Englewood Health: Transforming Healthcare Cybersecurity with AI-Driven SIEM



Executive Summary:

Englewood Health, a leading healthcare system in New Jersey, successfully transformed its cybersecurity posture by implementing Seceon's AI-driven aiSIEM™ platform. Faced with escalating cybersecurity threats and the inadequacy of traditional security tools, the organization partnered with *GS Lab | GAVS* to deploy a comprehensive AI-powered security solution that delivers real-time threat detection, automated incident response, and robust compliance capabilities.



Key Outcomes

- **Advanced Threat Detection:** 1.16 billion events analyzed with 80 million threat indicators flagged, achieving 95% reduction in false positives and 90% faster detection and response through AI automation.
- **Comprehensive Threat Coverage:** Seamless integration with the MITRE ATT&CK framework for end-to-end visibility and proactive threat hunting.
- **Regulatory Efficiency:** Automated HIPAA compliance reporting significantly reduces regulatory overhead.

Organization Background

Englewood Health is a leading healthcare system serving northern New Jersey through a multi-facility network that includes both acute-care hospitals and outpatient centers. Its complex IT infrastructure underpins critical patient-care operations and must satisfy stringent regulatory requirements - including HIPAA, HITECH, and state healthcare mandates while supporting growing digital transformation initiatives such as telemedicine services and extensive Internet of Medical Things (IoMT) device deployments.

Business Challenges

1. Traditional SIEM Limitations

Englewood Health's existing SIEM solution functioned primarily as a log aggregator, lacking advanced analytics and real-time threat detection capabilities. The system required extensive manual correlation rule writing and constant tuning, proving insufficient against modern threat vectors.

2. Complex Healthcare Environment

The organization operates in a complex healthcare environment where IT infrastructure spans diverse security elements, including firewalls, routers, web security tools, and intrusion detection systems. It also encompasses a wide range of medical devices, such as IoMT devices, patient monitoring systems, and diagnostic equipment, alongside legacy systems with limited security capabilities. The hybrid architecture, integrating on-premises systems with cloud services, further adds to operational complexity.

3. Regulatory Compliance Burden

Healthcare organizations face significant regulatory requirements. Continuous monitoring and audit trail generation ensure compliance with HIPAA, while regular risk assessments, vulnerability management, and documented incident response procedures address security gaps. Strict access controls, including robust user authentication and authorization mechanisms, are critical to protecting sensitive healthcare data.

4. Resource Constraints

Cybersecurity teams often operate under tight resource constraints. Limited availability of experienced professionals, alert fatigue from high volumes of false positives, time-intensive manual investigation and response processes, and integration challenges with legacy systems all contribute to operational strain.

5. Advanced Threat Landscape

Healthcare organizations face a sophisticated threat landscape. They are targeted by ransomware campaigns such as WannaCry and Ryuk, face risks from insider threats, and are exposed to supply chain attacks via third-party medical device vendors. State-sponsored APT groups increasingly focus on healthcare data, making proactive threat detection and mitigation essential.

Solution Approach

1. **Strategic Partnership -** Englewood Health collaborated with GS Lab | GAVS to deploy Seceon's aiSIEM™ solution. This tri-party partnership brought deep healthcare IT expertise, proven implementation methodologies, ongoing support, and industry-specific security knowledge.

2. Platform Selection Criteria - The solution was chosen for its AI/ML-driven analytics enabling advanced threat detection without manual rules, healthcare specialization for medical device environments and compliance, seamless integration with existing infrastructure, scalability for high-volume data processing, and built-in compliance automation for regulatory reporting and audits.

Implementation Strategy

- **Phase 1: Assessment & Planning (Months 1-2)**

Focused on risk mitigation, a comprehensive inventory of critical systems and high-risk patient care applications was conducted. Regulatory compliance obligations were analyzed, integration points with existing security tools evaluated, and success metrics defined. Stakeholders across IT, security, and clinical teams were aligned, and training and change management plans were developed.

