Purpose

This runbook outlines the investigation and remediation procedures for the “***Policy:IAMUser/RootCredentialUsage***” GuardDuty alert, which indicates that AWS root account credentials were used to perform actions in your environment. Usage of root credentials is a serious security concern and may indicate credential misuse or compromise.

Runbook Overview

The AWS root account has unrestricted permissions and should only be used in emergency scenarios. Regular use, especially for API calls, contradicts security best practices. This runbook helps security teams confirm whether root credentials were used legitimately and remediate any potential compromise.

Triggers

|  |  |  |
| --- | --- | --- |
| Trigger Name | Trigger Condition | Source |
| |  | | --- | | Root Credential Usage |  |  | | --- | |  | | |  | | --- | | An API call was made using AWS account root credentials |  |  | | --- | |  | | AWS GuardDuty, AWS CloudTrail |

Prerequisites

| Tools | Access and Permissions | Relevant Knowledge |
| --- | --- | --- |
| GuardDuty | GuardDuty console | Familiarity with AWS IAM concepts (root, IAM, STS), and interpreting GuardDuty and CloudTrail |
| CloudTrail | |  | | --- | | IAM permissions to access CloudTrail logs | | Familiarity with AWS IAM concepts (root, IAM, STS), and interpreting GuardDuty and CloudTrail |
| IAM | IAM entity configurations access cosole | Familiarity with AWS IAM concepts (root, IAM, STS), and interpreting GuardDuty and CloudTrail |

Escalation Point

|  |  |  |
| --- | --- | --- |
| Escalated From | Escalation Point | Escalation Condition |
| Contractor | CSIRT | When root credential usage is unauthorized or linked to sensitive API calls |
| CSIRT | CSIM | When there is confirmed or suspected compromise of AWS root credentials |

Investigation Steps

### **Identify Usage Context**

* + Extract the following from the GuardDuty alert:
    - **API call name**
    - **Time of request**
    - **Source IP address**
    - **User Agent**
  + Verify if the credential used is indeed the **root account** (UserType = Root).

### **Review CloudTrail Logs**

* + Search for additional root user activity in the time range before and after the event:

aws cloudtrail lookup-events --lookup-attributes AttributeKey=Username,AttributeValue=root

### **Determine Legitimacy**

* + Reach out to the primary AWS account owner or trusted admin to ask:
    - Was this root activity expected or authorized?
    - Was the activity executed from the listed source IP or device?

### **Review and Remove Root Access Keys (if any)**

* + Go to the **IAM dashboard** and check if the root account has access keys.
    - If so, **delete them immediately**:

aws iam delete-access-key --user-name root --access-key-id <key\_id>

### **Enable Root MFA**

* + If Multi-Factor Authentication (MFA) is not enabled on the root account, **enable it immediately**:  
    [Enable Root Account MFA](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html)

### **Audit and Restrict Further Activity**

* + Enable GuardDuty, AWS Config, and CloudTrail across all regions.
  + Check other high-privilege accounts for signs of misuse.
  + Disable or restrict root account access in operational runbooks.

## **Post-Incident Actions**

* Create an SCP (Service Control Policy) to **explicitly deny root account actions** (where applicable in AWS Organizations).
* If root credential exposure is suspected:
  + Rotate all IAM access keys.
  + Review recent changes made via the root account.
  + Re-evaluate the security of the email and phone associated with the AWS account.
* Use AWS Trusted Advisor to review credential hygiene.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Description of Change** |
| 19/06/25 | 1.0 | Ray Ferrufino | Initial Version |