INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 09:03 UTC

Hackers steal students' data during breach at education tech giant Instructure

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0115
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Instructure Canvas LMS platform, users including students and educators
Published	21 hours ago
Discovery Source	Serper

Executive Summary

ShinyHunters, a known data extortion group, claims to have breached Instructure, the company behind the Canvas learning management system used by universities and K-12 institutions worldwide. The group alleges exfiltration of data belonging to up to 275 million students and educators; Instructure has disclosed the breach, though the full scope of compromised data fields has not been confirmed. Organizations depending on Canvas face immediate regulatory exposure, reputational risk, and potential harm to student populations who cannot protect themselves.

Technical Analysis

Instructure disclosed a data breach claimed by ShinyHunters affecting its Canvas LMS platform. The threat actor claims up to 275 million records were exfiltrated. No CVE has been assigned; this is an unauthorized access and data exfiltration incident. CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) and CWE-284 (Improper Access Control) are the relevant weakness classifications. MITRE ATT&CK techniques mapped to this incident include T1078 (Valid Accounts, possible credential-based initial access), T1567 (Exfiltration Over Web Service), T1530 (Data from Cloud Storage), and T1619 (Cloud Storage Object Discovery). The initial access vector, specific authentication mechanism abused, and exact data schema of exfiltrated records have not been confirmed in open sources as of analysis date. No patch or software fix is applicable; this is an access control and data handling incident. Instructure has not published a vendor advisory with technical indicators as of this writing. Primary reporting from TechCrunch (T2); corroboration from SecurityWeek and Mashable (T3). Claims regarding the 275 million figure originate partly from the threat actor; treat as unverified until Instructure confirms scope.

Action Checklist

1. Containment, Audit all Canvas API integrations, service accounts, and OAuth tokens issued to third-party apps; immediately rotate all credentials with broad data access. Contact Instructure support immediately to request tenant-specific impact assessment.
2. Detection, Review Canvas audit logs and LMS access logs for anomalous bulk export activity, API calls pulling large student record sets, or access from unfamiliar IP ranges. Query for T1530/T1619 patterns: unusual cloud storage list or download operations tied to Canvas service accounts. No confirmed IOCs are publicly available at this time; monitor threat intelligence feeds for ShinyHunters-attributed indicators.
3. Eradication, No software patch applies. Revoke and reissue all Canvas API keys and service account credentials. Enforce least-privilege access on all LMS integrations. Disable or review any third-party Canvas integrations that were granted read access to student PII.
4. Recovery, Verify that rotated credentials are propagated to all dependent systems. Confirm that bulk export and data download permissions are restricted to authorized administrative roles only. Monitor Canvas audit logs for 30 days post-remediation for recurrence of anomalous access patterns.
5. Post-Incident, This incident exposes gaps in third-party data processor oversight and LMS access control governance. Review your institution's data processor agreements with Instructure under applicable privacy law (FERPA, GDPR where relevant). Assess whether student PII stored in Canvas exceeds minimum necessary data retention. Brief affected students and faculty per applicable breach notification obligations.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to institutional legal counsel, CISO, and data protection officer immediately if Instructure confirms your tenant was specifically enumerated in the ShinyHunters exfiltration, if Canvas audit logs show API bulk-export activity from unrecognized service accounts within the 90 days preceding disclosure, or if your institution holds Canvas data on EU-resident students (triggering GDPR Article 33 72-hour supervisory authority notification) or federally-enrolled students (triggering FERPA breach notification obligations).
Recovery Notes	After credential rotation and integration re-scoping, verify full Canvas functionality for instructors and admins using a test account before declaring systems restored, specifically confirming that SIS sync operations, gradebook exports, and LTI tool connections function with new API keys. Maintain elevated Canvas Audit Log review cadence (daily for first 2 weeks, weekly for weeks 3-8) watching specifically for re-appearance of bulk enrollment or user-record API calls from service accounts, which would indicate ShinyHunters retained a credential not captured in the initial rotation. Preserve all forensic artifacts — particularly the pre-rotation Canvas API key inventory and audit logs — for a minimum of 3 years to support potential regulatory investigation, FERPA compliance review, or civil litigation from affected students.

