Table of Contents

ABSTRACT

Threat intelligence refers to trusted information that is often known to be highly organized, analyzed and refined. It is often about likely or ongoing attacks that threaten an organization/institution. It is also known as cyber threat intelligence (CTI).

Threat intelligence is primarily focused on helping organizations identify and understand the risks of common as well as serious external threats. These threats include range from zero-day threats, advanced persistent threats (APTs) and exploits. Threat intelligence includes, but is not restricted to, gathering extensive material in relation to specific threats. This will enable an organization shield itself against assaults that could give way to dire damage.

Today's cyber landscape is so dynamic and rapidly-changing, so much so that the value of security investments is constantly called into question. On the other hand, there is also a constantly growing community of cyber attackers who are not taking a second's rest from inventing new smart and sly moves in the execution of threatening activities. Tech security experts work tooth and nail to prevent and analyze existing data and information in order to avoid future attacks. The resultant effect of all these is the growing popularity of threat intelligence.

However, threat intelligence is only valuable when it is 99% accurate, efficient and has a transmission process that is both safe and free of dire consequences. In basic terms, threat intelligence is the process of fully comprehending existing and potential threats that may befall an organization. It also includes data analysis in relation to specific companies based and contextual findings. These will enable a clear decision making as to the validity of action based on the options available.

In essence, if collected data can't be properly analyzed to inform possible actions against threats or impending threats, threat intelligence is as good as futile.

INTRODUCTION

Exchange of threat intelligence is currently ridden with too many flaws as a result of inefficiency of the processes involved. Customers and organizations alike face a high risk of bad public appearance in the event of a hack or any other security threat. There is also the issue of untrusted sources. In the past, organizations tend to rely on vendors whom they have no inkling about their credibility or efficiency for intel on how best to prevent attacks or rid themselves of one. This system places big companies and highly sensitive institutions such as military or government agencies, banks, etc., at great risk. In the process huge money is lost, lots of time is wasted and the organization's reputation is left in utter ruins. It is from this necessity that THRINTEL MARKET arises to bridge the gaps and amend the lapses of previous threat intelligence exchange.

What is THRINTEL MARKET?

THRINTEL market was coined from the phrase 'threat intelligence market'. It is a decentralized threat intelligence blockchain where data exchange occurs by means of buying and selling. An isolated cryptocurrency based on Ethereum cryptocurrency blockchain is used to control activities that are carried out in organizations such as contribution incentivization. Intel exchange is made to be as secure as possible by first decentralizing the database and scrutinizing all received data to ascertain their validity before they can be exchanged. This decentralization is done to avoid serious damage should an unforeseen attack occurs. Unlike other threat intelligence options available to organizations, THRINTEL is both security focused and public relation focused. That way, big corporations and governments will not face the mortal risk of damaging their reputation.

FEATURES OF THRINTEL MARKET

Decentralized Threat Intelligence Database

THRINTEL MARKET is fast, easy to access, and highly effective, irrespective of your location. It is built to be denial of service proof.

Immutable Threat Intelligence Database

Data uploaded to our database cannot be altered. Advanced Persistent Threat Groups are known to hack OSINTs (Open Source Threat Intelligence Servers) and remove data reporting their tools, tactics, or assets. They won't be able to do it against the THRINTEL MARKET.

FAST Blockchain based on a Genius Idea

New artifacts, and feedbacks on submitted artifacts are processed and updated speedily in real time. It is also absolutely free to trade data on the platform. It is OPEN SOURCE, hence will be updated/maintained by the community. Since all artifacts are encrypted until an account buys them, the account, to trade efficiently, needs to submit everything it has to the market before buying anything. This means new data will flow continuously into the blockchain, as long as there are trades being executed. The data submitted not only is needed, but will earn the account reputation points, and money in the process.

Anonymous Accounts

If your organization is facing an attack and you wish to share data about the hackers attacking your platform to inform others to watch out for them, you risk bad PR. All you need to do is share data anonymously on the THRINTEL MARKET.

