Using Amazon Inspector for vulnerability assesment and remediation

Lab overview

In this lab, you utilize Amazon Inspector to scan for vulnerabilities in your AWS resources, specifically AWS Lambda functions. You learn how to activate Amazon Inspector, interpret the vulnerability reports, and remediate the findings.

The developers at AnyCompany are in the initial phases of building an application primarily using AWS Lambda. Throughout the development process, they need an automated security tool that not only scans for vulnerable software packages, but also scans within the code itself. You decide to utilize Amazon Inspector to fill this need.

Amazon Inspector meets the requirements of being able to scan AWS Lambda functions by quickly responding to new deployments. It also automatically scans additional resources such as EC2 instances, Amazon ECRs within AnyCompany's AWS account.

Objectives

After completing this lab, you should be able to:

- Activate Amazon Inspector.
- Analyze and interpret vulnerability findings.
- Remediate the vulnerabilities found by Amazon Inspector.

Duration

This lab requires approximately **30 minutes** to complete.

Lab environment

The environment has Lambda functions with vulnerabilities which will be subsequently scanned by Amazon inspector and reported as per severity.

Accessing the AWS Management Console

1. At the upper-right corner of these instructions, choose ▸ **Start Lab**

   Troubleshooting tip: If you get an **Access Denied** error, close the error box, and choose ▸ **Start Lab** again.

2. The following information indicates the lab status:

   - A red circle next to **AWS** 🔴 at the upper-left corner of this page indicates that the lab has not been started.
   - A yellow circle next to **AWS** 🟡 at the upper-left corner of this page indicates that the lab is starting.
   - A green circle next to **AWS** 🟢 at the upper-left corner of this page indicates that the lab is ready.

   Wait for the lab to be ready before proceeding.

3. At the top of these instructions, choose the green circle next to **AWS** 🟢

   This option opens the AWS Management Console in a new browser tab. The system automatically sign you in.

   Tip: If a new browser tab does not open, a banner or icon at the top of your browser might indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

4. If you see a dialog prompting you to switch to the new Console Home, click **Switch to the new Console Home**.

5. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you should be able to see both browser tabs at the same time so that you can follow the lab steps.

   ⚠ **Do not change the lab Region unless specifically instructed to do so**.

Task 1: Activate the Amazon Inspector

In this task, you activate and run the Amazon inspector service to continuously scan the Lambda functions.

6. In the **AWS Management Console**, in the search bar at the top, type and choose `Inspector`.

7. Open the panel on the left and choose **Activate Inspector** to activate it for your account.

8. Under **Activate Inspector** choose **Activate Inspector** button.

   Note: This is only needed for the first time.
   After activation, you see a message at the top *Welcome to Inspector. Your first scan is underway.*

9. If you are prompted to respond to a survey titled **Feedback for Amazon Inspector**, choose **cancel**.

   - Close all the banner messages on top of the page.

10. Refresh the page periodically until you see the **Dashboard > Summary > Environment coverage> Lambda functions** at 100%

    The dashboard shows your account number and activation status for AWS Lambda. By default, scanning is activated for Amazon EC2, Amazon ECR, and AWS Lambda standard scanning.

Task 2: Reviewing the inspected resources

In this task, while you wait for the scan to finish, you review the current lab environment (the EC2 instance and the Lambda functions) to understand what specific resources are being scanned by Amazon Inspector.

Task 2.1: Reviewing your Lambda functions

11. From the **Findings** on the left, choose **All findings**.
12. Three rows are displayed, one for each vulnerability within Lambda function. You should see the following key details:
    - **Severity**:Medium
    - **Impacted resource** shows you the affected Lambda function.
    - **Title** shows the reason for the finding.
13. Choose the *Radio button* for Choose the finding **CVE-2023-32681 - requests.** This opens a pane containing the vulnerability information.
14. Within the information pane, under the **Vulnerability details** section choose the external link next to the **Vulnerability ID**.

    The link opens a new browser tab to the vulnerability detail webpage from the National Vulnerability Database (NVD), which is a repository of standardized vulnerability management data maintained by the National Institute of Standards and Technology (NIST). This page offers more detailed information about the vulnerability.
15. Within the information pane, find the the **Remediation** section.

    The issue is that the **requests** package is vulnerable and outdated, and the recommendation is to upgrade the package. Next, you apply the remediation to your Lambda function.

Task 3: Remediating the vulnerabilities findings

In this task, you analyze the findings reported by Amazon Inspector and interpret the vulnerability details. You update your Lambda functions to remediate the vulnerabilities. After updating the functions, you review the Amazon Inspector findings to confirm the vulnerability has been fixed.

Task 3.1: Remediating your Lambda function’s Package Vulnerabilities

16. On the AWS Management Console, in the search box, search for and choose `Lambda`
17. From the list of Lambda functions, choose the **get-request** function.
18. Within the Lambda function code editor’s file browser, choose **requirements.txt.**
19. Remove the version number and equal signs from `requests==2.20.0` so that the line becomes only `requests`.

   The **requirements.txt** file tells AWS Lambda which Python packages are required to run your function. When no version number is specified, the latest version of the package will be installed by default. This ensures that your Lambda funtion uses the latest version of the package.

20. Choose the **Deploy** button to deploy the function.

    A banner is displayed with the message Successfully updated the function **get-request**.

    This latest deployment of your Lambda function will trigger Amazon Inspector to initiate a new scan of the function.

21. On the AWS Management Console, in the search box, search for and choose `Amazon Inspector`.
22. In the navigation pane at the left of the page, under **Findings**, choose **All findings**.

    Note: If the navigation pane is collapsed, choose the menu icon.

23. In the findings dashboard, under finding status, change the selection from **Active** to **Closed**.
24. In the list of closed findings, you see **CVE-2023-32681 - requests.** This confirms the successful remediation of the vulnerability.

    Note: It may take a few minutes for the scan to initiate and finish. You can choose the refresh button to view the latest status of your scanned resources.

25. In the navigation pane at the left of the page, under **Resources coverage**, choose **Lambda functions**.
26. If needed, expand the width of the **Last scanned** column to display the full timestamp.

    You see that the most recently scanned Lambda function has an updated timestamp.

Conclusion

🏁 Congratulations! You now have successfully:

- Activated and configured Amazon Inspector
- Analyzed and interpreted vulnerability findings
- Remediated the vulnerabilities found by Amazon Inspector

Lab complete

27. Choose ■ **End Lab** at the top of this page, and then choose **Yes** to confirm that you want to end the lab.
28. An **Ended AWS Lab Successfully** message is briefly displayed indicating that the lab has ended.

    For more information about AWS Training and Certification, see AWS Training and Certification

    Your feedback is welcome and appreciated.

    If you would like to share any suggestions or corrections, please provide the details in our AWS Training and Certification Contact Form.

© 2025 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.