HealthManagement
Promoting Management and Leadership

Volume 17 - Issue 4, 2017 - Winning Practices

Global medical device security testing labs launched

A new initiative that will improve medical device security and facilitate sharing of best practice is being rolled out internationally this year.

The Medical Device Innovation, Safety and Security Consortium (MDISS) has launched the first of what are planned to be more than a dozen international medical device security testing labs and cyber-ranges.

The World Health Information Security Testing Lab (WHIST L), operating under MDISS will be made up of a web of medical device security testing labs. These facilities will be independently owned and operated by MDISS -member organisations that include medical device manufacturers, healthcare delivery organisations, universities and technology firms.

“MDISS WHIST L facilities will dramatically improve access to device security know-how while protecting patient privacy and stakeholder intellectual property,” said Executive Director of MDISS , Dr. Dale Nordenberg. “Solid cyber-lab governance will support an international-scale network of research and training centres of excellence, designed especially for medical device designers, hospital IT , and clinical engineering professionals.”

MDISS WHISTL will vet complex multi-vendor, multidevice critical care environments including Operating Theatres, Emergency Rooms and Hospital Intensive Care Units.

“Each WHISTL facility will launch and operate under a shared set of standard operating procedures,” a MDISS spokesperson said. “The goal is to help organisations work together to more effectively address the public health challenges arising from cybersecurity issues emergent in complex, multi-vendor networks of medical devices.”

By the year end, MDISS WHISTL facilities will open around the U.S. in New York, Indiana, Tennessee, California and further afield in the UK, Israel, Finland and Singapore.

WHISTL is not the first initiative to tackle enterprise IT security but it is the first lab network devised around the needs of HIT personnel, healthcare clinical engineering leaders and medical device researchers. The technology has already been rolled out to different healthcare facilities.

“Working with MDISS over the past year on WHISTL has helped us make real progress against some very complex risk scenarios, while keeping the focus on patient safety,” said CBET Manager/Clinical Engineer at Eskenazi Health, Benjamin G. Esslinger.

Current 2017 Trustee and past President of the Indiana Biomedical Society, Esslinger pointed out that medical devices were still at the forefront of cybersecurity and best security device practices were still maturing.

“Our new WHISTL facility enables us to run medical devices through tougher, more realistic test regimes. Hidden vulnerabilities surface more quickly, and that helps us build more responsive standard operating procedures,” he said.

Facilities operating WHISTL hone in on identification and mitigation of medical device vulnerabilities and, through their network, disseminate information on best practices. Critically, they also promote device security education and awareness. As soon as new vulnerabilities are uncovered, they are reported to device manufacturers and to the NH -ISA C-MDISS Medical Device Vulnerability Program for Evaluation and Response, or ‘MDVIPER ’.

“WHISTL will provide much-needed insight from actual developers and users of medical devices, which will result in increased relevant and actionable information sharing and situational awareness for all stakeholders in healthcare”, said president of NH-ISAC, Denise Anderson.

Under a $1.8 mln contract from the Department of Homeland Security (Science and Technology Directorate, Cyber Security Division), MDISS built the Medical Device Cyber Risk Assessment Platform, or 'MDRAP '. The platform helps health systems, device manufacturers, and technology firms collaborate to produce and share device risk assessments. The fast-growing and standards-based MDRAP platform features moderated crowdsourcing and facilitates timely, responsible sharing of risk assessments and threat indicators, while helping automate critical device inventory, audit, oversight and vulnerability tracking tasks for hospitals. WHIST L's device testing protocols will have their foundation in the UL Cybersecurity Assurance Program specifications especially with regards to fuzz testing, static binary analysis and structured penetration testing.

Key Points

- WHISTL facilities will operate under a shared set of standard operating procedures
- The initiative is aimed at helping organisations cooperate effectively to deal with public health challenges arising from cybersecurity issues for multivendor networks of medical devices
- MDISS built medical device cyber risk assessment platform (MDRAP) with a $1.8 mln contract from the Department of Homeland Security
- The platform supports collaboration amongst health systems, device manufacturers and technology firms to produce and share device risk assessments
- WHISTL's device testing protocols will have their foundation in the UL Cybersecurity Assurance Program specifications

The Medical Device Innovation, Safety and Security Consortium (MDISS), founded in 2010, is a non-profit public/private partnership dedicated to advancing patient safety and public health and the first to focus exclusively on medical device cybersecurity. MDISS develops and delivers practical technology, operations and policy solutions for member organisations, including hospitals, health delivery organisations, doctors, epidemiologists, clinical engineers, medical device manufacturers, academics, regulators, embedded security experts and cybersecurity researchers. **mdiss.org.**

The National Health Information Sharing and Analysis Center (NH -ISA C), the official healthcare information sharing and analysis center, offers non-profit and for-profit healthcare stakeholders, such as independent hospitals, IDN "providers", health insurance "payers", pharmaceutical/ biotech manufacturers, laboratory, diagnostic, medical device manufacturers, medical school and medical R&D organisations a community and forum for sharing cyber and physical threat indicators, best practices and mitigation strategies. NH-ISA C is a non-profit corporation funded and owned by its members. **nhisac.org**.

Published on : Tue, 19 Sep 2017