**Amazon EC2 Instance Isolation Challenge**

1. **Detach Compromised Instance from the Auto Scaling Group**

Detach the compromised instance from the auto scaling group and do not launch a replacement instance

Amazon EC2AWS Auto Scaling

* Select the check box next to your Auto Scaling group. A split pane opens up in the bottom of the Auto Scaling groups page. **On the Instance management tab, in Instances, select an instance and choose Actions, Detach**.

2. **Tag the Compromised Instance**

Tag the compromised instance with the following key and value:

* **IncidentStatus**
* **Isolate**

Amazon EC2

**Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ .**

1. In the left navigation pane, choose Instances.
2. Select an instance, and then choose Actions, Instance settings, then click manage tags.
3. Add given key and Value
4. Choose Save.

3. **Create a Security Group for Isolated Instances**

Create a security group that satisfies the following:

* Is named **Isolated**
* Does not allow inbound traffic
* Does not allow outbound traffic
* Has a tag with the key and value:
  + **IncidentStatus**
  + **Isolate**

*Note*: The group's description can be anything

Amazon EC2



**Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ .**

1. In the centre, choose Security groups.
2. Give name as Isolated.
3. Delete outbound traffic.
4. Add tags and create security groups.

4. **Update the Compromised Instance's Security Group**

Remove the existing security group from the compromised instance and add your isolation security group to block network traffic

Amazon EC2



**Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ .**

1. In the navigation pane, choose Instances.
2. Select your instance, and then choose Actions, Security, Change security groups.
3. For Associated security groups, select a security group from the list and remove it and choose Add security group. And add isolated security group...
4. Choose Save.

5. **Detach the Instance's IAM Role**

Remove the IAM role that is associated with the compromised instance so that it has no IAM role

AWS Identity and Access Management (IAM)Amazon EC2

* In the left navigation pane, choose Instances.
* Select an instance, and then choose Security, Modify IAM role, then click respected IAM role.
* Detach

6. **Snapshot the Compromised Instance**

Create a snapshot of the comprised instance's root volume and tag the snapshot with the following key and value:

* **IncidentStatus**
* **Isolate**

Amazon EC2



**Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ .**

1. In the navigation pane, choose Snapshots
2. Select a volume ID
3. Add tags, add key , add value
4. Create Snapshot.

7. **Create an AMI of the Compromised Instance**

Create an Amazon Machine Image (AMI) of the compromised instance that satisfies the following:

* Is named **Compromised**
* Has a tag with the key and value:
  + **IncidentStatus**
  + **Isolate**

Amazon EC2

* Log in to the AWS Management Console, display the EC2 page for your region, then click Instances. Choose the instance from which you want to create a custom AMI. Click Actions and click Create Image. Type a name for Image Name that is easily identifiable to you and, optionally, input text for Image Description and in Add new tag enter key and value..