Incident Response Playbook: Data Exfiltration & Cloud-Related Activity

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Quarterly or after major incident
Approver	SOC Manager / Head of IR

Contents

1 Introduction

1.1 Purpose

This playbook provides operational guidance for detecting, triaging, containing, investigating, eradicating, and recovering from incidents involving **Data Exfiltration & Cloud-Related Activity**. It targets scenarios where attackers or misconfigured systems move sensitive data out of the environment using cloud storage, file transfer protocols, or abused API keys. Intended audience: SOC analysts, cloud security engineers, incident responders, DevOps, legal/compliance, and leadership.

1.2 Scope

Applies to cloud storage (S3, Azure Blob, Google Cloud Storage, OneDrive, SharePoint), managed file services (FTP, SFTP, SCP), CI/CD pipelines, secrets in source control, service accounts and API keys, CASB/CSPM telemetry, DLP systems, and associated network/perimeter logs.

2 Overview of the Category

2.1 Definition

Data Exfiltration & Cloud-Related Activity covers unauthorized movement of sensitive data outside the organisational boundaries using cloud storage, file transfer mechanisms, or programmatic APIs. This includes accidental exposure (misconfigured buckets), deliberate exfil using compromised credentials or API keys, and covert staging via third-party cloud services.

2.2 Common Attack Chain

1. **Credential / Key Acquisition:** stolen user credentials, leaked API keys, compromised CI secrets, or abused service principals.
2. **Discovery:** attacker enumerates accessible storage, directories, or shares (S3 buckets, SharePoint sites, FTP locations).
3. **Collection / Staging:** attacker collects sensitive files locally or stages them in cloud storage under attacker-controlled buckets or accounts.
4. **Transfer / Exfiltration:** uploads to external cloud storage, FTP/SCP transfers to external hosts, or use of API calls to copy data out.
5. **Cleanup / Persistence:** attacker deletes logs, rotates keys, or leaves backdoors to resume exfiltration.

2.3 Primary Risks & Business Impact

- Exposure of regulated or sensitive data (PII, financials, IP).
- Data leakage to competitor or public repositories causing reputational and legal exposure.
- Long-term persistence via exposed access keys, service principals or malicious cloud resources.
- Financial and operational impacts including incident response costs and potential regulatory fines.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	Example	MTTD	MTTR
Critical	Confirmed large-scale exfiltration of sensitive data to external cloud storage or public internet, or systemic leak of long-lived API keys enabling broad access.	Multiple GBs of PII copied to attacker S3 and publicized.	$\leq$ 15 min	Contain within 4 hrs; recovery 24–72 hrs.
High	Confirmed exfiltration of limited sensitive datasets or discovery of abused API keys actively used to pull data.	Several confidential documents uploaded to external SCP server.	$\leq$ 1 hr	6–24 hrs.
Medium	Suspicious file transfer patterns or detection of anomalous API usage without confirmed sensitive-data access.	Large number of downloads from a non-standard account flagged by DLP.	$\leq$ 2 hrs	12–48 hrs.
Low	Single failed or blocked file transfer or misconfiguration flagged by automated scans (no confirmed data copied).	Public S3 bucket found but no evidence of downloads.	$\leq$ 4 hrs	Monitor / minor remediation within 24–72 hrs.

Table 1: Severity Matrix - Data Exfiltration & Cloud-Related Activity

4 Tools & Preparation (Recommended)

- **Cloud Monitoring:** CloudTrail, AzureActivity, GCP Audit Logs, Office365 audit logs, and CASB solutions.
- **DLP / Data Classification:** DLP engines for cloud/email, automated data discovery and classification, and content fingerprinting.
- **Secrets Management & Scanning:** Secrets managers (Vault), automated secret scanning for repos (truffleHog, git-secrets), CI/CD secret scanning.
- **Network Transfer Monitoring:** Proxy logs, egress firewall logs, NetFlow, FTP/SFTP server logs, and S3/Blob access logs.
- **EDR / Forensics:** Endpoint captures, filesystem activity monitoring, process trees, memory dumps.
- **Playbook Resources:** Cloud provider emergency contacts, registrar/hosting abuse contacts, legal/compliance templates for breach notification.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- DLP alerts for sensitive content uploaded to external cloud or attachments emailed externally.