Forensic Artifacts	Canvas Audit Log CSV (Admin > Audit Log): 90-day export capturing all API authentication events, SIS import/export operations, and OAuth token grants — the primary artifact for establishing whether your tenant was accessed during the ShinyHunters breach window | Canvas Live Events JSON stream (if subscribed): 'asset_accessed' events with actor.id, client_ip, and user_agent fields — records granular student record access that standard audit logs may not capture, enabling reconstruction of what PII was viewed or exported | Institution web proxy or WAF logs: HTTP requests to .instructure.com API endpoints, specifically filtering for response payload sizes >500KB from /api/v1/users, /api/v1/accounts/*/enrollments, or /api/v1/sis_imports — large responses indicate bulk record extraction consistent with ShinyHunters' claimed exfiltration of 275 million records | Identity Provider (IdP) authentication logs (Azure AD Sign-in Logs, Okta System Log, or Shibboleth idp-process.log): Canvas service account login events showing source IP, authentication method, and session duration — cross-reference source IPs against ShinyHunters infrastructure IOCs as they become available from threat intelligence feeds | Canvas Developer Keys configuration snapshot (Admin > Developer Keys): pre-eradication record of all OAuth token scopes granted to third-party integrations — establishes the maximum possible data exposure footprint if any of these keys were compromised or exfiltrated as part of the breach

Per-Action IR Details

Containment — Audit all Canvas API integrations, service accounts, and OAuth tokens issued to third-party apps; suspend or rotate any credentials with broad data access until scope is confirmed. Contact Instructure support immediately to request tenant-specific impact assessment.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected credentials and integrations to prevent continued exfiltration while preserving evidence of ShinyHunters access patterns

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export the full list of active Canvas OAuth tokens and API keys via Canvas Admin Console → Developer Keys (Admin > Developer Keys > API). For each key, record scope, creation date, and last-used timestamp. Pipe output to a CSV using curl against the Canvas REST API endpoint /api/v1/accounts/{account_id}/developer_keys with your admin token: 'curl -H "Authorization: Bearer " https://.instructure.com/api/v1/accounts/1/developer_keys > canvas_keys_audit.json'. Cross-reference against your institutional integration inventory; suspend any key lacking a documented owner or with 'manage_course_content' or 'read_sis' scopes.

Evidence: Before revoking any credential, capture: (1) Canvas Admin Audit Log export (Admin > Audit Log) filtered to the past 90 days showing all OAuth token grants and API key creation events — preserve as CSV; (2) Canvas API call logs from your institution's web proxy or firewall showing HTTP GET requests to /api/v1/users, /api/v1/accounts/*/enrollments, or /api/v1/sis_imports with volume spikes; (3) Instructure-provided tenant access logs if available via support ticket — request logs showing authentication events by service account username and source IP for the 60 days preceding disclosure.

Detection — Review Canvas audit logs and LMS access logs for anomalous bulk export activity, API calls pulling large student record sets, or access from unfamiliar IP ranges. Query for T1530/T1619 patterns: unusual cloud storage list or download operations tied to Canvas service accounts. No confirmed IOCs are publicly available at this time; monitor threat intelligence feeds for ShinyHunters-attributed indicators.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate Canvas API telemetry and SIS export logs against ShinyHunters TTPs to determine if your tenant was specifically targeted or collateral to a platform-level breach

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and

Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, run detection in three steps using free tooling: (1) Download Canvas Audit Log CSV (Admin > Audit Log, max 30-day window per export) and parse with Python pandas or grep for API calls to '/api/v1/accounts/*/users', '/api/v1/courses/*/enrollments', or '/api/v1/sis_imports/sis_csv' — flag any single service account exceeding 500 API calls/hour. (2) Query your institution's DNS or proxy logs for outbound connections from Canvas integration servers to known cloud storage endpoints (amazonaws.com, storage.googleapis.com, dropbox.com) that are not part of approved Canvas integrations. (3) Use the free Sigma rule 'AWS S3 Exfiltration' (SigmaHQ repo) adapted for your proxy logs to detect T1530 (Data from Cloud Storage) patterns attributable to Canvas service account credentials.

