Large Hospital Modernizes Cybersecurity with Seceon Platform

Executive Summary:

A large hospital with 10,000 staff and multiple specialty services faced increasing cyber threats, compliance challenges, and operational inefficiencies with their legacy Security Information and Event Management (SIEM) system. The hospital replaced its SIEM with Seceon's AI-driven Open Threat Management (OTM) platform, significantly reducing cyber risk, modernizing security operations, and ensuring continuous compliance for regulatory audits.

Seceon's real-time threat detection, automated response, and compliance management streamlined the hospital's security posture, eliminating the alert fatigue and slow response times associated with their previous SIEM. Within six months, the hospital experienced:

- 85% reduction in cyber threats before they escalated
- 60% improvement in response time to security incidents
- Real-time compliance monitoring for HIPAA, HITRUST, PCI-DSS, and NIST
- 40% Lower operational costs and increased SOC efficiency

The Challenge: Growing Cyber Risks and SIEM Limitations

Healthcare Under Cyberattack
Hospitals are prime targets for cybercriminals due to sensitive patient data, interconnected systems, and outdated IT infrastructure. The hospital faced several challenges:

- **Frequent Phishing & Ransomware Attacks-** Staff members were targeted with sophisticated phishing campaigns, some leading to compromised credentials and malware infections.
- **Slow Incident Detection & Response-** Their traditional SIEM was reactive, often missing advanced persistent threats (APTs) and taking hours or days to generate alerts.
- **Lack of Security Visibility-**IT and security teams struggled with fragmented security tools, making it difficult to monitor cloud, on-premises, and endpoint activity in real time.
- **Compliance Burden-** Meeting HIPAA, HITRUST, and NIST requirements were complex and required manual audits, increasing compliance risks.

Limitations of the Legacy SIEM

Their existing SIEM had several drawbacks, including:

- **Alert Fatigue** – Thousands of alerts per day with high false positive rates
- **No AI or Behavioral Analytics** – Relied on signature-based detection, missing zero-day threats
- **Manual Incident Response** – Security teams had to manually correlate events and react
- **High Costs** – Storage, maintenance, and licensing fees were expensive
- **No Continuous Compliance** – Lacked automated reporting for audits

The hospital needed a modern cybersecurity platform that could:

- Eliminate cyber threats in real time
- Automate security response to reduce workload
- Ensure continuous compliance readiness
- Integrate seamlessly with existing infrastructure

The Solution: Seceon’s AI-Driven Open Threat Management (OTM) Platform

To overcome these challenges, the hospital implemented Seceon’s OTM platform, replacing their legacy SIEM. Seceon’s AI-driven platform delivered:

1. **Real-Time Threat Detection & Automated Response**
• Behavioral AI & Machine Learning continuously analyzed network traffic, user behavior, and endpoint activity to detect phishing, insider threats, malware, and ransomware before damage occurred.
• Automated Playbooks instantly responded to incidents, such as blocking malicious IPs, isolating compromised endpoints, and enforcing security policies.

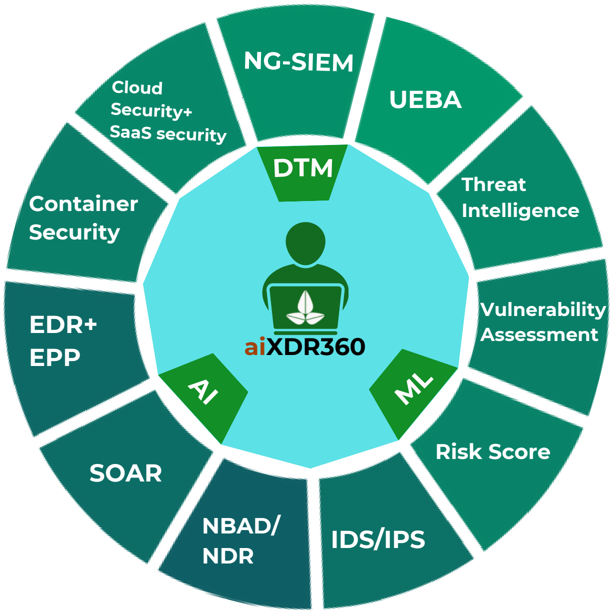
2. **Unified Visibility & Security Analytics**
    - Seceon provided a single-pane-of-glass dashboard, integrating with firewalls, cloud workloads, medical devices, and endpoints for real-time security monitoring.
    - Deep Packet Inspection (DPI) & Network Traffic Analysis (NTA) detected anomalies at the packet level, identifying data exfiltration attempts before they happened.

