

Tabla de Contenidos

RESUMEN	2
1. INTRODUCCIÓN	3
2. ¿QUÉ ES MERCADO THRINTEL?	3
3. CARACTERÍSTICAS DE MERCADO THRINTEL	4
4. ¿CÓMO FUNCIONA	4
5. MONEDA DETALLES	
8	
6. DISTRIBUCIÓN DE LA MONEDA	
9	
7. ¿Por qué THRINTEL mercado?	
11	
8. ALMACENAMIENTO	
12	
9. TOKEN LANZAMIENTO	13
10. ROADMAP	13
11. EQUIPO Y COMUNIDAD	15
CONCLUSIÓN	19

RESUMEN

Inteligencia de amenazas refiere a la información de confianza que se conoce a menudo para ser altamente organizado, analizado y refinado. A menudo se trata de ataques probables o en curso que amenazan una organización / institución. También se conoce como la inteligencia amenaza cibernética (CTI).

Inteligencia de amenazas se centra principalmente en ayudar a las organizaciones a identificar y entender los riesgos de común, así como graves amenazas externas. Estas amenazas incluyen la gama de las amenazas de día cero, amenazas avanzadas persistentes (APT) y exploits. Inteligencia de amenazas incluye, pero no se limita a, la recopilación extensa de material en relación a amenazas específicas. Esto permitirá un escudo contra las agresiones organización que podría dar paso a un daño grave.

Paisaje cibernético de hoy es tan dinámico y rápidamente cambiante, tanto es así que el valor de las inversiones en seguridad se llama constantemente ende tela juicio. Por otro lado, también hay una comunidad en constante crecimiento de los atacantes cibernéticos que no están tomando el descanso de un segundo de la invención de nuevos movimientos inteligentes y astutos en la ejecución de las actividades amenazantes. Los expertos en seguridad de alta tecnología trabajan con uñas y dientes para prevenir y analizar datos e información existentes a fin de evitar futuros ataques. El efecto resultante de todas ellas es la creciente popularidad de inteligencia de amenazas.

Sin embargo, la información sobre amenazas sólo es valiosa cuando es 99% preciso, eficiente y tiene un proceso de transmisión que es a la vez seguro y libre de consecuencias nefastas. En términos básicos, la inteligencia de amenazas es el proceso de comprender totalmente las amenazas reales y potenciales que pueden acontecer una organización. También incluye el análisis de datos en relación con empresas específicas basadas y consideraciones de contexto. Esto permitirá una toma de decisiones clara en cuanto a la validez de acción basado en las opciones disponibles.

En esencia, si los datos recogidos no pueden ser analizados adecuadamente para informar a posibles acciones contra las amenazas o amenazas inminentes, la inteligencia de amenaza es tan buena como inútil.

INTRODUCCIÓN

El intercambio de la información sobre amenazas está montado con demasiados defectos como resultado de la ineficiencia de los procesos involucrados. Los clientes y las organizaciones se enfrentan por igual un alto riesgo de mala aparición pública en el caso de un corte o cualquier otra amenaza a la seguridad. También está la cuestión de las fuentes no confiables. En el pasado, las organizaciones tienden a depender de los proveedores a los que no tienen la menor idea acerca de su credibilidad o la eficiencia de Intel sobre la mejor manera de prevenir los ataques o librarse de uno. Este sistema coloca grandes empresas e instituciones altamente sensibles, como las agencias militares o gubernamentales, bancos, etc., con gran riesgo. En el proceso se pierde grandes cantidades de dinero, un montón de tiempo se pierde y la reputación de la organización se deja en ruinas totales. Es a partir de esta necesidad que surge THRINTEL mercado para llenar los vacíos y modificar los lapsos de intercambio de inteligencia previa amenaza.

¿Cuál es THRINTEL MERCADO?

Mercado THRINTEL fue acuñado desde el 'mercado de inteligencia de amenazas' frase. Es un blockchain inteligencia de amenazas descentralizado en el que se produce el intercambio de datos a través de la compra y venta. Un aislado criptomoneda basado en Ethereum criptomoneda blockchain se utiliza para controlar las actividades que se llevan a cabo en organizaciones tales como incentivar contribución. Intercambio de Intel está hecho para ser lo más seguro posible mediante la descentralización de la primera base de datos y examinar todos los datos recibidos para determinar su validez antes de que puedan ser intercambiados. Esta descentralización se hace para evitar daños graves deben un ataque imprevisto ocurre. A diferencia de otras opciones disponibles de inteligencia de amenazas a organizaciones, THRINTEL es a la vez la seguridad centrado y relaciones públicas centrada. De esa manera, las grandes corporaciones y los gobiernos no se enfrentan al riesgo mortal de dañar su reputación.

CARACTERÍSTICAS DE THRINTEL mercado

descentralizado Amenaza Base de datos de inteligencia de

mercado THRINTEL es rápido, fácil acceso, y muy eficaz, independientemente de su ubicación. Está construido para ser denial de servicio proof.

