ManageEngine
Log360

SIEM in healthcare cybersecurity: Challenges, use cases, and compliance

www.manageengine.com/log-management/

Table of contents

Introduction

The healthcare industry is rapidly evolving, driven by digital transformation initiatives such as electronic health records (EHRs), telemedicine, cloud adoption, and connected medical devices. While these advancements improve patient care and operational efficiency, they also significantly expand the attack surface.

As a result, healthcare has become one of the most targeted industries for cyberattacks. From ransomware disrupting hospital operations to breaches exposing sensitive patient data, the risks are both frequent and severe. This makes a strong, centralized security approach, such as the implementation of a SIEM solution, essential for modern healthcare environments.

In 2025:

- 93% of healthcare organizations experienced a cyberattack with 1,542 confirmed data breaches.
- Healthcare accounted for 22% of global ransomware attacks.
- 168,647 individuals were affected per day by healthcare breaches.

Cybersecurity challenges in healthcare

Unlike other businesses, a cyberattack in healthcare doesn't just mean financial or reputational loss. It can directly endanger patients, compromise important medical research, and break the trust between patients and doctors. These problems come from many sides: complex hospital computer systems, easily attacked medical devices, and mistakes made by healthcare workers themselves.

This section focuses on the biggest problems that the healthcare industry currently faces.

1 Hospitals: Complex environments and critical operations

a. Highly complex infrastructures

Hospitals operate some of the most intricate IT environments in any industry. Their networks span EHR systems, diagnostic equipment, Internet of Medical Things (IoMT) devices, cloud-based services, and a multitude of third-party integrations. This complexity is compounded by the need to connect with external labs, remote consultants, and telehealth platforms, each introducing new vulnerabilities and expanding the attack surface.

b. Legacy systems and outdated devices

Many hospitals still rely on legacy systems that were never designed with cybersecurity in mind. These outdated components often lack basic security controls and are difficult to patch or monitor, creating persistent blind spots that attackers can exploit.

c. Disruption equals danger

Unlike other sectors, a cyberattack in a hospital can have immediate, life-threatening consequences. Ransomware or system outages can delay surgeries, disrupt emergency care, and force staff to revert to manual processes, putting patient lives at risk.

The Health-ISAC 2025 threat report highlights that loss of access to diagnostic tools or medical records can lead to patient diversions, canceled surgeries, and compromised quality of care.

2 Medical research: Protecting intellectual property and data integrity

a. Espionage and nation-state threats

Medical research institutions are prime targets for cyber-espionage, especially from nation-state actors seeking to steal valuable intellectual property, such as pharmaceutical formulas, clinical trial data, or pandemic research. The same threat report mentioned earlier notes a rise in targeted espionage campaigns against research organizations.

b. Data integrity and authenticity

The integrity of research data is paramount. Manipulation or corruption of clinical trial results can have catastrophic consequences, leading to incorrect conclusions, regulatory setbacks, or even patient harm. Attackers may target data for sabotage, extortion, or to undermine trust in research outcomes. Another avenue in healthcare that presents security risk is AI-based diagnostics and decision support. Adversarial attacks like evasion and poisoning attacks can result in misdiagnosis and threaten patients' safety.

c. Collaboration risks

Research increasingly involves collaboration across institutions and borders, often using cloud-based platforms and shared data repositories. Each new integration point introduces additional risk, especially when partners have varying security postures or controls. Learn how to improve cloud security in healthcare with a CASB.

3 Patient data integrity: The foundation of trust and care

a. Data breaches and privacy violations

Patient records are among the most valuable data on the black market, making them a perennial target for cybercriminals. Breaches not only violate privacy but can result in identity theft, insurance fraud, and long-term reputational damage for both patients and providers. Attackers have even started targeting emergency medical transportation service providers to expand the blast radius and access healthcare records, as observed in this major attack.

b. Cloud misconfigurations and data exposure

As healthcare shifts to the cloud, misconfigured storage or lax access controls have led to massive leaks of sensitive patient data. In 2025, a major U.S. health insurer exposed 4.7 million PHI records due to a misconfigured cloud bucket, underscoring the importance of proper monitoring and controls.

c. Insider threats

Healthcare is especially vulnerable to insider threats, whether from negligent staff clicking on phishing links or malicious insiders abusing their access to sensitive data. Weak password practices and lack of user monitoring exacerbate this risk.

d. Supply-chain and third-party risks

Hospitals and clinics depend on a web of third-party vendors for everything from billing to diagnostics. Breaches in these external systems can cascade into the core healthcare network, introducing new avenues for attackers. You can learn more about a third-party healthcare vendor breach affecting millions of people here.

4 IoMT: A new frontier of vulnerabilities

a. Device proliferation

Hospitals now deploy thousands of connected medical devices—pacemakers, infusion pumps, imaging machines, etc.—many of which lack robust security features or regular patching.

b. Patient safety risks

A compromised IoMT device can do more than leak data—it can directly endanger patient lives by malfunctioning or delivering incorrect dosages. Attacks on these devices are rising and often go undetected without specialized monitoring. You can learn more about the security risks associated with healthcare IoT devices here.

5 The human element: Training, stress, and social engineering

a. Phishing and social engineering

Healthcare staff operate in high-pressure environments, making them more susceptible to phishing and social engineering attacks. AI-powered phishing campaigns are becoming harder to detect, increasing the risk of credential compromise and unauthorized access.

b. Staff morale and operational resilience

Repeated breaches and prolonged outages take a toll on staff morale and operational resilience. The stress of managing crises can divert attention from patient care and weaken the institution's ability to recover from future incidents.

c. Budgetary constraints

Chronic under-investment in cybersecurity is a recurring issue. Budget limitations mean fewer resources for security staff, training, and modern defenses, leaving hospitals especially vulnerable to sophisticated attacks.

