Prominent Medical Center Broadens Scope and Efficiency of Defenses

Penn State Health Milton S. Hershey Medical Center Leverages FireEye Integrated Solutions and Intelligence

As a preeminent academic medical center, The Milton S. Hershey Medical Center is home to many top-tier academics focused on cutting-edge healthcare research. It is not uncommon for a scientist to dedicate his or her entire career to conducting exploration into a single disease or medical device. Matthew Snyder, chief information security officer at Hershey Medical Center, observed, “A single data compromise can negate the work that a researcher has performed over a 20-to-30 year span. This is just one of a multitude of reasons why cyber security is a mission-critical imperative for us.”

Cyber Challenges Facing the Healthcare Industry
Multiple sources cite that the healthcare industry has experienced a triple-digit increase in the annual number of cyber-related breaches. Within one ten-month period the Hershey Medical Center identified 83 million malicious attempts to penetrate its infrastructure. Snyder described, “These were not just run-of-the-mill scanning attempts; these were attacks where someone was attempting a specific threat action.”

Seeking an Integrated Solution
Drawing a parallel between unified electronic health records (EHR) and developing an integrated solution for cyber security, Snyder noted, “An electronic record is an assimilation of data from multiple diverse sources—including medical device data, diagnostic information, physician notes, etc.—all assembled in one place. We wanted a similar capability for our cyber defense and threat intelligence.”
“The comprehensive capabilities and intuitive integration between the multiple FireEye solutions enables us to stay at the forefront of the threat protection space. On top of this, FireEye Managed Defense fills a critical support role for us where the FireEye experts are an extension of our existing incident response capability.”

—Matthew Snyder, Chief Information Security Officer, Penn State Health Milton S. Hershey Medical Center

Hershey Medical Center has a rigorous process for evaluating new technology. “Before we purchase a new security-related solution, we ensure that it makes a unique and quantifiable contribution to what we already have in place from a risk and value perspective,” Snyder recounted. “Once the cyber security team decides to pursue a particular offering a structured onsite proof-of-concept is conducted to aggressively test both performance and fit.”

The FireEye Advantage

“The FireEye solutions all communicate with each other and the amalgamated intelligence is displayed on a single screen—our equivalent of the electronic health record—and that is of great value to us,” highlighted Snyder.

“In addition, FireEye Endpoint Security doesn’t simply tell us what just occurred, it promptly shows us what happened immediately before and after an attack; giving invaluable intelligence and context to each alert. We can replay an attack scenario or look at specific network traffic at the exact time the incident happened. If determined to be necessary, we can then leverage FireEye Managed Defense to execute a forensic deep-dive.”

Operating 24/365, FireEye Managed Defense acts as an extension to Hershey’s security team. Snyder commented, “We didn’t want to end up with a managed security service provider that would simply throw alerts at us; we chose FireEye Managed Defense because it provides quality reporting as well as high-fidelity detection, investigation and hunting. The FireEye experts augment and complement our in-house capabilities, and keep watch during our off-line hours.”

He continued, “A compromise report from FireEye Managed Defense contains a valuable step-by-step list of actions taken by the incident responder and the reasoning behind their conclusions. My incident response team then takes that information and performs the internal remediation actions necessary to ensure that we eliminate the threat and possible vulnerabilities associated with the alert. The timeliness of the FireEye Managed Defense reporting is vital because it enables us to mitigate risks in near real-time.”

Cost-effective and Innovative
Hershey Medical Center appreciates the cost-effective nature of FireEye Managed Defense. Snyder estimated, “Building out a security operations center would have required 12-15 additional full-time staff members but with FireEye Managed Defense we can accomplish an equivalent or better coverage for far less expense.”

FireEye is viewed a strategic partner to Hershey. “The comprehensive capabilities and intuitive integration between the multiple FireEye solutions enables us to stay at the forefront of the threat protection space. On top of this, FireEye Managed Defense fills a critical support role for us where the FireEye experts are an extension of our existing incident response capability,” summarized Snyder.

He concluded, “Our organization derives confidence from our partnership with FireEye. We can combine threat intelligence not just from our own network indicators but also from FireEye’s worldwide intelligence platform. This enables us to be aware of attacks that are occurring in other places around the globe; and to know what the indicators of compromise look like, as well as what needs to be done to address the risk. FireEye threat intelligence plays a business-critical role for us in intrusion detection, prevention and response.”

To learn more about FireEye, visit: www.FireEye.com