Amenaza inmutable base de datos de Inteligencia

datos cargados en la base de datos no pueden ser alterados. Grupos avanzada persistente amenaza son conocidos para cortar OSINTs (Amenaza de código abierto de Inteligencia Servers) y extraer datos de informes de sus herramientas, tácticas o activos. No van a ser capaces de hacerlo contra el mercado THRINTEL.

RÁPIDO Blockchain basa en un genio idea del

Nuevo artefactos y evaluaciones sobre los artefactos presentados son procesados rápidamente y actualiza en tiempo real. También es absolutamente libre para el comercio de datos en la plataforma. Es de código abierto, por lo tanto, se actualizará / mantenida por la comunidad. Dado que todos los artefactos son encriptados hasta una cuenta de ellos, la cuenta de compra, para el comercio de manera eficiente, tiene que presentar todo lo que tiene en el mercado antes de comprar nada. Esto significa nuevos datos fluyan continuamente en el blockchain, siempre que hay oficios siendo ejecutado. Los datos presentados no sólo es necesaria, pero ganarán los puntos de cuenta de reputación, y dinero en el proceso.

Las cuentas anónimas

Si su organización se enfrenta a un ataque y que desean compartir datos sobre los hackers atacar a su plataforma para informar a los demás a mirar hacia fuera para ellos, se arriesga a malas relaciones públicas. Todo lo que necesita hacer es compartir datos de forma anónima en el mercado THRINTEL.

Las cuentas verificadas

Si usted tiene una empresa de seguridad y sus investigadores encontraron día y precisos datos de cero en algunos hackers cuyo objetivo un determinado país, se publican en el mercado THRINTEL y ahora se sitúan muy alta en los principales proveedores de datos específicos en este país. Si usted tiene antivirus o de seguridad soluciones que empezar a ver mejores ventas, ya que los clientes ahora ven que la clasificación muy alta en su país o sector empresarial. Esto asegura que los clientes ven más allá de las campañas publicitarias de negocio de seguridad y en

sus resultados reales y cómo se comparan entre sí cuando se trata de detectar nuevos agentes de amenaza.

Cómo funciona (EL MERCADO Y LA MONEDA)

Amenaza de Inteligencia de Mercado o (MERCADO THRINTEL) es un mercado en el que los datos son compartidos e intercambiados por las grandes corporaciones, gobiernos, investigadores de inteligencia de amenazas y más. La moneda SEGURO ó SEC es una moneda utilizada para llevar a cabo transacciones en el mercado. El mercado THRINTEL está destinado esencialmente a ser un blockchain de bloques que contienen dos tipos de entradas. En las entradas de Bitcoin son A X enviado a B. Mientras que en el mercado THRINTEL tenemos dos tipos de entradas; esos son C, para ROW Contribución, y F, para Comentarios ROW.

Esto es lo que la fila contribución que parece:

REPORTERS SELL THIS [CONTRIBUTED ROW] : we refer to this as C row			
ACCOUNT	ARTIFACT (URL or IP)	MALICIOUS SCORE (percentage)	METADATA (timestamp, country code, sector code)
%STRING% : FLOATINGPOINT% : %DIGIT%	%STRING%	%FLOATING POINT%	%ARRAY OF 3 INTEGERS%
1BcVWPkPLSXh4ivo5pv s2rplhAsWW4Tnf1; 82; 1	8.8.8.8	85	03140719012018, 124p 10
Just an address to refer to you : REPUTATION : VERIFIED FLAG	Google DNS IP address	How confident is the reporter that this is malicious (the higher the number the more damage this artifact can cause)	First number says this was added on 03:14:07 19-01-2018 Second number says this is in country number 124 which is canada (ISO 3166) Third number refers to a specific industry or sector in our standard list for example 12 refers to financial sector

Bajo cuenta que tiene una dirección, una puntuación de reputación, y una bandera de VERIFICADO. Esto le representa, su reputación actual en el mercado, y si usted tiene una cuenta verificada o no (cuentas verificadas son a efectos de identificación por empresas de seguridad). Bajo artefacto que tiene una IP o URL. Esto es lo que usted está enviando comentarios acerca. Bajo SCORE malicioso, que tiene un número que representa lo que piensa del artefacto, 0 para no malicioso, 100 para esto es muy dañino. En virtud de metadatos, que

tiene una marca de tiempo, un código de país y un código de sector. Esto da contexto a su contribución.

