HITRUST™

CTX Deceptive Program Frequently Asked Questions

1710- v1

What is the purpose of this FAQ?

This Frequently Asked Question (FAQ) document has been prepared to accompany the "HITRUST and Trend Micro Announce Industry's First Collaborative Advanced Deception Program" press release.

What is a Collaborative Advanced Deception Platform?

This platform is introduced in the form of deceptive components across organizations to trap cyber attackers and enhance the defense of networks and systems with unprecedented speed and accuracy. Initially, the Collaborative Deception platform will be deployed across the healthcare ecosystem.

What is included in the platform?

The platform is based on HITRUST Cyber Threat Xchange (CTX) Deceptive technology which deploys decoys that work together to lure attackers and gain knowledge of their methods, processes, tactics and targets of interest.

CTX Deceptive identifies trends and provides never before seen insights into how threat actors are infiltrating and exploiting key systems, while capturing complete malicious activity IP addresses and domains. Advanced tactical intelligence on attack behaviors and possible attack paths can be anticipated, and IOC data and alerts on threats to specific applications and medical systems can be shared, anonymously, with organizations to prevent an attack and reduce the risk of breach or compromise.

What is a honeypot?

Honeypots are computer systems and artifacts designed to attract and monitor attacker's activities, and are typically deployed as stand-alone systems within individual organizations.

A honeypot is a computer security mechanism set to detect, deflect, or in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then observed. Those observations of tactics, techniques and procedures are invaluable and in turn used to create rules in current security controls to protect real healthcare systems.

What is Trend Micro's relationship to HITRUST?

Through its partnership with HITRUST, Trend Micro will contribute its extensive expertise and research lab resources to the CTX Deceptive program. Trend Micro researchers are monitoring and developing alerts, reports and necessary response and prevention rules on a 24/7 basis.

What kind of attacks will this help identify?

This solution is focused around TTPs (Tactics, Techniques, Procedures) used by cyber-criminals and would-be attackers attempting to gain access to privileged systems or critical data. This will help identify the threats trying to compromise systems which contain Protected Health Information (PHI) as well as medical systems and sensitive data. Because of the nature of the honeypot decoys and network, the system will have theoretically zero false positives, as no legitimate activity should ever occur on these systems.

The attack intelligence gathered within this deception solution differs from the Enhanced IOC program since it lures attackers to fake data within the decoys, whereas the Deep Discovery Inspector used today detects intrusions and breach stage visibility throughout the network, including patient zero.

Does it help detect ransomware threats?

Yes, this can detect the many types of ransomware threats such as WannaCry. It is also complimentary to the Deep Discovery capabilities deployed as part of CTX Enhanced, which also offers response integration.

Does this have to be deployed at my organization for us to get the benefits?

Yes, every CTX participant benefits from more timely and complete IOCs but only CTX Deceptive subscribers will have access to the more detailed TTP and other threat actor intelligence.

If I am a basic CTX member, will I still receive the benefits?

Yes, every CTX participant benefits from more timely and complete IOCs; however, only CTX Deceptive subscribers will have access to the more detailed TTP and other threat actor intelligence.

How can I have one deployed onsite at my organization?

Apply to join CTX at https://hitrustalliance.net/ctx-sign-up/.

How much does it cost?

There currently is no cost for organizations to participate in the program, but within the next (6) six months there will be a fee associated.

If you have any additional questions, please contact us at ***info@hitrustalliance.net****.*