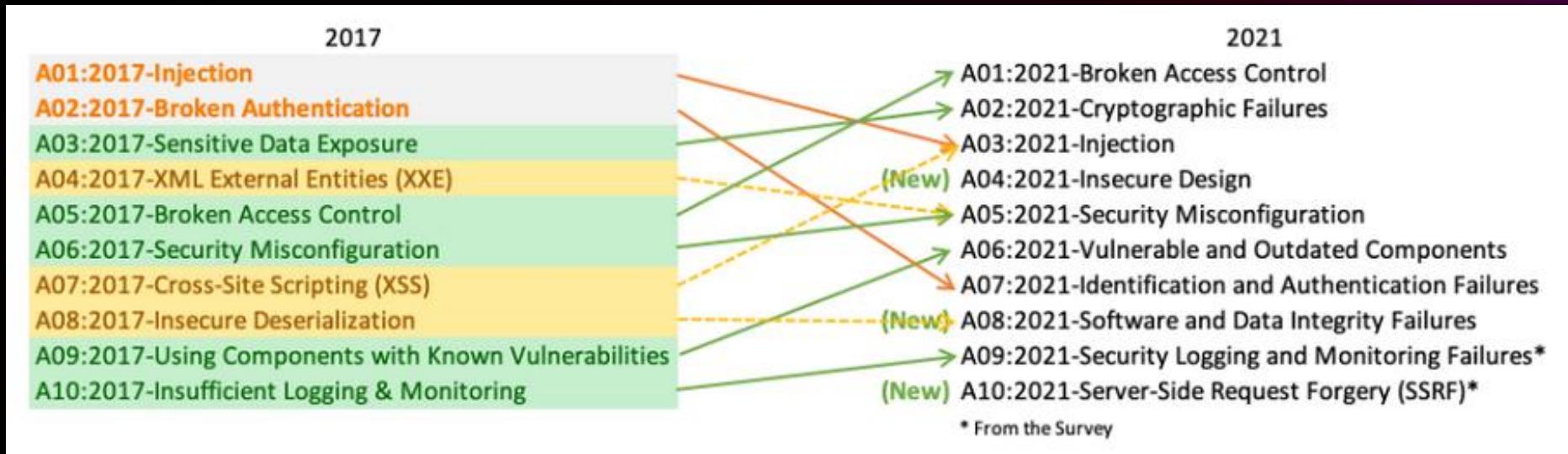


Parameter store

Be a better code reviewer



<https://owasp.org/www-project-top-ten/>



The OWASP Word Mark and OWASP & Design Logo are registered or unregistered service marks of OWASP Foundation, Inc. in the United States and other countries. All rights reserved. Unauthorized use strictly prohibited.

Cultural aspects

- Automation alone will not solve the problems
- Share security knowledge across different teams
 - **Build allies** – identify security champions and setup a community of practice
 - Conduct regular security-centric lunch-and-learn sessions
- Focus on building an inclusive culture and avoid the “blame game”

Let's start building!



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Exploit and remediate

Home About OWASP Top 10 Examples ▾



OWASP Top Ten Web Application Risks

This is an "Intentionally Vulnerable" Web Application meant for Training Purposes
Only. DO NOT Use in Production!