La fila de retroalimentación se ve así:

BUYERS SUBMIT THIS OPTIONALLY [FEEDBACK ROW] : we refer to this as F row

ACCOUNT	ARTIFACT (URL or IP)	FEEDBACK SCORE (percentage)	METADATA (timestamp, country code, sector code)
%STRING% : FLOATINGPOINT% : %DIGIT%	%STRING%	%FLOATING POINT%	%ARRAY OF 3 INTEGERS%
1BcVWPkPLsXh4ivo5pys2rjrhAsWW4Thf1; 82; 1	8.8.8.8	0	03140719012018, 124p 10
Just an address to refer to you : REPUTATION : VERIFIED FLAG	Google DNS IP address	Was this worth your money? 0 = scam 100 = great	First number says this was added on 03:14:07 19-01-2018. Second number says this is in country number 124 which is canada (ISO 3166) Third number refers to a specific industry or sector in our standard list for example 12 refers to financial sector

En Cuenta usted tiene una dirección, una puntuación de reputación, y una bandera de VERIFICADO. Esto le representa, su reputación actual en el mercado, y si usted tiene una cuenta verificada o no (cuentas verificadas son a efectos de identificación por empresas de seguridad). Bajo artefacto que tiene una IP o URL. Esto es lo que usted está enviando comentarios acerca. Bajo puntuación de votos, que tiene un número que representa lo que piensa del artefacto, 0 para no malicioso, 100 para sí, esto era malicioso y me salvó activos. En virtud de metadatos, que tiene una marca de tiempo, un código de país y un código de sector. Esto da contexto a su regeneración.

El mercado THRINTEL se va a utilizar en gran medida por las máquinas autónomas, la IO, las soluciones de seguridad, antivirus, cortafuegos, servidores, centros de datos de almacenamiento de nube, etc. La plataforma puede ser utilizado por los analistas de inteligencia de amenazas en el gobierno, sectores empresariales, grandes corporaciones, o incluso los investigadores, estos individuos pueden ser capaces de procesar los datos en el software de visualización por su cuenta. Pero nuestro software les da acceso a filas compilados como el siguiente. Llamamos a los que la fila O compilado, que no existe en el blockchain pero no es más que una representación de los datos de las listas enlazadas o cadenas en el blockchain. Máquinas compilan los de antes de tomar cualquier decisión sobre la plataforma, así, se trata de la única manera para un comerciante de datos, siendo humanos, o de la máquina, por igual, para tomar una decisión de compra o descarga un nuevo artefacto que aparece en la plataforma.

BUYERS COMPUTE AND BUY/USE THIS [OFFERED ROW] : we refer to this as Q row [IT IS A REPRESENTATION OF THE CHAIN OF C & F ROWS]				
REVENUE DISTRIBUTION	ARTIFACT (URL or IP)	TRUST SCORE (percentage)	PRICE (in SEC coins)	METADATA (timestamp, country code, sector code)
%ARRAY OF 10 FLOATING POINTS% : %ARRAY OF 10 STRINGS%	%STRING%	%FLOATING POINT%	%FLOATING POINT%	%ARRAY OF 3 INTEGERS%
80, 73.6, 61.88, 39.9, 22, 21.5, 17, 15, 12, 9 : 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1 1BcWMPkPLSxh4wo5pxs2qjhsaVW4Tnf1	8.8.8.8	10.54	2	03140719012018, 124, 10
Addresses of best 10 submitters and the cut they are getting of the price	Google DNS IP address [submitted by reporter(s)] This part is normally encrypted until the viewer pays for it then and only then it is decrypted	Score calculated by the system	Price calculated by the system	First number says this was added on 03:14:07 19-01-2018 [submitted by reporter(s)] Second number says this is in country number 124 which is canada (ISO_3166) [submitted by reporter(s)] Third number refers to a specific industry or sector in our standard list for example 12 refers to financial sector [submitted by reporter(s)]

Bajo distribución de los ingresos proviene de las direcciones de las personas que reciben una parte de los ingresos una vez que compre los datos o técnicamente compra una llave para abrir el artefacto. Estas direcciones se refieren a las mejores 10 peticionarios que reportaron el artefacto a ser maliciosas, que podrían ser de diferentes partes del mundo, algunos de ellos han encontrado que en una misión de caza amenaza, o durante la investigación, o pueden haber sido golpeado con ella y sufrido pérdidas. No sólo hay aborda allí, pero la cantidad de cada uno de ellos es hacer de cada moneda que paga SEC. Eso sí hay que pagar tasas cero para todo el mundo en la plataforma. Estos valores se calculan en función del # de la prensa, las propuestas presentadas marcas de tiempo, resultados maliciosos, reputaciones de los reporteros. Bajo artefacto que tiene la IP o URL que está comprando, pero por supuesto es codificadas hasta que comprar la llave que abre sólo para usted (la llave sólo trabajaría con su cuenta). Bajo SCORE TRUST encontrará una puntuación calculada por TRUST crujido abajo # de reporteros, la puntuación malicioso, reputaciones de los reporteros, la retroalimentación para darle una idea de cómo confiar en que

debe poner en el sistema. Bajo precio es un precio en la única moneda en la plataforma (Coin SEC) o SEGURO Coin. El precio de la moneda seguro se calcula en base a la puntuación de confianza, los valores de metadatos. Bajo metadatos, hay una marca de tiempo, un código de país y un código de sector. Estos ayudan a contextualizar el artefacto.