How SIEM can help protect healthcare networks

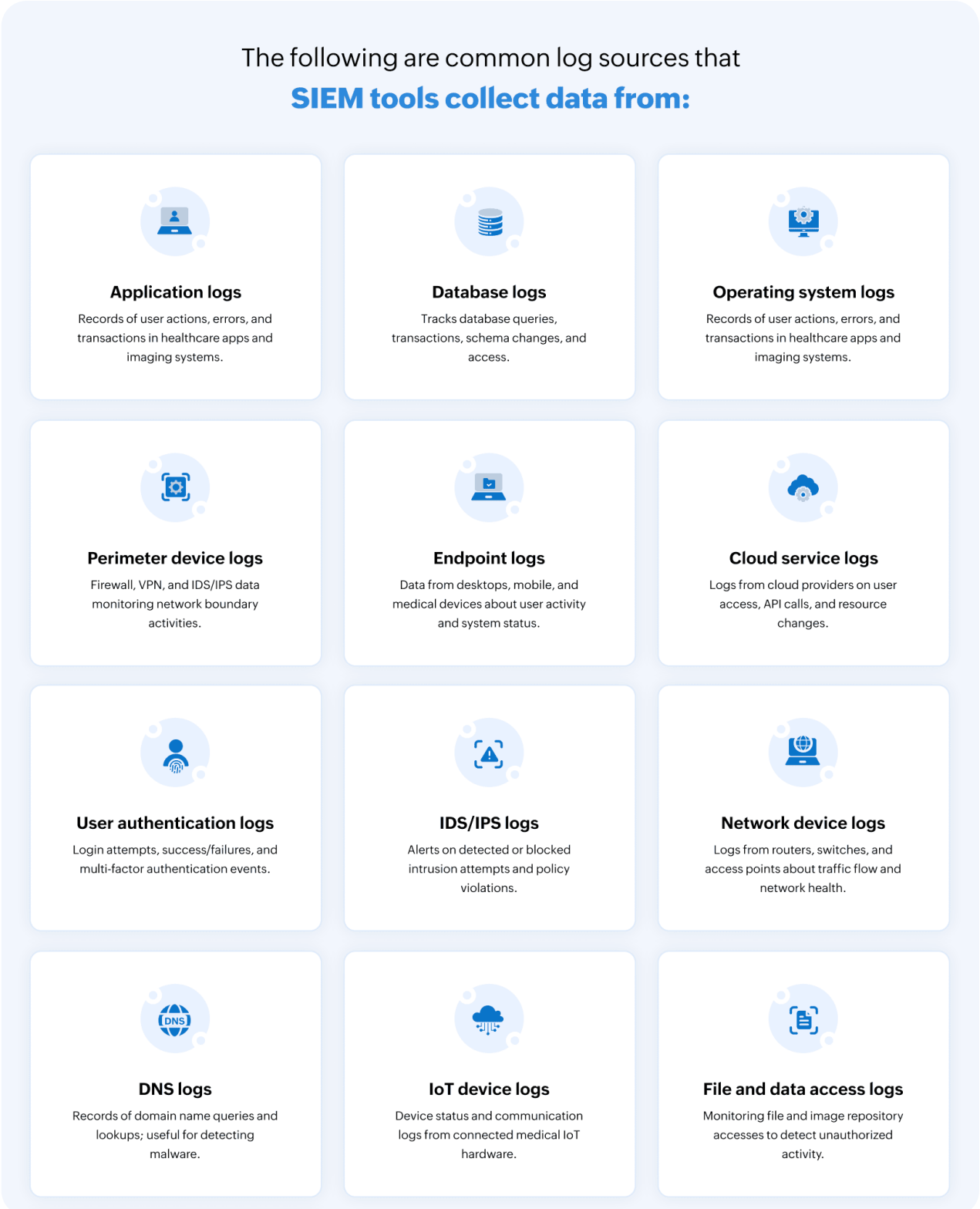
With cyberthreats lurking at every turn, healthcare organizations must mount a formidable defense to safeguard their reputation, financial stability, and the trust patients place in their care. A proactive security approach isn't just a necessity—it's the foundation of resilience against attackers aiming to disrupt operations and compromise sensitive health data.

For such a defense, healthcare industries must consider investing in a good SIEM solution. SIEM solutions can form the backbone of healthcare security and can help detect and fend off threats before they snowball.