This Web Application demonstrates the common web vulnerabilities as stated in

owasp.org



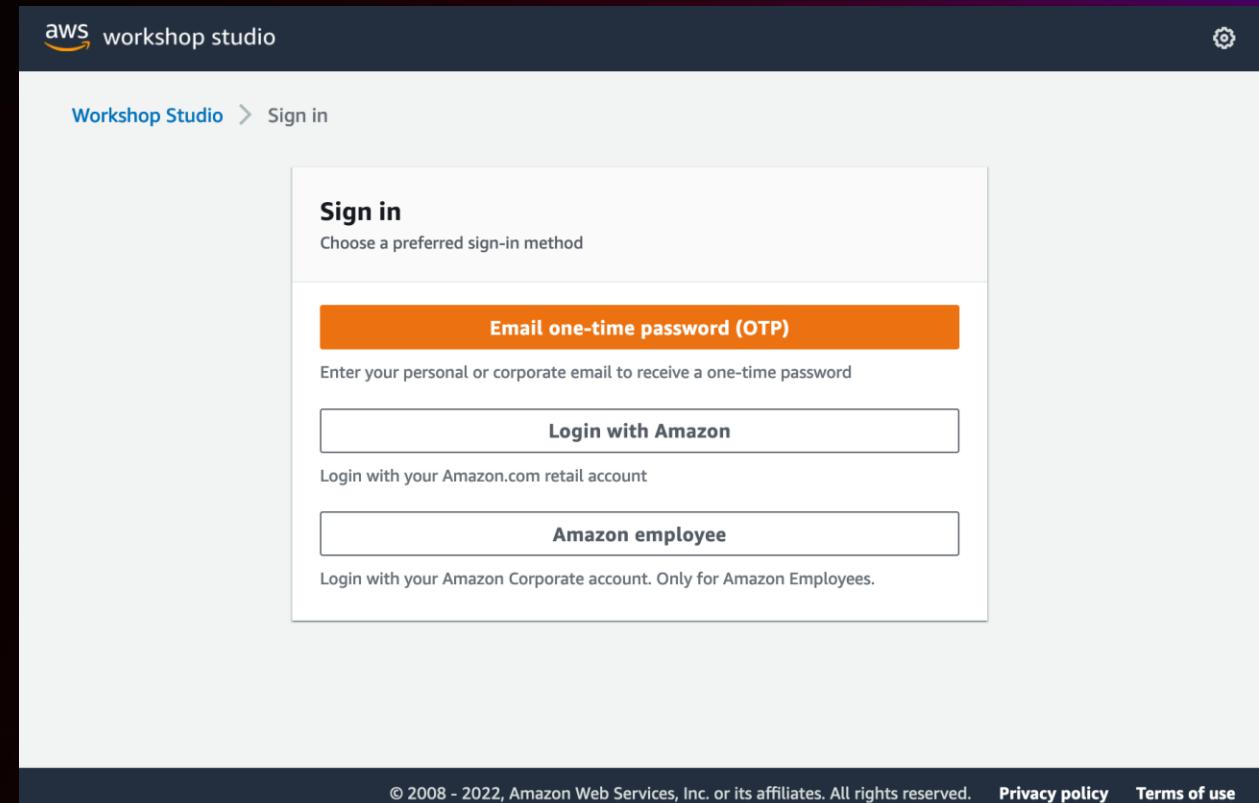
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started with this workshop

- As a participant, you will have access to an AWS account with any optional preprovisioned infrastructure and IAM policies needed to complete this workshop
- The AWS account will only be available for the duration of this workshop – you will lose access to the account thereafter
- The optional preprovisioned infrastructure will be deployed to a specific AWS Region. Check your workshop content to determine whether other Regions will be used.
- Be sure to review the terms and conditions of the event. Do not upload any personal or confidential information in the account.

Step 1: Sign in via your preferred method

One-click join link: <https://s12d.com/sec4devs>

A screenshot of the AWS Workshop Studio sign-in interface. The top navigation bar includes the AWS logo and the text "workshop studio". Below the navigation, the page title is "Workshop Studio > Sign in". The main content area is titled "Sign in" and prompts the user to "Choose a preferred sign-in method". Three options are listed: "Email one-time password (OTP)" (highlighted with an orange background), "Login with Amazon" (with a sub-note "Login with your Amazon.com retail account"), and "Amazon employee" (with a sub-note "Login with your Amazon Corporate account. Only for Amazon Employees").

aws workshop studio

Workshop Studio > Sign in

Sign in
Choose a preferred sign-in method

Email one-time password (OTP)
Enter your personal or corporate email to receive a one-time password