Evidence: Capture before analysis: (1) Canvas Live Events data stream if your institution subscribes — specifically 'asset_accessed' and 'grade_change' event types with actor.id, actor.metadata, and client_ip fields, stored as JSON; (2) SIS (Student Information System) integration sync logs showing the last 90 days of data pulls from Banner, Ellucian, or PowerSchool into Canvas — look for out-of-schedule or high-volume sync operations; (3) Web application firewall (WAF) or reverse proxy logs showing HTTP response sizes from Canvas subdomains — responses >1MB from /api/v1/users or /api/v1/enrollments endpoints are anomalous for normal use; (4) ShinyHunters infrastructure IOCs from threat intel feeds (MITRE ATT&CK Group G0114 profile, Recorded Future free tier, or OTX AlienVault community) to compare against source IPs in Canvas audit logs.

Eradication — No software patch applies. Revoke and reissue all Canvas API keys and service account credentials. Enforce least-privilege access on all LMS integrations. Disable or review any third-party Canvas integrations that were granted read access to student PII.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove ShinyHunters' persistent access vectors by eliminating all compromised or over-privileged credentials and integration points; verify no backdoor OAuth grants remain

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Execute credential eradication in sequence: (1) Via Canvas Admin Console, navigate to Admin > Developer Keys and delete all keys not in your approved integration inventory — do not deactivate, delete entirely. (2) For each remaining LMS integration (e.g., Turnitin, Zoom LTI, Panopto), review the LTI tool's requested Canvas permissions via Admin > Settings > Apps; remove 'edit_sis' and 'read_sis' scopes from any tool without documented business need using Canvas API: 'curl -X PUT -H "Authorization: Bearer " https://.instructure.com/api/v1/accounts/1/developer_keys/ -d "developer_key[scopes][]=url:GET|/api/v1/courses"'. (3) Audit Canvas service accounts in your IdP (Shibboleth, LDAP, Azure AD) and disable any account not mapped to a named human owner or documented integration.

Evidence: Before revoking, snapshot for forensic record: (1) Full Canvas Developer Keys page screenshot with all scopes visible — this is your pre-eradication baseline showing what access ShinyHunters or a compromised integration could have had; (2) Canvas LTI tool installation records from Admin > Settings > Apps exported as a list — document which tools had 'Public' privacy level (exposes student data to third-party LTI providers); (3) Your institution's IdP logs (Azure AD Sign-in Logs, Okta System Log, or Shibboleth idp-process.log) for Canvas service account authentication events — look for successful authentications from IP addresses not belonging to your campus network or approved integration hosts.

Recovery — Verify that rotated credentials are propagated to all dependent systems. Confirm that bulk export and data download permissions are restricted to authorized administrative roles only. Monitor Canvas audit logs for 30 days post-remediation for recurrence of anomalous access patterns.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore Canvas integrations to known-good configuration, verify no re-establishment of ShinyHunters access, and confirm PII export controls are enforced before returning systems to normal operational status

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Implement manual monitoring using two lightweight procedures: (1) Schedule a weekly cron job or Task Scheduler item to pull Canvas Audit Log CSV via API and run a Python script that flags any API call to '/api/v1/accounts/*/users' or '/api/v1/sis_imports' exceeding your defined baseline (recommend: median daily call count + 3 standard deviations from the 30-day pre-incident period). (2) Create a Canvas custom alert using built-in Admin Analytics (if your institution has Canvas Data 2 enabled) filtered to 'SIS export' event types — route email alerts to your security team. (3) Verify credential propagation by testing each dependent integration (Turnitin, Zoom, Banner) with a non-privileged test account to confirm new API keys are functional and old keys are rejected (HTTP 401).

Evidence: Document for recovery validation and future audit: (1) Canvas Admin Audit Log export immediately post-rotation showing zero activity from revoked key IDs — confirms eradication success; (2) Integration test results log showing new API key acceptance and old key rejection by each dependent system, with timestamps; (3) Canvas role permissions export (Admin > Permissions) showing that 'SIS Data' read/write and 'Bulk User Enrollments' permissions are scoped only to named administrative roles, not to integration service accounts or instructor roles.

