Incident Response Playbook: Data Exfiltration via Cloud Storage

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 **3**
- 1.1 Purpose . . . 3
- 1.2 Scope . . . 3

2 Overview of Data Exfiltration via Cloud Storage **3**

3 Incident Response Phases **3**
- 3.1 Phase 1: Preparation . . . 3
- 3.2 Phase 2: Identification & Analysis . . . 3
- 3.3 Phase 3: Containment . . . 4
- 3.4 Phase 4: Eradication . . . 5
- 3.5 Phase 5: Recovery . . . 5
- 3.6 Phase 6: Post-Incident Activities (Lessons Learned) . . . 5

4 MITRE ATT&CK Framework Mapping **6**

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a structured incident response plan for handling data exfiltration incidents via cloud storage services (e.g., OneDrive, Google Drive, Dropbox, AWS S3, Azure Blob). The objective is to detect unauthorized data transfers, prevent further data loss, and ensure compliance with regulatory requirements.

1.2 Scope

This playbook applies to all cloud storage accounts, associated user accounts, privileged roles, and connected applications. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of Data Exfiltration via Cloud Storage

Data exfiltration via cloud storage occurs when sensitive or proprietary data is uploaded, synced, or shared externally without authorization. Attackers may use compromised accounts, insider threats, or malicious applications to transfer data to personal or attacker-controlled cloud storage services. This poses risks of intellectual property theft, compliance violations, reputational damage, and regulatory fines.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure readiness to detect and respond to cloud data exfiltration incidents.

- **Roles and Responsibilities:** Define roles (Incident Commander, Cloud Security Lead, Data Protection Officer, Legal, Communications).
- **Tools & Resources:** Ensure availability of CASB, SIEM, DLP, IdP logs, and cloud activity monitoring tools.
- **Training:** Conduct simulations of insider threat and data exfiltration scenarios.
- **Contact Lists:** Maintain contacts for Microsoft, Google, AWS, and IR vendors.
- **Threat Intelligence:** Monitor campaigns targeting cloud storage misuse and data theft.

3.2 Phase 2: Identification & Analysis

Goal: To confirm data exfiltration via cloud storage and determine its scope and severity.

1. **Initial Triage:** Review CASB alerts, DLP logs, cloud storage audit logs, and correlate with threat intelligence.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
    - **Authentication:** Suspicious logins before large uploads, use of personal cloud accounts on corporate devices.

- **Data:** Large-scale uploads, downloads, or sync operations outside business hours.
- **Sharing:** Creation of unauthorized external sharing links.
- **Applications:** OAuth apps with broad data access permissions.

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 unusual upload detected with no sensitive data confirmed.	User uploads personal files to Google Drive from a corporate laptop.	6–12 hours	24 hours
Medium	Suspicious upload of potentially sensitive data, limited to one account.	An employee uploads a set of internal documents to their personal Dropbox account.	12–24 hours	2–3 days
High	Confirmed sensitive data uploaded or shared externally, multiple accounts involved.	A sales team account exfiltrates the customer database to a personal OneDrive account.	24–48 hours	4–7 days
Critical	Large-scale data exfiltration involving highly sensitive intellectual property or regulated data.	A compromised privileged account uploads gigabytes of intellectual property to an AWS S3 bucket controlled by attackers.	48 hours	7–14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious uploads or sharing activity with other data points and threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as unauthorized data exfiltration. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the cloud data exfiltration playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning DLP/CASB rules.
5. **Incident Declaration:** If confirmed, formally declare a data exfiltration incident and escalate to leadership, legal, and compliance teams.

3.3 Phase 3: Containment

Goal: To stop active data exfiltration and prevent further data loss.

- **Short-Term Containment (Immediate Actions):**
  - Disable affected user accounts and revoke active sessions.
  - Block external sharing and unauthorized OAuth applications.
  - Quarantine suspicious files and revoke public sharing links.
- **Evidence Preservation:** Acquire and preserve forensic artifacts (CASB, DLP, and cloud storage logs) **before** remediation.

- **Long-Term Containment Strategy:** Enforce stricter conditional access policies to block unmanaged devices.

3.4 Phase 4: Eradication

Goal: To remove the attacker's foothold and remediate the root cause.

- **Root Cause Analysis:** Identify the entry vector (e.g., compromised credentials, insider threat, misconfiguration).
- **Access Removal:** Remove unauthorized apps and access tokens.
- **Account Security:** Reset passwords and re-enforce MFA for compromised accounts.
- **Security Hardening:** Patch vulnerabilities in IdP or cloud platforms and enforce strict DLP rules.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- **System Restoration:** Restore normal account access with secure configurations.
- **Enhanced Monitoring:** Increase monitoring of cloud storage logs for signs of recurrence.
- **Validation:** Ensure no unauthorized apps or sharing links remain before full restoration.
- **Business Continuity:** Coordinate with leadership to resume business operations safely.

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

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem with security, legal, compliance, and cloud teams.
- **Final Incident Report:** Create a detailed report covering the timeline, scope, impact, and root cause.
- **Action Plan:** Create a tracked action plan to enhance DLP, CASB, and anomaly detection policies and train employees.

4 MITRE ATT&CK Framework Mapping

Data Exfiltration via Cloud Storage ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1078 – Valid Accounts*
  - *T1566 – Phishing*
  - *T1190 – Exploit Public-Facing Application*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping*
  - *T1556 – Modify Authentication Process*
- **Tactic: Persistence**
  - *T1098 – Account Manipulation*
  - *T1136 – Create Account*
- **Tactic: Privilege Escalation**
  - *T1078 – Valid Accounts*
- **Tactic: Defense Evasion**
  - *T1070 – Indicator Removal on Host*
  - *T1562 – Impair Defenses*
- **Tactic: Discovery**
  - *T1087 – Account Discovery*
  - *T1526 – Cloud Service Discovery*
- **Tactic: Collection**
  - *T1114 – Email Collection*
  - *T1530 – Data from Cloud Storage*
- **Tactic: Exfiltration**
  - *T1567.002 – Exfiltration to Cloud Storage*
  - *T1041 – Exfiltration Over C2 Channel*
- **Tactic: Impact**
  - *T1485 – Data Destruction*
  - *T1486 – Data Encrypted for Impact*