Incident Response Playbook: Physical Devices & Insider Threats

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 procedures to detect, triage, contain, investigate, eradicate and recover from incidents in the category **Physical Devices & Insider Threats**. It is intended for SOC analysts, incident responders, endpoint teams, HR, legal/compliance and leadership. The playbook focuses on two primary subcategories: suspicious USB device usage (unauthorised data transfer / autorun) and insider-driven data exfiltration.

1.2 Scope

Applies to corporate endpoints (Windows, macOS, Linux), removable media controls, DLP/-CASB, corporate cloud storage (OneDrive, Google Drive, S3), email gateways, VPN, privileged accounts, HR records, and physical access logs. Covers both accidental exposures and malicious insider activity.

2 Overview of the Category

2.1 Definition

Physical Devices & Insider Threats comprise incidents where data or access is compromised via physical peripherals (USB, external HDDs) or by trusted personnel abusing legitimate access to copy, move, or leak sensitive information. Insider threats include negligent or malicious actions (exfil via cloud/USB/email) and collusion with external actors.

2.2 Common Attack Chain

1. **Access:** insider or visitor gains physical or logical access to endpoint or storage containing sensitive data.
2. **Collection:** locate and gather sensitive files (manual search, scripted collection).
3. **Transfer:** use removable media, cloud sync, email, FTP/SCP, or personal devices to copy data.
4. **Covering Tracks:** delete logs, modify timestamps, use encrypted containers or personal accounts.
5. **Exfiltration / Disclosure:** data moved outside corporate control or shared publicly.

2.3 Primary Risks & Business Impact

- Loss of intellectual property, customer PII, financial records.
- Regulatory and legal exposure due to data breach.
- Reputational damage and loss of client trust.
- Operational disruption and cost of forensic investigations and remediation.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	MTTD Goal	MTTR Target
Critical	Confirmed exfiltration of large volumes of sensitive or regulated data by an insider or via removable media; evidence of collusion.	$\leq$ 30 min	Contain within 4 hrs; full remediation 24–72 hrs
High	Confirmed unauthorized USB transfers of sensitive files or insider uploads to external cloud; active abuse.	$\leq$ 1 hr	24–72 hrs
Medium	Suspicious but unconfirmed transfers (large copy activity flagged by DLP) or repeated policy violations.	$\leq$ 2 hrs	48–96 hrs
Low	Single blocked attempt or unsuccessful autorun/malware on USB; no sensitive data accessed.	$\leq$ 4 hrs	Monitor / minor remediation within 24–72 hrs

Table 1: Severity Matrix - Physical Devices & Insider Threats

4 Tools & Preparation (Recommended)

- **Endpoint Controls:** EDR with removable-media auditing, Microsoft Defender for Endpoint, CrowdStrike — ensure USB insert/remove events, file copy events are logged.
- **DLP / CASB:** Data classification, egress detection, cloud-storage anomaly detection (OneDrive/SharePoint, Google Drive, S3).
- **SIEM / Log Management:** Centralize Windows Event logs (4663, 4656), macOS endpoint logs, proxy/egress logs, VPN logs.
- **USB Management:** GPO/MDM controls to block unknown USBs, hardware whitelisting, USB device inventory.
- **UEBA / Insider Detection:** User behavior analytics to spot anomalous access patterns, off-hours downloads, and unusual file collections.
- **Forensics / IR Tools:** FTK Imager, WinPMEM, process and network captures, forensic analysis lab for USB content imaging.
- **Playbook Resources:** Legal/HR escalation templates, chain-of-custody forms, evidence handling guidance.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- DLP alerts: policy matches on sensitive data copied to removable media or uploaded to cloud/email.

- Endpoint logs: Windows Event 4663 (object access), 4656 (handle requested), USB insertion events, or macOS external device mounts.
- Proxy/CASB: unusual uploads to external cloud (personal Dropbox, Google Drive), or mass downloads from internal repositories.
- UEBA alerts: anomalous access patterns (off-hours, large file access, new repository access).
- Host EDR: processes reading large numbers of files, use of compression/encryption utilities, or autorun/malicious execution from removable media.

Quick actions:

- Validate the alert, identify the user, endpoint and files involved; classify severity using the matrix.
- Preserve logs (EDR, DLP, CASB, proxy), take forensic snapshot of endpoint (memory/disk) if active exfil suspected.
- If immediate risk: isolate endpoint from network and suspend user sessions pending investigation.