- **Phase 2: Core Deployment (Months 3-4)**

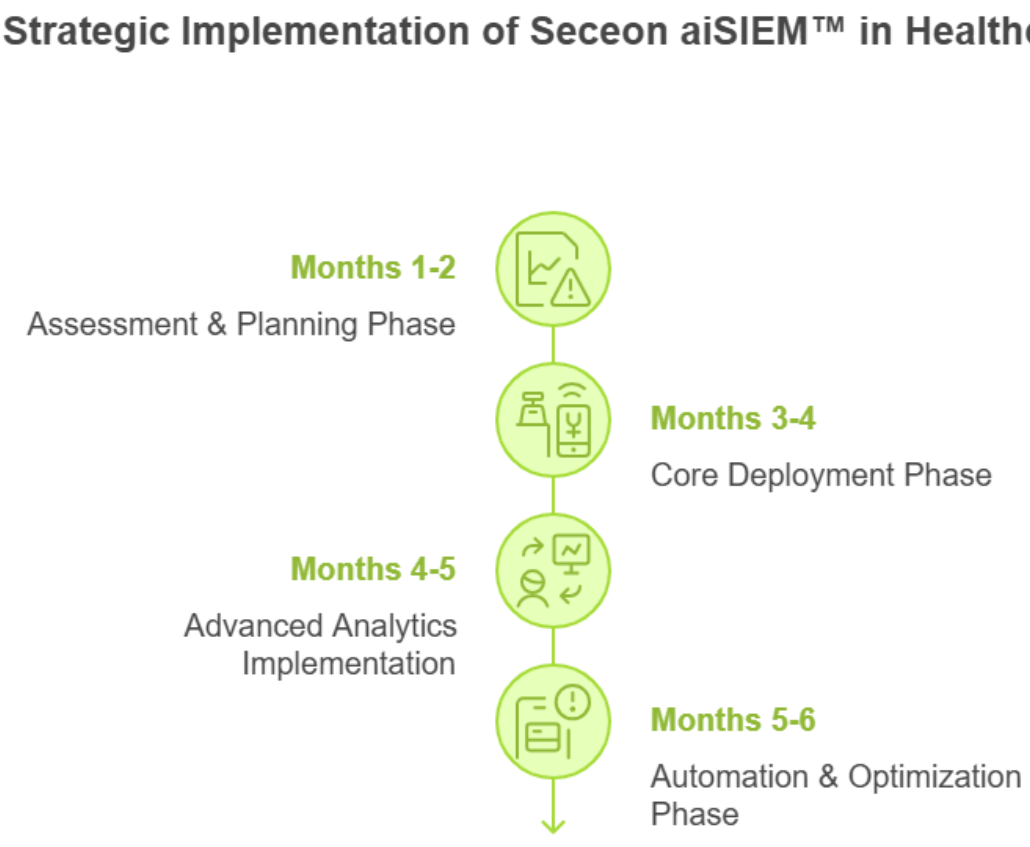
The Seceon aiSIEM™ platform was deployed and integrated with healthcare infrastructure, including medical devices. Implementation involved coordinated collaboration among Englewood Health, GS Lab | GAVS, and Seceon, with regular progress reviews and knowledge transfer. Core systems such as EHRs, IoMT networks, and identity management systems were fully connected.

- **Phase 3: Advanced Analytics Implementation (Months 4-5)**

Behavioral analytics and UEBA models were trained on healthcare-specific data, optimizing anomaly detection for medical environments. Threat intelligence feeds were integrated, mapped to MITRE ATT&CK frameworks, and customized for medical device vulnerabilities.

- **Phase 4: Automation & Optimization (Months 5-6)**

Automated incident response playbooks and compliance reporting were implemented, integrated with IT service management systems. Continuous performance monitoring reduced false positives, refined ML models, and expanded automated response capabilities.



Key Capabilities Deployed

1. AI-Driven Threat Detection
The platform uses patented technology to adapt dynamically to organizational usage patterns, eliminating manual rule tuning and updating threat models in real time. Advanced machine learning establishes behavioral baselines, detects anomalies across users, entities, and medical devices, and prioritizes alerts based on risk scoring.

2. Comprehensive Event Processing
Seceon processes up to 150 million events per second, correlating data from diverse sources including medical device logs, EHR audit trails, and network traffic. Integration with 70+ threat intelligence feeds provides enriched, real-time visibility across the healthcare environment.

3. MITRE ATT&CK Framework Integration
The system maps healthcare-relevant attack techniques, automates alert triage, and guides proactive threat hunting. Multi-stage attack detection and kill chain analysis enable the identification and correlation of advanced persistent threats.

4. SOAR & Automated Response
Pre-configured healthcare-specific playbooks automate containment, remediation, compliance reporting, and HIPAA audit trail generation. Integration with IT service management and clinical communication systems ensures efficient response workflows.

5. Healthcare-Specialized Features
Capabilities include IoMT device discovery, vulnerability assessment, and network segmentation for critical systems. Regulatory compliance is continuously monitored, with automated reporting, audit preparation, and risk assessment aligned to HIPAA, HITECH, and state regulations.

Results & Outcomes

The deployment of Seceon's AI-driven cybersecurity platform at Englewood Health delivered measurable improvements in operational efficiency and security resilience. By consolidating threat detection and response into a unified framework, the organization was able to streamline its security operations, cut down on noise from false alerts, and gain actionable visibility into emerging threats. These outcomes not only reduced the burden on the IT and security teams but also strengthened overall confidence in defending against increasingly sophisticated attacks.