Login with Amazon
Login with your Amazon.com retail account

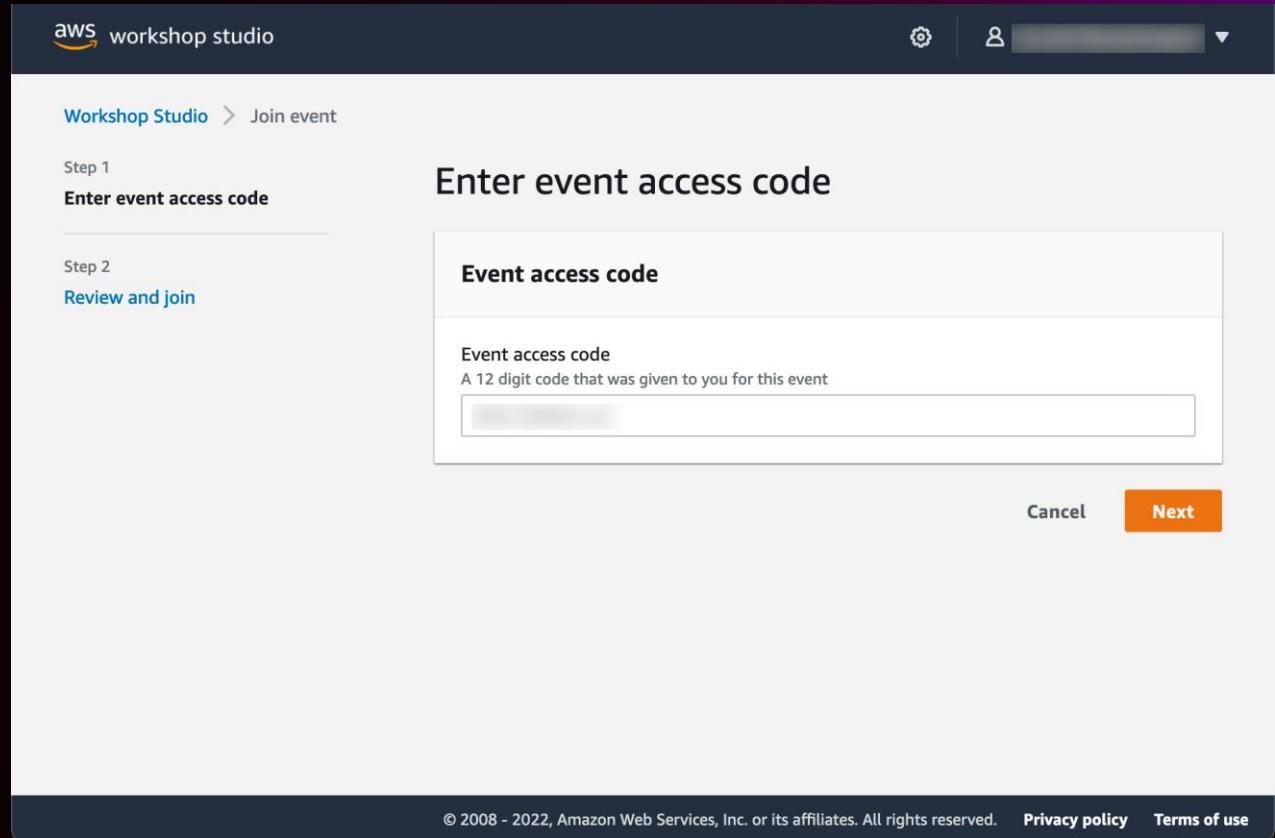
Amazon employee
Login with your Amazon Corporate account. Only for Amazon Employees.

Step 2 (optional): Enter event access code

Enter 12-digit event access code:

6586-0e0893-16

If you were given a one-click join link, you can skip this step



The screenshot shows a web browser window for 'aws workshop studio'. The title bar says 'aws workshop studio'. The main content area has a header 'Workshop Studio > Join event'. Below it, a sidebar on the left lists 'Step 1: Enter event access code' and 'Step 2: Review and join'. The main content area is titled 'Enter event access code' and contains a section for 'Event access code' with a placeholder text 'Event access code A 12 digit code that was given to you for this event'. At the bottom right of the content area are 'Cancel' and 'Next' buttons. The footer of the page includes the text '© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy policy' and 'Terms of use'.

Step 3: Review terms and join event

The screenshot shows the 'Review and join' step of the AWS Workshop Studio 'Join event' process. The page is titled 'Review and join' and displays 'Event details' and 'Terms and Conditions'.

Event details

Name	Start time	Duration	Level
AWS General Immersion Day	9/23/2022 01:13 AM	12 hours	-

Terms and Conditions
Read and accept before joining the event

1. By using AWS Workshop Studio for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivative works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of AWS Workshop Studio will comply with these terms and all applicable laws, and your access to AWS Workshop Studio will immediately and automatically terminate if you do not comply with any of these terms or conditions.

