ManageEngine
Log360

The role of SIEM in **education cybersecurity**

From threat detection to regulatory compliance

ManageEngine Log360

Table of Contents

Introduction — 1

Key cybersecurity challenges in the education industry — 2

Cybersecurity threats in the education sector — 4

Key logs to be monitored in the education industry — 6

Benefits of implementing SIEM in educational institutions — 10

SIEM use cases in the education industry — 15

How SIEM helps with regulatory requirements in the education industry — 18

How to choose the right SIEM solution for educational institutions — 19

Introduction

Educational institutions have become increasingly reliant on digital technologies to support learning, administration, research, and collaboration. This digital transformation has, however, increased the attack surface, exposing schools, colleges, and universities to a growing range of cyberthreats.

Did you know that 82% of K-12 schools suffered cyberattacks (between July 2023 and December 2024), and 63% were affected by ransomware in 2024? The average cost of recovery was reported to be $3.76 million for K-12 schools, and $4.01 million for higher educational institutions. Due to its vast repository of students' sensitive personal and medical data, along with its openness, diverse user base, and budgetary constraints, the education sector is a prime target for cybercriminals. Strengthening cybersecurity in education requires a multi-layered approach, addressing both technical vulnerabilities and human factors, including regular training, robust security protocols, and incident response planning.

Key cybersecurity challenges in the education industry

The following are the structural or operational limitations that make it difficult for educational institutions to defend against cyberthreats:

Budget constraints and understaffing

Many K-12 and higher education institutions operate with tight budgets and small IT teams, leaving cybersecurity under-prioritized or reactive. K-12 schools, in particular, allocate a maximum of 8%—with some using shockingly less than 1%—of their IT budgets on cybersecurity. Such limited funding restricts investment in advanced security tools and skilled personnel; and while the $200 million pilot program by the FCC to support cybersecurity services in education is a good start, the fact that it received requests totaling $3.7 billion emphasizes how tight budgets are and underscores the critical importance of cybersecurity in education.

Legacy infrastructure and unpatched systems

Many educational institutions continue to rely on outdated IT infrastructure—encompassing both software and hardware—that lacks robust security and is often incompatible with modern cybersecurity solutions. The discontinuation of security patch support for these legacy systems significantly increases vulnerability, making institutions prime targets for cyber exploitation.

Decentralized governance models

Universities and large school districts often operate within siloed IT environments across departments and campuses, resulting in inconsistent security policies and limited visibility. The continual turnover of students and faculty further complicates secure onboarding and offboarding processes. These dynamics make identity and access management (IAM) more complex and hinder the implementation of a unified cybersecurity strategy.

Remote learning and BYOD

The widespread adoption of remote learning and BYOD has expanded the attack surface within educational institutions. Personal laptops, tablets, and smartphones—often lacking enterprise-grade security controls—introduce vulnerabilities through unmanaged endpoints. These devices operate outside the traditional perimeter of institutional IT oversight, making it difficult for cybersecurity teams to enforce consistent policies, monitor activity, and respond to threats effectively.

Third-party and vendor risk management

Educational institutions rely heavily on third-party platforms—such as learning management systems, cloud storage, and student information systems—to support academic and administrative functions. However, these services can introduce vulnerabilities beyond institutional control. Educational institutions often lack effective frameworks to assess or monitor the cybersecurity posture of external vendors, resulting in limited visibility and increased exposure to third-party risks. Strengthening vendor oversight is critical to protecting institutional data and ensuring the resilience of digital education systems.

Lack of cybersecurity awareness

Students, educators, and administrative staff often lack formal training in cybersecurity or digital hygiene. This increases the risk of falling victim to phishing schemes, social engineering attacks, or mishandling sensitive data. As educational institutions increasingly depend on digital platforms, fostering cybersecurity awareness and equipping campus communities to identify threats and practice safe online behavior are vital to building a resilient learning environment.

Compliance complexities

Educational institutions are required to adhere to data protection regulations such as the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act, HIPAA, and the GDPR. Ensuring compliance becomes increasingly complex when institutions operate across jurisdictions and rely on a mix of on-premises and cloud-based tools, making it challenging to maintain consistent data governance and avoid regulatory penalties.

Cybersecurity threats in the education sector

Educational institutions face a growing number of cybersecurity threats due to their extensive storage of sensitive data (student and staff records, research data) and often limited cybersecurity resources. Microsoft reported that universities experience an average of 2,507 attempted cyberattacks per week.

The following are the key cybersecurity threats in the education sector:

Ransomware attacks

These attacks involve hackers encrypting data and demanding payment for its release, disrupting academic operations, corrupting backups, and exposing sensitive personal and personally identifiable data. This can cause significant financial and reputational damage to educational institutions. Schools are viewed as vulnerable due to inconsistent patching and under-resourced IT teams. As mentioned earlier, the mean recovery cost from a ransomware attack for K–12 organizations and higher education institutions has witnessed a multifold increase in 2024.