MONEDA DETALLES

Ticker:SEC:

Plataforma Ethereum

tipo de token: ERC20

disponible para pre-ICO venta: 90.000.000 SEC

inicio de la venta símbolo: 12 Marzo

casquillo suave: 300

ETH de cubierta dura: 3 000

ETH SEC total Fichas publicación: 2 000 000 000 SEC

Precio : 1 ETH = 30.000 SEC

Forma de pago: ETH contribución mínima:0,1 ETH

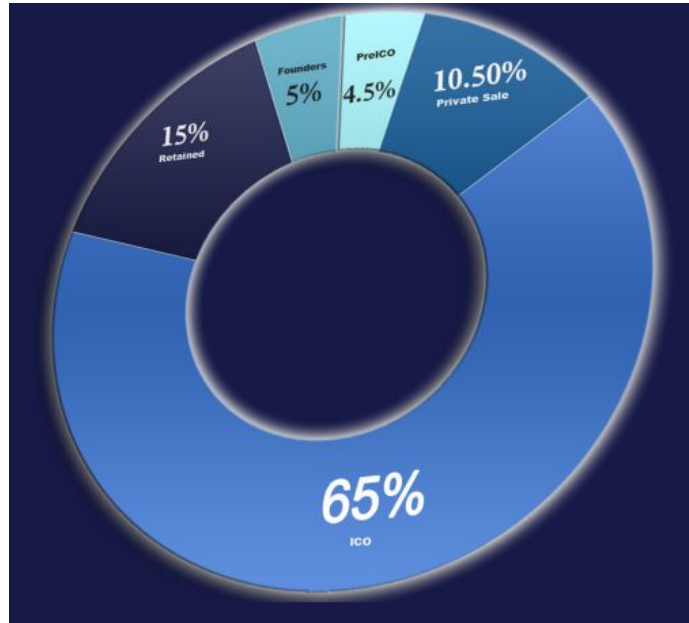
se requiere Todo el mundo a tener una cuenta en la plataforma. Las cuentas son anónimas de forma predeterminada hasta una empresa de seguridad quiere una cuenta verificada para la marca, ya que podría ser utilizado en los informes trimestrales que dicen que la empresa X es el proveedor de la información sobre amenazas líder para la BFSI Sector de América del Norte en 2019 Q3, que puede conducir a una mayor adopción de soluciones Company X en el marco de tiempo. Cuentas anónimas son un activo para los bancos de ser atacado y querer reportar un artefacto líder en el grupo APT atacarlos para advertir a otros. Pero esto conduce a malas relaciones públicas para el banco indiquen, por ejemplo. Por lo tanto, los canales actuales son sólo entre bancos o socios seleccionados, dejando la inteligencia fuera de las noticias o de la conciencia pública. Con blockchain es posible informar completamente anónima evitando la mala prensa.

A continuación se muestra la figura que muestra los dos tipos de cuentas:

ACCOUNTS LOOK LIKE THIS			
Verified vendor account used for branding and advertising for Kaspersky and a channel to sell their threat intel.			
Address	NAME	VERIFIED	REPUTATION (percentage)
%STRING%	%STRING%	%DIGIT%	%FLOATING POINT%
1BcVWPkPLSxh4ivo5pys2rpjhAsWW4Thf1	KASPERSKY LABS	1	82
Just an address to refer to you [needed]	The name given to the account [optional]	Is this a verified vendors account? (this can only be set by admin) [optional]	Score calculated by the system [needed]
An anonymous account used by TD Bank to submit IPs that were involved in a recent attack against their system. They share that anonymously to warn everybody else in the financial sector of these cyber gangs in real time without getting the BAD PR involved with banks publicly saying they got hacked.			
Address	NAME	VERIFIED	REPUTATION (percentage)
%STRING%	%STRING%	%DIGIT%	%FLOATING POINT%
1BcVWPkPLSxh4ivo5pys2rpjhAsWW4Thf2		0	97
Just an address to refer to you [needed]	The name given to the account [optional]	Is this a verified vendors account? (this can only be set by admin) [optional]	Score calculated by the system [needed]

MONEDA DE DISTRIBUCIÓN

4,50% de la moneda THRINTEL MERCADO se dará a conocer a durante el período pre-ICO mientras que el 65% se asigna a las rondas de la OIC de la venta de fichas. 10,5% se venderá de forma privada a los inversores seleccionados en el círculo THRINTEL mercado. 15% de las monedas será retenido para la difusión y promoción. Los fundadores se quedará con un 5% de las monedas.