Post-Incident — This incident exposes gaps in third-party data processor oversight and LMS access control governance. Review your institution's data processor agreements with Instructure under applicable privacy law (FERPA, GDPR where relevant). Assess whether student PII stored in Canvas exceeds minimum necessary data retention. Brief affected students and faculty per applicable breach notification obligations.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: document lessons learned specific to third-party LMS data processor risk, update data processor oversight procedures, and drive institutional control improvements to prevent recurrence via ShinyHunters or similar extortion actors

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-11 (Audit Record Retention), NIST SI-12 (Information Management and Retention), NIST RA-3 (Risk Assessment), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention), CIS 3.5 (Securely Dispose of Data)

Compensating: Conduct a two-person post-incident review using the following free resources: (1) Map Instructure's data processing obligations against your institution's existing DPA (Data Processing Agreement) using the IAPP Data Processing Agreement template checklist (free download at iapp.org) — specifically verify sub-processor disclosure clauses that would govern ShinyHunters-targeted cloud infrastructure Instructure relies on. (2) Run a Canvas Data retention audit using Canvas Data 2 (free to all Canvas institutions) or the legacy Canvas Data portal to enumerate all student PII fields actively stored: export the 'users' and 'enrollments' dimension tables and compare against your FERPA Records Retention Schedule to identify fields that can be purged. (3) Draft breach notification language using the EDUCAUSE Breach Notification Template (free, higher-ed specific) covering FERPA §99.64 notification requirements and applicable state breach laws.

Evidence: Preserve for regulatory and legal defensibility: (1) Instructure's official breach notification and tenant-specific impact assessment received via support ticket — timestamp and preserve as PDF with your ticket number; (2) Canvas Data 2 export of student PII fields active in your tenant at time of breach — this establishes scope for FERPA notification and demonstrates due diligence in data minimization assessment; (3) Your institution's current Data Processing Agreement with Instructure, including sub-processor schedules — required documentation for FERPA compliance review and potential GDPR Article 33 regulator notification if EU student data is involved; (4) Timeline reconstruction log combining Canvas Audit Log, IdP authentication logs, and network proxy logs establishing the earliest possible access date — critical for breach notification window calculations under applicable state laws and GDPR's 72-hour notification requirement.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) are publicly available from Instructure or verified threat intelligence sources at time of analysis. Detection should focus on behavioral indicators within Canvas audit logs and cloud

infrastructure logs: (1) Bulk API calls to student data endpoints from service accounts or third-party integrations outside normal operational hours; (2) Large-volume data exports or downloads via Canvas Data 2 (Instructure's data pipeline product) or direct API; (3) T1619 activity: enumeration of cloud storage objects associated with Canvas tenant storage; (4) T1567 activity: data staging or transfer to external web services from systems with Canvas database access. If your institution uses a SIEM, build detections around Canvas audit log events with high record-count thresholds and cross-reference with identity logs for T1078 (Valid Accounts) abuse. ShinyHunters has historically used credential stuffing and third-party data broker access as initial vectors; review whether any Canvas admin credentials appear in recent credential exposure datasets (third-party services: HaveIBeenPwned Enterprise, SpyCloud, or equivalent).

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1567** — Exfiltration Over Web Service
- **T1530** — Data from Cloud Storage
- **T1619** — Cloud Storage Object Discovery

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1530	Data from Cloud Storage	Collection
T1619	Cloud Storage Object Discovery	Discovery

Sources

Source	URL	Tier
	https://techcrunch.com/2026/05/05/hackers-steal-students-data-durin...	T2
ShinyHunters: Instructure breach affects 275 million teachers and ...	https://mashable.com/article/instructure-canvas-edtech-data-breach-...	T3
The data breach at education tech giant Instructure i - Facebook	https://www.facebook.com/techcrunch/posts/the-data-breach-at-educat...	T3
Edtech Firm Instructure Discloses Data Breach Amid Hacker Leak ...	https://www.securityweek.com/edtech-firm-instructure-discloses-data...	T3
Hackers steal students' data during breach at education tech giant ...	https://x.com/TechCrunch/status/2051672175053246609	T3

Generated 2026-05-06 09:03 UTC by TJS Security Command Center