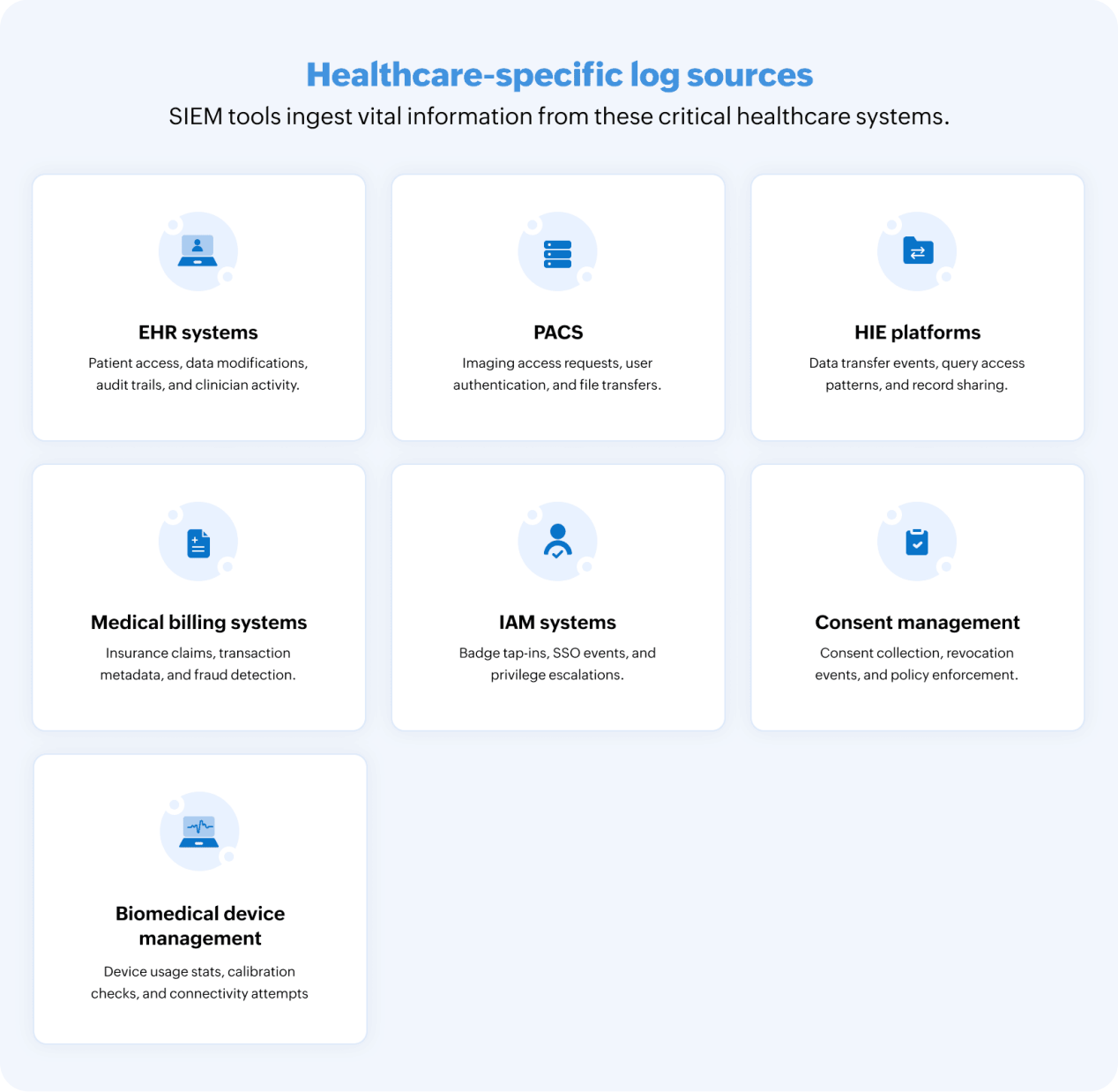
A robust SIEM architecture is designed to provide comprehensive, real-time security monitoring and rapid incident response across every layer of the organization. The SIEM solution collects data from several log sources across the organization's network and correlates them in real time to identify anomalies, track suspicious behavior, and generate actionable security alerts that support threat detection, compliance reporting, and forensic investigation.

Key log sources to be monitored

The common log sources that SIEM tools collect data from are shown in the figure below:



In addition to these, healthcare networks have industry-specific log sources like patient monitors and IoMT devices that also need to be fed into the SIEM tool to ensure all-around healthcare security.



Key benefits of SIEM in healthcare

Healthcare organizations face an unrelenting threat landscape while managing complex, heterogeneous IT environments spanning clinical systems, medical devices, and cloud platforms. A SIEM solution consolidates security monitoring across these environments, providing the visibility and control needed to protect patient safety and data integrity.

Implementing a SIEM solution provides the following benefits to healthcare organizations:

1. **Scalability for diverse healthcare environments:** Adapts to the logging and security needs of large hospital networks, research institutions, and smaller clinics alike.

2. **Centralized visibility across systems:** Consolidates logs and events from EHRs, IoMT devices, cloud platforms, and network infrastructure into a single pane of glass for unified monitoring.
3. **Enhanced protection of ePHI:** Continuously monitors access to sensitive patient data, ensuring confidentiality, integrity, and availability.
4. **Real-time threat detection:** Correlates events and identifies anomalies, suspicious behavior, and known attack patterns early, helping prevent ransomware, data breaches, and insider threats.
5. **Dark web monitoring:** Monitors the dark web for any mention of an organization's sensitive information, including domain names, employee credentials, patient health and financial information.
6. **Insider threat detection:** Uses behavioral analytics (UEBA) to identify unusual user activity, whether malicious or accidental.
7. **Secure cloud and telemedicine usage:** Monitors and enforces security policies across cloud applications and remote care platforms when integrated with a CASB.
8. **Faster incident response:** Integrates with SOAR capabilities to automate investigation and response playbooks, reducing attacker dwell time and minimizing damage.
9. **Improved compliance readiness:** Simplifies adherence to regulations like HIPAA, HITRUST, NIST, and the GDPR through automated log collection, audit trails, and reporting.
10. **Dashboard and reporting:** Offers real-time visibility, alerts, and compliance reporting tailored to healthcare regulations.

Scenario: How a SIEM tool can defend a hospital network

Situation

A large hospital experiences a sudden spike in failed login attempts on its servers that hold EHRs, followed by unusual data transfers from a radiology workstation to a cloud storage service.

