CNXN HELIX
CENTER FOR APPLIED A.I. AND ROBOTICS

CASE STUDY

National Healthcare Group Purchasing Organization

Transforming Healthcare Security Operations with AI Automation

Client Profile

The customer is a large U.S.-based healthcare organization supporting hospitals and health systems nationwide. The organization operates a complex technology environment across clinical, supply chain, and corporate operations, with approximately 7,800 endpoints supported by a centralized security operations team.

The Challenge

The customer's security team faced constant pressure to respond quickly and accurately to threats. Over time, the security operations center (SOC) became overwhelmed by alert volume, leading to analyst fatigue and inefficient, manual triage processes.

Despite working with an outsourced managed detection and response (MDR) provider, the team struggled to distinguish real threats from false positives. Analysts were frequently pulled into after-hours investigations, and meeting response time expectations became increasingly difficult. After missed alerts and ongoing operational strain, leadership approved adding more personnel to the SOC. At the same time, the organization began reassessing whether this alone would solve the underlying problem.

The Solution

The organization evaluated several approaches to improving security operations, including internal expansion, changing MDR providers, and adopting a more automated model. Key requirements included:

- Integration across phishing, SIEM, EDR, cloud, and identity alerts
- A meaningful reduction in false positives and repetitive investigations
- Automation that could operate in live production environments
- Clear improvements in response speed and operational consistency

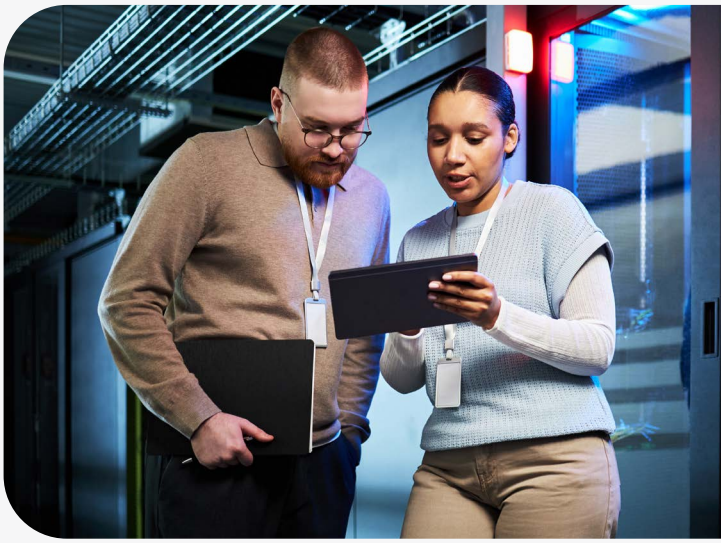
Working with Connection's AI practice, CNXN Helix™ Center for Applied AI and Robotics, the organization implemented an AI-driven SOC platform designed to autonomously triage, investigate, and respond to security alerts. The solution integrated directly into their existing security ecosystem, allowing alerts to be automatically closed, suppressed, or escalated based on verified threat context.

This approach enabled the security team to focus on true threats rather than manual alert processing.

The Results

Rather than acting as an advisory or copilot tool, the solution provided true end-to-end automation within the organization's existing environment. Seamless integration and strong execution during the evaluation period helped drive adoption and long-term success. The new AI-driven SOC platform delivered:

- Significant reduction in alert fatigue through automated triage and suppression of false positives
- Faster, more consistent investigation and response without further increasing SOC headcount
- Improved coverage and confidence in threat detection
- More time for analysts to focus on high-value security work



AI Solutions that Work for Healthcare

Contact your Account Team today to learn how we can help solve your healthcare IT challenges.

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.cnxnhelix.com