seceon

Global Healthcare Enterprise Case Study

A global integrated healthcare enterprise, in business for 55 years of businessand now employing 11,000 employees adopts Seceon's aiSIEM platform. As a research-based pharmaceutical with R&D and global manufacturing of branded and generic formulations, new drug development research, and multiple specialty hospitals executed on its vision to improve their cybersecurity program.

Objective: Secure critical assets and intellectual property

As a leading integrated healthcare enterprise, the company is holding sensitive information as well as intellectual property, and formulations, which are a target of financially motivated cyber actors and APT groups. The company's presence across all continents and a distributed global workforce also places additional challenges on the cybersecurity program such as:

- PHI and PII monitoring and security during data-at-rest and data-in-motion
- Numerous integrations with multiple partners and third-party vendors
- Company growth, transformation projects, and partner access to systems allows potential for misuse of access privilege
- A lack of context and the ability for analysts to have situational awareness extended both mean-time-to-detection and mean-time-to-response for cyber threats.
- Aging cybersecurity point solutions were narrowly focused on solving part of the problem, but a lack of context and correlation created too much noise and false alerts.

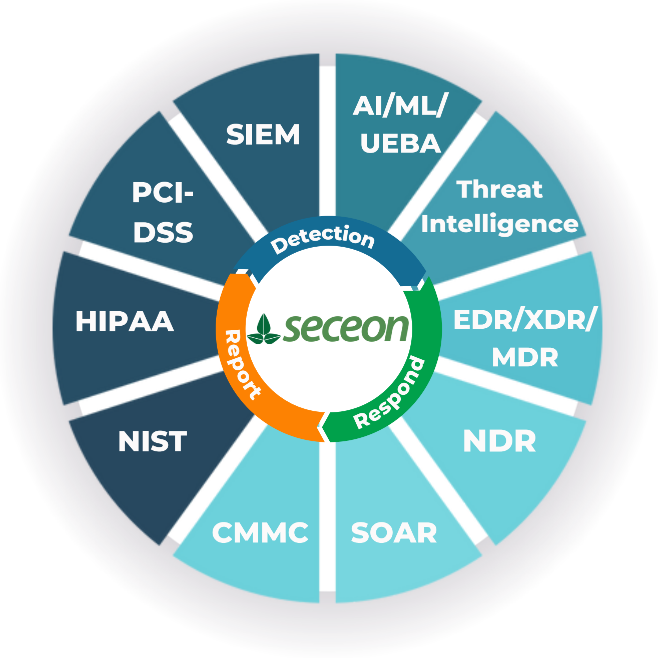
Seceon's Cyber Security Solution with aiSIEM

Unlike NG-SIEM (Next Generation SIEM) solutions, Seceon's aiSIEM relies on behavioral anomaly,dynamic threat models, and AI to detect threats in the early stage of an attack and provides automatic or playbooks drive responses with remediation to keep the organization safe from data breaches. After the Seceon solution was rolled out, machine learning took a couple of weeks to build a baseline pattern, which got further auto-tuned the detection models.

- Post implementation, Seceon detected many hygiene issues and existing attacks, which were rapidly acted upon by networking, IT, and security teams to improve the cybersecurity posture of the organization within 1st month of deployment.
- The Seceon aiSIEM platform was configured for auto-remediation on a few critical attack vectors and alerts were setup to ensure the organization stays ahead of data breaches.
- Network control policies and custom alerts were configured based on customer-specific conditions
- Multiple compliance monitoring and reports were created to ensure continuous compliance management and reporting
- The security operations team was trained in workflow to ensure faster MTTR

Visible Difference with Seceon aiSIEM

1. Enhanced Cybersecurity across the whole organization with a single platform instead of many point solutions and their associated complexity and lack of context.
2. Significantly reduced the risk of data breaches and operational issues and downtime.
3. Reduced unnecessary alerts (false positives) to a manageable number of alerts for detection and remediation.
4. Served as a deterrent for potentially malicious insiders and careless users.
5. Notifies SOC Analysts and IT Management instantly upon policy violations to take action, including education of the workforce, third-party contractors, and partners.
6. Full transparency is provided for each and every alert and threat indicator with the flexibility to add your own organizational intelligence.
7. Significantly lowers TCO and implements a modernized cybersecurity program.



As one of the customer executives noted – "*Some tools we reviewed were presented as turnkey but they neglected to tell us that they need 24 people to turn the key. Seceon can handle the lion's share of the work looking for breaches that happen within our system and has reduced our workload from a security standpoint by being able to assure that IP, formulations, employees, and patient data is secured.*"

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 300 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 7,500 clients.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/