3. **Continuous Compliance & Audit Readiness**
    - Automated Compliance Reports ensured HIPAA, HITRUST, NIST, and PCI-DSS adherence without manual effort.
    - User Behavior Analytics (UBA) identified anomalous activity related to privileged account abuse and unauthorized access.
    - Real-time Log Correlation & Forensics reduced compliance audit preparation time from weeks to hours.

4. **Cost-Effective and Scalable Security**
    - Eliminated high SIEM storage and licensing costs, replacing them with scalable AI-driven security.
    - Reduced the hospital's security team workload by 50%, enabling them to focus on proactive threat hunting.

Implementation: A Smooth Transition to Seceon

Step 1: Risk Assessment & Security Posture Evaluation
Seceon's team conducted a comprehensive security assessment, identifying gaps in threat detection, network monitoring, and compliance enforcement.



Step 2: Deployment & Integration

- Seamless integration with firewalls, cloud environments (AWS, Azure), EHR systems, VPNs, medical IoT devices, and Active Directory.
- Zero-downtime deployment ensured hospital operations were not disrupted.

Step 3: AI Training & Real-Time Threat Detection

- Within the first week, Seceon's AI started learning baseline behaviors to detect anomalous activities across the hospital's infrastructure.
- Detected unusual data transfers from a compromised staff account, blocking potential data exfiltration in real time.

Step 4: Automated Incident Response & Compliance Setup

- Configured automated security response workflows, ensuring instant threat mitigation without manual intervention.
- Established compliance dashboards for real-time HIPAA and HITRUST reporting.

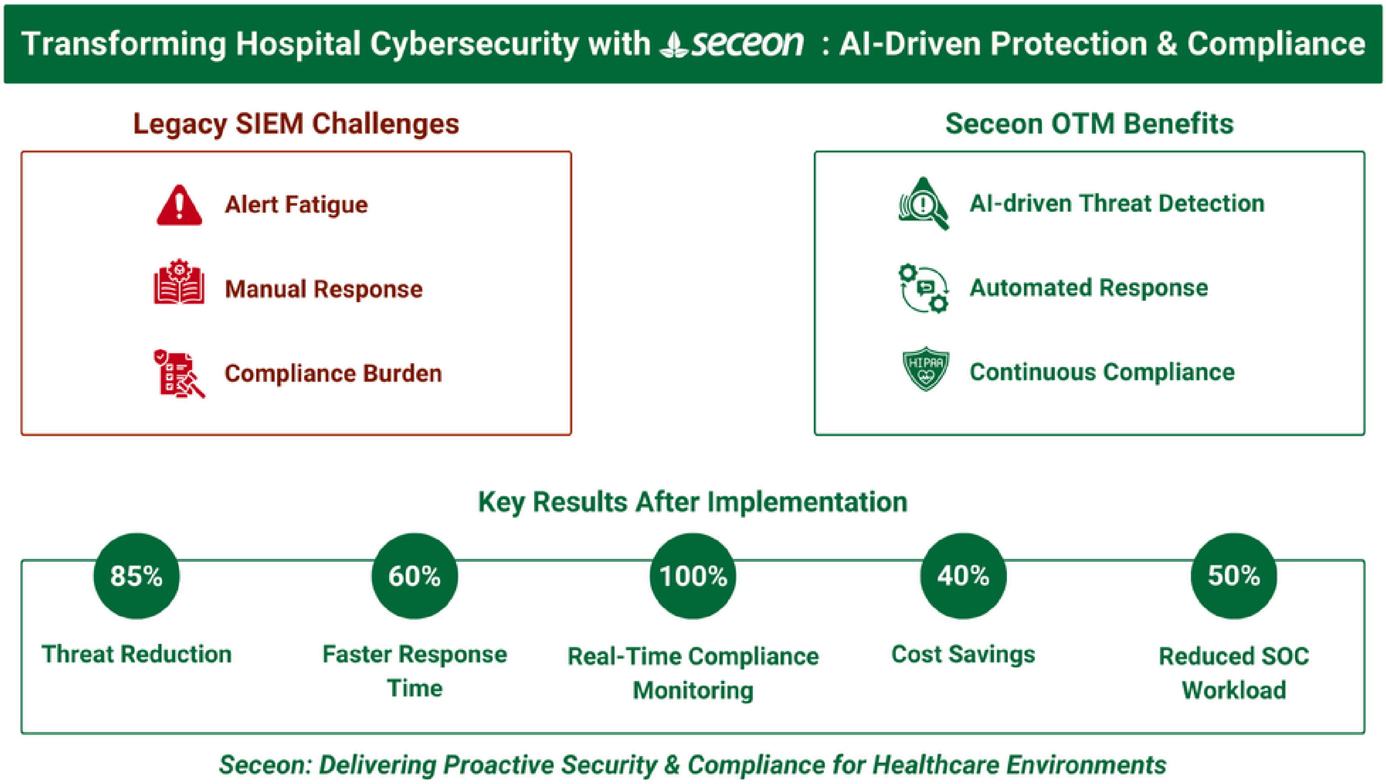
The Results: A Modernized Security Posture