How the SIEM tool responds

- **UEBA** detects the anomalous login behavior and flags the user account for review.
- **The CASB** identifies that the data transfer is to an unauthorized cloud service and immediately blocks the transaction.
- **Threat detection** correlates these events with a known ransomware campaign targeting healthcare.
- **SOAR** triggers an automated response: isolating the affected workstation, forcing password resets, and notifying the security team.
- **Reports** are automatically generated, documenting the incident for further investigation.

Outcome

The attack is contained before sensitive data is exfiltrated or systems are encrypted, and the hospital avoids both operational disruption and regulatory penalties.

SIEM use cases in healthcare

Use case 1: ePHI protection in a hospital environment

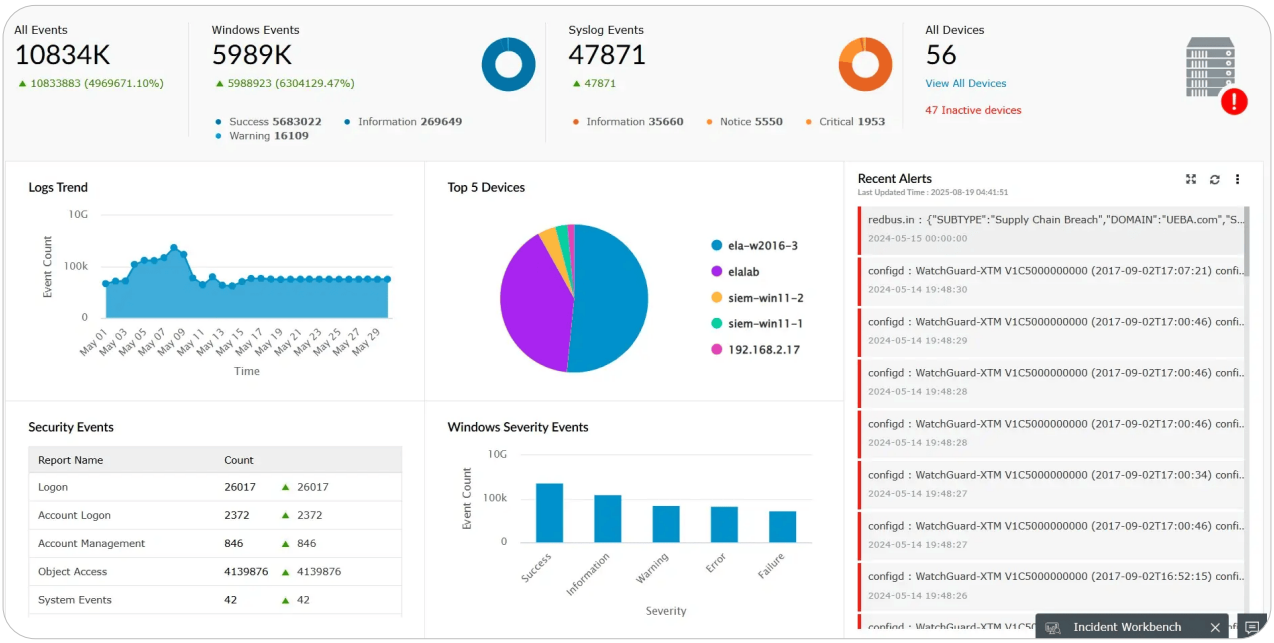
Hospital environments generate vast volumes of ePHI across interconnected systems. A SIEM solution helps monitor diverse log sources, detect threats, and safeguard sensitive patient data, including medical images, in real time.

Challenges

- Unauthorized access to EHR and patient workflows.
- Exposure of sensitive medical images stored in picture archiving and communication systems (PACS) and imaging repositories.
- Difficulty identifying all instances of sensitive data across a large, distributed hospital network.
- Security gaps from connected clinical IoT devices monitoring patient health.
- Data breaches across cloud platforms hosting healthcare applications and data.
- Limited visibility into compromised data during and after a security incident.

How a SIEM solution like Log360 helps

- **Log aggregation and correlation:** Collects and correlates logs from EHR systems, PACS, clinical IoT devices, and cloud services to provide unified visibility across hospital infrastructure.
- **Automated PHI discovery:** Predefined DLP rules scan the network for PHI and PII automatically, with support for custom rules configured to detect organization-specific data types.
- **Endpoint exposure flagging:** Identifies unnecessary copies of sensitive data stored on low-security endpoints and flags them for remediation before they become a liability.
- **File integrity monitoring:** Detects tampering with patient records and audit logs by alerting on creation, deletion, access, and modification events across the healthcare environment.
- **Threat intelligence and analytics:** Leverages external threat intelligence feeds and security analytics to identify risks and anomalous activity across all connected healthcare devices and networks.
- **Automated response orchestration:** Triggers timely, automated response actions to contain and mitigate policy violations and healthcare cybersecurity threats before they escalate.
- **Compliance and forensic reporting:** Supports root-cause analysis and audit-ready reporting to strengthen ePHI protection policies and meet healthcare compliance requirements.



Log360 dashboard providing unified security visibility

Use case 2: Ransomware prevention in healthcare

The critical nature of healthcare operations and the unpatched vulnerabilities in the legacy infrastructure make hospitals and related organizations a prime target for ransomware. SIEM solutions detect early ransomware indicators across hospital networks and executes automated containment before encryption begins.