Phishing and social engineering

Staff, faculty, and students often lack awareness, making them vulnerable to credential theft, especially for email, learning management systems, and administrative platforms. Adversaries often impersonate trusted sources such as IT departments or faculty, using spoofed domains and urgent financial messaging to trick victims into revealing sensitive information, leading to data breaches and financial losses. Additionally, QR code phishing is surging across campuses, with Microsoft reporting that over 15,000 malicious messages containing QR codes are sent daily to educational institutions via flyers, emails, and digital handouts.

Malware

This includes viruses, worms, and spyware that can compromise data integrity, disrupt learning environments, and pose security risks for connected devices. The malware usually infiltrates systems via compromised attachments or fake updates and targets smart devices and IoT infrastructure used in modern classrooms.

Distributed denial of service (DDoS) attacks

These attacks overwhelm networks with traffic, making online learning platforms, exam portals, administrative systems, and other resources unavailable. DDoS attacks are often executed via botnets or compromised student devices, and can be carried out by hackers or malicious insiders. You can learn more about DDoS in educational networks here.

Credential stuffing and account takeovers

Due to password reuse and weak or limited MFA adoption, attackers frequently exploit compromised credentials (often acquired from previous breaches) to access sensitive systems like student information and financial aid portals, grading systems, or HR databases.

Data breaches and identity theft

Schools and universities store PII, financial data, academic records, and even health data—making them attractive targets for identity theft, fraud, or black-market resale. Such privacy violations can result in hefty financial and reputational loss for educational institutions. This is evidenced by the IBM report, which reports that the average cost of a data breach in the education sector in 2025 is $3.8 million.

Insider threats

Current or former students and employees, or contractors with network access, can pose risks through malicious intent or negligence, leading to unauthorized access, data leaks, or security breaches.

IoT vulnerabilities

The increasing use of connected devices in education (e.g., interactive learning tools, security cameras, smart cards, wearables, and smart HVAC and lighting systems) creates new vulnerabilities, as these devices often lack strong security measures. Without the required security hardening, these devices give attackers new entry points into the institutional network.

Cloud security risks

These risks stem primarily from misconfigured cloud settings and inadequate access controls, which can expose sensitive student data, research records, and administrative information to unauthorized access or cyberattacks. As schools and universities increasingly rely on platforms like Google Workspace and Microsoft 365, improper permission settings or a lack of role-based access can lead to accidental data leaks or malicious breaches.

Key logs to be monitored in the education industry

To maintain a secure and efficient digital environment, educational institutions must monitor logs from various sources. This is crucial for protecting sensitive data, ensuring system performance, and complying with regulations such as FERPA and the GDPR.

Learning management system (LMS) logs

LMS platforms like Moodle, Blackboard, or Canvas hold sensitive student and faculty data.

What to monitor

- **User login and logout activity:** Track access patterns and detect unauthorized access and suspicious login patterns targeting faculty or admin accounts.
- **Course access logs:** Monitor which users access which courses and when.
- **Assignment submissions and grading logs:** Ensure the integrity of academic records and track unauthorized modifications to exams, grades, or learning content.
- **Permission changes:** Detect unauthorized privilege escalation.
- **API usage logs:** Monitor integrations with third-party tools for anomalies.
- **File uploads and downloads:** Identify mass downloads or uploads of potentially malicious files.
- **New user creations:** Spot fraudulent account creation to bypass authentication controls.

Student information system (SIS) logs

Monitoring SIS logs is essential for identifying unauthorized access, data manipulation, or misuse of student records—safeguarding data integrity, ensuring privacy compliance, and defending against internal and external threats.

What to monitor

- **Data access logs:** Track who accessed sensitive student data.
- **Record modification logs:** Monitor changes to grades, attendance, or personal details.
- **Authentication attempts:** Detect brute-force or credential stuffing attacks.
- **Role-based access changes:** Ensure only authorized personnel have access to sensitive data.

Firewall logs

Firewalls act as the first line of defense, making their logs vital for identifying perimeter threats.

What to monitor

- **Blocked and allowed connections:** Identify suspicious inbound or outbound connections, especially to high-risk geolocations. Doing so can help detect data exfiltration or malware communication.
- **Port scanning or unusual protocol usage:** Detect reconnaissance attempts targeting common service ports (e.g., 21, 22, 3389, 445, 1433) and flag reconnaissance activities.
- **VPN access logs:** Monitor unusual connection times or locations for remote faculty or administrative staff accessing internal systems.
- **Repeated denied access attempts:** Spot brute-force attacks or malware trying to exfiltrate data.