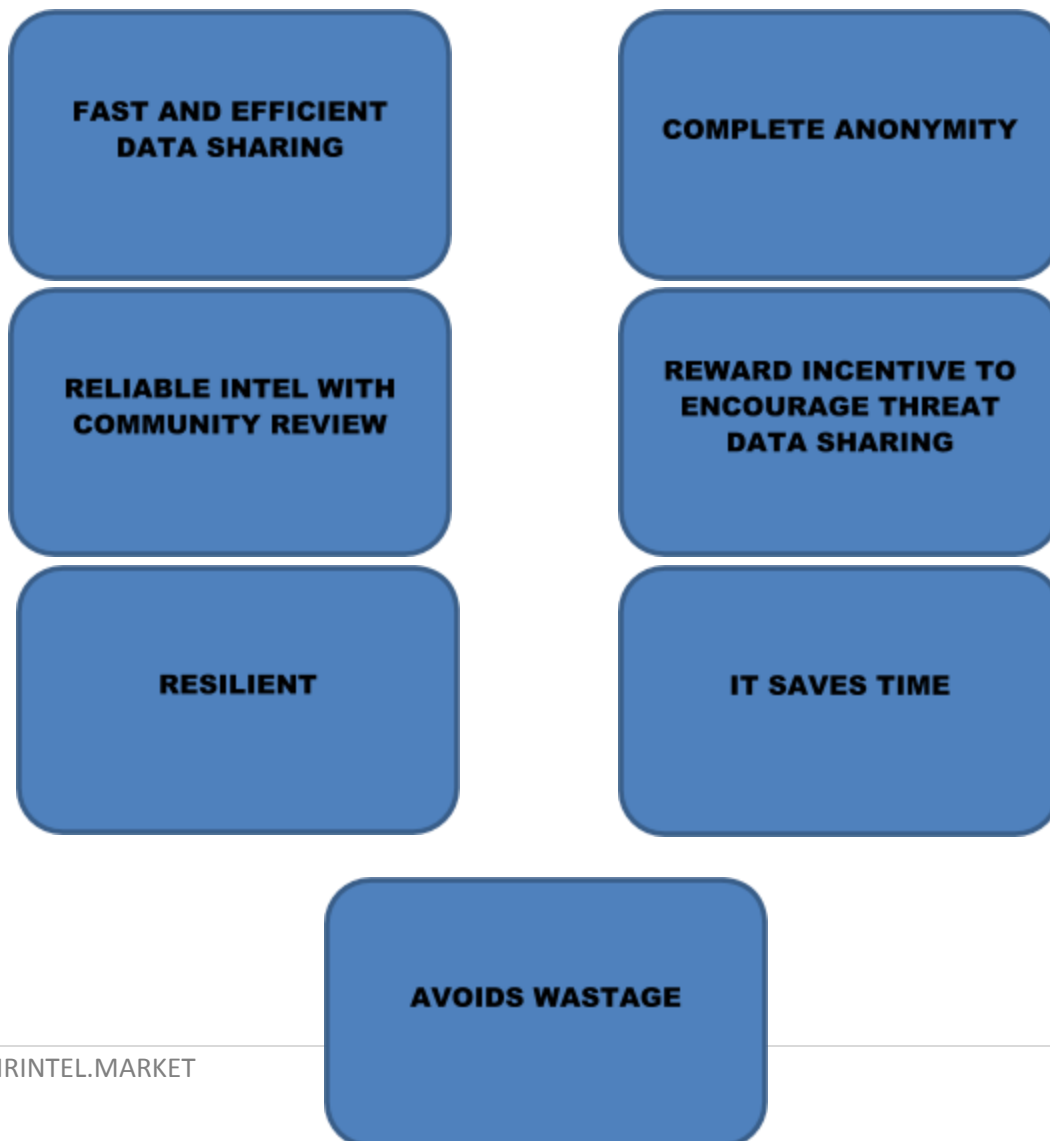


THRINTEL Market ofrece el intercambio de datos en tiempo casi real con el anonimato completo y Valoración de la comunidad y validaciones. Y con un incentivo para compartir sus datos de amenazas (hay que subir lo que tiene hasta que no lo compre de nuevo, y usted hace el dinero y la reputación de todo lo que envíe), sabemos que la gente nunca dejarán de investigación para las nuevas amenazas y en realidad va a compartirlo con los demás. Los vendedores pueden utilizar esto para conseguir una mejor reputación de su marca como líder en Intel amenaza en un determinado sector de la industria o de un país, por ejemplo, mientras que los bancos o gobiernos pueden compartir cosas de forma anónima con otros sin correr el riesgo de malas relaciones públicas o titulares de noticias. El bloque de la cadena es elástico, casi imposible de derrotar o manipular, inmutable, distribuida, y no tiene moderador o autoridad central de volver a utilizarla. Ahorramos compradores el dinero (que compran cosas una vez sin marcas injustos, lapso de tiempo, los procesos tediosos, o diferentes formatos) y hacer que los proveedores de dinero justo y la marca por su esfuerzo (mediante la distribución de los puntos de ingresos y la reputación de cada artefacto en el que informó que como pronto y más preciso posible). THRINTEL mercado también ofrecen a los compradores una forma más resistente, seguro de que realmente puede confiar para su Intel amenaza.

¿Por THRINTEL MERCADO?

