Table des matières

RÉSUMÉ

renseignement surmenace se réfère àinformations fiables qui est souvent connu pour être très organisé, analysé et raffiné. Il est souvent des attaques probables oucours qui menacent une organisation / institution. Il est également connu commeintelligence cybernétique menace (CTI).

Renseignements surmenaces se concentre principalement à aiderorganisationsidentifier etcomprendre les risques d'intérêt commun, ainsi quemenaces extérieures graves. Ces menaces comprennent gamme de menaces zero-day,menaces persistantes avancées (APTS) etexploits. Renseignements surmenaces comprend, mais nelimite pas à,collectematériel étendu par rapport àmenaces spécifiques. Cela permettraun bouclier d'organisation ellemême contreassauts qui pourrait céder àdommages dire.

Le paysage cybernétique d'aujourd'hui est si dynamique etévolution rapide, si bien que la valeur des investissements de sécurité est constamment remise en question. D'autre part, il y a aussi une communauté en constante augmentation des attaquants cyber qui ne prennent pas de repos une seconde d'inventernouveaux mouvements intelligents et rusés dans l'exécution des activités menaçantes.experts en sécurité Tech travaillent bec et ongles pour prévenir et analyserdonnées etinformations existantes afin d'éviterfutures attaques. L'effet résultant de tous ces est la popularité croissante deintelligence demenace.

Cependant,intelligence demenace est seulement valable quand il est99% précis, efficace et a un processus de transmission qui estfois sans danger et sans conséquences désastreuses. En termesbase,intelligence de menace est le processus de comprendre pleinementmenaces existantes et potentielles qui guettent une organisation. Il comprend égalementanalyse des données par rapport àsociétés spécifiquesfonction etrésultats contextuels. Ceuxci permettront une prise de décision claire quant à la validité deactionfonction des options disponibles.

En substance, sidonnées recueillies ne peuvent pas être analysées correctement pour informeractions possibles contremenaces ni menaces, renseignements surmenaces est aussi bonne que futile.

INTRODUCTION

Échange de renseignements surmenaces est actuellement trop de rouler avecdéfauts en raison deinefficacité des processus impliqués.clients etorganisations font face aussi bien un risque élevé de mauvaise apparition publique en cas de piratage outoute autre menace pour la sécurité. Il y a aussi la question des sources non fiables. Dans le passé,organisations ont tendance à compter surfournisseurs dont ils ont pasmoindre idée de leur crédibilité ouefficacité pourprocesseurs Intel sur la meilleure façonprévenirattaques ouse débarrasser d'un. Ce système metgrandes entreprises et institutions très sensibles telles queagences militaires ou gouvernementales, banques, etc., à grand risque. Dans l'argent énorme processus est perdu, beaucoup de temps est gaspillé et la réputation de l'organisation est laissée en ruine totale. Il est de cette nécessité que MARKET THRINTEL se pose pour combler les lacunes etmodifier les écarts de change précédent du renseignement demenace.

Qu'estce MARKET THRINTEL?

Marché THRINTEL a été inventé de l'expression « marché du renseignement de menace ». Il est une menace décentralisée renseignement blockchain oùéchange de données se produit au moyen d'achat etvente. Un isolé crypto-monnaie basé surEthereum de crypto-monnaie blockchainest utilisé pour contrôleractivités qui sont menées dansorganisations telles que incentivization de contribution. Échange Intel est fait pour être aussi sûr que possible parpremière basedonnées et décentralisant la scrutant toutesdonnées reçues pour vérifier leur validité avantpouvoir être échangés. Cette décentralisation est fait pour évitergraves dégâts si une attaque imprévue se produit. Contrairementautres options de renseignement des menacesdisposent les organisations, THRINTEL estfoissécurité ciblée et relations publiques ciblées.cette façon,grandes entreprises etgouvernements ne seront pas face au risque mortel de nuireleur réputation.

CARACTÉRISTIQUES DE MARCHÉ THRINTEL

Database Décentralisée Threat Intelligence

MARKET THRINTEL est rapide, facile d'accès, et très efficace, quelsoit votre emplacement. Il est construit à Denial de service proof.

Immuable menacede base de données de renseignement

donnéestéléchargées sur notre basedonnées ne peuvent pas être modifiés. Groupes de menaces persistantes avancées sont connus pour pirater OSINTs (Threat Intelligence Open Source Servers)etsupprimerdonnéesrapporter leurs outils, tactiques ou actifs. Ils ne seront pasmesure defaire contre le marché de THRINTEL.