Web proxy and content filtering logs

Educational institutions often need to control and monitor web usage for compliance and safety.

What to monitor

- **Access to prohibited or high-risk sites:** Detect visits to phishing or malware-hosting domains.
- **Unusual download activity:** Flag large or repeated downloads that could indicate data exfiltration.
- **Bypass attempts:** Monitor use of anonymizers, VPNs, or proxy tools that may hide malicious activity.
- **High volume HTTP/S requests:** Identify bot infections or compromised devices.

IAM logs

Authentication logs provide visibility into account security for staff, students, and administrative users.

What to monitor

- **Failed login attempts:** Identify brute-force attacks or credential stuffing attempts.
- **MFA status:** Ensure MFA is enforced and functioning.
- **Logins from unusual locations:** Spot potential account compromise by correlating with geolocation data.
- **Multiple concurrent logins:** Detect credential sharing or account misuse.
- **Group membership changes:** Track admin-level access changes or role modifications.
- **Account lockouts and password resets:** Detect potential account compromise.

Cloud application and application server logs

Educational institutions rely on these logs to monitor system performance, detect application errors, and investigate security incidents across LMS platforms and student portals.

What to monitor

- **HTTP request patterns:** Detect abnormal usage or potential DDoS attacks.
- **Error logs:** Identify application failures or misconfigurations.
- **Session management logs:** Monitor for session hijacking or replay attacks.
- **File access logs:** Track access to sensitive documents or resources.
- **Mass data downloads:** Detect attempts to extract large volumes of academic or personal data.

Database logs

Helps educational organizations monitor data access and changes, helping protect student records and support audits.

What to monitor

- **Query logs:** Detect unauthorized data access or data scraping.
- **Failed login attempts:** Identify brute-force attacks on database credentials.
- **Data modification logs:** Track changes to student records or financial data.
- **Privilege escalation attempts:** Monitor for unauthorized access to admin functions.

Email security gateway logs

Email remains a major attack vector in the education sector.

What to monitor

- **Phishing attempts and spam detection (including spoofed sender addresses):** Identify malicious emails targeting staff or students by impersonation and other tactics.
- **Email forwarding rules:** Detect data leakage via auto-forwarding.
- **Login anomalies:** Monitor for compromised email accounts.
- **Attachment scanning logs:** Flag malware or sensitive data sharing.
- **High-volume outbound emails:** Spot potential compromised accounts sending spam or phishing.

Endpoint detection and response logs

Endpoints in education environments pose a high risk due to shared devices and BYOD policies.

What to monitor

- **Malware and ransomware alerts:** Identify infected devices and respond to threats before they spread.
- **Unauthorized software installation:** Prevent the use of unapproved and risky applications.
- **Suspicious process executions:** Flag scripts, macros, or binaries attempting lateral movement.
- **USB device usage logs:** Monitor for data theft via removable media.
- **Device compliance status:** Ensure devices meet security standards.

Physical access control logs

Educational institutions use physical access control logs from RFID systems and biometric scanners to monitor entry and exit activity, ensuring campus safety and managing authorized access.

What to monitor

- **Entry and exit timestamps:** Track physical access to sensitive areas like server rooms.
- **Access denial events:** Detect unauthorized entry attempts.
- **Badge misuse:** Identify potential insider threats.

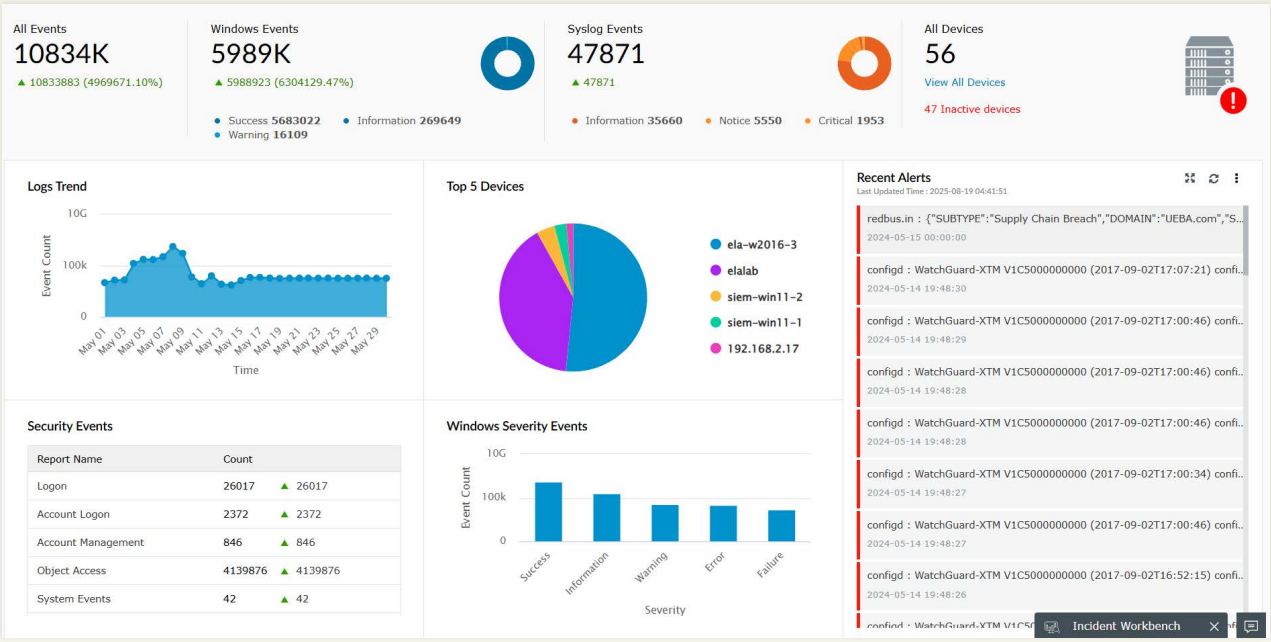
Benefits of implementing SIEM in educational institutions

