INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 13:59 UTC

ShinyHunters Breaches Kodak in Ongoing Enterprise Platform Campaign Targeting Third-Party Integrations

DATA BREACH | **HIGH** | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0177
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Eastman Kodak Company (customer PII and internal corporate data); campaign also targets Salesforce Aura, Salesloft Drift, Snowflake, Oracle PeopleSoft integrations
Published	2026-06-17T03:07:56
Discovery Source	Rss

Executive Summary

ShinyHunters (also tracked as UNC6395) has claimed responsibility for a breach of Eastman Kodak Company, threatening to publicly release 2.2 million records of customer PII and internal corporate data by June 18, 2026. Kodak has confirmed the breach but has not disclosed the access vector or the precise volume of data affected. This incident is part of a documented, active campaign targeting enterprise SaaS integrations, specifically Salesforce Aura, Salesloft Drift, Snowflake, and Oracle PeopleSoft, meaning organizations running these platforms with third-party integrations face elevated exposure independent of any direct Kodak relationship.

Technical Analysis

ShinyHunters (Mitiga tracking designation UNC6395) claimed unauthorized access to Kodak systems with a threatened data release deadline of June 18, 2026. Kodak confirmed the breach; the access vector and full data scope remain undisclosed as of available reporting. No CVE has been assigned, this is a breach campaign rather than a discrete software vulnerability. Attack surface analysis maps to these CWEs: CWE-284 (Improper Access Control), CWE-306 (Missing Authentication for Critical Function), and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques mapped to this campaign include T1199 (Trusted Relationship), T1078 (Valid Accounts), T1566 (Phishing), T1567 (Exfiltration Over Web Service), T1190 (Exploit Public-Facing Application), T1530 (Data from Cloud Storage), and T1657 (Financial Theft). The broader campaign pattern, documented by Mitiga and Black Kite, targets misconfigured or weakly

authenticated third-party integrations in Salesforce Aura components, Salesloft Drift connectors, Snowflake tenants, and Oracle PeopleSoft deployments. No patch is applicable; exposure reduction depends on access control hardening, integration audit, and credential hygiene across affected platforms.

Action Checklist

1. Step 1: Containment. Audit all active third-party integrations connected to Salesforce Aura, Salesloft Drift, Snowflake, and Oracle PeopleSoft. Revoke or suspend OAuth tokens, API keys, and service account credentials for any integration that cannot be immediately verified as authorized. Focus immediate remediation on internet-facing connectors with broad data-read permissions (maps to NIST AC-17, AC-20; CIS 5.1).
2. Step 2: Detection. Review authentication logs across Salesforce, Snowflake, and PeopleSoft for anomalous Valid Account activity (T1078): logins from unexpected geographies, service accounts accessing data outside normal patterns, or bulk data reads indicative of exfiltration (T1530, T1567). Query SIEM for large outbound data transfers to cloud storage or webhook endpoints. Enable AU-2 event logging on all SaaS admin consoles if not already active (maps to NIST AU-2, AU-6; CIS 8.2).
3. Step 3: Eradication. Rotate all credentials and API keys associated with the affected integration platforms. Enforce MFA on all administrative and integration service accounts across Salesforce, Snowflake, Salesloft, and PeopleSoft, no exceptions (maps to NIST AC-3, AC-6; CIS 6.3, 6.4, 6.5; D3FEND D3-MFA, D3-CRO). Remove or disable any integration with permissions exceeding documented business need, per least-privilege principles (NIST AC-6; D3FEND D3-UAP, D3-CH).
4. Step 4: Recovery. Verify remediation by re-auditing active integration permissions and confirming no residual unauthorized sessions exist. Monitor for re-entry attempts via the same Trusted Relationship vector (T1199) for a minimum of 30 days post-hardening. Confirm audit logging is active and capturing authentication events on all affected platforms (NIST AU-9, AU-11; CIS 8.2).
5. Step 5: Post-Incident. Conduct a formal third-party integration access review against documented business justifications (NIST AC-20; CIS 1.1, 3.2). Assess whether integration vendors, Salesforce, Salesloft, Snowflake, and Oracle have published specific hardening guidance in response to this campaign, and track their advisories. Review your vendor risk management program for coverage of SaaS integration attack surfaces (CWE-284, CWE-306 exposure gaps). Document findings for GRC and compliance teams.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel, privacy officer, and executive leadership if internal log analysis confirms unauthorized bulk reads of PII records from any of the four affected platforms, if ShinyHunters' June 18, 2026 publication deadline falls within the active incident window, or if the organization cannot confirm full scope of data accessed within 72 hours — the latter triggers mandatory breach notification obligations under CCPA, GDPR, and state SHIELD Act equivalents for customer PII.

