INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 14:23 UTC

Massive Data Breach at Global Schools Foundation Exposes Sensitive Student and Employee Data

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0161
Type	Data Breach
Severity	HIGH
Affected Products	Global Schools Foundation (GSF), student and employee data
Discovery Source	Gemini

Executive Summary

Ransomware group FULCRUMSEC has claimed responsibility for a data breach against the Global Schools Foundation (GSF), an international school network, with the claim listed on ransomware.live and reported by RedPacket Security. The breach likely exposed personally identifiable information for students and employees, including potentially sensitive records for minors. Organizations affiliated with GSF face elevated regulatory exposure under data protection frameworks governing children's data, combined with significant reputational risk given the education sector context.

Technical Analysis

FULCRUMSEC self-reported the intrusion by listing GSF on their ransomware leak site, tracked via ransomware.live. No CVE has been assigned; this is an intrusion and data exfiltration event, not an exploitation of a publicly disclosed vulnerability. MITRE ATT&CK techniques associated with this activity include T1566 (Phishing, likely initial access), T1078 (Valid Accounts), T1041 (Exfiltration Over C2 Channel), T1486 (Data Encrypted for Impact), and T1657 (Financial Extortion). No confirmed IOCs, ransom note content, or forensic artifacts are available from public sources. Attribution rests solely on FULCRUMSEC's self-reported claim; independent forensic confirmation has not been published. Data types compromised are unconfirmed; the education sector victim profile elevates the likelihood of PII exposure including minors' records. No patch or vendor advisory applies, as this is not a software vulnerability event.

Action Checklist

1. Step 1: Containment. If your organization has any data-sharing, integration, or partnership relationship with Global Schools Foundation, audit and temporarily suspend data flows pending clarification of breach scope. Inventory all systems or directories that exchange or store GSF-originating data.
2. Step 2: Detection. Monitor for inbound communications referencing GSF student or employee data. Review email gateway logs for T1566-pattern phishing activity targeting your education-sector accounts (NIST AU-6). Search SIEM for T1078 indicators: logon activity from unfamiliar geographies or off-hours access on accounts with GSF-adjacent roles. Apply NIST SI-4 (Information System Monitoring) to flag anomalous local account behavior.
3. Step 3: Eradication. No patch is applicable; this is an intrusion event. If your organization shares infrastructure or identity systems with GSF, enforce immediate credential rotation for any shared or federated accounts (NIST IA-4 Identifier Management). Revoke and reissue any API keys or service accounts connected to GSF systems. Apply NIST IA-5 (Authenticator Management) across affected identity surfaces.
4. Step 4: Recovery. Validate that MFA is enforced on all externally exposed and administrative accounts per CIS 6.3, CIS 6.4, and CIS 6.5. Confirm audit logging is active and capturing authentication and data access events per NIST AU-2 and CIS 8.2. Monitor for secondary extortion contact or data appearing on paste sites or dark web sources referencing GSF.
5. Step 5: Post-Incident. Assess whether your organization's vendor or partner onboarding process evaluates third-party data handling and security posture; this incident illustrates third-party risk in the education sector. Review data minimization practices under NIST AC-3 and AC-6 to ensure shared data is scoped to need. Document this event in your risk register as a supply-chain and third-party risk indicator.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if your organization confirms that GSF held, processed, or transmitted student or employee PII on your behalf, or if FULCRUMSEC's leak site posts data identifiable to your organization's personnel or students, triggering mandatory breach notification obligations under FERPA, GDPR, state privacy laws, or equivalent children's data protection regulations.
Recovery Notes	After credential rotation and data flow suspension, continuously monitor your identity provider's authentication logs and dark web sources for evidence that FULCRUMSEC is leveraging GSF-derived credentials or PII to target your organization through secondary phishing or credential-stuffing campaigns (MITRE ATT&CK T1078, T1566). Maintain heightened monitoring for a minimum of 90 days given FULCRUMSEC's known extortion model, which typically includes staged data releases to pressure additional victims. Verify that all audit logs covering the breach window are preserved in read-only, integrity-protected storage before any systems are returned to normal operational state.