A SIEM solution enhances operational efficiency and optimizes resources by automating incident response workflows, reducing the manual burden on understaffed security teams. By centralizing security monitoring into a single platform, SIEM streamlines visibility. Its ability to prioritize high-risk alerts ensures security teams focus on the most critical threats, enabling a proactive security posture that shifts from reactive security to predictive defense strategies.

Here's how SIEM solutions benefit the education industry:

1. Centralized visibility and monitoring

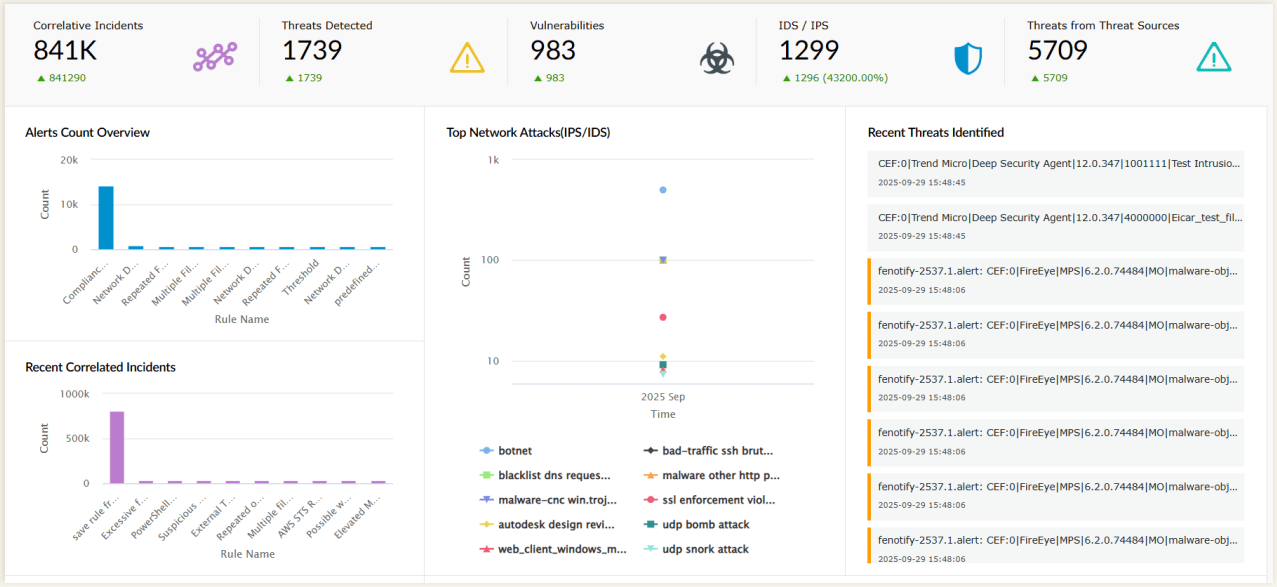
- **Unified security monitoring:** Consolidate logs from academic systems, LMS, SIS, and administrative platforms; firewalls; endpoints; servers; cloud applications; and databases into a single pane-of-glass view.
- **Cross-campus insight:** Monitor security activity across multiple campuses, departments, and remote learning environments in real time.
- **Device discovery:** Helps identify all connected devices and systems automatically, ensuring nothing is left unmonitored.
- **Unified visibility across cloud and on-premises systems:** SIEM bridges visibility across hybrid environments, allowing institutions to monitor both cloud-hosted applications (like Google Workspace or Microsoft 365) and on-premises servers from a single dashboard.