Inderpal Kohli, VP and CIO of Englewood Health, emphasized the tangible impact of adopting Seceon's platform:
"*The results were remarkable, we experienced faster threat detection, significantly fewer false alarms, and clearer operational insights. This strengthened our overall security posture and provides a path that other healthcare organizations can follow to address today's dynamic cyber threat landscape.*"

Quantitative Results

- **Event Processing & Analysis**: The platform analyzed 1.16 billion events across the healthcare environment, flagged 80 million threat indicators with contextual intelligence, and reduced false positives by 95%, enabling focus on genuine threats. Threat detection and response accelerated by 90% through AI automation.

- **Operational Efficiency**: Manual investigation time for analysts dropped by 70%, compliance preparation for audits decreased by 85%, and overall cybersecurity operational overhead fell by 60%, with intelligent automation allowing single-analyst operations.
- **Financial Impact**: Total cybersecurity ownership costs were reduced by 40–60%, licensing costs for multiple legacy tools were eliminated, compliance audit preparation costs dropped by 80%, and regulatory examination performance improved through documented effectiveness.

Qualitative Outcomes

- **Enhanced Security Posture**: Healthcare assets gained comprehensive threat visibility, proactive threat hunting reduced dwell time, advanced attack detection (including zero-day and APT campaigns) was enabled, and integrated response capabilities minimized incident impact.
- **Improved Compliance**: Continuous HIPAA monitoring, automated audit trails, and streamlined regulatory processes enhanced patient data protection and simplified examinations.
- **Operational Excellence**: Intelligent correlation eliminated alert fatigue, boosted analyst productivity, reduced dependency on specialized cybersecurity expertise, and improved cross-team collaboration.
- **Business Impact:** Patient care remained uninterrupted, PHI was better protected, medical device security improved, and life-critical systems maintained operational availability. Regulatory compliance and audit performance improved, reducing fines and enhancing reputation and trust. Cybersecurity transformed from an operational burden to a strategic enabler, supporting staff development, recruitment, retention, and laying the foundation for future digital initiatives.



Implementation Challenges & Solutions

Challenge 1: Medical Device Integration (Legacy medical devices with limited security capabilities and proprietary protocols)
Solution:

- Passive monitoring deployment to avoid operational disruption
- Custom protocol parsing for medical device communication
- Network segmentation strategy protecting critical care systems

Challenge 2: 24/7 Operational Requirements (Healthcare environments requiring continuous operation without maintenance windows)
Solution:

- Phased deployment minimizing system downtime
- Redundant architecture ensuring high availability
- Hot-swap capabilities for maintenance activities

Challenge 3: Regulatory Complexity (Multiple overlapping healthcare regulations with varying requirements)
Solution:

- Comprehensive regulation mapping and compliance automation
- Custom reporting templates for different regulatory frameworks
- Automated audit trail generation with legal defensibility

Challenge 4: Skills Transition (Existing staff adaptation to advanced AI-driven security platform)
Solution:

- Comprehensive training program with hands-on workshops
- Gradual responsibility transition with ongoing support
- Enhanced career development through exposure to cutting-edge technology

Lessons Learned

1. Phased Implementation Success Factors

- Engaging clinical, IT, and security teams early, starting with non-critical systems, and maintaining continuous communication were key to smooth adoption.