5.2 Containment (Immediate / Short-term)

- Isolate affected host via EDR (network quarantine) to prevent further transfers.
- Revoke or suspend offending user account and any associated cloud tokens; force MFA and credential reset if compromise suspected.
- Block destination domains/IPs in proxy or network controls (temporary).
- If physical device present, secure and image the USB device preserving chain-of-custody.

5.3 Investigation & Forensic Triage

- Collect endpoint artifacts: filesystem timestamps, recently opened files, process trees, shell/history logs, and memory image if volatile evidence required.
- Image removable media (bit-for-bit) and analyze in a forensic lab for file contents, hidden containers or malware.
- Correlate DLP findings with cloud access logs, email logs and VPN sessions to map exfil timelines.
- Interview user(s) and relevant managers (coordinate with HR/legal before interviews as per policy).

5.4 Eradication

- Remove malicious tools or scripts from endpoints, reimage hosts where compromise or persistence is suspected.
- Revoke/rotate any exposed credentials or tokens discovered; revoke unauthorized OAuth consents.
- Update endpoint policies to block unauthorized USBs and deploy enforcement for data movement restrictions.
- Apply disciplinary or legal actions as appropriate in coordination with HR/legal where insider malicious intent confirmed.

5.5 Recovery

- Restore endpoint from a known-good image; validate no residual backdoors or scheduled tasks remain.
- Reinstate user access only after remediation and controlled monitoring window.
- Review data integrity and restore any affected systems from validated backups if tampering occurred.
- Increase monitoring for the affected user and similar privileged roles for 30–90 days.

5.6 Post-Incident Activities

- Produce a full incident report with timeline, IOCs, affected data, and remediation steps.
- Update DLP rules, endpoint policies, onboarding/offboarding processes and USB controls.
- Run targeted user-awareness campaigns and technical controls to prevent recurrence.
- Conduct lessons-learned and update playbooks and disciplinary/HR procedures where necessary.

6 MITRE ATT&CK Framework Mapping

Physical Devices & Insider Threats - ATT&CK Mapping

- **Collection:** T1113 (Screen Capture), T1005 (Data from Local System), T1074 (Data Staged)
- **Exfiltration:** T1041 (Exfiltration Over C2 Channel) — e.g., via personal cloud; T1567 (Exfiltration Over Web Service)
- **Defense Evasion:** T1070 (Indicator Removal on Host), T1027 (Obfuscated Files)
- **Insider Threat:** mapped across collection and exfiltration tactics where legitimate credentials abused (T1078).

7 Key Telemetry & Logs to Collect

- Endpoint: removable-media events, file create/modify/delete events, process creation and parent-child relationships (EDR).
- Windows Events: 4663 (Object Access), 4656 (Handle Requested), 4698/4702 (Scheduled Tasks), 7045 (Service Install).
- macOS/Linux: mount events, syslog, auditd, shell histories.
- Network: proxy logs, CASB logs, VPN logs, egress firewall logs, DNS logs for external uploads.
- Cloud: object access logs (OneDrive, Google Drive, S3), OAuth token issuance and app consent logs.
- HR/Physical: badge access times, visitor logs, offboarding records.

8 Subcategory Scenarios (Realistic)

Note: Each scenario below is an operational SOC/IR narrative — includes detection, investigative steps, containment actions, eradication, recovery and lessons learned.

Scenario A: Suspicious USB Device Usage (Data Transfer / Autorun)

Summary: A contractor plugs a personal USB drive into a corporate Windows workstation to transfer design files. The DLP system triggers on multiple matches for sensitive project markers and flags a high-volume file copy. The USB device also contains an autorun-like executable that attempted to run but was blocked by application control.

Detection:

- DLP alert: bulk file copy matching sensitive project identifiers to removable-media destination.
- EDR: USB insert event and process creation of a suspicious launcher executed from removable drive (blocked by application control).
- Windows Security: Event 4663 entries for file read/write showing large counts in short window.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* — sensitive data transferred to personal media. Incident ticket created and IR lead notified.
2. **Immediate containment:** Isolate the workstation (EDR network quarantine), secure and image the USB device (forensic copy), and suspend contractor network access.
3. **Forensic collection:** Acquire volatile memory and disk snapshot of the workstation; export DLP logs and Windows event logs for the time window; image the USB for analysis.
4. **User interview / HR coordination:** Notify contractor supervisor and HR; preserve evidence and follow corporate HR/legal protocols before interview.