Log360 dashboard providing a single-pane-of-glass view of all security events

2. Early threat detection and response

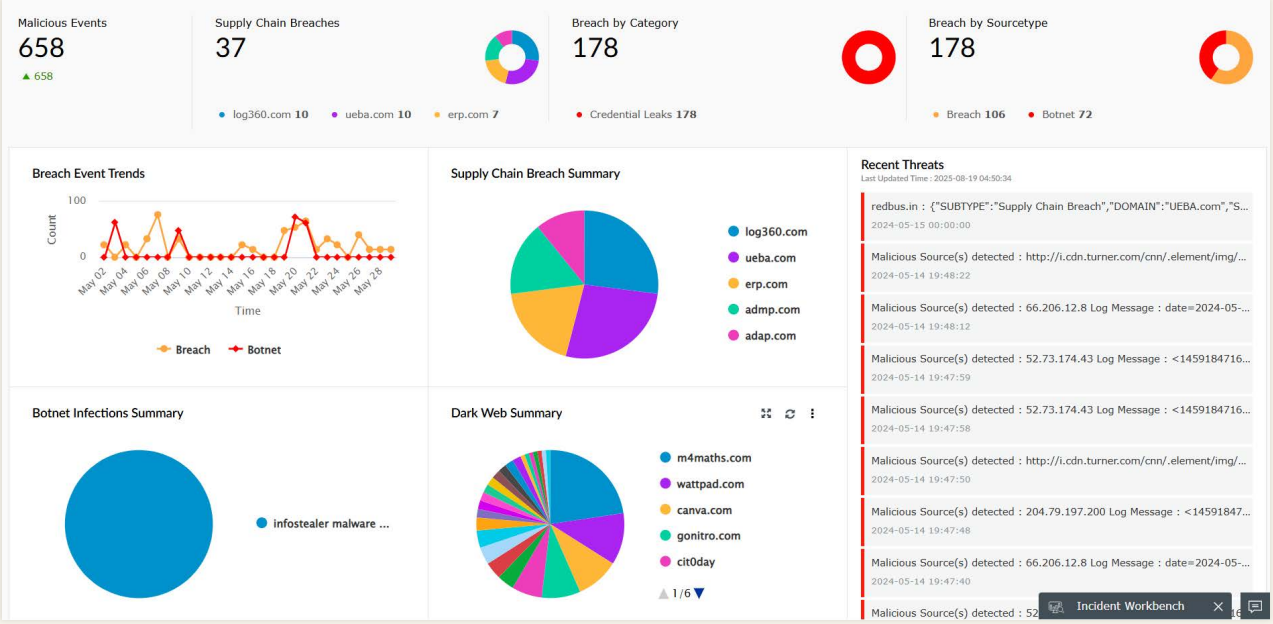
- **Detect sophisticated attacks early:** Leverage user and entity behavior analytics to identify threats like ransomware, APTs, or compromised accounts targeting student, faculty, or research data before they escalate.
- **Correlate multi-source events:** Combine logs from SISs, LMSs, firewalls, endpoints, and other sources to reveal hidden attack patterns and lateral movement.
- **Integration with threat intelligence:** SIEM solutions integrate with global threat feeds to recognize known attack signatures.
- **Receive real-time alerts:** Get instant notifications on suspicious activity to minimize mean time to detect and respond to security incidents.
- **Eliminate visibility gaps:** Monitor on-premises, cloud, and hybrid learning environments to reduce blind spots and strengthen overall detection capabilities.



