HITRUST and Healthcare Leaders Collaborate to Establish Cyber Threat XChange to Improve and Accelerate Cyber Threat Detection and Response

Enhanced Cyber Threat Sharing Acts as Early Warning System for Healthcare industry

Frisco, Texas – October 8, 2014 – HITRUST announced today the HITRUST Cyber Threat XChange (CTX) to significantly accelerate the detection of and response to cyber threat indicators targeted at the healthcare industry. HITRUST CTX will automate the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable formats that organization's of almost all sizes and cyber security maturity can utilize to improve their cyber defenses. HITRUST CTX will act as an advanced early warning system as cyber threats are perpetrated on the industry.

Healthcare leaders are collaborating with HITRUST to implement this capability that is crucial given the increase in cyber threats and attacks impacting the healthcare industry, such as the recent Bash bug. HITRUST CTX initial participating organizations include: Express Scripts; FireHost; Health Care Services Corp.; Highmark Health; Humana; Seattle Children's Medical Center; UnitedHealth Group; University of Rochester Medical Center; and WellPoint.

HITRUST CTX will enable the timely exchange of cyber threat indicators contributed by industry organizations - e.g. Indicators of Compromise (IOC), Tactics, techniques, and Procedures (TTPs), and malware signatures - that can be quickly analyzed and disseminated to provide holistic and actionable threat intelligence relevant to healthcare organizations. It will provide the most effective view of cyber threats being targeted at the healthcare industry.

Access to an automated service will not only provide early detection and faster analysis by the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3), but will also allow organizations to mitigate cyber threats quicker and more effectively. HITRUST CTX will leverage threat indicators contributed by industry organizations which will be analyzed against other threat sources such as U.S. CERT and other cross industry threat resources to understand prior awareness outside of the healthcare industry.

Cyber criminals are coordinated in their shared threats, practices and procedures and synchronize assaults across multiple companies. Organizations need a mechanism to identify these patterns and need to move quickly to address these cyber security threats before they are targeted and long before any of their internal systems pick up signs of an attack.

"Many of us in the industry have been sharing cyber threat information with the HITRUST C3 to support our own and industry's cyber threat preparedness and response," said Roy Mellinger, CISO, WellPoint. "One limitation of the process today is the ability to obtain quality threat indicators in a timely and machine consumable format, which the HITRUST CTX addresses."

"As a hosting organization focused on the healthcare industry, being able to have access to actionable, industry specific threat indicators, that can inform the rapid development of countermeasures, is the holy grail," said Jeff Schilling, CSO, FireHost. "Given the hundreds of healthcare organizations hosted in our data centers, we also have threat indicators that we can share with the HITRUST CTX for the benefit of the entire industry."

Although the methods used by threat actors may be similar across industries, understanding the motives and targets affords valuable insights currently not available and critical for early response and alerting specific for the entire healthcare industry. The HITRUST CTX model allows any participating organization to sift through tens of thousands of cyber threats to identify which threats they should be worried about now.

“The biggest challenge we face is not knowing how to prioritize and act upon the growing list of cyber threats - especially in healthcare organizations which are being increasingly targeted yet are often limited by smaller staffs or resources, and burdened with threat analysis and incident response,” said Cris Ewell, CISO, Seattle Children’s Hospital.

“HITRUST CTX is a great example of how collaboration benefits and safeguards the entire industry, and I applaud my colleagues for their leadership and willingness to work together to tackle this challenge,” said Raymond Biondo, Divisional Senior Vice President and CISO, Health Care Services Corp.

HITRUST CTX is also designed to be efficient, and support broad adoption by end users or their Managed Security Services Providers (MSSPs) through two-way compatibility with their Security Information and Event Management (SIEM) systems. The service will adopt and utilize the Structured Threat Information Expression (STIX), Trusted Automated eXchange of Indicator Information (TAXII) and Cyber Observable eXpression (CybOx) standards for transmission of information and will also support information exchange in other formats to facilitate adoption and participation.

“HITRUST CTX is component of a larger HITRUST strategy to safeguard the healthcare industry from cyber threats and minimize disruptions associated with cyber attacks,” said Daniel Nutkis, CEO, HITRUST. “Other components of the strategy include HITRUST C3, a cyber threat intelligence and incident coordination center, and CyberRX, industry cyber preparedness exercises, as well as timely updates to the HITRUST CSF to ensure existing security control guidance reflects cyber threats, and free monthly cyber threat briefings.”

About HITRUST
The Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information privacy, risk and security leaders, has established a number of programs to support any and all organizations that create, access, store or exchange personal health and financial information. HITRUST is supporting the industry through its framework, assurance program, cyber center, risk management tools, education and leadership. It is also driving the widespread confidence in the industry’s safeguarding of health information through awareness, education, advocacy and other outreach activities. For more information, visit www.HITRUSTalliance.net.

###

Media Contact:
Leslie Kesselring
Kesselring Communications for HITRUST
503.358.1012
leslie@kesselring.net or pr@HITRUSTalliance.net