INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-10 06:16 UTC

Cyberattack Disrupts Canvas Learning Platform, Parent Company Reports Alleged 275M Record Breach

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0119
Type	Data Breach
Severity	HIGH
Affected Products	Canvas LMS (Instructure), cloud-hosted platform; specific version not publicly disclosed
Published	2 days ago
Discovery Source	Serper

Executive Summary

An unattributed hacking group disrupted Instructure's Canvas learning management system on May 7, 2026, causing a multi-hour outage during academic finals and claiming exfiltration of approximately 275 million records. The breach scope and data types involved remain unverified by Instructure as of reporting. If substantiated, the scale of the alleged exfiltration represents significant risk to student and institutional data across hundreds of affected colleges and schools.

Technical Analysis

Instructure's Canvas LMS experienced a confirmed service outage attributed to an intrusion and alleged data exfiltration campaign. No CVE has been assigned; the attack does not appear to exploit a publicly documented vulnerability. Mapped MITRE ATT&CK techniques include T1078 (Valid Accounts, suggesting possible credential-based initial access), T1041 (Exfiltration Over C2 Channel), T1489 (Service Stop, consistent with observed platform outage), and T1486 (Data Encrypted for Impact, possible ransomware component or applied as extortion pressure). T1657 (Financial Theft) may apply if a ransom or extortion demand is confirmed. Specific initial access vectors, affected system components, and confirmed data types have not been disclosed by Instructure. No patch or vendor advisory is available as of reporting. The 275 million record figure is threat actor-claimed and unverified. Platform operates as a cloud-hosted SaaS; on-premises version exposure is unknown.

Action Checklist

1. Containment: Identify all institutional integrations with Canvas (SSO, SIS, LTI tools, API connections). Audit OAuth tokens and API keys issued to Instructure. Temporarily revoke or rotate credentials for any service accounts used to connect to Canvas if your institution has elevated privilege integrations.
2. Detection: Review IdP logs (Azure AD, Okta, Shibboleth) for anomalous authentication events tied to Canvas SSO between May 1-7, 2026. Check SIEM for unusual outbound data flows to Instructure-affiliated IPs during that window. Query for bulk data exports or API calls from Canvas admin accounts during the same period.
3. Eradication: No vendor-issued patch or specific remediation is available as of reporting. Rotate all service account credentials and API keys connected to Canvas. Disable unused LTI integrations and third-party app connections in the Canvas admin console until Instructure releases official guidance.
4. Recovery: Confirm platform availability via Instructure's status page (status.instructure.com). Validate that SSO and SIS integrations are functioning correctly post-outage. Monitor for any unauthorized changes to user accounts, course data, or administrative configurations. Request a formal incident notification from Instructure under your data processing agreement.
5. Post-Incident: Review your institution's data processing agreement and breach notification obligations with Instructure. Assess whether student PII shared with Canvas (names, emails, academic records) falls under FERPA notification requirements. Evaluate controls around third-party SaaS data custody and whether vendor breach notification SLAs are contractually defined.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel, institutional CISO, and registrar if Instructure confirms exfiltration of student PII (names, email addresses, enrollment or grade records) attributable to your institution, as this triggers FERPA breach notification assessment and potentially state-level student data privacy law obligations; also escalate if IdP log review reveals successful authentication to Canvas from unrecognized IPs or service accounts during May 1–7, 2026, indicating your institution's credentials may have been directly compromised rather than data lost solely at the Instructure level.
Recovery Notes	Post-containment, maintain enhanced monitoring of Canvas SSO authentication events and SIS integration sync logs for a minimum of 30 days following Instructure's formal incident closure notice, watching specifically for re-use of any credentials that were in scope during the breach window. Validate the integrity of course enrollment and grade records in your SIS of record (Banner, Colleague, Workday, etc.) against Canvas-reflected data to identify any unauthorized modifications that may have occurred during the outage period. Do not fully restore all LTI and third-party integrations until Instructure has published a root cause analysis and confirmed the attack vector is closed — restore integrations incrementally, logging each reactivation with a risk acceptance sign-off.

Forensic Artifacts	Canvas Authentication Log (Admin > Logging > Authentication): captures every login event with timestamp, user ID, IP address, and authentication method — primary artifact for identifying credential abuse or anomalous admin access during May 1–7, 2026 | IdP SAML/OIDC application-specific sign-in logs for the Canvas enterprise app: Azure AD Sign-In Logs filtered on application 'Canvas' or Okta System Log filtered on target.displayName eq 'Canvas' — captures the federation handshake details, user agent strings, and IP addresses that a threat actor would generate when accessing Canvas via compromised institutional SSO | Canvas SIS Import History (Admin > SIS Imports): records every bulk data import including timestamp, submitting account, file name, and row counts — an attacker with admin access may have exfiltrated data by triggering a full SIS export or injecting records, both of which leave entries here | Egress NetFlow or DNS query logs for institutional DNS resolvers: filter on *.instructure.com, *.canvaslms.com, and the Canvas Data 2.0 S3 bucket endpoints (canvas-data-2.instructure.com) during May 1–7, 2026 — abnormal byte counts or query volumes to these endpoints from non-SIS-connector hosts would indicate unauthorized bulk data access from within your network | Canvas Developer Keys audit trail (Admin > Developer Keys): records creation, modification, and deletion of API keys and LTI 1.3 registrations with timestamps and acting admin account — a threat actor with admin access may have created a persistent API key for ongoing access that would appear as an anomalous entry created during the breach window