Forensic Artifacts	Identity provider authentication logs (Azure AD, Okta, ADFS) covering 90 days prior to FULCRUMSEC's ransomware.live claim date — specifically logon events for accounts with access to GSF-shared student and employee data repositories, filtered for Event ID 4624 (successful logon) and 4648 (explicit credential use) | Email gateway and MTA message trace logs for inbound and outbound communications referencing GSF domains, student roster filenames, or employee PII field patterns (e.g., CSV attachments containing SSN or DOB columns), covering the same 90-day window | File system access logs or DLP audit trails for any shared drives, SharePoint sites, or cloud storage buckets containing GSF-originating student or employee records — specifically access events by service accounts or federated GSF identity principals | API gateway or integration middleware logs showing data payloads exchanged between your systems and GSF endpoints, preserved before any integration suspension removes the connection state evidence | Ransomware.live and FULCRUMSEC leak site content (screenshot with timestamp and URL) documenting the specific data categories claimed in the breach, to establish regulatory notification scope and compare against your organization's data inventory

Per-Action IR Details

Step 1: Containment — If your organization has any data-sharing, integration, or partnership relationship with Global Schools Foundation, audit and temporarily suspend data flows pending clarification of breach scope. Inventory all systems or directories that exchange or store GSF-originating data.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), 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: Use 'netstat -anob' (Windows) or 'ss -tulnp' (Linux) to identify active connections to GSF IP ranges or hostnames. Run PowerShell 'Get-ChildItem -Recurse -Path C:\DataShares | Where-Object { $_.Name -like "*GSF*" }' to locate locally stored GSF-originating files. For federated identity, pull Azure AD or LDAP sign-in logs manually and grep for GSF domain accounts.

Evidence: Before suspending data flows, capture current network connection state (netstat output with timestamps), firewall egress logs showing traffic to/from GSF-owned IP ranges, and a directory listing of any shared drives or cloud sync folders containing GSF student/employee records. Preserve these as timestamped artifacts before any network changes alter the connection state.

Step 2: Detection — Monitor for inbound communications referencing GSF student or employee data. Review email gateway logs for T1566-pattern phishing activity targeting your education-sector accounts (NIST AU-6). Search SIEM for T1078 indicators: logon activity from unfamiliar geographies or off-hours access on accounts with GSF-adjacent roles. Apply D3-LAM (Local Account Monitoring) to flag anomalous local account behavior.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AC-7 (Unsuccessful Logon Attempts), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell 'Get-WinEvent -LogName Security | Where-Object { $_.Id -eq 4624 -or $_.Id -eq 4625 }' filtered to accounts with GSF-adjacent roles, looking for logon type 3 (network) or type 10 (remote interactive) from unexpected source IPs. Deploy Sysmon with the SwiftOnSecurity config to capture process creation (Event ID 1) and network connection (Event ID 3) events. For email, export MTA logs and grep for sender domains referencing GSF or subject lines containing student/employee PII keywords.

Evidence: Capture Windows Security Event Log entries for Event ID 4624 (successful logon) and 4648 (logon using explicit credentials) on accounts with access to GSF data repositories prior to any account lockdowns. Export email gateway message trace logs covering the 30 days prior to FULCRUMSEC's claim date on ransomware.live. Preserve

SIEM or raw syslog entries for authentication events on any federated identity provider (ADFS, Okta, Azure AD) connected to GSF.

Step 3: Eradication — No patch is applicable; this is an intrusion event. If your organization shares infrastructure or identity systems with GSF, enforce immediate credential rotation for any shared or federated accounts (D3-CRO). Revoke and reissue any API keys or service accounts connected to GSF systems. Apply D3-CH (Credential Hardening) across affected identity surfaces.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use 'net user /domain' or 'Get-ADUser -Filter * | Select SamAccountName, LastLogonDate' to enumerate accounts with GSF federation trust and identify dormant ones for immediate disablement. Rotate API keys via each vendor's CLI (e.g., 'aws iam create-access-key' followed by 'aws iam delete-access-key' for AWS service accounts). For on-premise environments, run 'dsquery user -inactive 8' to surface accounts unused in the past 8 weeks that may retain GSF data access.

Evidence: Before rotating credentials, export a full list of service accounts, API keys, and federated trust relationships with GSF systems from your identity provider — this establishes the pre-rotation blast radius for post-incident review. Capture Active Directory replication metadata ('repadmin /showrepl') if GSF had any domain trust relationship, to check for unauthorized trust modifications. Preserve any OAuth token issuance logs from your identity provider covering the breach window.