- Cloud audit logs showing 'PutObject', 'CopyObject', or 'CreateBucket' events to external accounts or unusual locations.
- Unusual SCP/FTP transfers in network logs, or elevated volumes of outbound data from a host.
- Alerts from secret-scanning tools indicating leaked API keys in public repositories.

Quick actions:

- Validate alert, determine affected files/users/accounts, and classify severity using the Severity Matrix.
- Preserve relevant logs (CloudTrail, WAF, proxy, FTP logs), and capture endpoint artifacts (file timestamps, process lists).
- If keys or tokens are involved, immediately identify scope (which services they grant) and prepare to revoke/rotate.

5.2 Containment (Immediate / Short-term)

- Revoke or rotate compromised API keys, service principals, and user credentials; suspend affected accounts.
- Block destination IPs/buckets where feasible, or apply cloud provider object-level access controls to prevent further access.
- Isolate or quarantine involved endpoints to prevent additional data transfers.
- For suspected accidental exposure (misconfiguration), restrict bucket permissions and enable object-level MFA delete where supported.

5.3 Investigation & Forensic Triage

- Collect CloudTrail/AzureActivity/GCP logs, S3/Blob access logs, object metadata (timestamps, requester, requester IP), and DLP findings.
- Retrieve FTP/SCP server logs, firewall/egress logs, and endpoint forensic artifacts (file copies, process history).
- Determine what data was exposed (file hashes, names, classification) and whether data was downloaded or publicly shared.
- Identify the vector of exposure: misconfig, leaked key, compromised account, or malicious insider.

5.4 Eradication

- Remove attacker-staged objects where permissible (coordinate with Legal if deletion affects evidence).
- Revoke and rotate credentials, rebuild compromised endpoints where integrity suspect, and remove unauthorized accounts.
- Fix configuration issues (bucket policies, ACLs), implement least-privilege IAM roles, and enforce object encryption at rest.
- Implement automated secret scanning and CI/CD checks to prevent future key leaks.

5.5 Recovery

- Restore systems from trusted backups if corruption occurred; validate data integrity and restore service access carefully.
- Reissue credentials and re-enroll service accounts with short-lived, rotated credentials and use role-based access patterns.
- Monitor the environment closely for re-use of revoked keys or evidence of secondary exfiltration for at least 60–90 days.

5.6 Post-Incident Activities

- Prepare full incident report (timeline, indicators, impacted data) and notify stakeholders / regulators as required.
- Update DLP and detection rules, enforce stricter IAM policies, and refine secret-scanning thresholds.
- Conduct lessons-learned, adjust cloud security posture (CSPM), and run tabletop exercises simulating key-leak scenarios.

6 MITRE ATT&CK Framework Mapping

Data Exfiltration & Cloud-Related Activity - ATT&CK Mapping

- **Exfiltration:** T1041 (Exfiltration Over C2 Channel), T1537 (Transfer Data to Cloud Account), T1567 (Exfiltration Over Web Service)
- **Credentials / Keys Abuse:** T1078 (Valid Accounts), T1552 (Unsecured Credentials)
- **Defense Evasion:** T1070 (Indicator Removal on Host), T1027 (Obfuscated Files)
- **Collection:** T1074 (Data Staged)

7 Key Telemetry & Logs to Collect

- Cloud provider audit logs (CloudTrail, AzureActivity, GCP Audit), S3/Blob object access logs and metadata.
- DLP alerts and content fingerprints, email gateway logs, and SharePoint/OneDrive access logs.
- FTP/SFTP/SCP server logs, proxy logs, and egress firewall logs (source/destination IPs, bytes transferred).
- CI/CD logs, build artifacts, repository activity logs, and secret-scanning tool alerts.
- Endpoint forensic artifacts (file copies, opened files, processes, memory dumps).

8 Subcategory Scenarios (Realistic)

Note: The scenarios below are operational SOC/IR narratives — each includes detection, investigation steps, containment actions, eradication, recovery and lessons learned.

Scenario A: Data Exfiltration via Cloud Storage

Summary: An attacker uses a compromised developer's long-lived AWS access key (committed to a public GitHub repo) to copy several backup snapshots from internal S3 buckets to an attacker-controlled S3 bucket in another region. The S3 objects include database dumps containing customer PII.

Detection:

- CloudTrail: 'CopyObject' and 'PutObject' events showing data movement to an external bucket under an unfamiliar AWS account ID.
- DLP: matches on PII fingerprints for objects uploaded to external bucket.
- Secret-scanning alert: internal tool flagged an exposed AWS key in a public repository (correlates temporally).

Investigation & Actions:

1. **Triage & classification:** Classified as *Critical* due to exfiltration of PII to an external account.
2. **Immediate containment:** Revoke the compromised AWS access key and disable the implicated IAM user; block the external bucket and associated IPs if possible.
3. **Forensic collection:** Collect CloudTrail logs, S3 object metadata (timestamps, requester, request IDs), and copy hashes for evidence; preserve the Git commit showing the key exposure.
4. **Hunt:** Search for other leaked keys and other buckets/objects accessed with the same key or IP ranges.

Containment & Eradication:

- Delete or restrict access to attacker-staged objects (coordinate with Legal). Rotate all affected credentials and implement short-lived roles (assume-role) and MFA for sensitive operations.
- Revoke any third-party access and remove unauthorized IAM roles/policies the attacker created.
- Patch the CI/CD and developer workflows to prevent commits of secrets (pre-commit hooks, scanning).

Recovery:

- Restore affected systems from known-good backups if necessary and validate database integrity.
- Notify affected customers and regulatory bodies as required; provide remediation guidance.
- Implement proactive scanning for leaked credentials and run a full secrets audit across repositories and artifacts.

Outcome & Lessons:

- Root cause: hard-coded, long-lived credentials committed to public repository. Mitigations: enforce secrets manager use, rotate existing keys, enforce automated secret scanning and short-lived credentials.

Scenario B: Suspicious File Transfer (FTP / SCP)

Summary: Network logs show a developer workstation making repeated SCP connections to an external IP late at night. A large number of files from '/mnt/backups/finance' were transferred. The developer account had been phished and reused credentials on external machines.

Detection:

- Egress firewall/NetFlow: outbound SCP sessions to an external IP with large byte counts during non-business hours.
- DLP: alerts on transfer of files with financial patterns when inspected by proxy.
- Endpoint EDR: process 'scp' spawned from user shell with a sequence of file reads from backup mount.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to confirmed transfer of finance backups.
2. **Immediate containment:** Block destination IP at edge and isolate the developer workstation; disable the user's account pending investigation.
3. **Forensic collection:** Collect NetFlow records, SCP server logs (if accessible), endpoint process logs, and copies/hashes of transferred files where possible.
4. **Hunt:** Search for other hosts communicating with the same destination and for similar transfers from other accounts.

Containment & Eradication:

- Remove malware or malicious agents from developer workstation; reimage if persistence suspected.
- Rotate credentials for the user and any service accounts the workstation could access; tighten remote-transfer policies.
- Deploy egress filtering rules to restrict SCP/FTP to whitelisted destinations and require VPN or bastion for administrative transfers.

Recovery:

- Restore the developer workstation from a clean image and ensure no residual exfil tooling remains.
- Review backup access patterns and introduce stricter access controls and monitoring for backup stores.

