Purpose

To provide a structured response to the AWS GuardDuty finding “Discovery:IAMUser/AnomalousBehavior,” which indicates that an IAM user's behavior deviated from historical norms and may reflect adversarial reconnaissance activity or a compromised IAM credential.

Runbook Overview

This runbook outlines the investigative and remediation steps for identifying, assessing, and responding to anomalous API activity generated by an IAM user in AWS. This detection is linked to reconnaissance tactics, where APIs like *ListAccessKeys, DescribeInstances*, and *GetRolePolicy* are called in an unusual pattern or context. The objective is to validate the legitimacy of the activity, prevent potential data exposure, and remediate compromised credentials.

Triggers

|  |  |  |
| --- | --- | --- |
| Trigger Name | Trigger Condition | Source |
| |  | | --- | | Discovery:IAMUser/AnomalousBehavior |  |  | | --- | |  | | GuardDuty finding indicating anomalous API activity for a single IAM identity | AWS GuardDuty |

Prerequisites

| Tools | Access and Permissions | Relevant Knowledge |
| --- | --- | --- |
| AWS CloudTrail  AWS IAM Console  AWS CLI (optional)  GuardDuty Console | IAM:ReadOnlyAccess  GuardDuty:ReadOnlyAccess  CloudTrail:LookupEvents  Permissions to disable access keys or revoke sessions | Understanding of AWS IAM policies and credential types  Familiarity with CloudTrail logs and GuardDuty findings  Knowledge of IAM access key types (AKIA vs. ASIA) |

Escalation Point

|  |  |  |
| --- | --- | --- |
| Escalated From | Escalation Point | Escalation Condition |
| Contractor | CSIRT | When there is confirmed impact to a system’s confidentiality, integrity, or availability |
| CSIRT | CSIM | When potential impact extends to business operations, systems, or data |

Investigation Steps

**Review GuardDuty Finding**

* Open the GuardDuty finding and extract the following:
  + IAM Entity Name and Type (user or role)
  + API called
  + Access key type (AKIA = long-term, ASIA = STS temporary)
  + IP address, AWS region, and timestamp of activity

**Identify the IAM Entity and Credential Type**

* Use the *User name* and *Access key ID* to determine if the IAM entity is a long-term user or a temporary STS role.
* Keys beginning with AKIA: Customer-managed access key (IAM user or root)
* Keys beginning with ASIA: Temporary security token (IAM role or temporary session)

**Verify CloudTrail Logs**

* Use CloudTrail to locate the sessionIssuer, userAgent, and source IP for the anomalous activity.
* Confirm if the activity aligns with known behavioral patterns for the IAM entity.

**Validate With User**

* Contact the IAM user (if known) to verify:
  + Whether they recognize the API call
  + If they used that IP address at the given time
  + Whether the access was expected

**Review IAM Permissions**

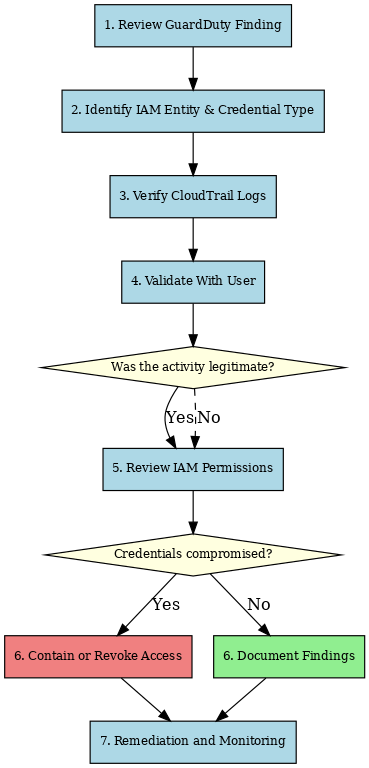
* In the IAM console, locate the entity and review its attached policies via the *Permissions* and *Access Advisor* tabs.
* Look for excessive or unnecessary permissions (e.g., wildcard \* actions).

**Contain or Revoke Access**

* If credentials are confirmed compromised or suspicious:
  + **AKIA (user key):** Disable access key, rotate keys
  + **ASIA (STS token):** Revoke active sessions
* Optionally, attach a deny-all policy to the user or role for emergency lockdown.

**Remediation and Monitoring**

* Rotate credentials and apply principle of least privilege.
* Enable CloudTrail logging if not already enabled.
* Consider enabling AWS Config rules to monitor IAM configuration drift.
* Re-enable access only after completing the review and hardening IAM policies.



Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Description of Change** |
| 2025-07-03 | 1.0 | Ray Ferrufino | Initial Version |