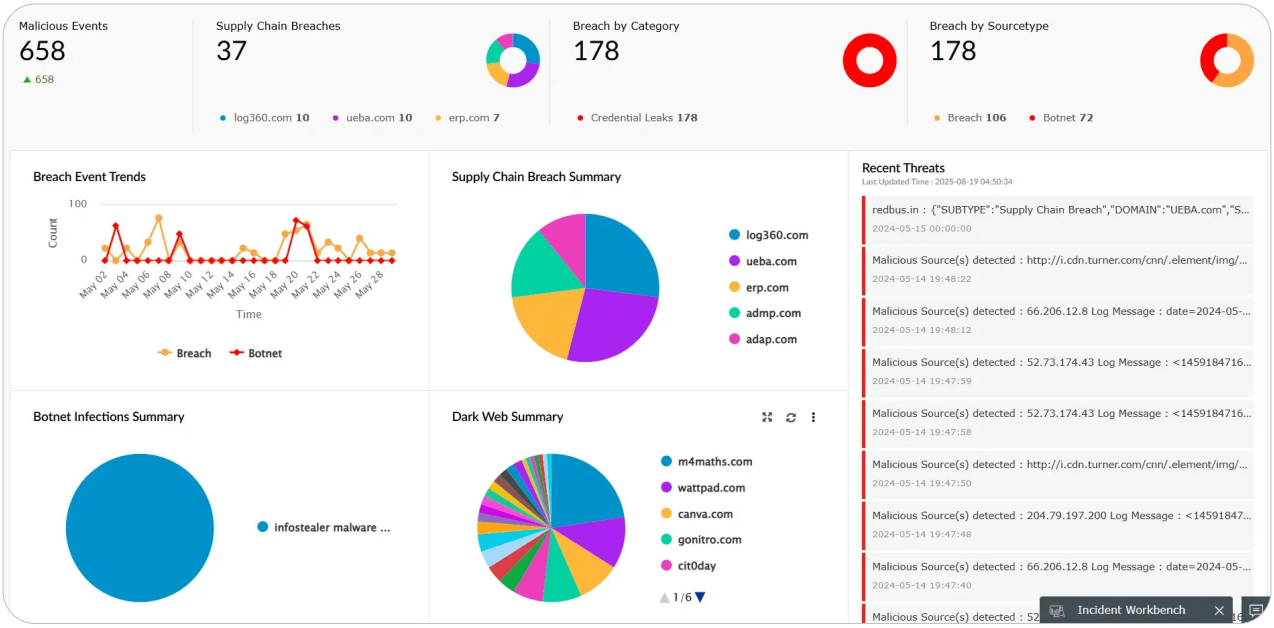
Challenges

- Legacy clinical systems cannot be easily patched or rebooted, leaving persistent vulnerabilities across the environment.
- Ransomware stages silently for weeks, evading signature-based detection until it activates and encrypts.
- Clinical staff prioritizing patient care are more susceptible to phishing techniques used as initial access vectors.
- Distributed hospital networks create numerous lateral movement pathways between departments and systems.

How a SIEM solution like Log360 helps

- **Early indicator detection:** Detection rules identify ransomware precursors, such as RDP configuration changes, unauthorized software installations, and shadow copy deletions, before encryption begins.
- **ML-based behavioral analytics:** UEBA flags mass file modifications and access escalations indicative of ransomware activities, especially those that evade signature-based tools.

- **Dark web monitoring:** Continuously scans the dark web for organization domain names, employee credentials, and vendor account data, and correlates leaked credentials with active login attempts in the environment.
- **Threat intelligence integration:** Identifies known ransomware command-and-control infrastructure, blocking communication before attackers can execute the attack chain.
- **Automated response orchestration:** SOAR playbooks automatically shut down affected systems or terminate malicious processes upon confirmation, without requiring analyst intervention.



Log360 providing visibility into dark web leaks and supply chain breaches

Use case 3: Genomic research data protection

Genomic research environments handle some of the most sensitive data such as patient genetic sequences, research results, and proprietary intellectual property. A SIEM solution helps detect suspicious data access attempts, prevent data theft, and safeguard genomic data integrity across research infrastructure in real time.

