HITRUST and Trend Micro Announce First Collaborative Advanced Cyber Deception Program

Unique Partnership Continues to Advance the State of Cyber Threat Management and Response

Frisco and Dallas, TX – October 3, 2017 – With the healthcare industry under constant cyberattack, organizations need to do more to protect themselves and understanding cyberattack methods and techniques is an important step to enhancing defenses. HITRUST and Trend Micro announced today the HITRUST Cyber Threat XChange (CTX) Deceptive, a deception-based threat detection collaboration platform that deploys honeypots across the healthcare ecosystem. With this announcement, the two organizations have launched the second phase of the recently enhanced HITRUST Cyber Threat Management and Response Center.

HITRUST CTX Deceptive deploys decoys that work together to deceive attackers and gain knowledge of their methods, processes, tactics and targets of interest. These decoys, or honeypots, are computer systems designed to attract and monitor attackers and are typically deployed as stand-alone systems within individual organizations. HITRUST has taken the concept to the next level by designing a deception environment that spans across many healthcare organizations via the HITRUST CTX threat sharing infrastructure. HITRUST has also deployed decoys of commonly-used systems including leading EHRs, medical devices and other healthcare-specific systems. HITRUST facilitates the 24/7 monitoring of the activity.

"This is the first time that multiple organizations have come together to undertake such a sophisticated and aggressive approach to cyber deception. By working together and sharing the different types of traps and decoys, as well as intelligence gathered related to specific threat actors, systems or medical devices, cyber defenders now have insight beyond basic IOC information," said Kevin Charest, DSVP and CISO, Health Care Service Corp.

HITRUST CTX Deceptive is able to identify trends - providing insight into how threat actors are infiltrating and exploiting networks, applications and systems while capturing complete malicious activity, IP addresses and domains. Advanced tactical intelligence on attack behaviors and possible attack paths can be anticipated, and indicators of compromise (IOC) data and alerts on threats to specific applications and medical systems can be shared with organizations to prevent an attack and reduce the risk of breach or compromise.

"Our experience with honeypots allows us to understand the results of malicious activity within the HITRUST CTX and provide an advanced level of protection. With enhanced visibility into the network, early detection of attacks in the decoy environment can improve the industry's time-to-respond with third-party integrations to isolate and block attacks. Trend Micro's industry expertise is now taking the healthcare industry to a much higher level," said Mike Gibson, Vice President, Threat Research, Trend Micro.

"HITRUST has been innovating IOC collection and sharing for many years and HITRUST CTX Deceptive represents a key missing piece within the current IOC collection approach. This development builds on

our commitment and partnership with industry and government to build trust and collectively improve the industry's cyber defenses and resilience," said Daniel Nutkis, CEO, HITRUST.

HITRUST CTX Deceptive is the next phase in the HITRUST vision to deliver capabilities that address real world issues facing CISOs like cyber threat management, defense and response. Similar to other HITRUST CTX programs, it is based on an organization's cyber maturity level and subsequent ability to defend against the increasing volume and sophistication of cyber threats. HITRUST CTX Deceptive builds on the existing HITRUST Enhanced IOC Collection Program, which has already demonstrated significant, measurable and tangible improvements in quality, timeliness and accuracy of IOCs.

HITRUST CTX Deceptive is deployed and operational at organizations in the healthcare industry. HITRUST is announcing the program in order to solicit participants, as part of the HITRUST Cyber Threat Management and Response Center, but will not publicly disclose any information about the participating organizations or the target systems that decoys have been developed or will be in the future. HITRUST continues to offer basic access to the HITRUST CTX and the new HITRUST Cyber Threat Management and Response Center at no cost.

Sign up here to be part of the CTX Deceptive program: https://hitrustalliance.net/ctx-sign-up/

HITRUST Cyber Snapshot

The HITRUST CSF is the most widely adopted controls framework in the healthcare industry and the basis for the HPH Sector implementation for the NIST Cybersecurity Framework.

The HITRUST CTX supports over 1,600 organizations in cyber information sharing. The Enhanced IOC Collection Program has significantly increased the usability of IOC data and in the latest six-month analysis reported seeing IOCs as early as 150+ days in advance, and on average 21 days in advance, of other exchanges. HITRUST has worked closely and in partnership with government, through the existing programs like the DHS Cyber Information Sharing and Collaboration Program (CISCP) and the DHS Automated Indicator Sharing (AIS).

Trend Micro Threat Research Snapshot

Trend Micro is a global leader in cybersecurity solutions with over 27 years of industry experience and award-winning solutions across User Protection, Hybrid Cloud Security and Network Defense.

Trend Micro security research and operations consists of global researchers, engineers, and other experts in various security functions working 24 hours a day, seven days a week to deliver solutions to the plethora of threats that confront users and businesses on a daily basis. This includes:
- The industry's most respected and prolific broker of responsibly disclosed security vulnerabilities. This award-winning group operates Pwn2Own, the industry's oldest and most successful vulnerability research competition.
- A 24x7 Global Threat Research and Emergency Response team that is responsible for ongoing population of timely threat intelligence to the Trend Micro Smart Protection Network (SPN). SPN is at the core of Trend Micro solutions to help organizations combat today's threats. This

includes threat hunting operations, rapid response capabilities, and cleanup and remediation services for our customers.
- A global team of researchers tasked with scouting the likely future risks in security focusing primarily on:
    - Cybercrime and APT campaign research of threat actors using OSINT and other threat data
    - Research into wider attacks in the emerging world of IOT and where old technologies meet with the new
    - Exploring how societies changing social use of the web exposes new attacks
- Collaboration with law enforcement agencies during cybercriminal investigations and botnet takedowns

About HITRUST

Founded in 2007, the HITRUST Alliance, a not for profit, 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 public and private healthcare technology, privacy and information security leaders—has championed programs instrumental in safeguarding health information and managing information risk while ensuring consumer confidence in the organizations that create, store or exchange their information.

HITRUST develops, maintains and provides broad access to its common risk and compliance management and de-identification frameworks, and related assessment and assurance methodologies, as well as programs supporting cyber sharing, analysis and resilience. HITRUST also leads many efforts in advocacy, awareness and education relating to information protection.

For more information, visit www.HITRUSTalliance.net.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

Media Contacts:
HITRUST
Leslie Kesselring
leslie@kesscomm.com or pr@HITRUSTalliance.net
+1 503 358 1012

Trend Micro Incorporated
Cara West
publicrelations@trendmicro.com
+1 817 569 1993