Security Overview dashboard in Log360

3. Protection of sensitive student and research data

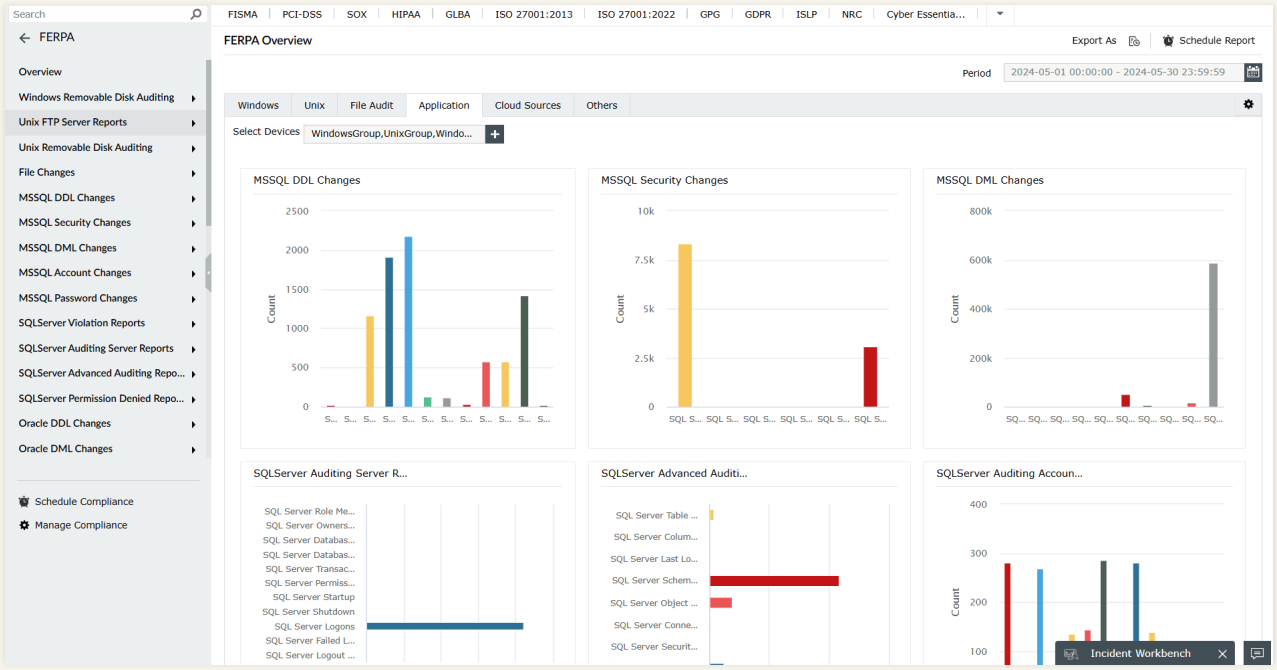
- **Safeguard PII:** Prevent unauthorized access to student records, financial details, and health data.
- **Detect compromised credentials:** Leverage dark web monitoring capabilities to identify the compromised credentials of students, faculty, and administrative staff before attackers exploit them.
- **Prevent data exfiltration:** Detect unusual outbound traffic that may signal a data breach.
- **Mitigate insider threats:** Identify suspicious access patterns and privilege escalation attempts from faculty, staff, or students.
- **Ensure data integrity:** Maintain accurate academic records and research results by monitoring tampering attempts.



Threat analytics dashboard in Log360 providing insights on breach data

4. Compliance with data privacy regulations

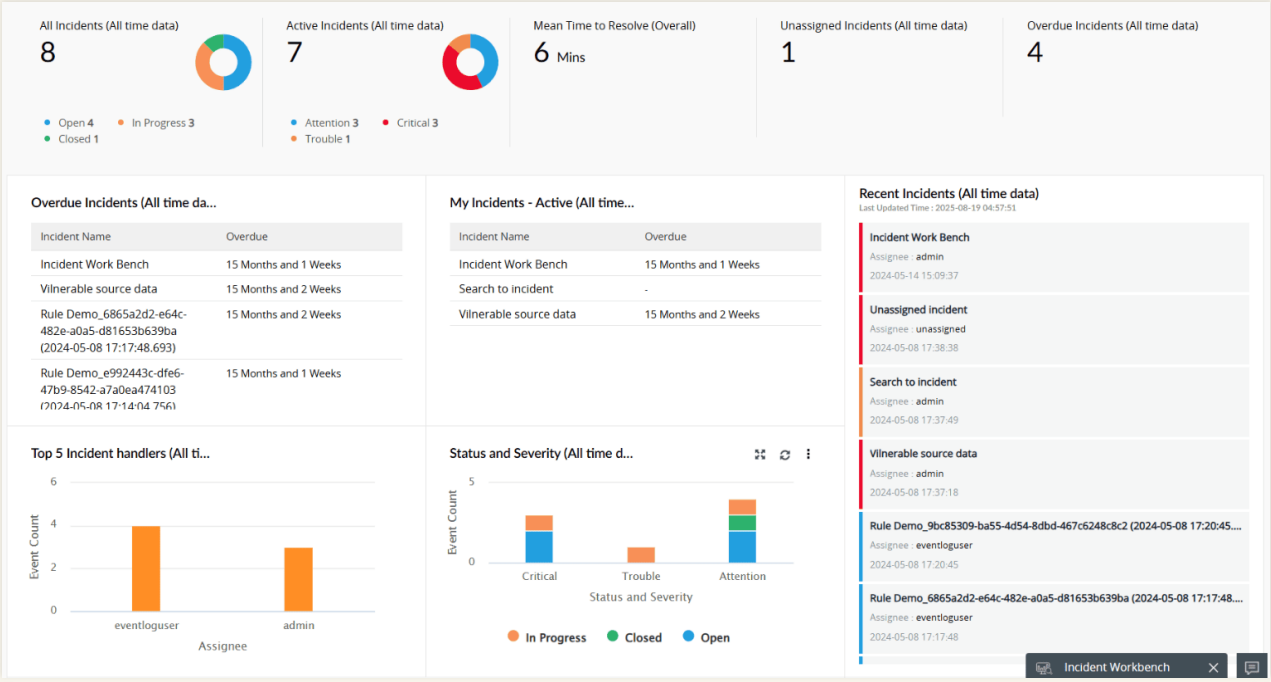
- **Regulatory alignment:** Automate log collection and retention to align with compliance mandates like FERPA, the GDPR, and HIPAA.
- **Enable continuous compliance monitoring:** Use automated alerts and dashboards to detect potential regulatory breaches in real time.
- **Streamline audit readiness:** Generate compliance reports with minimal manual effort.
- **Demonstrate due diligence:** Provide evidence of proactive cybersecurity measures to boards and regulators.
- **Policy enforcement:** Educational institutions can enforce access controls and monitor policy violations.



