Scenario # 5 Incident Response Playbook

Table of Contents

Scenario 5 – By Default Cloud Service Provider Privileges (AWS S3 Misconfiguration)

Organization: Viva la Vita Online
Playbook Version: 2.0
Last Updated: December 3, 2025

1. Introduction

Objective: The objective of this section is to define the scope, assumptions, and stakeholders involved in responding to cloud misconfiguration incidents caused by overly permissive default IAM policies. This ensures that all team members understand when to use this playbook and what operational expectations apply.

1.1 Incident type

This playbook is designed for cloud-based security incidents where sensitive or regulated data becomes accessible due to default cloud service provider privileges. These include incidents where AWS, Azure, or GCP default-managed IAM policies grant excessive read or list permissions, resulting in unauthorized access by internal users, external vendors, or third-party service providers.

This playbook covers incidents involving:

- Data leakage or data breach caused by cloud IAM misconfigurations
- Over-privileged IAM roles (e.g., AWS “ReadOnlyAccess”)
- Unauthorized vendor access to sensitive S3 data
- Violations of least-privilege principles
- Improper S3 bucket segmentation (shared environments)
- Unauthorized viewing or exfiltration of tax, financial, or personal data

1.2 Assumptions

For the purposes of this playbook, the following assumptions are made:

- AWS CloudTrail and S3 Access Logs are enabled with ≥90-day retention.
- Sensitive tax data is properly classified but stored in shared S3 environments.
- Vendor access is documented but may not undergo rigorous least-privilege review.
- Third-party Data Handling Agreements (DHAs) may not enforce minimum privilege controls.
- All IAM and S3 changes are logged and attributable.
- Impacted S3 buckets cannot be offline due to business operations.
- SOC/IRT has authority to modify IAM roles and S3 policies for containment actions.

1.3 Audience

This Playbook is intended for the following audiences:

- Incident Response Team (IRT)
- SOC Analysts / Cloud Security Analysts
- Cloud Engineering / DevOps
- Legal, Compliance and Privacy Office
- Vendor Management
- Senior Leadership (if required for breach notification decisions)

According to NIST SP 800-61r2, organizations should clearly define incident types, roles, responsibilities, and assumptions to ensure coordinated and effective incident response (NIST SP 800-61r2, §2.3).

2. Preparation

Objective: The objective of this section is to ensure all required tools, configurations, communication channels, and readiness processes are in place before an incident occurs. Preparation ensures the organization maintains a state of operational readiness and can act quickly, consistently, and effectively.

2.1 Tools and Resources

The following tools, technologies, and resources must be available and routinely maintained to ensure rapid and effective response:

Cloud Security Tools

- AWS IAM Console
- AWS CloudTrail & CloudWatch Logs
- AWS S3 Server Access Logs
- AWS IAM Access Analyzer (for privilege validation)
- AWS Macie (recommended for sensitive data discovery and leakage detection)

Enterprise Security Tools

- IBM QRadar SIEM 7.5
- Tenable Nessus 10.6 (cloud misconfiguration scanning)
- Suricata IPS 6.0.15
- Fortinet FortiGate firewall logs
- Symantec Endpoint Protection 14.3

Forensic & Response Resources

- Chain-of-custody templates
- Secure evidence storage (encrypted)
- Log archival tools
- Secure workspace for cross-team response coordination

Periodic Requirements

- Quarterly IAM privilege and access reviews
- Annual Cloud Security Posture Review (CSPR)
- Third-party access auditing aligned with vendor management policy
- Continuous review of S3 bucket policies, ACLs, and default AWS managed policies

2.2 Communication Channels

Primary Channels

- Encrypted IR Slack/Teams channels
- Internal ticketing systems
- SOC 24/7 hotline

Secondary Channels

- Secure encrypted corporate email
- Emergency IR conference bridge

Tertiary Channels (as needed)

- Legal privacy-breach hotline
- Public relations (only after executive authorization)

Communication Requirements

- Strict need-to-know and least-privilege communication
- No transmission of regulated or tax data in plaintext
- All communication must be logged for audit and post-incident review
- All stakeholder notifications must follow formal internal escalation paths

NIST highlights that preparation including tools, communication plans, and evidence handling procedures is essential to ensure timely and efficient incident response (NIST SP 800-61r2, §3.1).Proper chain-of-custody processes should be established to maintain the integrity of evidence during response activities (NIST SP 800-61r2, §3.2.4).