Por ahora, muchas preguntas están apuntando en su mente. ¿Por qué el mercado THRINTEL? ¿Que es diferente? Hay un montón de razones por las thrintel mercado supera a todas las demás opciones en el campo hoy en día. Amenazade Inteligencia no anima a nadie a trabajar fuera de la zona de confort. Si usted es un proveedor y se está trabajando en otra cosa que lo que se enfrentan la mayoría de sus clientes nada, sufrirá. Y el mercado está dominado por grandes nombres que han reducido los presupuestos de investigación y han aumentado los presupuestos de marketing en su lugar. Mostrando un monopolio sobre el mercado y matar a cualquier nuevo esfuerzo de investigación en un esfuerzo por mantener un mercado saturado y monopolizado, que se pueden beneficiar fuera. Esto conduce fundamentalmente a una industria de seguridad muy débil y por lo tanto conduce a todos los fallos o “hacks” /”brechas” /”escándalos” que afectan a la plataforma víctima y por extensión la economía negativamente.

Hemos recopilado las razones siguientes:



Nuestro enfoque se basa en grandes organizaciones y la comunidad, tales como los de Defensa y empresas de consultoría, agencias gubernamentales, las telecomunicaciones, la seguridad cibernética investigadores, analistas de Inteligencia de amenaza, los arquitectos de seguridad, de Operaciones de Amenazas de caza, oficiales de inteligencia, Big Data Ingenieros, Machine Learning investigadores, Operaciones de Seguridad Penetración probadores, la amenaza vendedores Intel, empresas de seguridad, Electrodomésticos Networking proveedores, empresas con enormes redes, empresas de gran escala, el sombrero blanco hackers, etc. y de estas colaboraciones una comunidad grande y poderoso está obligado a emerger.

ALMACENAMIENTO

está previsto El problema de almacenamiento, hemos desarrollado un algoritmo para permitir a sus pequeños dispositivos incapaces sólo para descargar las partes pertinentes de la blockchain (de acuerdo con los metadatos “marco temporal, país, sector industrial”) esto permite que dispositivos como el teléfono para que todavía se benefician de la la red, pero sólo se alimentan de amenaza relevante alimenta. Este algoritmo introducirá un poco de una dependencia de un grupo de nodos vecinos que va a ser totalmente actualizada y tener una copia completa del blockchain. La aplicación de teléfono le pedirá entonces uno de los nodos para ejecutar las operaciones en su nombre. En este punto, el resto de los nodos validar la autenticidad de las operaciones ejecutadas por el nodo seleccionado y actualizar la reputación y la recompensa del nodo seleccionado. Una operación como la que se discute aquí costará el teléfono cuenta un poco más ya que hay un modelo de comisión que se impongan. Por lo tanto recompensar el nodo que mantiene una copia completa de la blockchain y operaciones ejecutadas en cuenta nombre del teléfono.

LANZAMIENTO DETOKEN

PREICO (inicial de la moneda de Oferta) tiene previsto su lanzamiento el 12 de desde 03 hasta 03 18 2018, que dura sólo 7 días, mientras que el lanzamiento de ICO (Coin de primera emisión) está previsto que tenga lugar en julio de 2018. Durante estas ventas, el se espera que la demanda de la SEC para estar en un gran aumento. Sin embargo, hay monedas limitados disponibles para la venta. Las tasas de bonificación de hasta el 37,5%. Recompensas (BOUNTY) por valor de programa de hasta 10.000.000 de monedas a la SEC.

	>100ETH	>20 ETH	>5 ETH	>1 ETH
Day 1	37.5%	32%	30%	25%
Days 2-4	30%	27%	25%	20%
Days 5-6	25%	22%	20%	15%
Day 7	20%	17%	15%	10%

