Incident Response Playbook: Cloud Account Compromise

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a structured incident response plan for handling cloud account compromise incidents across platforms such as Office365, AWS, and Azure. The objective is to minimize attacker impact, prevent data exfiltration, and restore secure access to cloud resources.

1.2 Scope

This playbook applies to all cloud services, user accounts, privileged accounts, and administrators of Office365, AWS, and Azure environments. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of Cloud Account Compromise

Cloud account compromise occurs when an attacker gains unauthorized access to cloud services through credential theft, phishing, brute force, or token/session hijacking. Compromised accounts can lead to email abuse, data exfiltration, resource hijacking (e.g., cryptomining), privilege escalation, and potential compliance/regulatory issues.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to respond to a cloud account compromise before it occurs.

- **Roles and Responsibilities:** Define roles (Incident Commander, Cloud Security Lead, Identity Lead, Legal, Communications).
- **Tools & Resources:** Ensure availability of SIEM, CASB, IdP logs, CloudTrail/Azure Activity Logs, audit logging, and forensic tools.
- **Training:** Conduct simulations of cloud account takeover scenarios.
- **Hardening Controls:** Enforce MFA, conditional access, least privilege, monitoring of risky sign-ins, and automated anomaly detection.
- **Contact Lists:** Maintain contacts for Microsoft, AWS, Azure support, executive leadership, and IR partners.
- **Threat Intelligence:** Monitor campaigns targeting Office365, AWS, and Azure accounts.

3.2 Phase 2: Identification & Analysis

Goal: To confirm cloud account compromise activity and determine its scope and severity.

1. **Initial Triage:** Review sign-in logs, CASB alerts, IdP logs, and correlate with threat intel.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:

- **Authentication:** Impossible travel logins, login from TOR/proxies, brute-force attempts.
- **Account:** Unexpected MFA disablement, unauthorized role assignments, mailbox forwarding rules (Office365).
- **Cloud Resources:** Creation of unauthorized EC2/Azure VMs, suspicious IAM activity.
- **Network:** Unusual data transfer volumes from cloud storage.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the operational impact, the criticality of the affected systems and data, and the scope of the compromise.

Level	Description	Example	MTTD	MTTR
Low	Single account suspicious login, no impact confirmed.	Office365 account login from unusual IP, user confirms legitimate activity.	6-12 hours	24 hours
Medium	Confirmed unauthorized login with limited activity.	AWS account logged in from unusual location but no changes made.	12-24 hours	2-3 days
High	Multiple accounts compromised with changes to resources or data.	Office365 mailbox rules created to auto-forward sensitive emails externally.	24-48 hours	4-7 days
Critical	Widespread compromise with critical business impact.	Attackers create privileged IAM roles, exfiltrating data and deploying cryptomining workloads.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious cloud account activity with other logs and threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as account compromise. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the cloud account compromise playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.
5. **Incident Declaration:** If confirmed, formally declare a cloud account compromise and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To limit the attacker's access and prevent further damage.

- **Short-Term Containment (Immediate Actions):**
  - Disable or suspend compromised accounts.
  - Block malicious IPs and revoke active access tokens/sessions.
  - Disable unauthorized mailbox rules or suspect IAM roles.

- **Evidence Preservation:** Acquire forensic logs (CloudTrail, Azure AD, Office365 Unified Audit Log) **before** remediation.
- **Long-Term Containment Strategy:** Review and tighten conditional access policies and identity protection controls.

3.4 Phase 4: Eradication

Goal: To remove attacker artifacts and prevent re-entry.

- **Root Cause Analysis:** Identify the entry vector (phishing, credential stuffing, etc.).
- **Artifact Removal:** Reset passwords and enforce MFA re-enrollment for affected accounts. Remove unauthorized IAM roles, mailbox rules, or API keys.
- **Persistence Removal:** Review and revoke any persistent attacker access methods (e.g., OAuth applications, service principals).
- **Security Hardening:** Patch vulnerabilities in IdP or cloud services.

3.5 Phase 5: Recovery

Goal: To safely restore accounts and cloud services.

- **System Restoration:** Restore accounts from a secure state and validate cloud services are uncompromised.
- **Enhanced Monitoring:** Increase monitoring of affected accounts and related cloud resources post-restoration.
- **Validation:** Ensure restored accounts are clean before re-enabling full production access.
- **Business Continuity:** Coordinate with business units to resume normal operations with enhanced monitoring.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem meeting within two weeks of incident closure with all stakeholders.
- **Final Incident Report:** Create a detailed report covering the attack path, timeline, root cause, and response actions.
- **Action Plan:** Create a tracked action plan to implement security improvements (e.g., improve access policies, enhance detection with anomaly alerts, enforce least privilege).

4 MITRE ATT&CK Framework Mapping

Cloud Account Compromise ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1078 – Valid Accounts*
  - *T1566 – Phishing*
  - *T1110 – Brute Force*
  - *T1539 – Steal Web Session Cookie*
- **Tactic: Persistence**
  - *T1098 – Account Manipulation*
  - *T1136 – Create Account*
  - *T1528 – Steal Application Access Token*
- **Tactic: Privilege Escalation**
  - *T1078.004 – Cloud Accounts*
  - *T1068 – Exploitation for Privilege Escalation*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses*
  - *T1070 – Indicator Removal on Host*
  - *T1556 – Modify Authentication Process*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping*
  - *T1621 – Multi-Factor Authentication Request Generation*
- **Tactic: Discovery**
  - *T1087 – Account Discovery*
  - *T1526 – Cloud Service Discovery*
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services*
  - *T1534 – Internal Spearphishing*
- **Tactic: Collection**
  - *T1114 – Email Collection*
  - *T1530 – Data from Cloud Storage Object*
- **Tactic: Exfiltration**
  - *T1567 – Exfiltration Over Web Service*
  - *T1041 – Exfiltration Over C2 Channel*
- **Tactic: Impact**
  - *T1496 – Resource Hijacking*
  - *T1485 – Data Destruction*