1. **Significant Reduction in Cyber Risk**
   - 85% decrease in cyber threats by detecting and neutralizing attacks before impact.
   - 95% reduction in phishing-related incidents, preventing compromised credentials.
   - Eliminated ransomware attempts through AI-driven endpoint security.

2. **Faster Incident Detection & Response**
   - Detection time was reduced from hours to seconds with AI-driven analysis.
   - Response time improved by 60%, stopping threats automatically.

3. **Enhanced Compliance & Audit Readiness**
   - Real-time compliance monitoring eliminated manual audit preparations.
   - Automated compliance reporting reduced HIPAA and NIST audit costs by 40%.

4. **Cost Savings & Operational Efficiency**
   - Saved 40% on cybersecurity costs by replacing SIEM with Seceon's cost-effective model.
   - Reduced SOC team workload by 50%, allowing security analysts to focus on proactive defense.



Transforming Hospital Cybersecurity with seceon : AI-Driven Protection & Compliance

Legacy SIEM Challenges

- Alert Fatigue
- Manual Response
- Compliance Burden

Seceon OTM Benefits

- AI-driven Threat Detection
- Automated Response
- Continuous Compliance

Key Results After Implementation

85%	60%	100%	40%	50%
Threat Reduction	Faster Response Time	Real-Time Compliance Monitoring	Cost Savings	Reduced SOC Workload

Seceon: Delivering Proactive Security & Compliance for Healthcare Environments

Conclusion: Why Seceon is the Future of Healthcare Cybersecurity

By replacing its legacy SIEM with Seceon's AI-driven OTM platform, the hospital transformed its cybersecurity, compliance, and risk management strategy.

Key Takeaways

- Proactive AI-Powered Threat Prevention – Stopped cyberattacks before they escalated.
- Automated Security & Compliance – Ensured continuous HIPAA, HITRUST, PCI-DSS and NIST compliance.
- Faster & Cost-Effective Security – Reduced costs, alert fatigue, and operational overhead.

In an era of increasing cyber threats, healthcare organizations must move beyond traditional SIEMs. Seceon provides the modern, AI-driven cybersecurity approach needed to protect patient data, reduce risk, and maintain compliance effortlessly.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 464 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 8,800 clients.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/