2. Healthcare-Specific Considerations

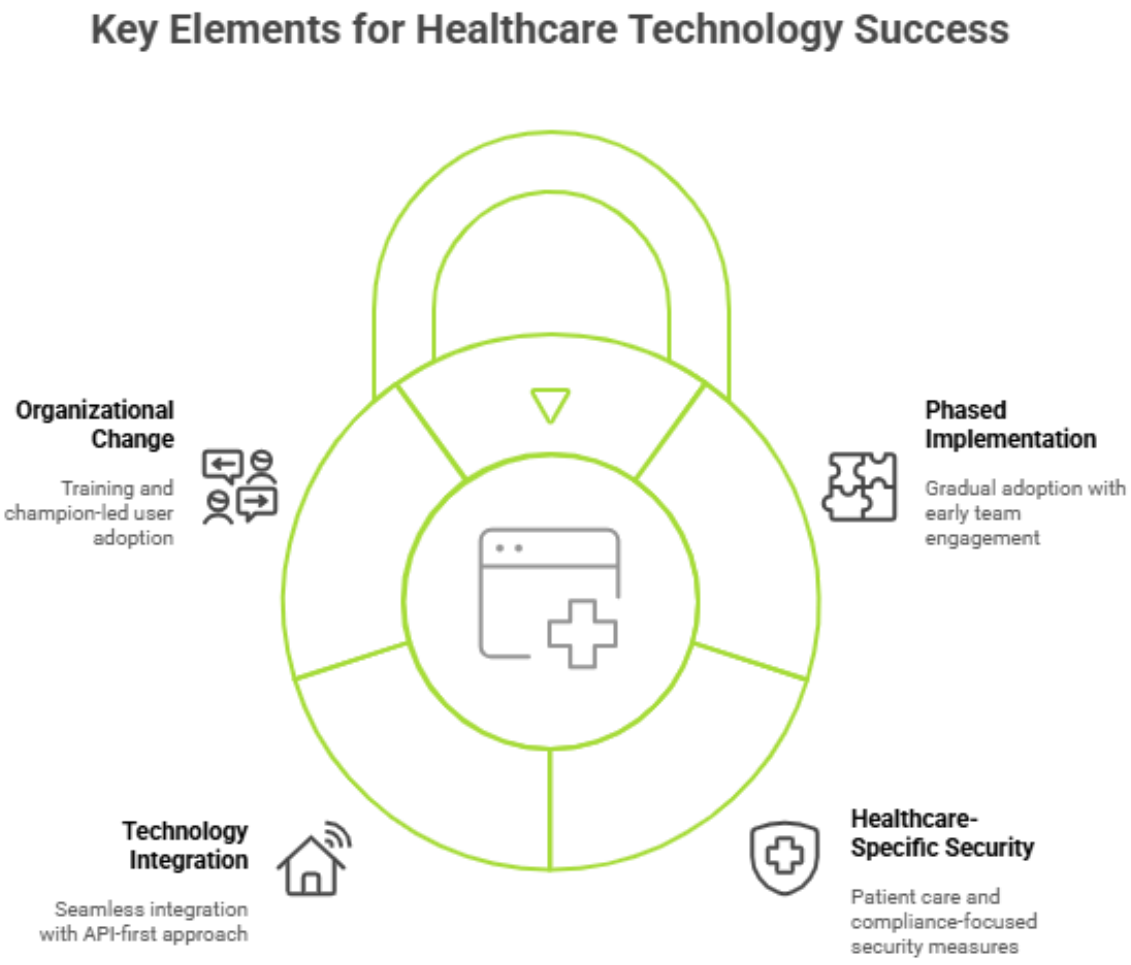
- All security measures preserved patient care, compliance automation was embedded from the start, and creative solutions were required to secure legacy medical devices.

3. Technology Integration Insights

- An API-first approach, clean and consistent data feeds, and high-performance processing were critical to effectively integrate complex healthcare systems and maximize AI/ML capabilities.

4. Organizational Change Management

- Comprehensive training, identifying key adoption champions, and defining clear success metrics ensured effective user adoption and sustained value.



Englewood Health

Transforming Healthcare Cybersecurity with AI-Driven SIEM

Key Challenges

Traditional SIEM Limitations
Basic log aggregation without advanced analytics

Complex Healthcare Environment
IoMT devices, legacy systems, hybrid architecture

Regulatory Compliance
HIPAA, HITECH compliance requirements

Resource Constraints
Limited staff, alert fatigue, manual processes

Healthcare Threat Landscape

- **Ransomware campaigns (WannaCry, Ryuk) targeting healthcare infrastructure**
- **Insider threats and supply chain attacks via medical device vendors**
- **State-sponsored APT groups increasingly focusing on healthcare data**

Seceon Solution



IoMT Device Discovery
Medical device vulnerability assessment and monitoring



AI/ML Analytics
Behavioral baselines without manual rule writing



MITRE ATT&CK
Healthcare-relevant attack technique mapping



HIPAA Automation
Automated compliance reports and audit trails

Proven Results

95%
Faster threat detection and response

70%
Less manual investigation time

82%
Reduced compliance prep time

40-60%
Lower total ownership costs

Conclusion

Englewood Health's implementation of Seceon's aiSIEM™ platform represents a transformative success in healthcare cybersecurity. By embracing AI-driven security technology and partnering with experienced implementation specialists, the organization achieved significant improvements in threat detection, compliance automation, and operational efficiency while maintaining the highest standards of patient care and safety.

The success of this implementation demonstrates that healthcare organizations can overcome traditional cybersecurity challenges through strategic technology adoption, comprehensive planning, and commitment to continuous improvement. As cyber threats continue to evolve, Englewood Health is well-positioned to maintain its leadership in healthcare cybersecurity while serving as a model for other healthcare organizations seeking to enhance their security posture.

This case study was developed in collaboration with Inderpal Kohli and the Englewood Health team, whose insights and experiences shaped the strategies and outcomes highlighted here.

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 680 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

Learn more about Seceon

Schedule a Demo

www.seceon.com/contact-us/



© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, aiMSSP are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.