3. Identification

Objective: This section defines how incidents are detected, validated, escalated, and initially assessed. The objective is to ensure early identification of unauthorized access and accurate scoping of potential exposure.

3.1 Incident Detection Methods

Incident discovery may occur through any of the following mechanisms:

- CloudTrail events showing unauthorized GetObject / ListBucket requests
- QRadar alerts flagging anomalous S3 access
- Vendor notifications
- S3 Access Logs showing abnormal access patterns
- IAM Access Analyzer excessive privilege alerts
- AWS billing anomalies due to unexpected data egress
- Discovery of misconfigured IAM roles during routine review

3.2 MITRE ATT&CK Techniques

- T1530
- T1526
- T1078
- T1087
- T1567

3.3 Incident Reporting Mechanism

- All suspected or confirmed cloud data exposure incidents must be reported through the organization's internal IR reporting process.
- SOC analysts triage all regulated-data alerts within 15 minutes.
- High-risk incidents must be escalated to:
    - Legal & Compliance
    - Data Protection Officer / Privacy Office
    - Senior Leadership
    - Vendor Management
- All reports must be logged in the ticketing and SIEM platform.

3.4 Initial Assessment Procedure

1. Confirm unauthorized access to S3 bucket resources by a third-party entity.
2. Determine the classification of accessed data (regulated tax information).
3. Identify which IAM entity (role, access key, user) performed the actions.
4. Review object-level and bucket-level access logs.

5. Establish the time window of exposure.
6. Assess whether data was viewed, accessed, or exfiltrated.
7. Validate whether access violated contractual vendor restrictions.
8. Conduct breach impact scoring per internal standards.
9. Notify legal, privacy, and leadership if impact exceeds defined thresholds.

NIST requires organizations to analyze alerts, logs, and indicators of compromise to verify incidents and establish initial scope (NIST SP 800-61r2, §3.2).NIST also recommends maintaining detailed documentation during initial detection and triage to support later stages of the response (NIST SP 800-61r2, §3.2.7).

4.Containment

Objective: The objective of containment is to immediately stop the unauthorized access, secure impacted cloud resources, preserve evidence, and prevent further exposure while maintaining operational continuity wherever possible.

4.1 Short-Term Containment Strategies

Actions steps:

1. Alert the Incident Response Team

- SOC notifies IRT and activates cloud IR protocol.
- Assign IR Lead, Cloud SME, and Forensics Lead.

2. Isolate Affected Cloud Resources

- Disable or suspend third-party IAM roles.
- Remove AWS “ReadOnlyAccess” from vendor accounts.
- Revoke excessive S3 permissions.
- Block external access to impacted buckets.

3. Contain Exposure

- Apply deny-all bucket policy temporarily.
- Rotate/disable IAM access keys.
- Disable S3 object sharing and cross-account access.
- Freeze IAM configurations.

4. Identify Scope of Unauthorized Access

- Review CloudTrail logs and S3 access logs.
- Identify accessed objects and data exfiltration.
- Define exposure timeframe.

5. Preserve Evidence

- Export CloudTrail logs securely.
- Snapshot S3 bucket policies and IAM configurations.
- Log every action with timestamps.