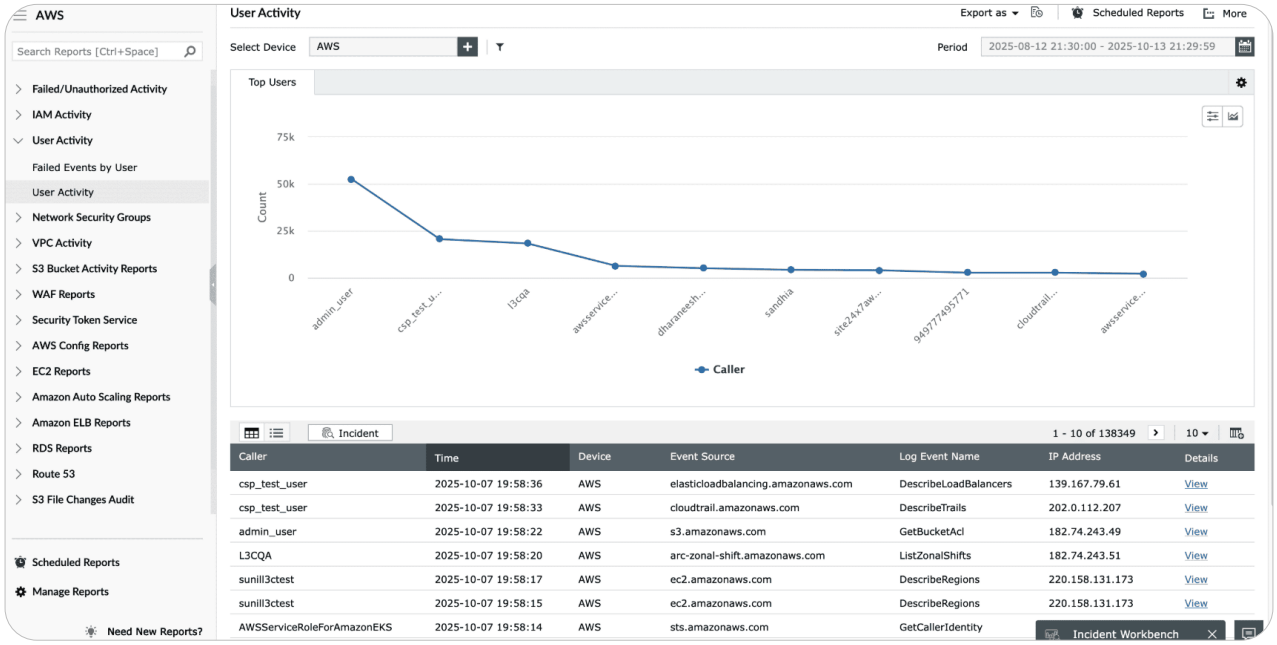
Challenges

- Vulnerabilities in bioinformatic tools that can be exploited by threat actors
- Targeted theft of patient data and proprietary research results
- Unauthorized access or tampering with genetic databases used for personalized medicine
- Limited visibility into network and application activities that may indicate cybersecurity threats

How a SIEM solution like Log360 helps

- **Custom log parsing:** Supports custom log parsing for proprietary application or device logs.

- **Log correlation:** Collects and correlates logs from genomic databases, bioinformatics tools, network and security devices, and applications to deliver unified visibility across research infrastructure.
- **Anomaly detection:** Flags abnormal user or system behaviors indicative of insider threats, credential misuse, or data exfiltration attempts.
- **Threat analytics:** Identifies threats from external sources that target genomic data and tools, including DDoS, SQL injection, and cross-site scripting attacks.
- **Automated response orchestration:** Triggers predefined response actions to neutralize threats rapidly and prevent escalation.
- **Cloud data integrity monitoring:** Provides detailed insights into data held in the cloud to detect tampering and ensure the integrity of hosted genomic datasets.



Log360 providing detailed insights into user activity in the cloud

Use case 4: Securing telehealth and remote access

Telehealth has extended clinical workflows far beyond the hospital perimeter with clinicians accessing EHR systems from personal devices, and vendors maintaining critical infrastructure remotely with limited oversight. A SIEM solution with CASB capabilities can identify shadow IT, policy violations, and unauthorized cloud applications used to share patient data.

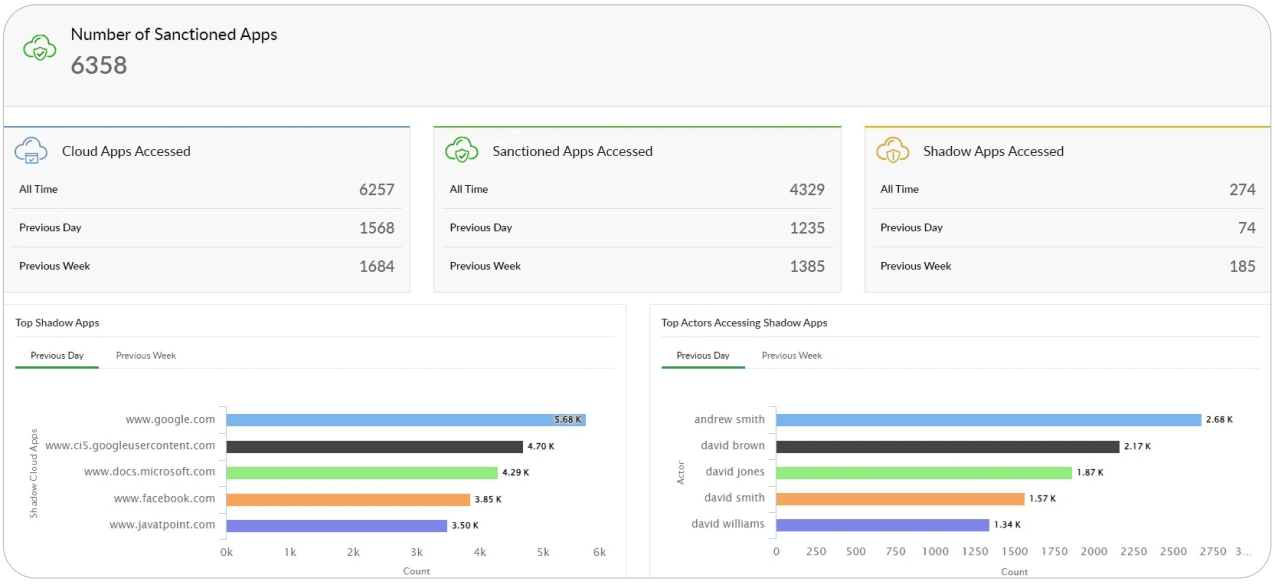
Challenges

- Personal devices lack the endpoint security controls enforced on hospital-managed devices, increasing the attack surface.
- VPN and RDP endpoints are frequent targets for credential stuffing and brute-force attacks.

- Shadow IT, wherein clinicians use personal file-sharing applications to handle patient data, is widespread and difficult to detect.
- Third-party vendor sessions are difficult to define, monitor, and restrict to only the access required.