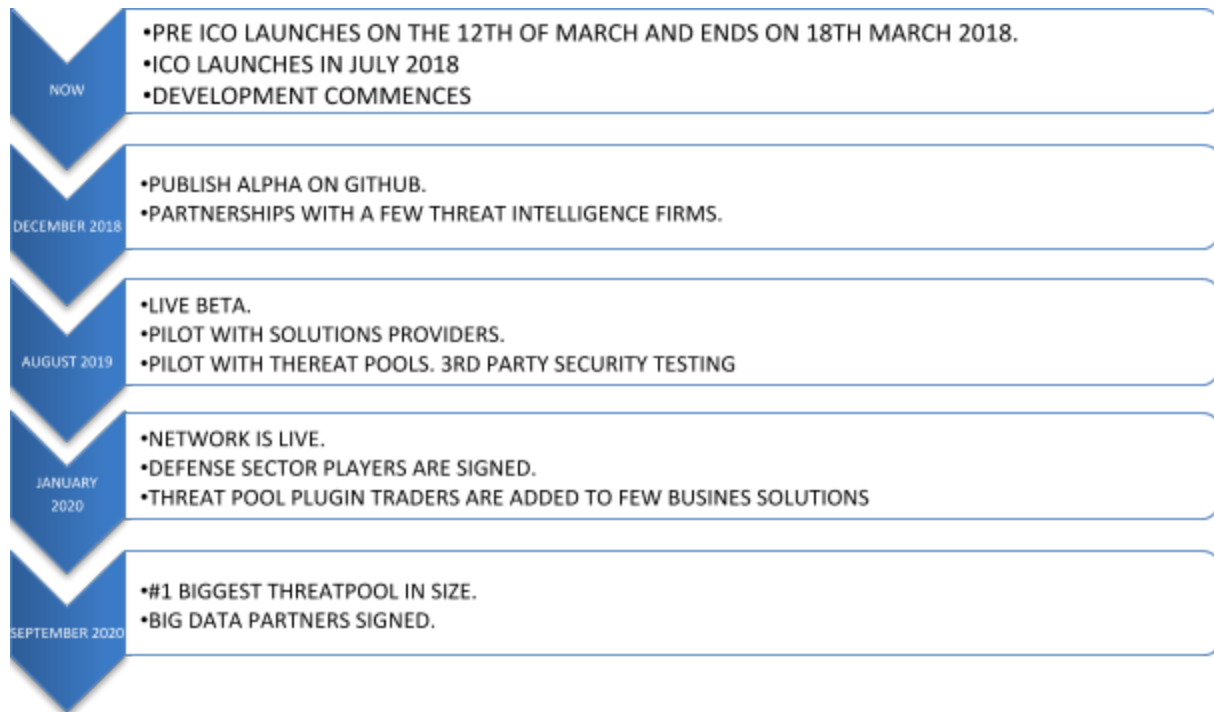
Semanal de aire baja a

los miembros de nuestro equipo lanzamientos desde el aire diversas cantidades de fichas a la SEC carteras al azar, en forma semanal, hasta el final de nuestra completa ICO (julio de 2018). Lanzamientos serán distribuidos en base a la SEC cantidades proporcionales a su saldo.

HOJA DE RUTA

El tamaño del mercado inteligencia de amenazas se estima que crecerá a partir de USD 3,83 mil millones en 2017 a USD 8,94 mil millones en 2022, a una tasa compuesta de crecimiento anual (CAGR) del 18,4%. El año de referencia considerado para el estudio es de 2016, y el tamaño del mercado se calcula a partir de 2017 a 2022. Con el lanzamiento de la señal en las 12^{de} Marzo 2018 a partir únicamente con las ventas pre ICO, se proyecta MERCADO THRINTEL para grabar rápido crecimiento exponencial por el comienzo de 2020.

Aquí está el mapa de la ilustración:



Equipo y COMUNIDAD

THRINTELMercado está formado por una comunidad de expertos con experiencia suficiente en sus diferentes campos de especialización. Cada miembro del equipo es muy valiosa y disciplinado de miembros del núcleo a Tech Asesores comerciales asesores y no dejando fuera asesores jurídicos y una multitud de otros. El objetivo común de un espacio digital más segura es la principal fuerza impulsora y el objetivo principal de todos en este equipo. Echa un vistazo a la lista:

Core Miembros:

Ezzeldin Tahoun -Visión ∞ InvestigadorCyber Security & Royal Canadian oficial de inteligencia de la marina de guerra

Enamul Haquee - Finanzas, Análisis de Seguridad ∞ de Expertos sobre el Aprendizaje y la profunda seguridad de la computadora | MBA, MSc (Comp Sci)

Marcus Alayche - Liderazgo ∞ vicepresidente de Banca de Inversión de Capital Partners Distintos | Ex operador asociado en el Bank of America

Tamir AlBalkhi - Negocios, Estrategia ∞ Analista de Negocios en Canadian Tire Servicios Financieros

Abhinab Chakraborty - Sistema Dev, Inteligencia de amenaza ∞ Amenaza Consultor de Inteligencia en Deloitte

Eric Madan - Sistema Dev, de privacidad y de Inteligencia de amenaza ∞ Inteligencia de amenaza y Consultor en Accenture privacidad

Nour Hossain - Sistema de Proyectos, Proyecto Mgmt ∞ Ingeniería de Sistemas y Proyectos de expertos y Facultad | PhD (Sfwr Eng)

John Peng - Sistema Dev, Core y la interfaz de usuario ∞ Blockchain y Sistemas Ingeniero y ex ingeniero de software TD Banco Raamtin Bayat - Sistema Dev, Infraestructura ∞

Senior Software Engineer | MSc (Eng Sfwr)

Johnny Dimatteo - Sistema Dev, Análisis y Seguridad ∞ Machine Learning Ingeniero

Juan Navarro - Sistema Dev, Ingeniero de Seguridad de Red de Seguridad

Mohammed Hammoudah - Sistema Dev, Investigación ∞ Investigador Sistemas | MSc (Eng Elec) y MSc (Comm)

Komi Chaudhry - Seguridad ∞ de seguridad informática Ninja | BSc (Comp Sec)

Asesores de Negocios:

James Politeski - Visión, Negocio ∞ El ex presidente de Samsung Electronics Canadá