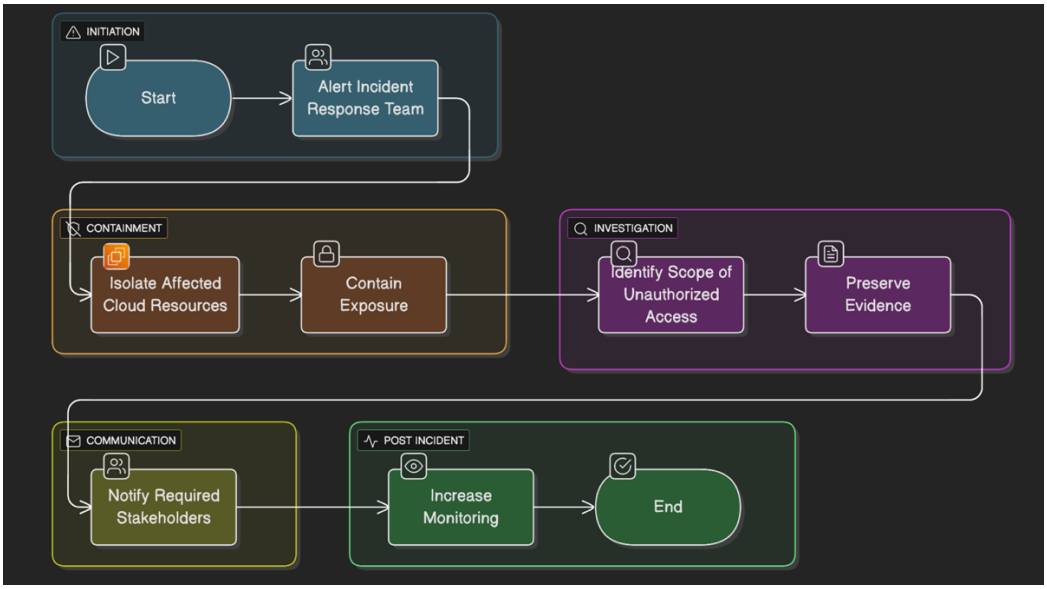
6. Notify Required Stakeholders

- SOC Manager, CISO, Legal, Privacy, Vendor Management.

7. Increase Monitoring

- Enable real-time CloudTrail alerts.
- Monitor S3 egress volumes.
- Enable QRadar cloud-misuse correlation rules.

4.1.1 Activity Diagram- Short-Term Containment



4.2 Long-Term Containment Measures

- Implement custom least-privilege IAM policies to replace broad AWS managed policies, ensuring that all permissions are tightly scoped to necessary S3 resources.
- Restrict all vendor access to approved S3 bucket prefixes only, preventing unauthorized viewing of sensitive or regulated data.
- Require multi-party approval, such as from Cloud Security and Vendor Management, for all vendor IAM permission changes to prevent privilege escalation.

- Enforce strict S3 access segmentation by separating buckets based on data sensitivity levels, reducing exposure and limiting unauthorized access routes.
- Enable automated alerts to detect anomalous IAM role activity, including unusual S3 access patterns, unexpected permissions changes, or high-risk operations.
- Conduct quarterly vendor access audits to verify privilege usage, identify unnecessary permissions, and ensure compliance with Data Handling Agreements.

NIST states that containment strategies must limit the damage, prevent further unauthorized access, and preserve evidence for subsequent forensic investigation (NIST SP 800-61r2, §3.3.1). Containment strategies should be selected based on potential damage, evidence preservation requirements, and operational impact (NIST SP 800-61r2, §3.3.1).

5. Eradication

Objective: The objective of eradication is to remove misconfigurations, eliminate root causes, and restore the cloud environment to a secure baseline to prevent recurrence.

5.1 Root Cause Analysis

Identify the chain of technical and governance failures that allowed unauthorized access.

Root Cause Factors:

- AWS "ReadOnlyAccess" policy granted broad, excessive permissions.
- Vendor role inherited policy without security review.
- S3 buckets not segmented by sensitivity.
- Vendor governance process lacked least-privilege enforcement.
- No explicit deny policies on sensitive buckets.
- No automated IAM validation or policy-as-code controls.