Step 4: Recovery — Validate that MFA is enforced on all externally exposed and administrative accounts per CIS 6.3, CIS 6.4, and CIS 6.5. Confirm audit logging is active and capturing authentication and data access events per NIST AU-2 and CIS 8.2. Monitor for secondary extortion contact or data appearing on paste sites or dark web sources referencing GSF.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), 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), CIS 8.2 (Collect Audit Logs)

Compensating: Validate MFA enrollment using your IdP's user report export (e.g., Azure AD MFA status report via 'Get-MsolUser -All | Select UserPrincipalName, StrongAuthenticationMethods'). For paste site and dark web monitoring without commercial tooling, configure free alerts via Have I Been Pwned's domain search API and manually check ransomware.live and FULCRUMSEC's known leak site at defined intervals. Use osquery with the 'last' table to continuously verify that only expected accounts are authenticating to systems holding former GSF data.

Evidence: Document the current MFA enrollment state for all externally exposed accounts as a recovery baseline — photograph or export the IdP MFA status report with a timestamp. Confirm that audit log storage capacity (NIST AU-4) is sufficient to retain authentication and data-access events for the retention period required by applicable children's data regulations (e.g., FERPA, GDPR-K). Preserve any extortion communications received from FULCRUMSEC in original format (email headers intact, screenshots of dark web postings) as potential legal evidence.

Step 5: Post-Incident — Assess whether your organization's vendor or partner onboarding process evaluates third-party data handling and security posture; this incident illustrates third-party risk in the education sector. Review data minimization practices under NIST AC-3 and AC-6 to ensure shared data is scoped to need. Document this event in your risk register as a supply-chain and third-party risk indicator.

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-20 (Use Of External Systems), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management

Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a tabletop exercise specifically scoped to a FULCRUMSEC-style ransomware-and-extortion scenario in the education sector using a two-person team with a printed runbook. Use a free GRC spreadsheet template (CIS CSAT or a custom risk register) to document the GSF incident as a third-party risk indicator with likelihood and impact scores. Review all current third-party data-sharing agreements for language requiring breach notification to your organization within a defined window, and flag any that lack this clause.

Evidence: Assemble a lessons-learned package including: the timeline of FULCRUMSEC's ransomware.live claim versus your organization's internal detection date, a list of all GSF-shared data categories (especially student PII and records of minors), and a copy of the current vendor onboarding checklist to document the gap that allowed a third party to hold sensitive data without adequate security posture verification. This package supports both internal improvement and any regulatory inquiry under FERPA, GDPR, or equivalent children's data frameworks.

Detection Guidance

No confirmed IOCs are available from public sources. Detection should focus on behavioral indicators consistent with FULCRUMSEC's claimed TTPs. Monitor for T1566 phishing attempts targeting education-sector accounts; review email gateway and proxy logs for suspicious attachment or link patterns. For T1078, query authentication logs for valid account use at unusual hours, from new geographies, or following password resets. For T1041, inspect egress traffic logs for large or anomalous outbound data transfers to unfamiliar external destinations. For T1486, monitor endpoint and file server logs for mass file encryption events or shadow copy deletion commands. If your organization has any data relationship with GSF, apply NIST SI-4 to flag local account anomalies and review NIST AU-6 audit record analysis cadence. Subscribe to threat intelligence feeds including CISA Automated Indicator Sharing (AIS), K-12 ISAC alerts (if applicable), and vendor threat feeds (Mandiant, CrowdStrike, Proofpoint) for updated FULCRUMSEC IOC releases as investigation details emerge.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft
- **T1566** — Phishing

NIST-800-53R5

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

- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Victim: Global Schools Foundation - Ransomware.live	https://www.ransomware.live/id/R2xvYmFsIFNjaG9vbHMgRm91bmRhdGlvbkBm...	T3
GSF - Global School Foundation	https://gsf.info/community-connect/gsg/	T3

Source	URL	Tier
Global Schools Group | Top Global Network of International Schools	https://globalschools.com/	T3
Global Schools Foundation: Shaping Leaders Of Tomorrow - YouTube	https://www.youtube.com/watch?v=7hcW3z0BJik	T3
[FULCRUMSEC] - Ransomware Victim: Global Schools Foundation	https://www.redpacketsecurity.com/fulcrumsec-ransomware-victim-glob...	T3

Generated 2026-06-11 14:23 UTC by TJS Security Command Center