Incident Response Playbook: Data Breach

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

This playbook provides a structured and actionable guide for AnubisX team members to follow in the event of a suspected or confirmed data breach. Its purpose is to ensure a swift, effective, and coordinated response to minimize impact, protect sensitive data, and meet all legal and regulatory obligations.

1.2 Scope

This document applies to all incidents involving the unauthorized access, disclosure, or exfiltration of sensitive, confidential, or proprietary data from the organization's systems, networks, or applications.

2 Overview of a Data Breach

A data breach is a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property. The consequences can range from reputational damage and financial loss to significant legal and regulatory penalties.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is ready to respond to an incident before it occurs.

- **Roles and Responsibilities:** Ensure all team members understand their roles during an incident (e.g., Incident Commander, Lead Analyst, Forensic Analyst, Communications Lead, Scribe).
- **Tools & Resources:** Ensure all necessary software (e.g., forensic imaging tools, log analysis platforms, EDR, SIEM, secure communication channels) is available and team members have appropriate access.
- **Training:** Conduct regular tabletop exercises and simulations of data breach scenarios (at least semi-annually).
- **Contact Lists:** Maintain an up-to-date, centrally located contact list for all key stakeholders, including executive management, legal counsel, HR, public relations, and third-party forensic firms.
- **Threat Intelligence:** Proactively monitor threat intelligence feeds for TTPs relevant to our industry and technology stack.

3.2 Phase 2: Identification & Analysis

Goal: To confirm whether a data breach has occurred and determine its scope and severity.

1. **Initial Triage:** Gather initial reports, open an official incident ticket, and establish a secure communication channel. Assemble the AnubisX team.

2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
   - **Network:** Unusual outbound traffic, communication with known malicious IPs/domains (C2), large data transfers.
   - **Endpoint:** Unexpected processes or services, presence of hacking tools, unauthorized registry changes, suspicious script execution (PowerShell, etc.).
   - **Account:** Anomalous privileged user activity, logins from unusual locations, multiple failed login attempts followed by a success.
3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the operational impact, the sensitivity of the data exposed, and the scope of the breach.

Level	Description	Example	MTTD	MTTR
Low	Minor incident with limited scope and no sensitive data involved.	A single workstation infected with commodity malware, with no evidence of lateral movement.	1-7 days	24-48 hours
Medium	Incident with potential for data exposure but limited in scope.	A departmental file server accessed by an unauthorized internal user.	7-30 days	3-7 days
High	Confirmed exposure of non-critical PII or proprietary data. Affects a significant number of systems.	Ransomware outbreak contained to a single network segment, with evidence of some data staging.	30-90 days	1-4 weeks
Critical	Confirmed breach of highly sensitive data (PHI, financial, etc.) or widespread system compromise.	Domain controller compromise with evidence of mass data exfiltration.	90+ days	1-3+ months

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points and threat intelligence.
   - **If True Positive (TP):** The activity is confirmed malicious. **Action:** Immediately proceed to the Containment phase and escalate to the Incident Commander.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.
5. **Incident Declaration:** Based on a TP finding, formally declare a data breach incident and escalate to leadership and legal counsel.

3.3 Phase 3: Containment

Goal: To prevent the breach from spreading and causing further damage.

- **Short-Term Containment (Immediate Actions):**
  - Isolate affected systems from the network (e.g., disconnect NIC, use EDR isolation).

  - Disable or reset compromised user accounts and credentials. Invalidate active sessions.
  - Block malicious IP addresses or domains at the network perimeter.

- **Evidence Preservation:** Create forensic images of affected systems before remediation. Maintain a strict chain of custody for all evidence.
- **Long-Term Containment Strategy:** Determine a broader strategy, which may involve network segmentation or temporarily disabling certain services to prevent lateral movement.

3.4 Phase 4: Eradication

Goal: To remove the attacker from the environment and eliminate the root cause.

- **Root Cause Analysis:** Identify the initial attack vector and the full extent of the attacker's actions.
- **Removal of Malicious Artifacts:** Rebuild compromised systems from a known-good baseline. Remove any attacker-created persistence mechanisms.
- **Security Hardening:** Patch exploited vulnerabilities. Implement additional controls such as MFA, enhanced egress filtering, application whitelisting, and stronger password policies.

3.5 Phase 5: Recovery

Goal: To restore systems and operations to a normal, secure state.

- **System Restoration:** Restore data from clean backups and bring rebuilt, hardened systems back online in a phased manner.
- **Enhanced Monitoring:** Implement a period of heightened monitoring for all restored systems and related network traffic.
- **Validation:** Confirm that systems are operating normally and securely. Formally declare the system as recovered.

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

Goal: To review the incident and improve future response capabilities.

- **Post-Incident Meeting:** Schedule a blameless post-mortem meeting within two weeks of incident closure with all stakeholders.
- **Final Incident Report:** Create a detailed report covering an executive summary, a detailed timeline (from detection to recovery), root cause analysis, impact assessment, and actionable recommendations.
- **Action Plan:** Create a tracked action plan to implement the recommendations. Assign ownership and deadlines to ensure accountability.

4 MITRE ATT&CK Framework Mapping

Data Breach ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing:* Gaining access via malicious emails.
  - *T1190 – Exploit Public-Facing Application:* Exploiting a web server vulnerability.
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping:* Stealing credentials from memory (e.g., LSASS).
  - *T1110 – Brute Force:* Guessing passwords for accounts.
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services:* Using protocols like RDP or SSH to move to other systems.
- **Tactic: Collection**
  - *T1005 – Data from Local System:* Staging files for exfiltration.
  - *T1530 – Data from Cloud Storage Object:* Accessing data stored in the cloud.
- **Tactic: Exfiltration**
  - *T1041 – Exfiltration Over C2 Channel:* Sending data through a command and control channel.
  - *T1567 – Exfiltration Over Web Service:* Uploading data to cloud storage.