5.2 Eradication Procedures

- Replace "ReadOnlyAccess" with custom least-privilege IAM policies.
- Re-segment S3 buckets by sensitivity.
- Enable SSE-KMS encryption and object-level logging.
- Rotate or revoke all IAM access keys involved.
- Update vendor Data Handling Agreements with security requirements.
- Implement IAM guardrails (AWS Config, SCPs).
- Conduct a full IAM/S3 permission hygiene audit.

NIST specifies that eradication activities should remove malicious artifacts, fix exploited vulnerabilities, and address underlying weaknesses that enabled the incident (NIST SP 800-61r2, §3.3.2).

6. Recovery

Objective: The objective of recovery is to restore secure operations, verify that no unauthorized access persists, and ensure systems return to a compliant and functional state.

6.1 System Restoration Process

- Restore vendor access only under least-privilege configurations.
- Re-enable IAM roles after Cloud Security approval.
- Remove deny-all ACLs once validated as safe.
- Reopen production pipelines after full verification.

6.2 Validation Checks

Ensure full remediation, validate secure configuration, and confirm that no additional exposure occurred. Validation Checklist:

- Review the last 48–72 hours of CloudTrail logs to confirm no repeat or ongoing access anomalies.
- Ensure there are no additional unauthorized S3 access attempts or abnormal data egress patterns.
- Validate that IAM roles and policies align with vendor contract requirements and least-privilege principles.
- Confirm proper S3 bucket segmentation and permission isolation based on data sensitivity levels.
- Perform regulatory or compliance breach notifications, where applicable under privacy or tax-data regulations.

6.3 Ongoing Monitoring

- Weekly access monitoring for the first month, focusing on vendor behavior, S3 activity, and IAM role usage.
- Monthly scans using IAM Access Analyzer to detect unintended privilege creep or cross-account access.
- Quarterly IAM and vendor-access audits to confirm ongoing compliance with policies and contracts.
- Annual review of overall cloud permission architecture, S3 segmentation, and vendor security requirements.

NIST requires organizations to restore impacted systems to normal operations while thoroughly validating that vulnerabilities are eliminated and monitoring for signs of recurring issues (NIST SP 800-61r2, §3.3.3)

7. Post-Incident Activity

Objective: The objective of post-incident activities is to ensure lessons learned are captured, systemic weaknesses are corrected, and a fully documented incident report is prepared for compliance and governance purposes.

7.1 Lessons Learned Session

A formal Lessons Learned session must be conducted within five (5) business days after containment and recovery. The purpose is to evaluate the response, identify gaps in IAM governance, and ensure cloud security improvements are integrated into long-term strategy. The Incident Response Team is responsible for coordinating the session and ensuring all relevant stakeholders contribute. Key discussion and documentation points include:

- Must occur within 5 business days.
- Validate timeline accuracy from detection to recovery.
- Identify governance failures (IAM, vendor oversight).
- Identify prevention improvements (alerts, guardrails, policies).
- Determine required vendor contract revisions.
- Define updates to S3 segmentation, IAM controls, CloudTrail, monitoring.

7.2 Incident Report Writing

A comprehensive incident report must be prepared by the Incident Response Team and approved by the CISO. The report serves as the authoritative record and may be used for compliance audits, regulatory inquiries, and vendor management follow-ups.The final report should include the following sections:

- Executive Summary
- Data Impact Assessment
- Timeline of Events
- Discovery & Identification
- Root Cause Analysis
- Containment & Eradication Summary
- Regulatory Notifications
- Preventive Measures Implemented
- CISO/IR Manager Sign-Off

NIST recommends that organizations conduct a Lessons Learned meeting shortly after the incident to review what happened, assess response performance, and identify improvements (NIST SP 800-61r2, §3.4). NIST also requires maintaining comprehensive incident documentation to support audits, investigations, and long-term process improvement (NIST SP 800-61r2, §3.4.2).

References

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). Guide for cybersecurity event recovery. *Guide for Cybersecurity Event Recovery*. https://doi.org/10.6028/nist.sp.800-184

CISA. (2021). *Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*. https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2