Project Solution



[**Task 1: Hardening The Service**](#_35eld5hikdzn) **2**

[Task Challenge:](#_byue9qb67e1e) 2

[Task Solution:](#_kt83phhow0fz) 2

[**Task 2: Planning Layer Of Defense**](#_7nvz5s4dpw66) **4**

[Task Challenge:](#_3ygcwr2og886) 4

[Task Solution:](#_flwk12hu34qb) 4

[**Task 3: Integrating the Yara Scanning function With S3 Bucket**](#_vv8yrxe4cf0m) **5**

[Task Challenge:](#_sbmq3krst99u) 5

[Task Solution:](#_cp2rwpkyd6p7) 5

[**Task 4: Scanning Suspicious Files**](#_3g0arggnk2do) **7**

[Task Challenge:](#_anjgr23u5c1w) 7

[Task solution:](#_hmau9qovlpqj) 7

[**Task 5: Defense-in-Depth**](#_ev1rw1lvwuvh) **9**

[Task Challenge:](#_mn77vpklhp8b) 9

[Task Solution:](#_ft8yi063arrf) 9

[**Task 6: Complete Architecture Diagram**](#_em1y9jdgbhp7) **11**

[Project Challenge:](#_4yuv8weyxs44) 11

[Project Solution:](#_m7kh7qqwqcii) 11

For this project, an AWS command line, as well as console access, is required.

Set up the command line access using the instructions listed below and based on your machine's operating system.

## Task 1: Hardening The Service

Create and apply a bucket policy using the command line or the AWS UI and apply it on the file-scan-upload bucket to make it defensible against binary file uploads.

Using what you learned from the course, harden the bucket so that anyone can upload only the suitable types of files using AWS Policies.

Submit the policy as a JSON file and name it bucket\_restriction.json.

Also, submit a snapshot below or as a jpeg of the command line or AWS UI showing that an error pops up when uploading a non-image filetype. **Name the snapshot as failed\_upload.jpeg if you include it as a separate file.**

Please include an answer to the question below.

What did you find when attempting to upload your files? How might you harden this bucket, and why is that the best solution?

## 

## Task 2: Planning Layer Of Defense

### Task Challenge:

What AWS service would you propose to the WPO team to build the Yara scanning feature on the S3 uploads and why?

## 

## Task 3: Integrating the Yara Scanning function With S3 Bucket

### Task Challenge:

Launch the AWS dashboard and navigate to the Lambda functions page. You will notice a lambda called ***bucket-scan-function***.

Address the following in the template:

* What changes should you make to the lambda function's settings so that it can start scanning the file uploads?
* Perform the change you have suggested above and submit a snapshot of the change you have made and name the file as ***lambda\_s3\_trigger.jpg.***

## 

## Task 4: Scanning Suspicious Files

### Task Challenge:

Upload the provided three images to the f***ile-scan-upload-[random]*** bucket and answer the following:

* Using the cloudwatch logs, determine and provide the ***detection\_name*** that is triggered within the image files.
* Based on the logs, the lambda function writes the result of the scan to another AWS service. Which service is it? Navigate to the service and post the JSON result of the suspicious file saved in that service.

## 

## Task 5: Defense-in-Depth

### Task Challenge:

Task goal is to modify the Denylist-parsing-function lambda code so that it is able to match the uploaded files against a set of pre-defined hashes.

Submit the modified lambda function's code either as "**denylist\_match.py**" or as a screenshot in the template as evidence. The snapshot should show the changes you have made in the code.

Also, submit a snapshot of the cloudwatch logs showing the successful hash match for the same suspicious image file which triggered the Yara alert. Name the file as ***denylist\_cloudwatch.jpg***.

## 

## Task 6: Complete Architecture Diagram

### Project Challenge:

Modify the starter architecture diagram and add it to the template showing evidence of the following elements (you could also include the image file in your submission):

* The flow of file from the User to the file-upload S3 bucket
* Bucket-scan-function Lambda Trigger to scan files through the Yara engine.
* SQS queue message invoking the Denylist-parsing-function.
* Presence of Hashlist in a separate S3 bucket, which the Denylist-parsing-function will read.