How a SIEM solution like Log360 helps

- **Anomaly detection:** Detects impossible travel scenarios and geographically anomalous login patterns that indicate credential compromise across remote clinical and vendor sessions.
- **Account takeover detection:** Correlates failed authentication attempts, MFA bypass events, and session anomalies to identify active account takeover attempts before damage occurs.
- **Integrated CASB:** Identifies and blocks shadow IT applications, enforcing policies that restrict patient data sharing to sanctioned applications.
- **Dark web monitoring:** Monitors and alerts security teams when clinician or vendor credentials appear in breach datasets, enabling proactive remediation before attackers weaponize stolen credentials.



Log360 offering insights into sanctioned and shadow applications

How SIEM helps with regulatory compliance

As if ensuring top-tier patient care while battling relentless cyberthreats wasn't challenging enough, healthcare organizations must also navigate an intricate web of compliance mandates. Regulatory audits can be overwhelming, and for institutions already stretched thin on time and resources, maintaining compliance isn't just a legal requirement—it's an ongoing struggle that can drain operational efficiency and escalate costs.

Healthcare organizations must navigate a complex regulatory landscape including HIPAA, HITRUST, and even NIST and ISO to an extent. Both frameworks are designed to protect sensitive health information, but they approach security and interoperability from different angles.

HIPAA: Safeguarding ePHI

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that sets the standard for protecting sensitive patient data. The HIPAA Security Rule specifically requires covered entities and their business associates to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

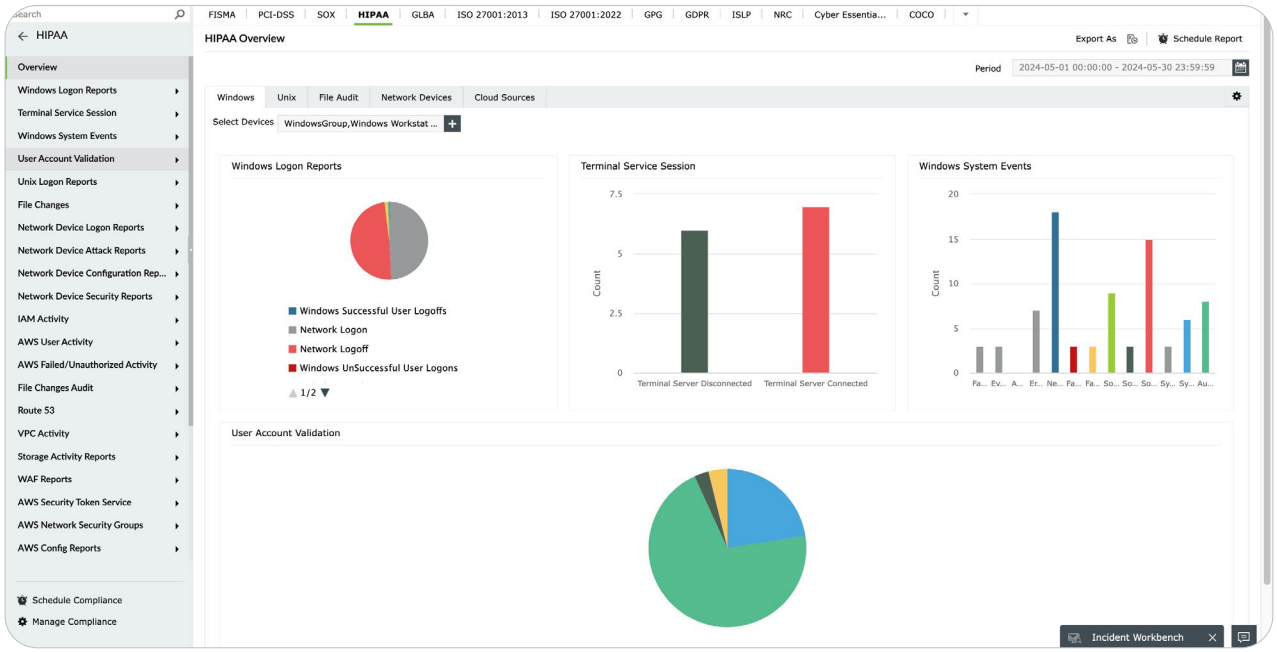
Key HIPAA Security Rule requirements

- **Safeguard ePHI:** Protect the confidentiality, integrity, and accessibility of all ePHI generated, received, managed, or transmitted.
- **Risk management:** Conduct regular risk assessments to identify and mitigate vulnerabilities.
- **Audit controls:** Implement hardware, software, and procedural mechanisms to record and examine access and other activity in information systems.
- **Workforce compliance:** Ensure employees follow security policies and procedures.

How SIEM supports HIPAA compliance

A robust SIEM platform directly addresses several HIPAA requirements:

- **Comprehensive audit logging:** SIEM solutions automatically collect, store, and retain logs of all access to ePHI, creating an auditable trail that meets HIPAA's stringent requirements for tracking and monitoring system activity.
- **Continuous monitoring and real-time alerts:** SIEM solutions monitor network activity for suspicious or unauthorized access, immediately alerting security teams to potential violations, such as unauthorized attempts to view patient records.
- **Automated compliance reporting:** SIEM platforms generate detailed reports documenting security measures and activities, streamlining the audit process and demonstrating compliance to regulators.
- **File integrity monitoring (FIM):** By tracking changes to files containing ePHI, SIEM helps maintain data integrity and alerts administrators to unauthorized modifications.
- **Incident response and forensics:** In the event of a breach, SIEM solutions provide the forensic data necessary to investigate incidents, contain threats, and document the organization's response for regulatory purposes.



Log360 offers built-in HIPAA compliance reports

HITRUST CSF: Unifying security and compliance

What is HITRUST CSF?

