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 | MySQL Database | MySQL Database | MySQL Database | MySQL Database |
| System Administrator | GitHub, EC2 instances | GitHub, EC2 instances | GitHub, EC2 instances | GitHub, EC2 instances |
| Network Engineer | VPC and ELB | VPC and ELB | VPC and ELB | VPC and ELB |
| Application Owner | Applications logging running on 2 EC instances | Applications logging running on 2 EC instances | Applications logging running on 2 EC instances | Applications logging running on 2 EC instances |
| Security Analyst | Security alerts CloudTrail & CloudWatch | Security alerts: CloudTrail & CloudWatch | Security alerts: CloudTrail & CloudWatch | Security alerts: CloudTrail & CloudWatch |
| Incident Responder | All assets | All assets | All assets | All assets |

# Micro-Assurances AWS Asset Inventory

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Instance**  **Name** | **Instance-ID** | | **Availability Zone** | **Public IP** | **Volume-ID** |
| LAMP01 | i-0cc39114bea09a63c | | Us-east-1a | 44.204.203.151 | Vol-0d363e472da76a898 |
| LAMP02 | i-0adab279adfbe91b7 | | us-east-1b | 54.204.214.79 | vol-0ac551f00bedabfe9 |
| **ELB** | | **ELB PORTS** | | **ELB DNS NAME** | |
| Course4Re-LoadBala-1AOBM3D303NZQ | | 80 | | Course4Re-LoadBala-1AOBM3D303NZQ-512663421.us-east-1.elb.amazonaws.com (A Record) | |

# Logging and Alerting Inventory

|  |  |
| --- | --- |
| **Log Source** | **Enabled** |
| **CloudWatch** | Yes |
| **CloudWatch** | Yes |

Establish Control

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

|  |  |
| --- | --- |
| **Action** | **Required Steps** |
| **Create IAM role for Automation Incident Response** | Create an IAM Role using SAC3T6FL01IAMROLE.txt |
| **Create Lambda function to automate the process** | Create the function using SAC4T6LF01.txt |
| **Add Tag to LAMP01** | {“Name”:”tag-key”,”Value”:” IR-Snapshot”} |

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

|  |  |
| --- | --- |
| **Action** | **Required Steps** |
| **Create a snapshot** | Run command:  *aws ec2 create-snapshot –volume vol-0ac551f00bedabfe9 –description “SAC4T4”* |
| **Implement Isolation and Containment** | 1. Create a new Security Group that blocks all incoming and outcoming traffic 2. Attach the Security Group to LAMP02 |

Recovery  
  
**Business Continuity Plan**

|  |  |  |
| --- | --- | --- |
| **Resource** | **Business Continuity Action** | **Status** |
| EC2 LAMP Servers | Implement Auto Scaling Groups | completed |
| Load balancer | Implemented for all EC2 instances | Completed |
| Applications | Implement cloudwatch and cloud trail for logging | completed |

# 

# 

# 