Containment & Eradication:

- Remove the autorun executable and any dropped files after imaging; reimage the workstation if evidence of attempted execution exists.
- Update application control to block similar executables and add the device ID to hardware-blocklist if malicious.
- Enforce immediate credential rotation if any credentials were accessed during the event.

Recovery:

- Restore workstation from a trusted image; reinstall and validate security agents; restore network access after approval.
- Remediate data exposure: determine which files were copied, notify data owners, and if required, notify legal/compliance and affected parties.
- Review contractor access policy and restrict removable-media privileges on contractor workstations.

Outcome & Lessons:

- Root cause: permissive removable-media policy on contractor endpoints. Mitigations: enforce hardware whitelisting, block unknown USBs, strengthen application control, and require encrypted corporate media for approved transfers.
- Add automated DLP workflows that quarantine devices and block further transfers pending review.

Scenario B: Insider Threat — Data Exfiltration by Employee

Summary: A mid-level employee with legitimate access to financial reports begins systematically downloading end-of-quarter spreadsheets and uploading zipped archives to a personal cloud account over several weeks. UEBA flagged anomalous download cadence and CASB shows repeated uploads to personal cloud domain outside business hours.

Detection:

- UEBA: anomalous access pattern (large dataset downloads at 02:00 AM) for an account that usually accesses small daily reports.
- CASB / Proxy: repeated POSTs to ‘dropbox.com‘ with archived file sizes matching sensitive data.
- DLP: multiple policy matches for finance PII in outbound uploads.

Investigation & Actions:

1. **Triage & classification:** Classified as *Critical* due to repeated, targeted exfiltration of financial data. IR engaged and legal/HR briefed.
2. **Immediate containment:** Suspend the user’s account and revoke active sessions and API tokens; isolate the workstation and preserve forensic images.
3. **Forensic collection:** Collect endpoint images, browser history, CASB logs, DLP alerts, and cloud access metadata (timestamps, IPs, object names). Preserve copies of uploaded artifacts (hashes).
4. **Interview and legal coordination:** Coordinate with HR/legal for interview and evidence preservation, following local labor laws and company policy.

Containment & Eradication:

- Remove any exfil tools, revoke OAuth consents, and rotate credentials for accounts accessed.
- If the employee acted maliciously, follow HR disciplinary processes and coordinate with legal for potential criminal referral.
- Search for additional accounts or resources used by the insider and remediate (remove shared links, revoke access).

Recovery:

- Restore systems after reimaging and validation; restore minimal necessary access for ongoing work under monitoring.
- Notify affected stakeholders and, if required by law, regulators and impacted customers; execute breach notification processes.

- Review and tighten data access controls for financial data (just-in-time access, approval workflows).

Outcome & Lessons:

- Root cause: excessive access rights and lack of monitoring on high-value datasets. Mitigations: enforce least-privilege, periodic access reviews, improved UEBA tuning and CASB blocking for personal cloud domains.
- Implement data handling agreements, remove local export permissions for sensitive datasets, and strengthen offboarding procedures.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

Splunk: detect large file copies to removable media (example Windows):

```
index=wineventlog EventCode=4663 OR EventCode=4656
| where Object_Name!="C:\Windows\System32"
| stats count by host, user, Object_Name, EventCode
| where count > 50
```

Proxy / CASB: find uploads to personal cloud domains:

```
index=proxy (host="dropbox.com" OR host="drive.google.com" OR host="onedrive.live.com
    ")
| stats count by user, host, uri_path
```

9.2 Appendix B — Forensic Artifact Locations

- Windows: USB device records (Registry ‘HKLM‘), Prefetch, Windows Event Logs (4663/4656), EDR artifacts.
- macOS/Linux: ‘/var/log/system.log‘, mount events, ‘dmesg‘, ‘auditd‘ logs.
- Cloud: CASB logs, object metadata (upload IP, requester), OAuth consent logs.
- Network: Proxy logs, NetFlow slices for high-volume uploads, DNS logs for suspicious domains.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Playbook invoked.
- Affected accounts/endpoints/data sets; timeline of actions (who accessed what, when).
- Evidence preserved (EDR images, DLP records, CASB logs), IOCs (device IDs, external accounts, IPs).
- Actions taken (containment, eradication, recovery) with timestamps and owners.
- HR/legal actions taken, notifications to regulators/customers, and follow-up remediation tasks.