Verified Accounts

If you are a Security Business and your researchers found zero day and accurate data on some hackers targeting a certain country, you publish them on the THRINTEL MARKET and now you rank really high in top providers of data specific to this country. If you have anti-virus or security solutions you start seeing better sales, since customers now see you ranking really high in their country or business sector. This makes sure the customers see beyond security business ad campaigns and into their actual results and how they compare to each other when it comes to detecting new threat actors.

HOW IT WORKS (THE MARKET AND THE COIN)

Threat Intelligence Market or (THRINTEL MARKET) is a market where data is shared and exchanged by large corporations, governments, threat intelligence researchers and more. The SECURE coin or SEC is a coin used to carry out transactions in the market. The THRINTEL MARKET is essentially intended to be a blockchain of blocks containing two types of entries. In

bitcoin entries are A sent X to B. Whereas on the THRINTEL MARKET we have two types of entries; those are C, for Contributed ROW, and F, for Feedback ROW.

Here's what the contribution row looks like:

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

Under ACCOUNT you have an ADDRESS, A REPUTATION SCORE, and a VERIFIED FLAG. This represents you, your current reputation on the market, and whether you have a verified account or not (verified accounts are for branding purposes by security firms). Under ARTIFACT you have an IP or URL. This is what you are submitting feedback about. Under MALICIOUS SCORE, you have a number representing what you think of the artifact, 0 for not malicious, 100 for this is extremely malicious. Under METADATA, you have a timestamp, a country code, and a sector code. This gives context to your contribution.

The feedback row looks like this:

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

Under ACCOUNT you have an ADDRESS, A REPUTATION SCORE, and a VERIFIED FLAG. This represents you, your current reputation on the market, and whether you have a verified account or not (verified accounts are for branding purposes by security firms). Under ARTIFACT you have an IP or URL. This is what you are submitting feedback about. Under FEEDBACK SCORE, you have a number representing what you think of the artifact, 0 for not malicious, 100 for yes this was malicious and it saved my assets. Under METADATA, you have a timestamp, a country code, and a sector code. This gives context to your feedback.

The THRINTEL MARKET is to be used largely by autonomous machines, IoT, security solutions, antiviruses, firewalls, servers, cloud storage data centers, etc. The platform may be used by Threat Intelligence analysts in the government, business sectors, large corporations, or even researchers, these individuals may be able to process the data into visualization software on their own. But our software gives them access to compiled rows like the following. We call those the compiled O row, which does not exist in the blockchain but is nothing but a representation of the data in linked lists or chains in the blockchain. Machines compile those before making any decisions on the platform as well, these are the only way for a data trader, being human, or machine, alike, to make a decision of buying or dumping a new artifact that appears on the platform.

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 : 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1, 1BcMPkPLSXh4xp5pxs2pjhAsWW4Tnf1	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)]

Under REVENUE DISTRIBUTION comes addresses of people who get a cut of the revenue once you buy the data or technically buy a key to unlock the artifact. These addresses refer to the best 10 submitters who reported the artifact to be malicious, they could be from different parts of the world some of them have encountered it on a threat hunting mission, or during research, or may have been hit with it and suffered losses. Not only are there addresses there but how much is each of them making of every SEC coin you pay. Mind you there are zero fees for everybody on the platform. These values are calculated as a function of the # of reporters, submissions timestamps, malicious scores, reporters' reputations. Under ARTIFACT you have the IP or URL you are buying but of course it is encrypted until you buy the key that unlocks it only for you (the key would only work with your account). Under TRUST SCORE you will find a TRUST score calculated by crunching down # of reporters, malicious score, reporters' reputations, feedback to give you an idea of how trust you should put in the system. Under PRICE is a price in the only currency on the platform (SEC Coin) or SECURE Coin. The Secure Coin price is

calculated based on the trust score, metadata values. Under METADATA, there is a timestamp, a country code, and a sector code. These help to contextualize the artifact.

