GE Healthcare Launches New Medical Device Cybersecurity Offering to Help Health Systems Better Protect against Risk

February 20, 2020

Vendor-agnostic solution helps hospitals to proactively monitor and mitigate cybersecurity threats through GE Healthcare's dedicated network of IT and OT security professionals

FEBRUARY 20, 2020 – CHICAGO – GE Healthcare today introduced a new cybersecurity service offering that brings together medical device expertise, artificial intelligence and process management tools to help hospital groups in their fight against cybersecurity threats. The new solution, called Skeye, augments hospitals' existing resources and capabilities by providing proactive monitoring through a remote security operations center (SOC) – helping them detect, analyze and respond to cybersecurity threats and events in real time.

As more devices become connected, cybersecurity risk increases – and security incidents can profoundly impact an organization's productivity, finances, quality of care and reputation. In 2018 alone, 82 percent of hospital technology experts reported a "significant security incident," with the average data breach costing $3.86 million.1

GE Healthcare's Skeye aims to address those risks by providing customers with a complete medical device security assessment to help identify risks and vulnerabilities, recommended action plans, remediation advice and execution strategies – facilitating collaboration across customers' clinical engineering, IT and security teams. Additionally, AI tools will automate connected device inventory and equipment risk profiling throughout a hospital to create a dynamic management system for device onboarding and decommissioning.

"Our customers need visibility to what medical devices are connected to their networks and the right resources to mitigate potential threats. This new offering provides customers with 360˚ threat visibility and a resolution roadmap to help defend and protect against vulnerabilities," said Matt Silva, Chief Information Security Officer, GE Healthcare. "Our security operations center can augment customers' in-house security teams by addressing cybersecurity events, as well as providing the latest information on malware and other malicious threats."

GE Healthcare's Skeye utilizes AI-enabled tools together with the security operations center to analyze, monitor and help manage cybersecurity vulnerabilities. As a vendor-agnostic solution, Skeye helps protect networked medical devices, regardless of age, OEM or operating system. Its 360˚ coverage starts with risk assessment and moves to real-time networked device discovery. A SOC team provides monitoring and threat detection and remediation for connected medical devices under a GE Healthcare service contract.

"We strongly believe that security is a shared responsibility across various stakeholders, and with this new solution, hospitals will now have access to a range of proactive and reactive cybersecurity services to support their own security programs ," added Silva.

"*Who knows the devices better than an equipment manufacturer*"

T.J. Regional Health is an independent, multisite organization with two hospitals, a health pavilion and eight outlying clinics to support communities in southern Kentucky. As a growing health provider, T.J. partnered with GE Healthcare to pilot the new Skeye offering and ensure they had robust cybersecurity systems to help protect against vulnerabilities and breaches.

"Defending T.J. Regional Health against malicious cyberattacks and protecting our patients, data and medical facilities is a top priority," said Chad Friend, Director of IT at T.J. Regional Health. "We wanted to stay current with cybersecurity trends, assess the risk across our hospitals and clinics and analyze our own preparedness. GE Healthcare's Skeye offering helps us do just that."

The assessment and recommendations from GE Healthcare helped T.J. Regional Health to implement a more proactive cybersecurity plan, better connect between departments, define a cybersecurity policy and install proper procedures and policies for device security management.

"As a small hospital group, we don't have a large IT team," explained Friend. "Accessing the global scale, tools and expertise of GE Healthcare gave us a partner to ensure we have a robust cybersecurity process in place and access to the latest information and action plans. After all, who knows how to protect the devices better than an equipment manufacturer?"

Skeye is currently available to customers in the U.S. Further details on the offering can be found here.

1. https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/

###

About GE Healthcare

GE Healthcare is the $19.8 billion healthcare business of GE (NYSE: GE). As a leading provider of medical imaging, monitoring, biomanufacturing, and cell and gene therapy technologies, GE Healthcare enables precision health in diagnostics, therapeutics and monitoring through intelligent devices, data analytics, applications and services. With over 100 years of experience in the healthcare industry and more than 50,000 employees globally, the company helps improve outcomes more efficiently for patients, healthcare providers, researchers and life sciences companies around the world.

Follow us on Facebook, LinkedIn, Twitter and Insights for the latest news, or visit our website www.gehealthcare.com for more information.

For media inquiries, please contact:

Amy Sarosiek
Directrice executive, Communication Externe
GE Healthcare
+1 224 239 6028
amy.sarosiek@ge.com