Per-Action IR Details

Containment — Identify all institutional integrations with Canvas (SSO, SIS, LTI tools, API connections). Audit OAuth tokens and API keys issued to Instructure. Temporarily revoke or rotate credentials for any service accounts used to connect to Canvas if your institution has elevated privilege integrations.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export all OAuth applications from your IdP: in Okta, navigate to Applications > All Applications and filter by Canvas/Instructure client IDs; in Azure AD, run `Get-AzureADServicePrincipal -All $true | Where-Object {$_.DisplayName -like '*Canvas*' -or $_.DisplayName -like '*Instructure*'}` and cross-reference against your SIS connector service accounts. For API key inventory, query Canvas REST API with an admin token: `GET /api/v1/audit/authentication/logins` to list all active tokens, or pull the Canvas admin console under Account > Settings > Integrations. Document and revoke tokens not explicitly approved.

Evidence: Before revoking tokens, capture a full export of active Canvas OAuth tokens and LTI developer keys from the Canvas admin console (Admin > Developer Keys) — this establishes the pre-incident integration surface. Export your SIS sync logs (typically CSV or XML files from Ellucian Banner, Colleague, or PeopleSoft connectors) to document what data was flowing to Canvas and at what frequency in the May 1–7, 2026 window. Preserve your IdP's service principal audit logs showing Canvas app consent grants and permission scopes before any rotation occurs.

Detection — Review IdP logs (Azure AD, Okta, Shibboleth) for anomalous authentication events tied to Canvas SSO between May 1–7, 2026. Check SIEM for unusual outbound data flows to Instructure-affiliated IPs during that window. Query for bulk data exports or API calls from Canvas admin accounts during the same period.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: For Azure AD without Sentinel: use the free Azure AD Sign-In Logs (retained 30 days in P1/P2, 7 days free tier) — run `Get-AzureADAuditSignInLogs -Filter "appDisplayName eq 'Canvas' and createdDateTime ge 2026-05-01" | Export-Csv canvas_sso_audit.csv`. For Okta without SIEM: use Okta System Log API — `GET /api/v1/logs?filter=target.displayName+eq+"Canvas"&since=2026-05-01T00:00:00Z`. For network analysis without SIEM, use Zeek or Wireshark on egress captures and filter on Instructure ASN (query ARIN for Instructure Inc. ASN blocks, currently AS54600 range — verify current allocation before use). Flag sessions with abnormally high byte counts outbound to Instructure-owned IPs. Apply the free Sigma rule `proc_creation_win_susp_data_exfil` as a baseline for bulk export behavior on any on-prem Canvas-integrated systems.

Evidence: Collect IdP sign-in logs specifically for the Canvas SAML/OIDC application between May 1–7, 2026, flagging: failed authentications followed by success (credential stuffing indicator), logins from geographic anomalies or residential ISPs inconsistent with your institution's user base, and service account authentications outside business hours. From Canvas itself, pull the authentication log (Admin > Logging > Authentication) and the page view log (Admin > Logging > Grade Change and Course Activity) for admin-privileged accounts — bulk page view counts or grade export events in this window are indicators of pre-exfiltration reconnaissance. Capture NetFlow or DNS query logs for queries to `*.instructure.com` and `*.canvaslms.com` during the outage window to identify whether outage-period traffic differed in volume or destination from baseline.

Eradication — No vendor-issued patch or specific remediation is available as of reporting. Rotate all service account credentials and API keys connected to Canvas. Disable unused LTI integrations and third-party app connections in the Canvas admin console until Instructure releases official guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: In the Canvas admin console, navigate to Admin > Settings > Apps to enumerate all active LTI 1.1 and LTI 1.3 integrations; disable any not confirmed as operationally required within the last 30 days. For API key rotation without automated tooling, use the Canvas REST API: `DELETE /api/v1/users/:user_id/tokens/:token_id` for each service account token, then reissue with scoped permissions limited to minimum required endpoints. Document all disabled integrations in a change log with timestamp, responsible party, and business justification — this log supports both recovery and any regulatory inquiry. Since no Instructure patch is available, treat credential rotation as the primary eradication action and set a calendar trigger to reassess once Instructure publishes a formal incident report.