FAST Blockchain basé sur une idée de génie

nouveaux artefacts etévaluations surobjets soumis sont traités et misjour rapidement en temps réel. Il est également toutfait libre d'échangerdonnées sur la plateforme. Il est OPEN SOURCE, sera donc misejour / maintenu par la communauté. Étant donnétousartefacts sont chiffrés jusqu'à ce qu'un compte les achète, le compte, le commerce efficace, doit soumettre tout a sur le marché avantacheter quoice soit. Cela signifienouvelles donnéesflux continu dans le blockchain, tant qu'il y aura des opérationscoursexécution. Les données présentées non seulement sont nécessaires, mais gagneront les points de réputation de compte, etargent dans le processus.

comptes anonymes

Si votre organisation fait faceune attaque etvous souhaitez partagerdonnées sur les piratesattaquent votre plateforme pour informerautresfaire attention pour eux, vous risquezmauvais PR. Toutvous devez faire estpartagerdonnéesanonyme sur le marché THRINTEL.

Comptes vérifiés

Si vous êtes une entreprisesécurité et vos chercheurs ont trouvé jour zéro etdonnées précises sur certains pirates ciblant un pays, les publier sur le marché THRINTEL et maintenant vous classent très haut dansprincipaux fournisseurs de données spécifiques à ce pays. Si vous avezsolutions anti-virus ousécurité vous commencezvoirmeilleures ventes, puisqueclients voient maintenant vous rang très élevé dans leur pays ou secteur d'activité. Cela fait que les clients voient audelàcampagnes publicitaires commerciales desécurité et dans leurs résultats réels et comment ilscomparent les unsautres en matière de détectionnouveaux acteurs demenace.

COMMENT ÇA MARCHE (LE MARCHE ET LA COIN)

menace Intelligencemarché ou (MARKET THRINTEL) est un marché oùdonnées sont partagées et échangées pargrandes entreprises,gouvernements,chercheurs de renseignement des menaces et plus. La pièce PROTEGE ou SEC est une piècemonnaie utilisée pour effectuer des transactions sur le marché. Le marché de THRINTEL est essentiellement destiné à être un blockchain de blocs contenant deux types d'entrées. Dansentrées Bitcoin sont A envoyé X à B. considérant que sur le marché THRINTELnous avons deux types d'entrées; ce sont C, pour apport ROW et F, pour commentaires ROW.

Voici ce que la ligne de contribution ressemble:

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 s2rpjhAsWW4Tnf1; 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

souscomptevous avez une adresse, une note de RÉPUTATION, et un drapeau Vérifiée. Cela vous représente, votre réputation actuelle sur le marché, et si vous avez un compte vérifié ou non (comptes vérifiés sontà titre de marque parentreprises de sécurité). Sous ARTEFACT vous avez une adresse IP ou URL. C'est ce que vous présentezcommentaires sur. Sous POINTAGE MALVEILLANT, vous avez un nombre représentant ce que vous pensez de l'artefact, 0 pour ne pas malveillant, 100 pour ceest extrêmement malveillant. Sous MÉTADONNÉES, vous disposezun horodatage, un code pays et un code du secteur. Cela donne à votre contexte contribution.

La ligne de rétroaction se présente comme suit:

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%
1BcVWPKPLSXh4ivo5pvs2rpjhAsWW4Thf1; 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

Sous comptevous avez une adresse, une note de RÉPUTATION, et un drapeau Vérifiée. Cela vous représente, votre réputation actuelle sur le marché, et si vous avez un compte vérifié ou non (comptes vérifiés sontà titre de marque parentreprises de sécurité). Sous ARTEFACT vous avez une adresse IP ou URL. C'est ce que vous présentezcommentaires sur. Sous FEEDBACK POINTAGE, vous avez un nombre représentant ce que vous pensez de l'artefact, 0 pour ne pas malveillant, 100 pour oui cela était malveillant et il sauvé mes biens. Sous MÉTADONNÉES, vous disposezun horodatage, un code pays et un code du secteur. Cela donnecontexte de vos commentaires.

Le marché de THRINTEL doit être largement utilisé parmachines autonomes, IdO, solutions de sécurité, antivirus, parefeu, serveurs, centres de données de stockage en nuage, etc. La plateforme peut être utilisée parmenaceanalystesrenseignement au sein du gouvernement,secteurs d'activité,grandes entreprises, ou mêmechercheurs, ces personnes peuvent êtremesure de traiter les données danslogiciel de visualisation sur leur propre. Mais notre logiciel leur donne accès àlignes compilées comme suit. Nous appelons ceuxla ligne O compilé,qui n'existe pas dans le blockchain mais rienautre qu'une représentation des données danslistes ouchaînes liées à la blockchain. Machines compilent les avantprendre toute décision sur la plateforme ainsi, ce sont le seul moyen pour un commerçant de données, être humain, oumachine, aussi bien, de prendre une décision d'achat oudumpingun nouvel artefact qui apparaît sur la plateforme.