COIN DETAILS

Ticker: SEC

Platform: Ethereum

Token Type: ERC20

Available for Pre-ICO sale: 90,000,000 SEC

Start of token sale: 12 March

Soft cap: 300

ETH Hard cap: 3 000

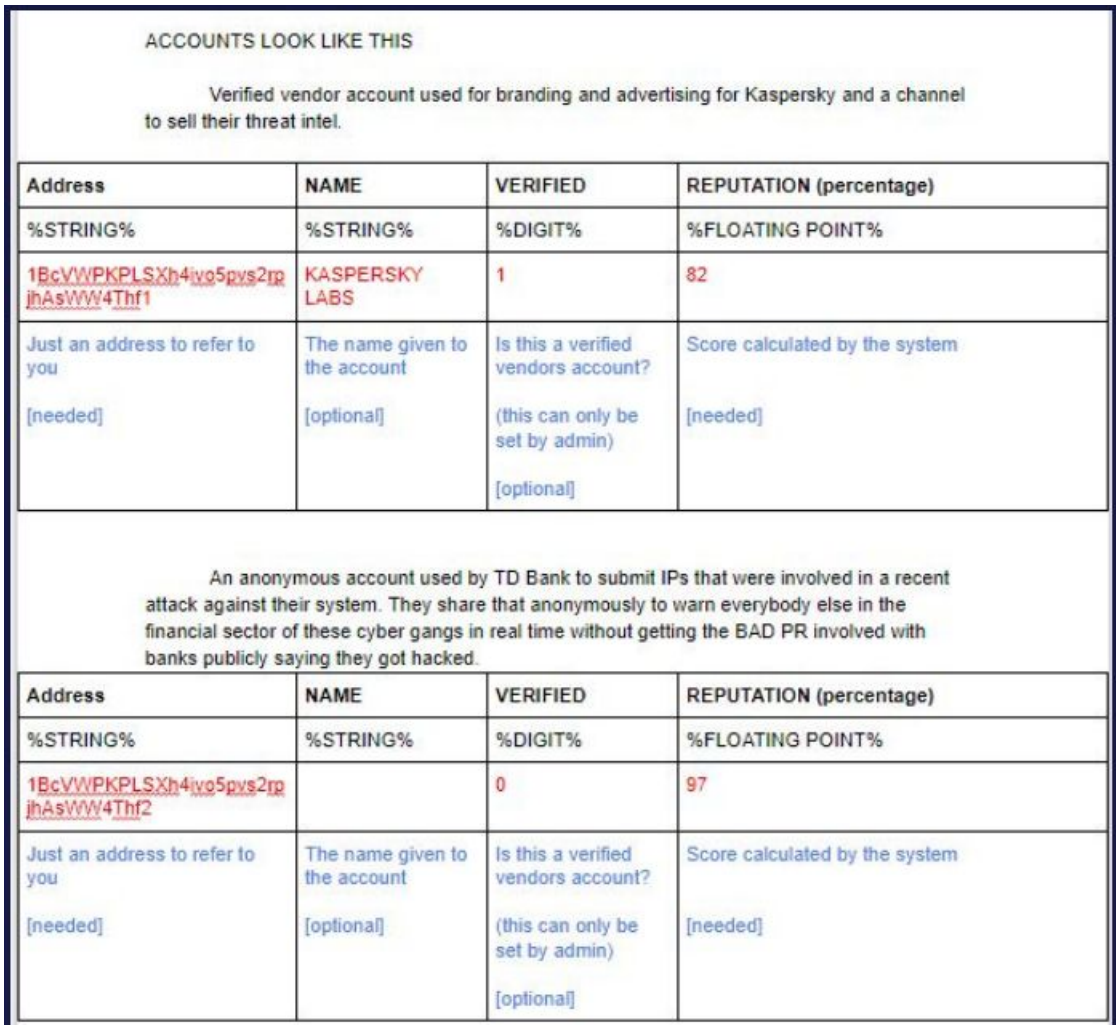
ETH SEC Total Tokens issued: 2 000 000 000 SEC

Price: 1 ETH = 30,000 SEC

Payment method: ETH Minimum contribution: 0.1 ETH

Everybody is required to have an account on the platform. Accounts are anonymous by default until a Security Firm wants a verified account for branding, as it could be used in quarterly reports saying that Company X is the leading threat intelligence provider for the North American BFSI Sector in 2019 Q3 which may lead to increased adoption of Company X solutions in the time frame. Anonymous accounts are an asset for banks getting hacked and wanting to report an artifact leading on the APT group attacking them to warn others. But this leads to bad PR for the reporting bank for instance. So, the current channels are only between selected banks or partners, leaving the intel out of the news or public awareness. With blockchain it is possible to report completely anonymously avoiding the bad PR.

Below is the figure showing the two types of accounts:



ACCOUNTS LOOK LIKE THIS

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

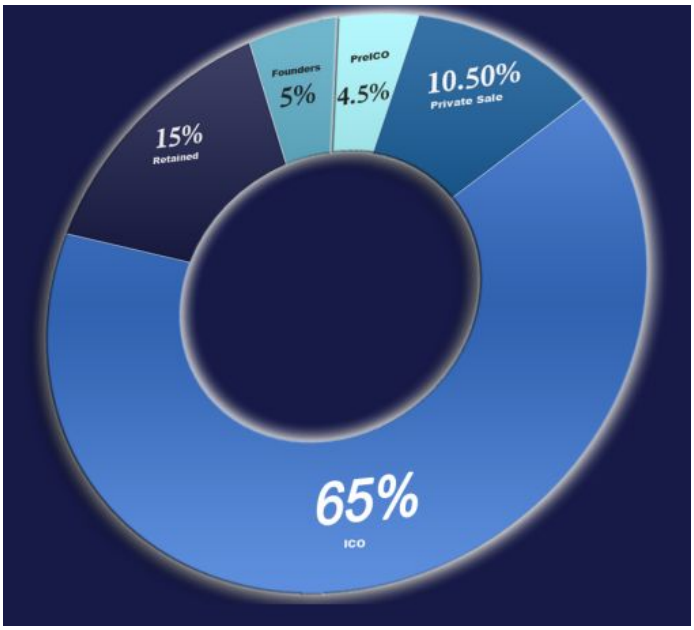
Address	NAME	VERIFIED	REPUTATION (percentage)
%STRING%	%STRING%	%DIGIT%	%FLOATING POINT%
1BcVWPKPLSXh4ivo5pvs2rpjhAsWW4Thf1	KASPERSKY LABS	1	82
Just an address to refer to you [needed]	The name given to the account [optional]	Is this a verified vendors account? (this can only be set by admin) [optional]	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% of the THRINTEL MARKET coin will be released to during the PRE-ICO period while 65% is allocated to the ICO rounds of token sale. 10.5% will be sold privately to selected investors in the THRINTEL MARKET circle. 15% of the coins will be retained for outreach and promotional purposes. The founders will be left with 5% of the coins.

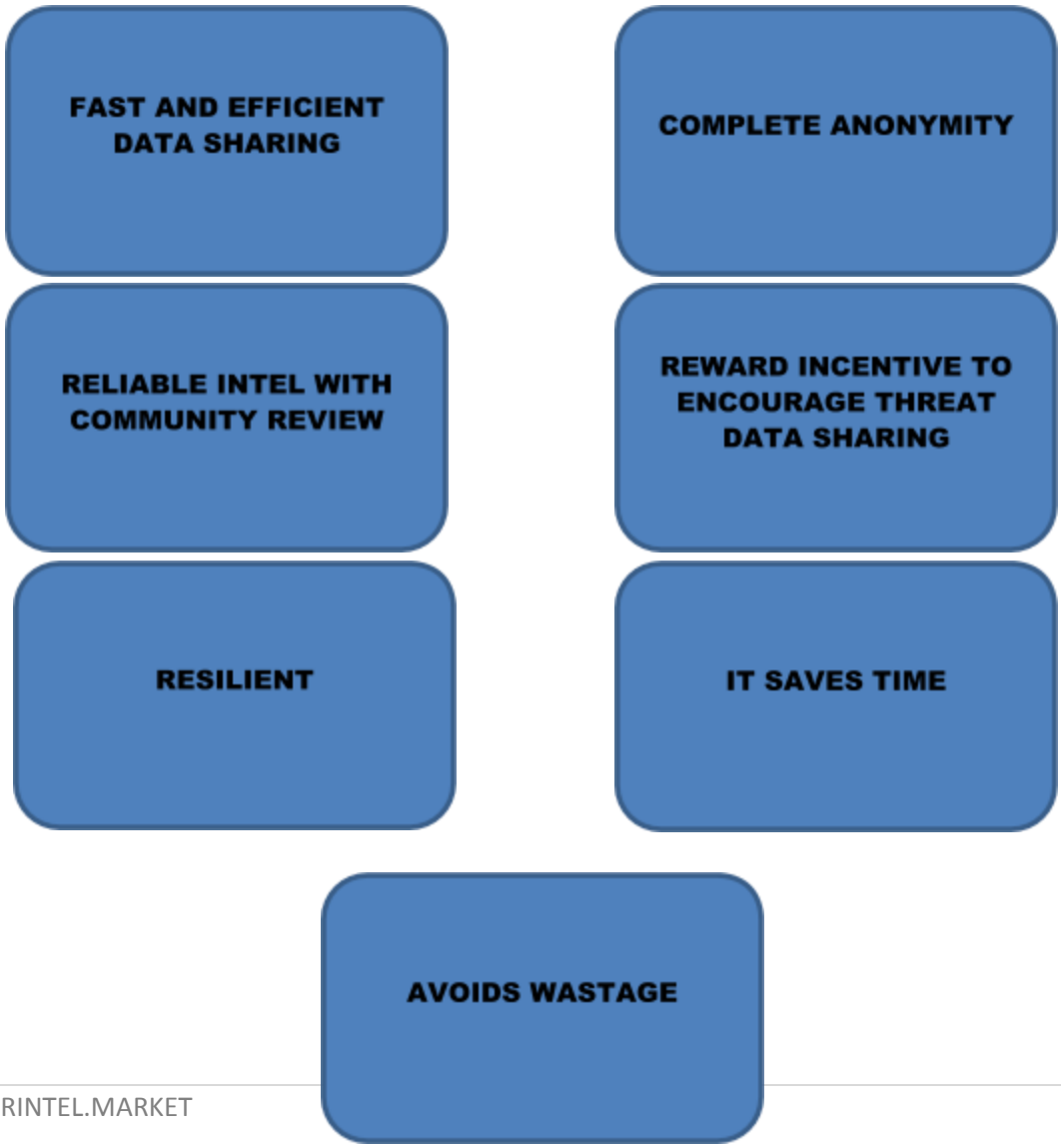


THRINTEL Market offers sharing data in almost real time with complete anonymity and community ratings and validations. And with an incentive to share your threat data (you have to upload what you have so that you don't buy it again, and you make money and reputation off everything you submit), we know that people will never stop researching for new threats and will actually share it with others. Vendors can use this to get better reputation for their brand as a leader in threat intel in a certain industry sector or a country for example while Banks or governments can share stuff anonymously with others without risking bad PR or news headlines. The block chain is resilient, almost impossible to take down or manipulate, immutable, distributed, and has no moderators or central authority operating it. We save buyers money (they buy stuff once with no unfair markups, time lag, tedious processes, or different formats) and make vendors fair money and branding for their effort (by distributing the revenue and reputation points of each artifact on who reported it as soon and accurate as possible). THRINTEL Market also offer buyers a more resilient, safe, secure way that they can actually rely on for their threat intel.

Why THRINTEL MARKET?

By now, a lot of questions are propping up in your mind. Why THRINTEL market? What is different? There are a lot of reasons why thrintel market trumps every other option in the field today. Current Threat Intelligence doesn't encourage anybody to work outside the comfort zone. If you are a vendor and you are working on anything other than what is faced by most of your clients, you will suffer. And the market is dominated by big names that have reduced research budgets and have increased marketing budgets instead. Showing a monopoly over the market and killing off any new research efforts in an effort to maintain a saturated and monopolized market, which they can benefit off. This fundamentally leads to a really weak security industry and hence leads to all the failures or “hacks”/”breaches”/”scandals” that affect the victim platform and by extension the economy negatively.

We have compiled reasons below:



Our focus rests on big organizations and community such as those in Defense and Consulting Firms, Government Agencies, Telecommunications, Cyber Security Researchers, Threat Intelligence Analysts, Security Architects, Threat Hunting Ops, Intelligence Officers, Big Data Engineers, Machine Learning Researchers, Security Operations, Penetration Testers, Threat Intel Vendors, Security Firms, Networking Appliances Vendors, Enterprises with huge networks, Corporations of great scale, White Hat Hackers, etc. And out of these collaborations a vast and powerful community is bound to emerge.

STORAGE

The storage problem is foreseen, we have developed an algorithm to enable your small incapable devices to only download relevant parts of the blockchain (according to metadata "timeframe, country, industry sector") this allows devices like your phone to still benefit of the network but only feed on relevant threat feeds. This algorithm will introduce a bit of a dependency on a cluster of neighbour nodes that is to be fully updated and have a full copy of the blockchain. The phone app will then ask one of the nodes to execute the trades on its behalf. At this point the rest of the nodes validate the authenticity of the trades executed by the selected node and update the selected node's reputation and reward. A transaction like the one discussed here will cost the phone account a bit more since there is a commission model to be imposed. Hence rewarding the node that kept a full copy of the blockchain and executed trades on the phone's account behalf.

TOKEN LAUNCH

PRE ICO (Initial Coin Offering) is scheduled to launch on MARCH 12 - MARCH 18 2018, lasting for only 7 days while the launch of ICO (Initial Coin Offering) is planned to take place in JULY 2018. During these sales, the demand for SEC is expected to be on a great increase. However, there are limited coins available for sale. Bonus rates up to 37.5%. Rewards (BOUNTY) program worth up to 10,000,000 SEC Coins.