Evidence: Before disabling LTI tools and third-party connections, capture a screenshot or API export of all currently enabled integrations (Canvas Admin > Developer Keys > show all) with their last-used timestamps — this establishes whether any integration was activated or modified anomalously in the breach window. Preserve the Canvas admin audit log (Admin > Logging) showing which admin accounts performed configuration changes between May 1–7, 2026, specifically additions or modifications to LTI placements or external tool configurations, which could indicate an attacker used compromised admin credentials to implant a persistent LTI backdoor.

Recovery — Confirm platform availability via Instructure's status page (status.instructure.com). Validate that SSO and SIS integrations are functioning correctly post-outage. Monitor for any unauthorized changes to user accounts, course data, or administrative configurations. Request a formal incident notification from Instructure under your data processing agreement.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST IR-6 (Incident Reporting), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Write a lightweight osquery query to continuously monitor your on-prem SIS connector host for anomalous outbound connections: `SELECT * FROM process_open_sockets WHERE remote_address NOT IN (SELECT address FROM known_canvas_ips) AND process.name IN ('banner_extract','ellucian_sync','sis_connector');` — adapt process names to your environment. For Canvas admin

change monitoring without SIEM, configure a daily cron job to export the Canvas authentication log via API and diff against the prior day's export, alerting on new admin account creations or role escalations. Formally log your data processing agreement (DPA) inquiry to Instructure in writing (email to your CSM and Instructure's privacy@instructure.com) with a timestamped record — this creates the paper trail required for regulatory response if breach is confirmed.

Evidence: Capture a baseline snapshot of all Canvas admin user accounts and their role assignments (Admin > People > filter by Admin role) at the time of recovery validation — compare against any pre-incident snapshot to identify accounts added or privilege-escalated during the breach window. Pull SIS import logs (Admin > SIS Imports) to verify no unauthorized bulk user or enrollment data was injected into Canvas from an external source during or after the incident, which would indicate attacker persistence via SIS import manipulation.

Post-Incident — Review your institution's data processing agreement and breach notification obligations with Instructure. Assess whether student PII shared with Canvas (names, emails, academic records) falls under FERPA notification requirements. Evaluate controls around third-party SaaS data custody and whether vendor breach notification SLAs are contractually defined.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST AU-11 (Audit Record Retention), NIST RA-3 (Risk Assessment), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a data inventory exercise using a spreadsheet template (no tooling required): enumerate every Canvas data field your institution populates — student names, institutional email addresses, course enrollment records, grade data, login timestamps, LTI tool usage records — and classify each against FERPA's definition of education records (34 CFR § 99.3). Map this inventory to the 275 million record claim to estimate your institutional exposure. For DPA review, cross-reference your Instructure Master Agreement and Data Processing Addendum against the NIST IR-6 requirement that vendors notify you within a defined window — if no SLA is defined, document the gap as a finding for contract renegotiation. Retain all incident-related communications, log exports, and timeline documentation for a minimum of 3 years consistent with FERPA record retention guidance and your institution's records policy.

Evidence: Preserve all Instructure-issued communications (status page updates, email notifications, CSM communications) between May 7 and the date of your post-incident review — these constitute the vendor notification record required for FERPA and any state breach notification analysis. Retain a copy of the Canvas Data 2.0 (CD2) or Canvas Data exports your institution received in the 90 days prior to the incident; these establish the schema and scope of data Instructure held on your behalf and are essential for scoping any required student or regulatory notifications.

Detection Guidance

No confirmed IOCs have been publicly released. Detection focus should be on anomalous activity correlated with the May 1-7, 2026 window. Check IdP logs for bulk Canvas authentication failures or unusual session creation volume. Review Canvas audit logs (Admin > Logging) for mass account queries, grade exports, or API token generation outside normal patterns. Monitor for spike in API calls using institutional admin tokens. If your institution uses Canvas Data or Canvas Data 2 (Instructure's data pipeline product), audit recent data sync logs for unexpected access or export events. Watch for downstream phishing attempts targeting students and faculty using Canvas-branded lures, a common follow-on to LMS breaches.

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1489** — Service Stop
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CM-6** — Configuration Settings
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1489	Service Stop	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
	https://www.nytimes.com/2026/05/07/education/canvas-hacked-down-dat...	T2
Canvas back online after cyberattack shuttered learning platform for ...	https://www.cbsnews.com/news/cyberattack-shutters-canvas-learning-p...	T3
Canvas learning platform hit by cyberattack - YouTube	https://www.youtube.com/watch?v=rI6oTHKO9yw	T3
Alleged cyberattack temporarily shuts down Canvas - ABC News	https://abcnews.com/Technology/alleged-cyberattack-temporarily-shut...	T3
Chaos erupts as cyberattack disrupts learning platform Canvas amid ...	https://arstechnica.com/civis/threads/chaos-erupts-as-cyberattack-d...	T2

Generated 2026-05-10 06:16 UTC by TJS Security Command Center