I agree with the Terms and Conditions

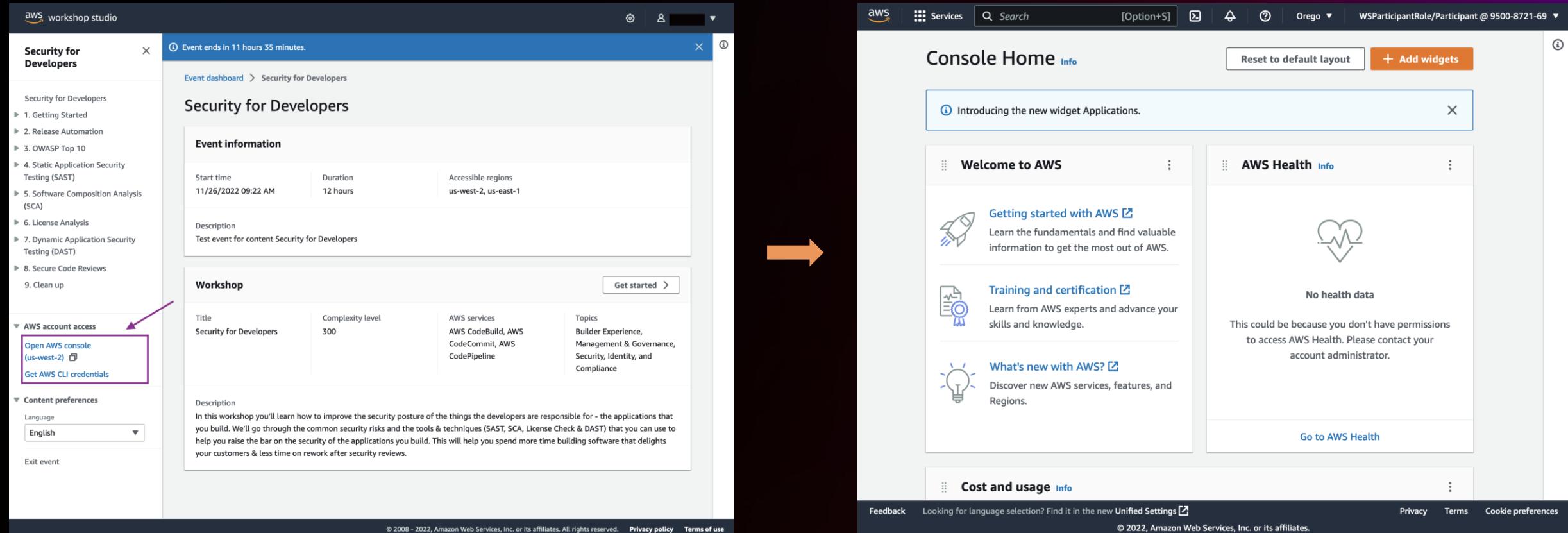
Cancel Previous Join event

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)



Step 4: Access AWS account

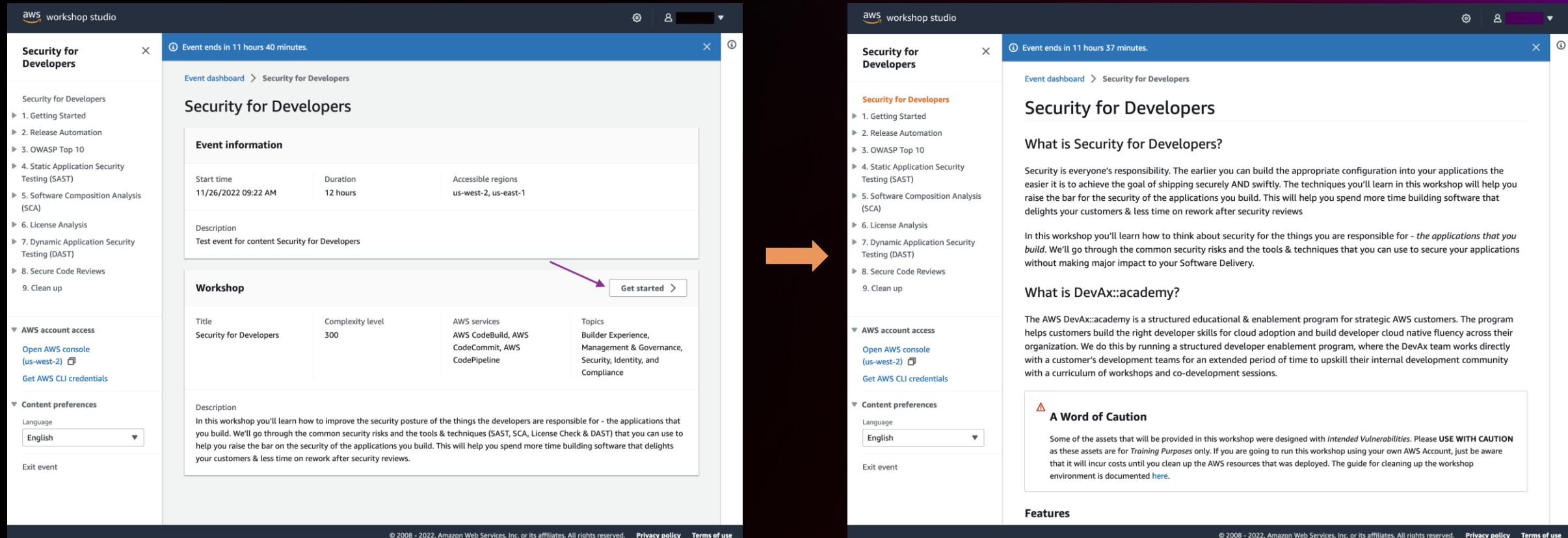
Access the AWS Management Console or generate AWS CLI credentials as needed