The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) is a privately developed, certifiable framework that consolidates requirements from multiple regulations, including HIPAA, NIST, ISO 27001, and the PCI DSS, into a single, unified set of security controls. It is widely adopted by healthcare organizations and their business associates as a benchmark for demonstrating rigorous, auditable information security practices across people, processes, and technology.

Key HITRUST CSF requirements

- **Access control:** Restrict access to sensitive systems and data to authorized individuals, enforcing least-privilege principles across the organization.
- **Audit logging and accountability:** Maintain comprehensive records of user activity, system events, and data access to support monitoring, investigation, and regulatory review.
- **Incident management:** Establish and operationalize processes for detecting, responding to, and recovering from security incidents in a documented and repeatable manner.
- **Risk management:** Continuously assess and remediate risks to the confidentiality, integrity, and availability of sensitive information across all systems.

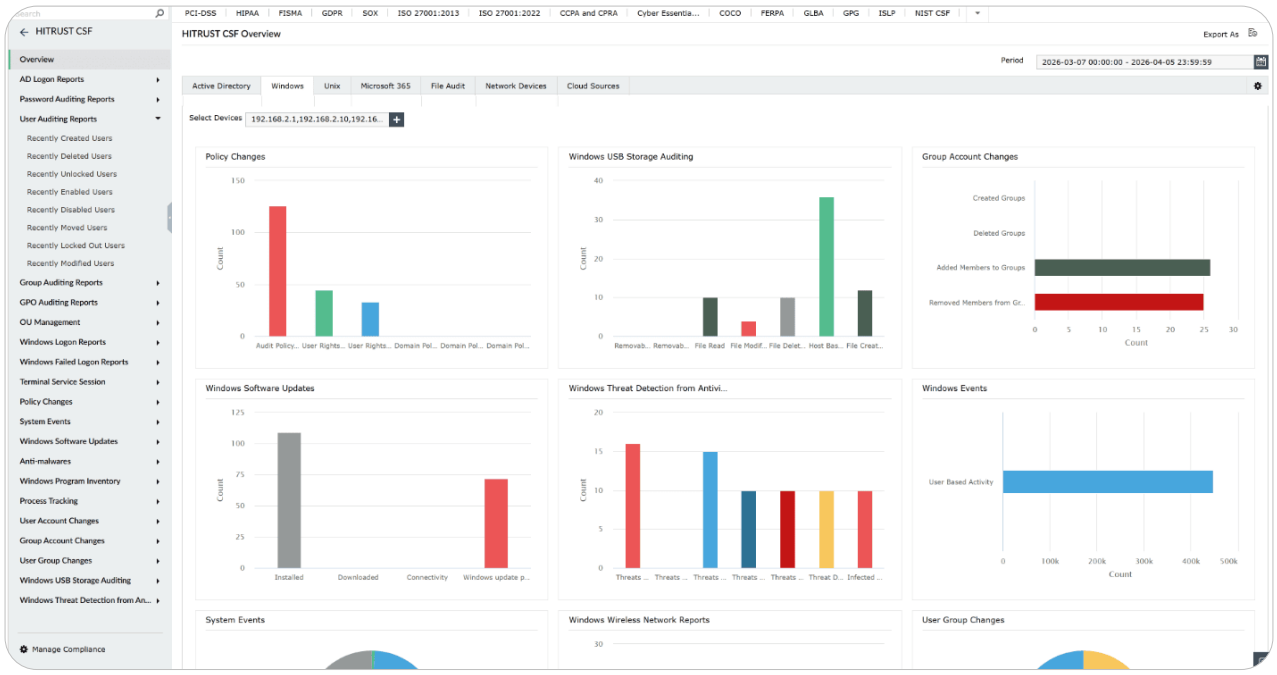
How SIEM supports HITRUST compliance

SIEM solutions help in complying with HITRUST CSF in the following ways:

- **Centralized audit log management:** SIEM solutions automatically collect, normalize, and retain

logs across all systems in scope, creating the comprehensive audit trail required by HITRUST's accountability and audit logging controls.

- **Continuous monitoring and real-time alerting:** SIEM solutions constantly monitor user and system activity, alerting security teams to policy violations, unauthorized access attempts, and anomalous behavior as they occur.
- **Automated compliance reporting:** SIEM solutions generate detailed, audit-ready reports that map security activity to HITRUST control requirements, simplifying assessments and demonstrating compliance to auditors and certifying bodies.
- **File integrity monitoring:** By tracking changes to files and configurations, SIEM helps maintain data integrity and identifies unauthorized modifications that could indicate a control failure.
- **Incident response and forensics:** In the event of a security incident, SIEM solutions provide the forensic depth needed to investigate root causes, contain threats, and provide documented evidence required for HITRUST compliance.



HITRUST CSF reports offered by Log360

Conclusion

As healthcare organizations accelerate digital transformation and face an increasingly complex cyberthreat landscape, implementing a comprehensive SIEM solution is critical for safeguarding patient data, ensuring operational continuity, and maintaining regulatory compliance. A unified SIEM platform like ManageEngine Log360 delivers centralized visibility, real-time threat detection, automated incident response, and compliance support to protect sensitive health information, secure critical healthcare infrastructure, and strengthen cyber resilience. To learn more, request a personalized demo.

ManageEngine
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 effective remediation. With reengineered detection—including a centralized detection console, multi-mode rule creation, tuning insights, and object-level filters—Log360 elevates signal quality and reduces false positives. The solution provides holistic visibility across on-premises, cloud, and hybrid environments with intuitive security analytics and monitoring. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

Request a demo **Download**

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus