Deepwatch Expands Healthcare Organization Expertise

Nationally-recognized organization trusts Deepwatch to the unique challenges of security in healthcare.

OVERVIEW

Deepwatch protects a nationally-recognized rehabilitation provider, specializing in research-based physical therapy, workers' compensation rehab, and a variety of specialty therapies. They operate hundreds of clinics nationally and employ over 6,000 clinicians and physical therapy clinic staff, as well as corporate team members.

CHALLENGE

This large healthcare organization operates in one of the most highly-regulated, and highly- targeted industries. They needed additional engineering expertise, not simply an outsource for analysts. This customer had challenges with security team coverage and wanted to craft better internal roles to drive retention.

Skilled Security Staffing

Deepwatch provides the customer with expert security coverage as a way to maintain the work-life balance of their in-house talent.

"Deepwatch stepped in from an engineering and expertise perspective, providing level one analysts,and 24/7 monitoring capability as a contracted partner,," said a Senior IT Security Director. "Your teams look at our alerts and escalate them overnight when my team's asleep. And that's probably the biggest value in the sense that Deepwatch is able to take off some of those additional resource requirements in order for us to monitor it overnight. That allows us to build specific shifts. It can have an impact on how attractive a particular in-house job or role is, because those activities are being conducted by a partner of ours.

ENTERPRISE DETAILS

Industry: Healthcare

Headquarters: Illinois

Number of Employees: 6,000

Number of Security Employees: 8

Customer since: 2018

Product: Deepwatch MDR

Squad: CSM, SM, Analysts, MDR Engineer

PROBLEM ANALYSIS

Third-Party Risk in Healthcare

Deepwatch helps this customer address security challenges particular to the healthcare industry.

"One of the biggest challenges in our industry is the complexity of interdependencies, the relationships that exist between different organizations. It's probably the most difficult aspect of cybersecurity at this point in time."

"It's no longer an unsecure web application. There certainly still is phishing, but more often than not, it's now a partner that gets compromised, a partner that has some sort of secondary, tertiary access to the primary target's environment," said the Senior IT Security Director.

"That's a challenge because you have this trusted relationship, right? So you tend to scrutinize it a little bit less than you would your typical front doors. Now you have this sort of back end access from a partner then a few partner accounts get compromised. It's only a matter of time before your environment is polluted with that same sort of bad account. Honestly, that's like, one thing that keeps me up at night right now is third party risk management or even fourth party risk management. Deepwatch helps improve visibility into those interdependencies."

SOLUTION

Human-led, Expert Coverage that Understands Healthcare Environments

Deepwatch provides 24/7/356 human, US-based coverage as an extension of your security team. A dedicated Deepwatch squad, including analysts and detection engineers with deep security tool expertise, help SecOps teams focus on security outcomes unique to their environment. Along with improved detection through machine learning and active threat hunting, Deepwatch extends response capability speed, expertise, and coverage.

- 24/7/365 human, US-based coverage for real time response
- Managed Detection and Response through dedicated Squads
- Splunk expertise collaboration and integration
- Deepwatch Adversary Threat Intelligence (ATI) integration and active threat hunters

SECURITY OUTCOMES

- Better coverage, with a Squad that understands their environment
- Better visibility into complex security environments
- Better metrics, better narratives for other stakeholders
- Better threat intelligence through integration with Deepwatch threat hunters

"The metrics approach that you took, such as Deepwatch quarterly and monthly reporting especially, is extremely powerful. Our ELT members are very impressed by the fact that we ingest over 4 billion events monthly, yet can whittle that down to a few 100 events of interest, which then goes down the funnel even more to maybe a dozen or two dozen critical alerts monthly."

-Senior IT Security Director