Recovery Notes	Post-containment verification must include a full re-enumeration of all OAuth-authorized applications and service account permission sets across Salesforce, Snowflake, Salesloft, and PeopleSoft to confirm no ShinyHunters-associated sessions persist via refresh token reuse, which is a documented persistence mechanism in this campaign's TTPs. Monitor Snowflake ACCOUNT_USAGE.ACCESS_HISTORY and Salesforce LoginEvent streams daily for a minimum of 30 days for re-entry attempts consistent with the Trusted Relationship vector, using the same integration partner and service account identifiers identified during triage. Any re-entry indicator should be treated as a new incident given ShinyHunters' documented pattern of returning to compromised environments via residual third-party connector access.
Forensic Artifacts	Snowflake ACCOUNT_USAGE.QUERY_HISTORY rows with ROWS_PRODUCED > 100,000 during the 90-day pre-incident window — primary artifact for quantifying the scope of bulk data reads consistent with ShinyHunters' cloud storage exfiltration pattern | Salesforce Event Monitoring logs for ReportExport and ApiTotal event types showing record-volume outliers tied to integration service account UserIDs, correlatable to the specific Connected App OAuth client_id used during the breach window | PeopleSoft Integration Broker message logs and web server access logs (access.log under $PS_CFG_HOME/webserv/) for repeated high-volume REST or CI-based API calls to HR or customer data objects outside normal batch windows | OAuth refresh token issuance and redemption records from Salesforce Identity Logs and Snowflake ACCOUNT_USAGE.SESSIONS, specifically tokens issued to third-party integration accounts that were redeemed from IP ranges inconsistent with the registered integration partner's infrastructure | Salesloft Drift webhook delivery history and outbound payload logs showing data routed to external endpoints not matching documented CRM or marketing automation destinations — relevant to identifying whether Salesloft's Drift connector was used as a data exfiltration relay to attacker-controlled webhook receivers

Per-Action IR Details

Step 1: Containment — Audit all active third-party integrations connected to Salesforce Aura, Salesloft Drift, Snowflake, and Oracle PeopleSoft. Revoke or suspend OAuth tokens, API keys, and service account credentials for any integration that cannot be immediately verified as authorized. Prioritize internet-facing connectors with broad data-read permissions (maps to NIST AC-17, AC-20; CIS 5.1).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-20 (Use Of External Systems), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Export the Salesforce Connected Apps list via Setup > Connected Apps > Manage and cross-reference against an authorized integration register maintained in a shared spreadsheet. For Snowflake, run 'SELECT * FROM SNOWFLAKE.ACCOUNT_USAGE.ACCESS_HISTORY WHERE QUERY_START_TIME > DATEADD(day, -90, CURRENT_TIMESTAMP)' to enumerate recently active service accounts. Revoke unrecognized OAuth tokens immediately using Salesforce CLI ('sf org revoke') or Snowflake's 'ALTER USER SET DISABLED = TRUE'. For PeopleSoft, audit Integration Broker service operations in PeopleTools > Integration Broker > Monitor > Monitor Message.

Evidence: Before revoking any token or credential, capture a full export of all currently active OAuth tokens, connected app session metadata, and API key last-used timestamps from Salesforce Setup > Security > Session Management, Snowflake ACCOUNT_USAGE.SESSIONS view, and PeopleSoft Integration Broker logs. Also capture active network connections from any integration middleware hosts using 'netstat -ano' or 'ss -tulnp' to document live outbound connections to ShinyHunters-associated infrastructure before sessions are terminated. These records establish the pre-containment baseline and are destroyed upon revocation.

