Micro-Assurances

Incident Response Runbook

*Compromised Database Administrator Account*

The objective of this runbook is to provide specific guidance on how to manage a compromised Database Administrator Account in the Micro-Assurance Amazon Web Services (AWS) environment.

This runbook focuses on the IR lifecycle:

• Establish Control

• Determine Impact

• Recover as Needed

• Investigate the Root Cause

# 

# Roles and Responsibilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Control** | **Determine Impact** | **Recover** | **Investigate Root Cause** |
| Database Administrator | Monitor and secure access to the database; apply security patches and updates. | Assess impact on the database, such as data loss, corruption, or unauthorized access. | Restore database from backups, repair damaged data, and apply security measures to prevent future incidents. | Identify vulnerabilities, misconfigurations, or other causes that led to the incident. |
| System Administrator | Ensure proper system configurations, monitor system logs, and maintain security updates. | Determine impact on systems, such as downtime, data loss, or unauthorized access. | Restore systems from backups, repair damage, and apply security measures to prevent future incidents. | Investigate and identify issues in the system that contributed to the incident. |
| Network Engineer | Monitor network traffic, maintain network security devices, and apply security configurations. | Assess the impact on the network, such as downtime, unauthorized access, or data exfiltration. | Repair network damage, restore connectivity, and apply security measures to prevent future incidents. | Determine the root cause of network vulnerabilities or misconfigurations that contributed to the incident. |
| Application Owner | Ensure application security, monitor application logs, and maintain security updates. | Determine impact on the application, such as downtime, data loss, or unauthorized access. | Restore application functionality, repair damage, and apply security measures to prevent future incidents. | Investigate and identify issues in the application that contributed to the incident. |
| Security Analyst | Monitor security alerts, analyze threats, and recommend mitigations. | Assess the overall impact of the incident on the organization's security posture. | Assist in incident recovery efforts and recommend security improvements. | | Collaborate with other roles to determine the root cause of the incident. |
| Incident Responder | Coordinate and manage the incident response process. | | Assess the overall impact of the incident on the organization. | | Oversee the recovery efforts and ensure timely restoration of services. | | Lead the investigation to determine the root cause of the incident and recommend preventive measures. |

# 

# Micro-Assurances AWS Asset Inventory

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Instance**  **Name** | **Instance-ID** | | **Availability Zone** | **Public IP** | **Volume-ID** |
| |  |  | | --- | --- | | LAMP01 |  | | |  |  | | --- | --- | | [i-0542844daefd69cbd](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstanceDetails:instanceId=i-0542844daefd69cbd) |  | | | us-east-1a | 34.207.80.50 | [vol-04e10f012a615987f](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#VolumeDetails:volumeId=vol-04e10f012a615987f)  /  [vol-0246612bcc6df09b5](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#VolumeDetails:volumeId=vol-0246612bcc6df09b5)(snap-0d6a2ac1feca4cf17) |
| LAMP02 | [i-0aae268e087627536](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceId=i-0aae268e087627536) | | us-east-1b | 54.89.59.55 | [vol-01978923a790f4c04](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#VolumeDetails:volumeId=vol-01978923a790f4c04)  /  [vol-0cfc3564fc8eb5097](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#VolumeDetails:volumeId=vol-0cfc3564fc8eb5097)(snap-0d6a2ac1feca4cf17) |
| udacity-inventory |  | | us-east-1a | 34.228.55.250 | [vol-0011b9afa58f36e08](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#VolumeDetails:volumeId=vol-0011b9afa58f36e08) |
| **ELB** | | **ELB PORTS** | | **ELB DNS NAME** | |
| [Course4Re-LoadBala-10PG3K04OVTXT](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LBDetails:clbName=Course4Re-LoadBala-10PG3K04OVTXT) | | **80 (HTTP) forwarding to 80 (HTTP)** | | Course4Re-LoadBala-10PG3K04OVTXT-1196392831.us-east-1.elb.amazonaws.com | |

**Graphical user interface, text, application

Description automatically generated**

# Logging and Alerting Inventory

|  |  |
| --- | --- |
| **Log Source** | **Enabled** |
| [**IR-log-01**](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/IR-logs/log-events/IR-log-01) | Yes |
|  |  |

Establish Control

**Automated Response Actions (Lambda Function Based on Tags)**

|  |  |
| --- | --- |
| **Action** | **Required Steps** |
| Create IAM ROLE TO SNAPSHOT FOR LAMP01 | Create role |
| Create Lambda Function to snapshot for Lamp01 | Create Lambda Function |

**Manual Response Actions (AWS CloudShell Commands)**

|  |  |
| --- | --- |
| **Action** | **Required Steps** |
| **Create Snapshot of LAMP02** | 1. Execute the command: aws ec2 create-snapshot --volume “vol-01978923a790f4c04” --description "SAC4T4"  2. Save the output to a file named SAC4T4.txt |
| **Create Security Group of isolation** | aws ec2 create-security-group --group-name isolation-security-group --description "Isolation Security Group" |
| **Revoke all traffic inbound and outbound in security group.**  **Per default egress deny all** | aws ec2 authorize-security-group-ingress --group-name isolation-security-group --protocol all --cidr 0.0.0.0/0  aws ec2 authorize-security-group-egress --group-name isolation-security-group --protocol all --cidr 0.0.0.0/0 |
| **Added isolation-security-group to instance LAMP2** | aws ec2 modify-instance-attribute --instance-id i-0aae268e087627536 --groups isolation-security-group |
| **Cofirmed attached of security group to ec2 lamp2** | aws ec2 describe-instances --instance-ids -0aae268e087627536 |

Recovery  
  
**Business Continuity Plan**

|  |  |  |
| --- | --- | --- |
| **Resource** | **Business Continuity Action** | **Status** |
| LAMP01 | TERMINATE | TERMINATED |
| LAMP02 | TERMINATE | TERMINATED |
|  |  |  |

# 

# 