Audit-ready compliance reports for FERPA offered by Log360

5. Faster incident response

- **Automated workflows:** SIEM can trigger automated responses to certain threats, such as account lockdown, disabling the user, and shutting down the system, reducing manual intervention.
- **Root cause analysis:** It helps security teams quickly identify the source of an incident and contain it.
- **Incident prioritization:** Alerts are ranked by severity, allowing teams to focus on the most critical threats first.
- **Reduced recovery time:** Faster response leads to quicker recovery and less disruption to academic operations.



Incident overview dashboard in Log360

SIEM use cases in the education industry

Preventing insider threats and shadow IT in academic environments with SIEM

The decentralized nature of educational institutions often results in departments independently adopting cloud applications and granting broad access permissions. A SIEM solution helps security teams detect insider threats, uncover shadow IT, and reduce the risk of sensitive data exposure.

Challenges

- Academic environments support thousands of users with varying access privileges across campus networks, cloud services, and research platforms.

  Risks include:

  1. Faculty or students intentionally or unintentionally accessing data beyond their authorized roles.

  2. Use of unauthorized cloud applications and file sharing services (shadow IT) to store or exchange institutional data.

  3. Excessive privileges, dormant accounts, or policy violations increasing the risk of data leaks and insider threats.

- Security teams often lack centralized visibility into user activity and unauthorized application usage across distributed academic environments.

How a SIEM solution like Log360 helps

- **Cross-platform event correlation:** Correlates authentication logs, file access events, administrative changes, endpoint activity, and network traffic to detect indicators of insider threats and unauthorized activities.
- **Behavior analytics:** Uses UEBA to detect anomalous activities such as unusual data downloads, after-hours access, privilege misuse, or abnormal access to research and student records.
- **Privilege monitoring:** Tracks account modifications, privilege escalation attempts, and changes to sensitive groups to reduce the risk of insider abuse.
- **Cloud security:** A SIEM solution with CASB capabilities helps detect and ban shadow and risky applications, and enforce policies to ensure the use of only sanctioned applications in educational institutions.
- **Automated incident response:** Triggers alerts and predefined response workflows and playbooks to investigate suspicious users, revoke access, or isolate affected endpoints before sensitive data is compromised.

To learn more, read: Educational institutions: How a CASB will help secure them.

Securing email, collaboration tools, and smart campus devices with SIEM

Fragmented systems and shared access points create blind spots and vulnerabilities across smart campus environments. A SIEM solution centralizes visibility and correlates events across platforms to detect threats and enforce security policies.

Challenges

- Smart campuses depend heavily on email, cloud collaboration, Wi-Fi networks, and shared devices.

  Risks include:

  1. Phishing and credential theft via faculty and student emails.

  2. Unauthorized access to lab devices and shared resources.

  3. Spread of malware in open computer labs.

- CISOs lack a unified view of these disparate attack surfaces.

How a SIEM solution like Log360 helps

- **Centralized visibility:** Aggregates logs from email gateways, Wi-Fi controllers, endpoint security, and lab systems.
- **Dark web monitoring:** Identifies compromised credentials of students, faculty, and staff.
- **Threat detection:** Identifies spear-phishing, suspicious file sharing, privilege escalation attempts, or simultaneous logins from different geographies.
- **Data loss prevention:** Tracks suspicious file accesses, modifications, uploads, and downloads to prevent the exfiltration of sensitive academic research, student data, and intellectual property.
- **Automated response:** Incident response playbook actions get triggered to isolate compromised accounts and devices to contain the threat.

To learn more, read: Comprehensive cybersecurity for smart campuses: Securing email and collaboration tools, computer labs, and shared devices.