Step 2: Detection — Review authentication logs across Salesforce, Snowflake, and PeopleSoft for anomalous Valid Account activity (T1078): logins from unexpected geographies, service accounts accessing data outside normal patterns, or bulk data reads indicative of exfiltration (T1530, T1567). Query SIEM for large outbound data transfers to cloud storage or webhook endpoints. Enable AU-2 event logging on all SaaS admin consoles if not already active (maps to NIST AU-2, AU-6; CIS 8.2).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query Salesforce Event Monitoring logs via the EventLogFile API or Salesforce Inspector browser extension, filtering for 'ReportExport' and 'ApiTotal' event types with record counts exceeding 10,000 in a single session. In Snowflake, run 'SELECT USER_NAME, CLIENT_APPLICATION_ID, BYTES_SCANNED, ROWS_PRODUCED FROM SNOWFLAKE.ACCOUNT_USAGE.QUERY_HISTORY WHERE ROWS_PRODUCED > 100000 AND START_TIME > DATEADD(day, -30, CURRENT_TIMESTAMP)' to surface bulk read operations consistent with ShinyHunters exfiltration behavior. For PeopleSoft, review the web server access logs (typically under $PS_CFG_HOME/webserv//logs/access.log) for repeated large GET requests to PS_TOKEN or CI-based REST endpoints. Write a Sigma rule targeting Snowflake query history for rows_produced outliers and apply it manually against exported CSVs.

Evidence: This step is analytical and does not alter live state, so no volatile capture is prerequisite to the analysis itself. However, before any log forwarding pipeline is enabled or modified, snapshot the current state of Salesforce Event Log Files via API download (retained only 24 hours on non-Event Monitoring licenses), Snowflake ACCOUNT_USAGE.LOGIN_HISTORY and QUERY_HISTORY views (93-day retention window — export immediately), and PeopleSoft psadmin and web server access logs from the integration middleware tier. Salesloft Drift webhook delivery logs should be exported from the Salesloft admin portal before any integration disable action, as disabling a webhook may purge its delivery history.

Step 3: Eradication — Rotate all credentials and API keys associated with the affected integration platforms. Enforce MFA on all administrative and integration service accounts across Salesforce, Snowflake, Salesloft, and PeopleSoft — no exceptions (maps to NIST AC-3, AC-6; CIS 6.3, 6.4, 6.5; D3FEND D3-MFA, D3-CRO). Remove or disable any integration with permissions exceeding documented business need, per least-privilege principles (NIST AC-6; D3FEND D3-UAP, D3-CH).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without a PAM solution, use Salesforce's built-in permission set review ('sf org list permissions') to identify and remove object-level READ ALL permissions from integration users, replacing with named-record or field-level security. Snowflake credential rotation can be scripted via SnowSQL: 'ALTER USER SET PASSWORD = MUST_CHANGE_PASSWORD = FALSE'. For PeopleSoft integration accounts lacking native MFA support, enforce IP allowlisting via PeopleTools > Security > Network and place the service account behind a dedicated integration middleware host. Enable Salesloft's IP restriction feature in Settings > Security to limit Drift webhook callbacks to known internal ranges.

Evidence: Before rotating any credential or enforcing MFA policy changes, capture a memory dump from any integration middleware hosts (using WinPmem on Windows or 'dd if=/dev/mem' equivalent via LiME on Linux) and run 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' to document active connections at the moment of credential revocation. Also export the Salesforce Debug Logs for the past 72 hours and Snowflake ACCOUNT_USAGE.ACCESS_HISTORY for any service account being rotated — ShinyHunters tooling consistent with this campaign has been observed staging exfiltration via long-lived OAuth refresh tokens that survive password rotation if not explicitly revoked at the authorization server level.

Step 4: Recovery — Verify remediation by re-auditing active integration permissions and confirming no residual unauthorized sessions exist. Monitor for re-entry attempts via the same Trusted Relationship vector (T1199) for a minimum of 30 days post-hardening. Confirm audit logging is active and capturing authentication events on all affected platforms (NIST AU-9, AU-11; CIS 8.2).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: Configure Snowflake's ACCOUNT_USAGE alert policies using CREATE ALERT to fire on any new service account login originating from a CIDR block outside your known integration IP ranges. For Salesforce, enable Real-Time Event Monitoring on the LoginEvent object and route to a syslog forwarder or S3 bucket if no SIEM is available. Implement a weekly manual review cadence using a Sigma rule applied against exported Snowflake LOGIN_HISTORY CSVs, filtering for CLIENT_APPLICATION_ID values associated with known ShinyHunters tooling (e.g., generic Python requests or curl user-agent strings in SaaS API logs). Verify PeopleSoft Integration Broker service operations are logging to a write-protected network share under a service account that is not the same account used for integration operations.