Viktors Engelbrehts - Visión, diseño de sistemas ∞ Inteligencia de amenaza director del Cyber en eSentire

Pete Lewis - Ventas y Proceso ∞ Ex Director de Ventas

de Fujitsu Jonathan Boulanger - Estrategia ∞ Director de Desarrollo de Negocios, PhD

Micheal Paz - Estrategia ∞ anterior Communitel

negocioMentor Tecnología Asesores:

Douglas Stebilla ∞ Criptografía profesor, PhD Universidad de Waterloo

Sherif El-Kassas ∞ Profesor CTO SecureMisr y de InfoSec, PhD Eindhoven University of Tech

Adam Pariente Presidente Accelyst Distinguido Blockchain y Aceleradores Eng, PhD

Sherif Saad ∞ Aplicada aprendizaje automático en ciberseguridad e IOT profesor, PhD

Rong Zheng ∞ profesor Networks, PhD Universidad de Illinois

Ridha Khedri ∞ Seguridad Cibernética e información profesor confidencialidad, PhD Laval Univ.

Asesores legales:

Louis Béliveau ∞ Abogado Corporativo| BCL / LL.B McGill University Monika Yazdanian ∞

De América del Norte La ley Asesor Legal,de

Colaboradores doctorado:

Zhi Qu con experiencia en el sistema de comunicaciones y la interfaz de usuario | MSc(Ing Sfwr)

Ingeniero Weilin Hu Software | Crypto del drogadicto- 2xBEng Mike Lucas Computer Eng y
Crypto Analista

iluminación Hassan Aleian ordenador

Vijay Maulkhan informático

Dazana Samreen Ingeniero de automatización de procesos

Manar Dakho experimentados, Ingeniero

Ingeniero Ali Shahid software y de aplicaciones Dev

yThiva Athesivan Software

Ahmed Fagem Informática y Eléctrica Ing Estudiante

Negocios Ishmam Ahsany Finanzas Estudiante Nashua Luk Seguridad Ingeniero

el plan a largo plazo es crear una comunidad grande e inmensamente eficaz de partícipes de datos que son creíbles y dignas de confianza que reciben recompensas por el intercambio de inteligencia con el fin de abordar y evitar la inteligencia de amenazas de manera adecuada. Esta comunidad de comerciantes estará respaldada por nuestros esfuerzos y comunidad de desarrollo para actualizar y poner a prueba la base de código (blockchain Thrintelmarket, y la moneda segura) y emitir las nuevas versiones y actualizaciones trimestrales.

CONCLUSIÓN

- MERCADOTHRINTEL es un invento revolucionario en el mundo constantemente cambiante de la seguridad cibernética, criptomoneda y toda la comunidad tecnológica.
- Monedas seguras son similares a bitcoins pero son más seguro, eficiente y apreciarán en valor tan pronto como las ventas del encuentro. Se necesitan para que podamos controlar el sistema financiero del mercado THRINTEL, lo que nos permite de incentivar malas inyecciones de datos, volver a colocar los datos, la red de envío de correo basura, y otros ataques, que se describe en un documento técnico independiente.
- La hoja de ruta no sólo es alcanzable, pero también realistas. El equipo, los asesores, los socios, los inversores y los pocos clientes potenciales, han verificado la hoja de ruta, y su alcanzable. La visión ha sido revisado por múltiples partes que participan en el sector de inteligencia de amenazas Actualmente también.
- Post-ICO, el número limitado de se espera que la SEC monedas apreciaren valor como los blockchain volúmenes de usuario aumentan, y por lo tanto aumenta la demanda en el número limitado de la SEC monedas que hay.
- d constructivas y útiles a Presentaciones deben ser recompensados, por lo tanto, se espera que vemos un cambio de OSINTs en el mercado. Esto también se alinea con la visión de negocio discutido con los socios fuera, inversores y asesores.

Aunque existen piscinas de amenaza, y los datos son objeto de dumping de forma gratuita, los expertos entienden que los datos de estas piscinas amenaza no es tan útil, y por lo tanto obsoleta, o en necesidad de procesamiento excesiva y validación a menudo cuesta más que el valor de los datos. Sin embargo, algunas piscinas son para ser invitado a los intercambios de datos. Se basa en la relación de la piscina amenaza. Ellos dan el 10% de la piscina amenaza de nuevos datos frescos y reciben el 15% del volumen de la piscina amenaza de nuevos datos a ellos también. Estos intercambios son enormes y le cuestan a la red mucho poder si vierten a la vez. Hemos desarrollado un algoritmo para descentralizar el proceso de intercambio, donde se entregarán los intercambios cuentas en el mercado y se les dará monedas por sus contribuciones que canjeen en nuevos datos de inmediato a través de un algoritmo desarrollado y está pendiente de patente. Esto generará la integración de varios grupos de inteligencia de amenazas fácilmente en el mercado THRINTEL, aunque estos datos todavía permanecerán descentralizada ya que residen en todos los dispositivos actualizados en la red.