The image shows two screenshots illustrating the process of accessing an AWS account. On the left, the 'AWS workshop studio' interface displays the 'Security for Developers' event dashboard. A purple arrow points to the 'Open AWS console (us-west-2)' button in the 'AWS account access' section. A large orange arrow points from this interface to the 'Console Home' page on the right. The 'Console Home' page features a 'Welcome to AWS' section with links to 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. It also includes a 'AWS Health' section and a 'Cost and usage' section. The top navigation bar of the AWS Management Console is visible, showing 'Services', 'Search', and the user's role 'WSParticipantRole/Participant @ 9500-8721-69'.



Step 5: Get started with the workshop



The screenshot shows the AWS Workshop Studio interface with the 'Security for Developers' workshop selected. The left panel displays the 'Event information' and 'Workshop' details, while the right panel shows the expanded 'What is Security for Developers?' content. A purple arrow points from the 'Get started' button in the left panel to the expanded content in the right panel.

Event information

- Start time: 11/26/2022 09:22 AM
- Duration: 12 hours
- Accessible regions: us-west-2, us-east-1

Description

Test event for content Security for Developers

Workshop

Title	Complexity level	AWS services	Topics
Security for Developers	300	AWS CodeBuild, AWS CodeCommit, AWS CodePipeline	Builder Experience, Management & Governance, Security, Identity, and Compliance

Description

In this workshop you'll learn how to improve the security posture of the things the developers are responsible for - the applications that you build. We'll go through the common security risks and the tools & techniques (SAST, SCA, License Check & DAST) that you can use to help you raise the bar on the security of the applications you build. This will help you spend more time building software that delights your customers & less time on rework after security reviews.

Get started >

Security for Developers

What is Security for Developers?

Security is everyone's responsibility. The earlier you can build the appropriate configuration into your applications the easier it is to achieve the goal of shipping securely AND swiftly. The techniques you'll learn in this workshop will help you raise the bar for the security of the applications you build. This will help you spend more time building software that delights your customers & less time on rework after security reviews

In this workshop you'll learn how to think about security for the things you are responsible for - *the applications that you build*. We'll go through the common security risks and the tools & techniques that you can use to secure your applications without making major impact to your Software Delivery.

What is DevAx::academy?

The AWS DevAx::academy is a structured educational & enablement program for strategic AWS customers. The program helps customers build the right developer skills for cloud adoption and build developer cloud native fluency across their organization. We do this by running a structured developer enablement program, where the DevAx team works directly with a customer's development teams for an extended period of time to upskill their internal development community with a curriculum of workshops and co-development sessions.

A Word of Caution

Some of the assets that will be provided in this workshop were designed with *Intended Vulnerabilities*. Please **USE WITH CAUTION** as these assets are for *Training Purposes* only. If you are going to run this workshop using your own AWS Account, just be aware that it will incur costs until you clean up the AWS resources that was deployed. The guide for cleaning up the workshop environment is documented [here](#).

Features



Key takeaways

- Security **is everyone's responsibility**
- Embrace security as an **integral part of the process**, use **feedback** to refine the process
- Security must be **empowering**, not blocking
- DevSecOps **is not** one size fits all

Thank you!

Alvin Delagon

adelagon@amazon.com

adelagon (GitHub)

 adelagon

Anitha Deenadayalan

anithade@amazon.com

awsanitha (GitHub)

 anitha-deenadayalan



Please complete the session
survey in the **mobile app**



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.