	>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%

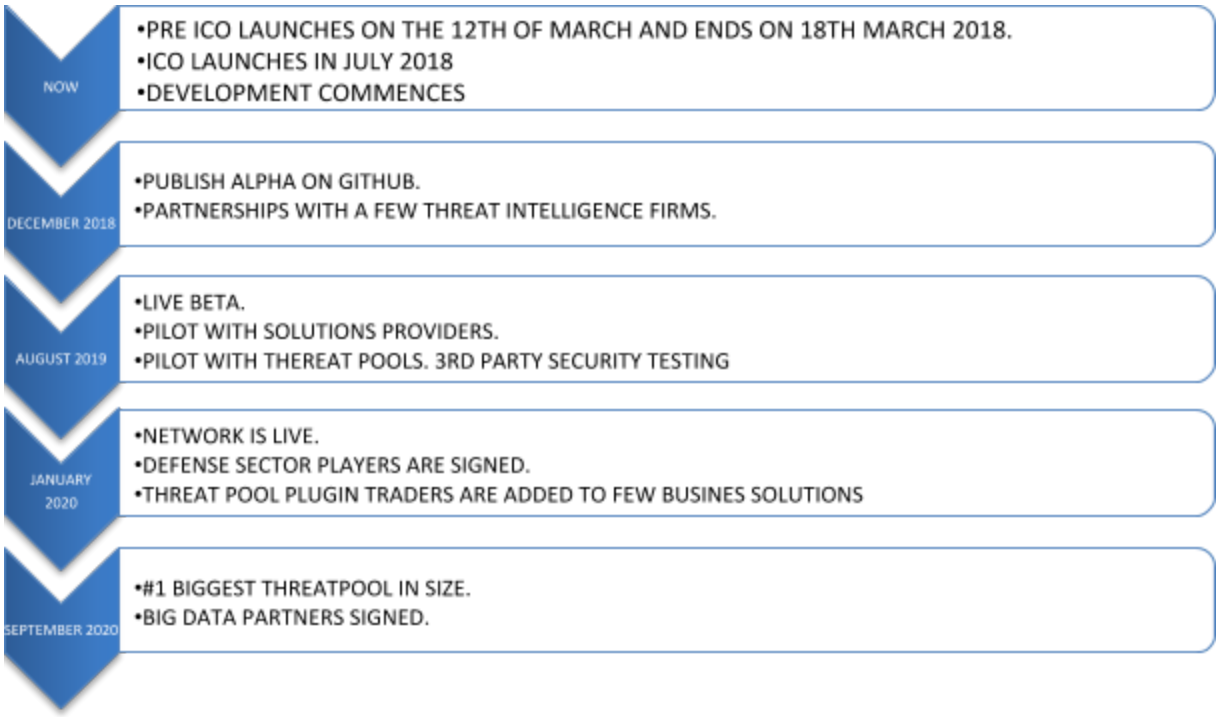
Weekly Air Drops

Members of our team will airdrop various amounts of SEC tokens to random wallets, on weekly basis, until the end of our full ICO (July 2018). Airdrops will be distributed based on SEC amounts proportional to your balance.

ROAD MAP

The threat intelligence market size is estimated to grow from USD 3.83 Billion in 2017 to USD 8.94 Billion by 2022, at a Compound Annual Growth Rate (CAGR) of 18.4%. The base year considered for the study is 2016, and the market size is calculated from 2017 to 2022. With the launch of token on the 12th of March 2018 beginning only with pre ICO sales, THRINTEL MARKET is projected to record rapid exponential growth by the beginning of 2020.

Here is the map below for illustration:



TEAM & COMMUNITY

THRINTEL MARKET is made up of a community of experts sufficiently experienced in their different fields of specialization. Every member on the team is highly valuable and disciplined from Core members to Tech Advisers to Business AdviserS and not leaving out Legal Advisers and a host of others. The common goal of a more secure digital space is the main driving force and primary focus of everyone on this team. Check out the list:

The plan in the long run is to create a large and immensely effective community of data sharers that are credible and worthy of trust who get rewarded to exchange intelligence so as to tackle and avoid threat intelligence adequately. This community of traders will be backed by our efforts and development community to update and test the code base (thrintelmarket blockchain, and secure coin) and issue new releases and upgrades quarterly.

CONCLUSION

- THRINTEL MARKET is a revolutionary invention in the constantly-changing world of cyber security, cryptocurrency and the entire tech community.
- SECURE coins are similar to Bitcoins but they are more secure, efficient and will appreciate in value as soon as sales kick off. They are needed so that we control the financial system of the THRINTEL MARKET, which allows us to de incentivize bad data injections, reposting data, spamming the network, and other attacks, to be outlined in a separate technical document.
- The roadmap is not only achievable but also realistic. The team, the advisers, the partners, the investors, and few prospective clients, have verified the roadmap, and its achievability. The vision has been reviewed by multiple parties participating in the threat intelligence sector currently as well.
- Post-ICO, the limited number of SEC Coins is expected to appreciate in value as the blockchain user volumes increase, and hence the demand increases on the limited number of SEC Coins out there.
- Constructive and useful data submissions are to be rewarded, hence it is expected that we see a shift of OSINTs into the market. This also aligns with the business vision discussed with out partners, investors, and advisers.

Although threat pools exist, and data are being dumped for free, experts understand that the data on these threat pools is not so useful, and hence outdated, or in need of excessive processing and validation often costing more than the data value. However, some pools are to be invited to data exchanges. It is based on threat pool ratio. They give 10% of the threat pool in fresh new data and receive 15% threat pool volume of fresh data to them as well. These exchanges are huge and cost the network much power if dumped at once. We have developed an algorithm to decentralize the exchange process where the exchanges will be given accounts on the market and they will be given coins for their contributions that they redeem in fresh data right away via an algorithm developed and is patent pending. This will engender integration of multiple threat intelligence pools easily into the THRINTEL MARKET, although these data will still remain decentralized as they reside in all updated devices on the network.