BUYERS COMPUTE AND BUY/USE THIS [OFFERED ROW] : we refer to this as O 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 : 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1, 1BcWWPkPLSXh4wo5pxs2rpjhAsWW4Tnf1	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)]

Sous DISTRIBUTION DES REVENUS vient adresses des personnes qui obtiennent une baisse des revenus une foisvous achetez des données ou techniquement acheter une clé pour déverrouiller l'artefact. Ces adressesréfèrent aux 10 meilleurs auteurs qui ont déclaré l'artefact à être malveillant, ils pourraient être de différentes parties du monde certains d'entre eux ont rencontré sur une mission de chasse demenace, ou pendantrecherche, ou peut avoir été frappé avec et souffert pertes. Non seulement y atil aborde làmais combien est chacun d'eux faisant de chaque piècemonnaievous payez SEC. Rappelezvous il y afrais zéro pour toutmonde sur la plateforme. Ces valeurs sont calculées en fonction du nombre de journalistes,présentations estampilles, scores malveillants, la réputation des journalistes. Sous ARTEFACT vous avez l'adresse IP ou URLvous achetez mais bien sûril est crypté jusqu'à ce que vous achetez la clé qui déverrouille seulement pour vous (la clé ne fonctionneavec votre compte). Sous SCORE TRUSTvous trouverez un score de TRUST calculé par crissement bas nombre de journalistes,score malveillant, la réputation des journalistes,commentaires pour vous donner une

idée defaçon dont vous devriez mettreconfiance dans le système. Sous prix est un prix dans la seule devise sur la plateforme (SEC Coin) ou SECURISE Coin. Le prix Secure Coin est calculéfonction du score de confiance,valeurs de métadonnées. Sous MÉTADONNÉES, il y a un horodatage, un code pays et un code du secteur. Ceuxci aident à contextualiser l'artefact.

COIN DÉTAILS

Ticker: SEC

Plateforme: Ethereum

Typejeton: ERC20

disponibles àvente pré-ICO: 90000000 SEC

Début devente jeton 12 Mars

soft cap: 300

ETH cap dur: 3 000

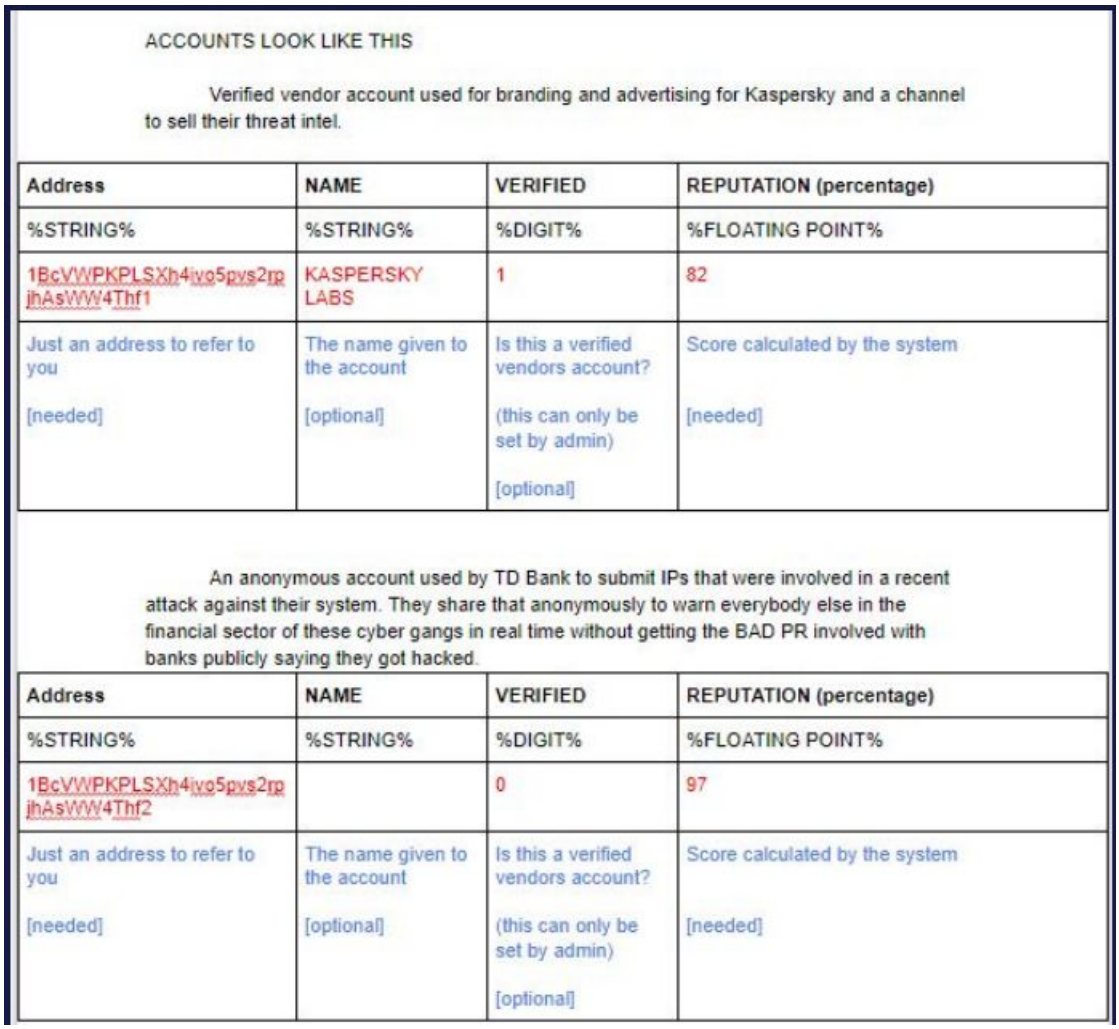
ETH SEC Totaljetons émis: 2 000 000 000SEC

Prix: 1 = 30 000 ETH SEC

mode de paiement: ETH contribution minimum: 0,1 ETH

Toutmonde doit avoir un compte sur la plateforme.comptes sont anonymes par défaut jusqu'à ce qu'une entrepriseécurité veut un compte vérifié pourimagemarque, car il pourrait être utilisé dansrapports trimestriels disant quesociété X est le principal fournisseur de renseignements surmenaces pour le secteur BFSI nordaméricain en 2019 Q3 qui peut conduire à l'adoption accrue de solutions Company X dans le laps de temps.comptes anonymes sont un atout pourbanques se piraté etveulent signaler un artefactpremier plan sur le groupe APT les attaquer pour avertirautres. Mais cela conduit àmauvaise PR pour la banque déclarante par exemple. Ainsi, les canaux actuels sont seulement entrebanques ou partenaires, laissant le processeur Intel sur les nouvelles ousensibilisationpublic. Avec blockchain il est possible de signaler complètement anonymeévitant le mauvais PR.

Cidessous la figure montrant les deux types de comptes:



ACCOUNTS LOOK LIKE THIS

Verified vendor account used for branding and advertising for Kaspersky and a channel to sell their threat intel.

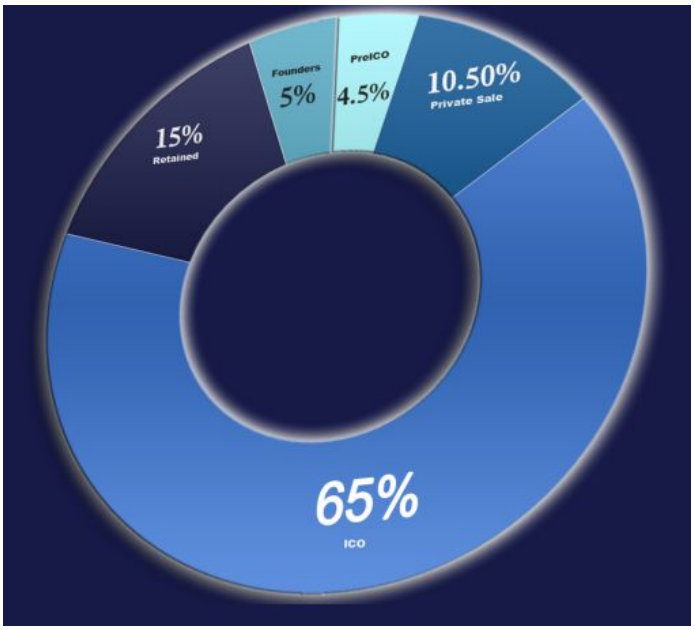
Address	NAME	VERIFIED	REPUTATION (percentage)
%STRING%	%STRING%	%DIGIT%	%FLOATING POINT%
1BcVWPKPLSXh4ivo5pvs2rpjhAsWW4Thf1	KASPERSKY LABS	1	82
Just an address to refer to you [needed]	The name given to the account [optional]	Is this a verified vendors account? (this can only be set by admin) [optional]	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%
1BcVWPKPLSXh4ivo5pvs2rpjhAsWW4Thf2		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]

COIN DISTRIBUTION

4,50% de la médaille MARKET THRINTEL sera publié au coursla périodepré-ICO tandis que 65% sont alloués aux tours ICO de vente jeton. 10,5% seront vendusprivé àinvestisseurs sélectionnés dans le cercle MARKET THRINTEL. 15% des pièces seront conservés àfinssensibilisation etpromotion. Les fondateurs seront laissés avec 5% des pièces.

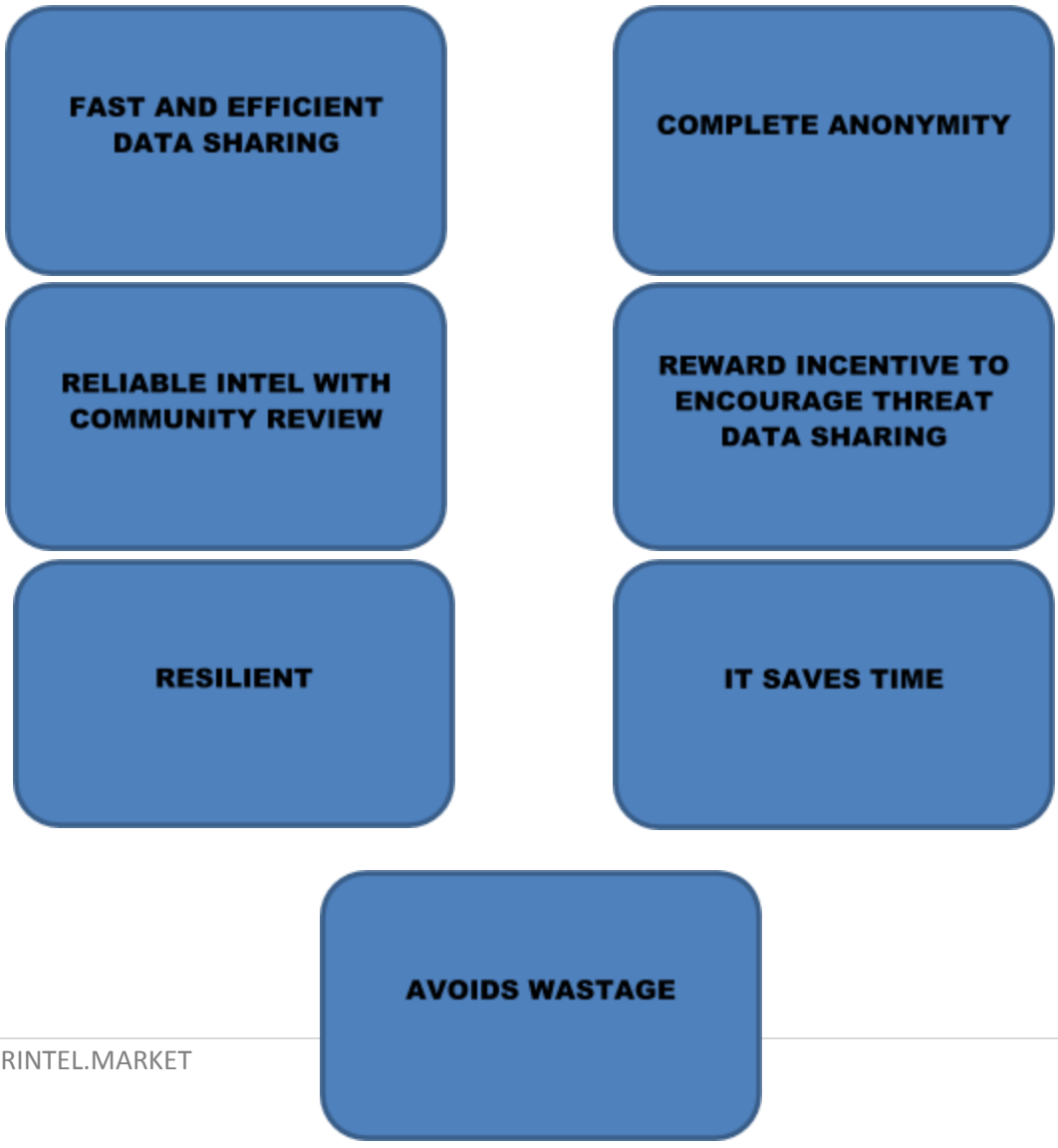


THRINTEL marché propose de partagerdonnées en temps quasi réel avecanonymat complet et évaluations communautaires et validations. Et une incitation à partager vos données de menace (vous devez télécharger ce que vous avez afin que vous neachetez pas encore, et vous faireargent etréputation de tout cevous soumettez), nous savons quegens vont jamais cesserrechercher de nouvelles menaces et partagerontfait avecautres.vendeurs peuvent utiliser pour obtenirmeilleure réputation de leur marquetant que leader dans intel des menaces dans un secteur deindustrie ouun pays par exemple tandis quebanques ougouvernements peuvent partagerchoses avecautresanonyme sans risquermauvais titres de relations publiques ounouvelles. La chaîne de blocs est élastique, presque impossible d'abattre oumanipuler, immuable, distribuée, et n'a pasmodérateurs ouautorité centraleutiliser. Nous économisons acheteursargent (ils achètentchoses une fois sans marges injustes, décalagele temps,processus fastidieux, ou différents formats) et fairefournisseursargent juste etimagemarque pour leurs efforts (en répartissant les points de revenus etréputation de chaque artefact sur quisignalé comme bientôt et précis que possible). THRINTEL marché offrent égalementacheteursune manière plus souple, sûr qu'ils peuvent réellement compter sur leur intel menace.

Pourquoi MARKET THRINTEL?

Maintenant, beaucoup de questions sont étaiement dans votre esprit. Pourquoimarché THRINTEL? Qu'est-ce qui est différent? Il y a beaucoup de raisonslesquelles thrintel marchéemportetoutesautres options dans le domaine aujourd'hui.actuelle Threat Intelligencen'encourage personne à travaillerdehorsla zone de confort. Si vous êtes un fournisseur etvous travaillez sur autre chose que ce qui est fait facela plupart de vos clients, vous souffrez. Et le marché est dominé pargrands noms qui ont réduitbudgets de recherche et ont augmentébudgets de marketingplace. Affichageun monopole sur le marché et tuer tousnouveaux efforts de recherche dans un effort pour maintenir un marché saturé et monopolisé, qu'ils peuvent bénéficier de. Cela conduit fondamentalement à une industrie desécurité vraiment faible et conduit donc à tous les échecs ou « hacks » / » brèches » / » scandales » qui affectent la plateforme devictime et par extension l'économie négative.

Nous avons compilé raisons cidessous:



Notre objectif repose surgrandes organisations etcommunauté tels que ceux dedéfense etcabinetsconseils, Organismes gouvernementaux,télécommunications, la cybersécuritéchercheurs,analystes du renseignement des menaces, Architectessécurité, opérations de chasse des menaces,agentsrenseignement,ingénieurs Big Data, apprentissage chercheurs,opérationssécurité , pénétration testeurs, menacefournisseurs Intel,entreprisessécurité, réseau Appareils fournisseurs,entreprises avecénormes réseaux, sociétés de grande envergure,pirates informatiques White Hat, etc. et de ces collaborations une communauté vaste et puissant est lié à émerger.

STOCKAGE

Le problème de stockage est prévu, nous avons développé un algorithme pour permettrevos petits appareils incapables seulement téléchargerparties pertinentes du blockchain (fonction des métadonnées « calendrier, pays,secteur deindustrie »)cela permetappareils comme votre téléphone encore bénéficier de la réseaumais uniquement suralimentation alimentemenace pertinente. Cet algorithme introduira un peu d'une dépendance àégardun groupe de noeuds voisins qui doit être complètement misjour une copie complète du blockchain. L'application de téléphone vous demandera alorsun des nœuds pour exécuter les opérations en son nom. A ce stadele reste des nœuds valider l'authenticité des transactions exécutées par le noeud sélectionné et mettrejour la réputation etrécompense du nœud sélectionné. Une transaction comme celle discuté ici coûtera compte au téléphone un peu plus car il est un modèle de commission à imposer. Récompensant donc le nœud quigardé une copie complète du blockchain etopérations exécutées au nom du compte du téléphone.

TOKENLANCER

PRE ICO(initial Coin placement) est prévue pourlancement le 12 mars à 18 mars 2018,durée de seulement 7 jours tandis que le lancement de ICO (initial Coin placement) est prévu pour avoir lieu en juillet 2018.coursces ventes, lademande deSEC devrait être une grande augmentation. Cependant, il y apièces limitées disponibles àvente. Taux de bonus jusqu'à 37,5%. Récompenses (BOUNTY) programmevaleur de 10.000.000 pièces 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%

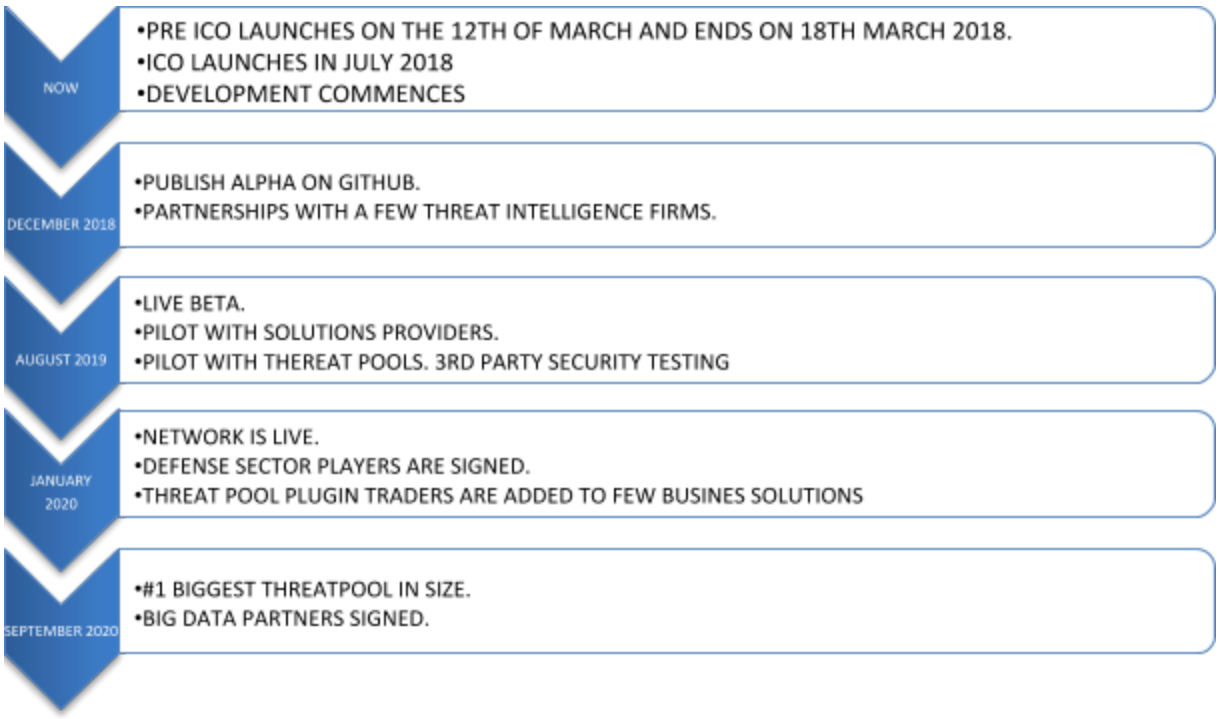
Parachutages hebdomadaire

membres de notre équipe parachuter diverses quantités de jetons SEC àportefeuilleshasard, surbase hebdomadaire, jusqu'à la fin de notre pleine ICO (Juillet 2018). largages seront distribuésfonction deSECmontants proportionnels à votre solde.

FEUILLEROUTE

La taille du marché du renseignement de menace devrait croître de 3,83 milliardsdollars en 2017 à 8,94 milliardsdollars US en 2022, à un taux de croissance annuel composé (TCAC) de 18,4%. L'année de base considérée pour l'étude est 2016, et la taille du marché est calculépartir2017 à 2022. Avec le lancement de jeton sur le 12^{e} de Mars 2018 commençant seulement avecventes pré ICO, MARKET THRINTEL devrait enregistrercroissance exponentielle rapide par le début de 2020.

Voici la carte cidessous pour illustration:



ÉQUIPE eT cOMMUNAUTAIRES

MARCHÉ THRINTEL se compose d'une communauté d'experts suffisamment expérimentés dans leurs différents domaines de spécialisation. Chaque membre de l'équipe est très précieuse et disciplinée des membresbase à Tech conseillers aux entreprises et CONSEILLERS ne laissant des conseillers juridiques et une foule d'autres. L'objectif commun d'un espace numérique plus sûr est la principale force motrice et objectif principal de toutmonde dans cette équipe. Consultez la liste:

Membresbase:

Ezzeldin Tahoun - Vision ⋈ sécurité Cyber chercheur et officierRoyal Navy Intelligence canadienne

Enamul Haquee - Finances, analysesécurité ⋈ Expert Deep apprentissage etsécurité informatique | MBAMS & MSc (Comp Sci)

Marcus Alayche - Leadership ⋈ viceprésident des services bancairesinvestissement à Distinct Capital Partners | Trader Ancien associé à Bank of America

Tamir AlBalkhi - Business, Stratégie ⋈ Senior Business Analyst chez Canadian Tire Financial Services

Abhinab Chakraborty - Système Dev, renseignementmenace ⋈ Threat Consultant Intelligence chez Deloitte

Eric Madan - Système Dev, Intelligence Confidentialité et menace ⋈ Threat Intelligence et Consultant chez Accentureconfidentialité

NourHossain - système Design, projet Mgmt ⋈ Systems Engineering & Design Expert & Faculté | PhD (Sfwr Eng)

John Peng - Système Dev, Core & UI ⋈ Blockchain & Ingénieur Systèmes & Banque TD Ancien Ingénieur Sepehr Bayat - Système Dev, Infrastructure ⋈

Senior Software Engineer | MSc (Sfwr Eng)

Johnny Dimatteo - Système Dev, analyse et sécurité ⋈machineapprentissage ingénieur

John Navarro - Système Dev, Ingénieur sécurité réseausécurité

Mohammed Hammoudah - Système Dev,recherche ⋈ chercheurSystems | MSc (Elec Eng) & MSc (Comm)

Komi Chaudhry - Sécurité ⋈ informatiqueNinja Sécurité | BSc (Comp Sec)

Conseillers commerciaux:

James Politeski - Vision, Affaires ⋈ ancien présidentSamsung Electronics Canada

Viktors Engelbrehts - Vision,conceptionsystème de directeur de Cyber Intelligence demenaceà eSentire

Pete Lewis - Sales & Process ⋈ Ancien Directeur des ventes

Fujitsu Jonathan Boulanger - Stratégie ⋈ Manager Business Developer, PhD

Micheal paix - Stratégie de ancien Communitech

Mentoraffaires conseillerstechnologie:

Douglas Stebilla ⋈ Cryptographie Professeur, Ph.D. Université de Waterloo

Sherif El-Kassas CTO SecureMisr & InfoSec Professeur, PhD Eindhoven University of Tech

Adam Kinsman Président Accelyst distingué Blockchain & Accélérateurs Eng, PhD

Sherif Saad ⋈ Learning Applied Machine Professeur Cybersécurité et IOT, PhD

Zheng Rong professeur Réseaux, Ph.D. Université deIllinois

Ridha Khedri ⋈ Cyber sécurité et confidentialité Infos professeur, PhD Laval Univ.

Conseillers juridiques:

Louis Béliveau Avocat Corporate | BCL / LL.B McGill Univ Monika Yazdanian ⋈

Nord lois américaines Conseiller juridique, Ph.D.

Collaborateurs:

Zhi Qu Expérimenté danssystèmecommunication et interface utilisateur | MSc (Sfwr Eng)

Weilin Hu Ingénieur Logiciel | 2xBEng Mike Lucas Computer Eng & Crypto Analyste - Crypto Junkie

Hassan Aleian Ingénieur informatique

Vijay Maulkhan Informaticien

Dazana Samreen Process Automation Ingénieur

Manar Dakho Ingénieur expérimenté informatique

Ali Shahid Software Ingénieur & App Dev

Thiva Athesivan Ingénieur logiciel

Ahmed Fagem informatique et génie électrique étudiant

Ishmam Ahsan affaires & Finance Ingénieur étudiant Nashua Luk sécurité

le plan à long termeest de créer une communauté importante et extrêmement efficace des partageurs de données qui sont crédibles et dignes de confiance qui obtiennentrécompenseedpour échangerrenseignements afin d'aborder etévitermanière adéquateintelligence des menaces. Cette communauté des commerçants sera soutenu par nos efforts etcommunauté de développement pour mettre à jour et tester la base de code (thrintelmarket blockchain et pièce sécurisée) etémettrenouvelles versions etmisesniveautrois mois.

CONCLUSION

- MARKET THRINTEL est une invention révolutionnaire dans le mondeconstante évolution decybersécurité, et l'ensemblecrypto-monnaie communauté technologique.
- Pièces SECURE sont similaires à Bitcoins mais ils sont plus sûrs, efficaces et apprécieront la valeur dès queventes coupenvoi. Ils sont besoined afin que nous contrôlons le système financier du marché THRINTEL,qui nous permet à de mauvaises injections de motiverdonnées,données reposter, spammer le réseau, etautres attaques, être décrites dans un document technique.
- La feuilleroute est non seulement réalisable mais aussi réaliste. L'équipe, les conseillers, les partenaires, les investisseurs, et quelques clients potentiels, ont vérifié la feuilleroute et sa réalisabilité. La vision a été examinée par plusieurs parties prenantes dans le secteur du renseignement de menace actuellement aussi bien.
- Post-ICO, le nombre limité de pièces SEC devrait apprécier en valeur les blockchain volumes utilisateuraugmentent, etconséquent la demande augmente sur le nombre limité de pièces SEC làbas.
- Dconstructives et utilesata soumissions doivent êtrerécompensés,où il est prévu queon voit un changement de OSINTs sur le marché. Ceci aligne également avec la vision d'affaires discuté avecpartenaires sur,investisseurs etconseillers.

Bien quegroupes de menaces existent, etdonnées sont sous évaluées gratuitement, experts comprennent que les données sur ces pools de menace n'est pas si utile, et donc pasjour, ou dansbesoin de traitement etvalidation excessivecoûts souvent plus que la valeur desdonnées.Cependant, certaines piscines doivent être invités àéchanges dedonnées.Il est basé surratio depiscine de menace. Ils donnent 10% de la piscine de menace dansdonnées nouvelles fraîches etrecevoir15% volume depiscinede menace de nouvelles données pour eux.Ces échanges sont énormes et coûtent le réseaupouvoir se sousévaluées àfois. Nous avons mispoint un algorithme de décentraliser le processus d'échange où les échanges seront donnéscomptes sur le marché et ils serontpiècesmonnaie donnée pour leur contribution qu'ils rachètent ànouvelles données toutsuite par un algorithme développé et estattentebrevet. Cela engendreraintégration de plusieurs piscines de renseignement de menace facilement sur le marché du THRINTEL, bien que ces données restent encore décentralisée car ils résident dans tousappareils misjour sur leréseau.