Evidence: This step does not alter live system state in a way that destroys volatile evidence, but confirm before closing the recovery phase that all log streams are intact and have not been tampered with — validate AU-9 compliance by checking Salesforce event log file hashes against the API-returned checksums, and verify Snowflake ACCOUNT_USAGE data has not been altered by querying SNOWFLAKE.ACCOUNT_USAGE.QUERY_HISTORY for any 'DROP TABLE' or 'DELETE' operations on audit-adjacent objects during the incident window. Retain all exported log artifacts from Steps 1-3 in an evidence-preserved, write-once location for a minimum of 12 months given the PII volume involved and likely regulatory notification requirements.

Step 5: Post-Incident — Conduct a formal third-party integration access review against documented business justifications (NIST AC-20; CIS 1.1, 3.2). Assess whether integration vendors — Salesforce, Salesloft, Snowflake, Oracle — have published specific hardening guidance in response to this campaign, and track their advisories. Review your vendor risk management program for coverage of SaaS integration attack surfaces (CWE-284, CWE-306 exposure gaps). Document findings for GRC and compliance teams.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-20 (Use Of External Systems), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Produce a third-party integration inventory in a structured spreadsheet mapping each integration to: owning business unit, data objects accessible, OAuth scopes granted, last access date (from Step 2 log exports), and documented business justification — this is achievable by two analysts in one sprint using the Salesforce Connected Apps export and Snowflake ACCOUNT_USAGE.GRANTS_TO_USERS view. File vendor advisory tracking items against Salesforce Trust (trust.salesforce.com), Snowflake's Security Bulletins page, Salesloft's changelog, and Oracle's CPU advisory stream. For GRC documentation, map any access-review gaps to your existing SOC 2 Type II or ISO 27001 control library to surface audit findings ahead of the next assessment cycle.

Evidence: No volatile evidence capture is required at this phase. However, the post-incident review should incorporate all log exports, session records, and permission snapshots captured in Steps 1-4 as the evidentiary basis for the formal access review. Specifically, the Snowflake QUERY_HISTORY bulk-read records and Salesforce ReportExport event logs captured during detection should be included in the breach notification package for legal and regulatory counsel, given the 2.2 million PII records at stake and applicable state breach notification statutes (e.g., CCPA, SHIELD Act) triggered by the confirmed Kodak breach affecting customer data.

Detection Guidance

Focus detection efforts on three data sources: SaaS platform authentication logs, cloud storage access logs, and outbound network telemetry. In Salesforce, query login history and connected app activity for service accounts or OAuth tokens accessing Aura components outside business hours or from unrecognized IPs. In Snowflake, review query history and access logs for bulk SELECT statements against tables containing PII, particularly from integration service accounts. In Oracle PeopleSoft, audit application server logs for unauthenticated or weakly authenticated requests to critical function endpoints (CWE-306 indicator). For exfiltration detection (T1567, T1530), alert on large outbound transfers to cloud storage services or webhook destinations not in your approved vendor list. Behavioral indicators consistent with T1078 (Valid Accounts): service account logins outside scheduled windows, accounts accessing data volumes significantly above baseline, and accounts authenticating from multiple geographies in short succession. No confirmed public IOCs (IP addresses, domains, file hashes) were available in the provided source material; do not populate IOC blocklists from unverified sources. Monitor Mitiga and BleepingComputer for IOC releases as the June 18 deadline approaches.

Framework Mappings

MITRE-ATTACK

- **T1199** — Trusted Relationship
- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1567** — Exfiltration Over Web Service
- **T1190** — Exploit Public-Facing Application
- **T1530** — Data from Cloud Storage
- **T1657** — Financial Theft

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement

- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1199	Trusted Relationship	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1190	Exploit Public-Facing Application	Initial-Access
T1530	Data from Cloud Storage	Collection
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/kodak-confirms-data-...	T3
ShinyHunters Hit Oracle PeopleSoft and Your Vendors May Already ...	https://blackkite.com/blog/shinyhunters-hit-oracle-peoplesoft-and-y...	T3
ShinyHunters and UNC6395: Inside the Salesforce and Salesloft ...	https://www.mitiga.io/blog/shinyhunters-and-unc6395-inside-the-sale...	T3
Salesforce Customers—You're On the Hook If You Use Salesloft Drift!	https://www.linkedin.com/posts/vernonkeenan_hundreds-of-salesforce-...	T3
Oracle PeopleSoft Breached by The ShinyHunters Data Theft Attack	https://pathlock.com/blog/security-alerts/peoplesoft-breached-by-th...	T3

Generated 2026-06-17 13:59 UTC by TJS Security Command Center