Securing gamification and e-learning platforms with SIEM

Gamified learning platforms and e-assessments are prone to cheating, data leaks, and unauthorized access. A SIEM solution helps track user behavior, detect anomalies, and protect sensitive educational data in real time.

Challenges

- Adoption of gamified learning and online exams creates risks:

  Risks include:

  1. Account misuse (shared or stolen credentials).

  2. Exam integrity breaches (unauthorized content access, script automation of quiz attempts).

  3. DDoS attacks targeting exam servers during critical times.

- Traditional monitoring lacks forensic depth for incident analysis.

How a SIEM solution like Log360 helps

- **Authentication monitoring:** Detects multiple logins from different geographies on the same account, suspicious access, or token misuse.
- **Anomaly detection:** Flags anomalous user and entity behavior, such as automated scripts attempting rapid submissions or manipulation of scores.
- **Custom rule creation:** Enables the creation of custom rules and alerts for identifying suspicious threat patterns, unauthorized access, and data exfiltration.
- **Access control integration:** Works with IAM solutions to enforce strict identity validation for online exams.
- **Forensic investigation:** Enables root-cause analysis and reporting to strengthen digital exam policies.

To learn more, read: Securing e-learning and gamification platforms: Risks and best practices

How SIEM helps with regulatory requirements in the education industry

For CISOs in the education sector, maintaining compliance with regulatory requirements is critical to protecting student privacy, institutional reputation, and funding eligibility. SIEM solutions play a pivotal role in achieving and demonstrating compliance by centralizing log collection and retention from diverse systems such as SISs, LMSs, network devices, and cloud platforms for the mandated retention periods. They automate compliance reporting with prebuilt and customizable templates that address frameworks like FERPA, the GDPR, HIPAA (for research or health data), and other regional education data policies.

SIEM solutions also enable real-time compliance monitoring by continuously tracking access, data usage, and system activity to ensure adherence to policies while detecting violations early. Additionally, they support audit readiness and forensic investigations by providing complete, time-stamped event trails, reducing the time and effort needed to respond to compliance inquiries. In the education sector, SIEM is an indispensable tool to ensure that data governance, access control, and incident response protocols align with regulatory mandates.

A unified SIEM solution like ManageEngine Log360 can further strengthen compliance efforts in the education industry by offering an integrated platform for log management, threat detection, and compliance reporting. With centralized monitoring of student and institutional data, Log360 helps detect anomalies, prevent data misuse, and maintain a secure digital ecosystem. It also comes with built-in compliance-specific report templates for major regulations, making it easier to generate audit-ready documentation without manual effort.

Log360's real-time alerting and correlation capabilities help detect policy violations the moment they occur, while its long-term log archival ensures records are retained securely in line with regulatory requirements. With centralized visibility and advanced search features, Log360 allows CISOs to quickly trace incidents, prove adherence during audits, and proactively address compliance risks across on-premises, cloud, and hybrid learning environments.

How to choose the right SIEM solution for educational institutions

01 **Assess institutional needs:** Evaluate the scale of your IT infrastructure, number of users, and mix of on-premises, cloud, and hybrid learning environments.

02 **Consider deployment flexibility:** Whether on-premises, cloud-based, or hybrid, the SIEM solution should align with your institution's IT strategy and data residency requirements.

03 **Ensure broad log collection:** Choose a SIEM solution that can gather logs from SISs, LMSs, endpoints, firewalls, applications, databases, and cloud services.

04 **Look for advanced analytics:** Prioritize solutions with correlation rules, behavioral analysis, and AI and ML to detect sophisticated threats such as ransomware, phishing, and insider attacks.

05 **Enable real-time detection and response:** Ensure the SIEM solution offers real-time alerts, automated workflows, and tools to reduce mean time to detect (MTTD) and mean time to respond (MTTR) to security events in your institution.

06 **Verify scalability:** Confirm the SIEM solution can process high log volumes across multiple environments without performance issues.

07 **Check integration capabilities:** Ensure compatibility with other tools like IAM, UEBA, CASB, EDR, and DLP for a unified security posture. You should also ensure that the SIEM solution integrates smoothly with your existing infrastructure.

08 **Simplify compliance management:** Opt for SIEM solutions with built-in compliance reporting for FERPA, HIPAA, the GDPR, and the PCI DSS to ease audit preparation.

09 **Look for education-specific use cases:** Look for SIEM solutions that offer preconfigured rules and dashboards tailored to common threats and operational needs in academic environments.

10 **Validate log retention and forensic capabilities:** Ensure that the SIEM solution offers secure, tamper-proof log storage and easy access to historical data for investigations and audits.

11 **Evaluate usability and support:** Look for ease of deployment, intuitive dashboards, customization options, and responsive vendor support for long-term operational success.

ManageEngine
Log360

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

Demo Download

Our Products

Log360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus