Incident Response Playbook: Suspicious API Key Usage

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 process for detecting and responding to suspicious API key usage—whether due to leaked, stolen, or abused API keys. The objective is to quickly identify unauthorized use, revoke or rotate compromised credentials, and limit impact to services and data.

1.2 Scope

This playbook applies to all API keys, service principals, application credentials, secrets stored in cloud/provider platforms, and systems that consume or issue API keys (e.g., CI/CD, cloud services, SaaS integrations). It covers detection, containment, eradication, recovery, and post-incident activities.

2 Overview of Suspicious API Key Usage

API keys and service credentials enable machine-to-machine authentication. If leaked or abused, attackers can access cloud resources, exfiltrate data, spin up resources, or perform fraudulent actions. Detecting unusual API key usage patterns early is essential to limit damage.

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 API key compromise.

- **Roles and Responsibilities:** Define roles (Incident Commander, Cloud Security Lead, DevOps/Platform Lead, IAM Lead, Communications Lead).
- **Tools & Resources:** Ensure availability of SIEM, CASB, CloudTrail/Activity Logs, secret scanning tools, IAM audit logs, and forensic tools.
- **Training:** Conduct drills for secret leakage scenarios and secret-rotation exercises.
- **Hardening Controls:** Implement secret scanning in CI/CD, rotate keys regularly, use short-lived credentials and managed identities, enforce least privilege.
- **Contact Lists:** Maintain contacts for cloud providers, dev teams, and external IR partners.
- **Threat Intelligence:** Monitor for leaked keys on paste sites, GitHub, and underground forums; subscribe to token-leak feeds.

3.2 Phase 2: Identification & Analysis

Goal: To confirm suspicious API key usage and determine its scope and impact.

1. **Initial Triage:** Collect logs from API gateways, CloudTrail/Activity logs, application logs, and secret scanning alerts. Open an incident ticket and activate secure communications.

2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:

    - **Authentication/Usage:** Requests from unusual IPs or geolocations, spikes in API calls, use outside normal business hours, or to uncommon endpoints.
    - **Resource Activity:** Creation of unexpected cloud resources, unusual data exports, high-cost API usage.
    - **Artifacts:** Detection of API keys in public repositories, paste sites, or in telemetry from secret scanners.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the permissions of the key, the impact of the unauthorized activity, and the sensitivity of the data accessed.

Level	Description	Example	MTTD	MTTR
Low	Single API key exposed but no successful unauthorized use detected.	An API key is leaked in a private repo, but no suspicious calls are observed; the owner rotates the key immediately.	6-12 hours	24-48 hours
Medium	Unauthorized API calls observed from unusual IPs, with limited resource impact.	An API key is used to call read-only endpoints from unknown IPs; limited data is accessed.	12-24 hours	2-4 days
High	Compromised keys used to create resources, exfiltrate sensitive data, or escalate privileges.	An attacker uses a leaked AWS access key to spin up EC2 instances and copy S3 buckets containing sensitive data.	24-48 hours	4-7 days
Critical	Widespread abuse of privileged keys leading to significant data loss, financial impact, or full account takeover.	Multiple high-privilege keys are abused to exfiltrate regulated data and modify IAM policies, enabling persistence.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious API usage with other telemetry and threat intelligence.

    - **If True Positive (TP):** The activity is confirmed as leaked/abused API keys. **Action:** Immediately proceed to the **Containment** phase, revoke/rotate compromised keys, and activate the API key playbook.
    - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and adjust detection thresholds or whitelists.

5. **Incident Declaration:** If confirmed, formally declare an API key compromise incident and escalate to leadership, DevOps, and legal teams.

3.3 Phase 3: Containment

Goal: To immediately revoke unauthorized access and prevent further damage.

- **Short-Term Containment (Immediate Actions):**
  - Revoke or rotate compromised API keys and secrets immediately.
  - Block offending IP addresses and throttle suspicious API endpoints.
  - Disable implicated service accounts or application credentials.
- **Evidence Preservation:** Preserve API gateway logs, CloudTrail, and application logs **before** remediation.
- **Long-Term Containment Strategy:** Review and restrict permissions on related service accounts to enforce least privilege.

3.4 Phase 4: Eradication

Goal: To remove attacker artifacts and close the exposure vector.

- **Root Cause Analysis:** Identify how the API key was leaked or compromised.
- **Artifact Removal:** Remove leaked keys from repositories, paste sites, and build artifacts.
- **Credential Remediation:** Reissue credentials following least-privilege principles and with short lifetimes.
- **Security Hardening:** Patch any code or pipeline that stored secrets insecurely (use secret managers). Harden CI/CD pipelines and enforce secrets scanning.

3.5 Phase 5: Recovery

Goal: To safely restore systems and validate security.

- **System Restoration:** Restore normal service access with rotated credentials.
- **Validation:** Validate that no unauthorized resources or data access remains.
- **Enhanced Monitoring:** Monitor for re-attempts to use old keys and for anomalous activity on new keys.
- **Business Continuity:** Review billing and resource usage for unauthorized costs.

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 DevOps, security, and legal teams.
- **Final Incident Report:** Produce a detailed incident report including the timeline, root cause, and remediation steps.
- **Action Plan:** Implement stronger secret management (vaults, short-lived tokens, automated rotation). Enforce repository scanning and developer training.

4 MITRE ATT&CK Framework Mapping

Suspicious API Key Usage ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1078 – Valid Accounts*
  - *T1552 – Unsecured Credentials*
- **Tactic: Credential Access**
  - *T1552 – Unsecured Credentials*
  - *T1606 – Forge Web Credentials*
- **Tactic: Discovery**
  - *T1526 – Cloud Service Discovery*
  - *T1538 – Cloud Service Dashboard*
- **Tactic: Collection**
  - *T1530 – Data from Cloud Storage Object*
- **Tactic: Impact**
  - *T1496 – Resource Hijacking*
  - *T1485 – Data Destruction*