Outcome & Lessons:

- Root cause: credential theft enabling direct SCP transfers. Mitigations: restrict direct outbound SCP/FTP, require bastion access for transfers, and improve phishing resilience and monitoring.

Scenario C: Suspicious API Key Usage (Leaked / Abused API Keys)

Summary: A CI job executed with a service account that used an API key with broad permissions. The key was present in a legacy CI variable and was used by an attacker to enumerate and download sensitive artifacts to an external repository.

Detection:

- CI/CD logs: job steps spiking in activity and pulling artifacts not typical for the pipeline.
- Secret-scan: retrospective scan identified the API key in an older pipeline config file.
- Cloud logs: API calls from the CI service principal to list and get object contents in production artifact storage.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to API key abuse and potential artifact/-data theft.
2. **Immediate containment:** Revoke the API key and disable the affected CI variable; suspend the implicated CI runner if needed.
3. **Forensic collection:** Gather CI logs, timestamps, job traces, and cloud audit logs showing the API calls; capture any downloaded artifacts' hashes.
4. **Hunt:** Search for other legacy credentials in CI and repos; pivot on the API key to find other accessed resources.

Containment & Eradication:

- Rotate and replace keys with short-lived tokens, migrate to role-assumed ephemeral credentials, and remove legacy variables from CI systems.
- Implement least-privilege service accounts for CI and restrict artifact repositories to authorized runners.
- Enforce automated scans for secrets in repos and CI variables on pre-merge and pre-deploy stages.

Recovery:

- Validate integrity of artifacts and rebuild any compromised pipelines; rotate any keys used by the CI ecosystem.
- Conduct a secrets audit and mandatory remediation for all identified exposed credentials.

Outcome & Lessons:

- Root cause: stored long-lived API keys in CI with excessive permissions. Mitigations: adopt short-lived tokens, secrets manager integration, strict IAM roles for CI, and automated secret scanning.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

AWS CloudTrail: find 'PutObject' to external buckets (example)

```
SELECT eventTime, userIdentity.arn, eventName, requestParameters.bucketName,
requestParameters.key, sourceIPAddress
FROM cloudtrail_logs
WHERE eventName IN ('PutObject','CopyObject')
AND requestParameters.bucketName NOT LIKE '%our-corp-bucket-prefix%'
AND eventTime >= date_sub('day', 7, current_date)
```

Splunk: detect large outbound SCP/FTP transfers (example)

```
index=network sourcetype=netflow dest_port IN (20,21,22)
| stats sum(bytes) as total_bytes by src_ip, dest_ip
| where total_bytes > 100000000
```

Kusto / Sentinel: find suspicious API key usage in AzureActivity

```
AzureActivity
| where TimeGenerated > ago(7d)
| where OperationNameValue contains "Storage" and Identity contains "ci-service"
| project TimeGenerated, Caller, OperationName, Resource, CallerIpAddress
```

9.2 Appendix B — Forensic Artifact Locations

- Cloud: CloudTrail, S3/Blob object metadata, presigned URL logs, AzureActivity, GCP access logs.
- CI/CD: pipeline job logs, runner logs, variable/secret stores, and historical configs.
- Endpoint: filesystem copies of transferred files, process history, shell history, and EDR captures.
- Network: NetFlow/IPFIX, proxy logs, FTP/SFTP server logs, and PCAPs for transfer windows.
- DLP: content fingerprint matches, policy triggers, and quarantined object metadata.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Playbook invoked.
- Affected data sets (classifications), accounts/keys involved, and destination of exfiltrated data.
- Evidence preserved (CloudTrail, S3 metadata, NetFlow, EDR dumps) and IOCs (IPs, bucket names, API keys patterns).
- Actions taken (containment, eradication, recovery) with timestamps and owners.
- Root cause analysis, remediation actions, policy changes, and follow-up items.
- Notifications performed (customers, regulators), legal coordination, and lessons learned.