SIMPLY TRADE DATA NOW

Whitepaper v1.0

Contents

Background

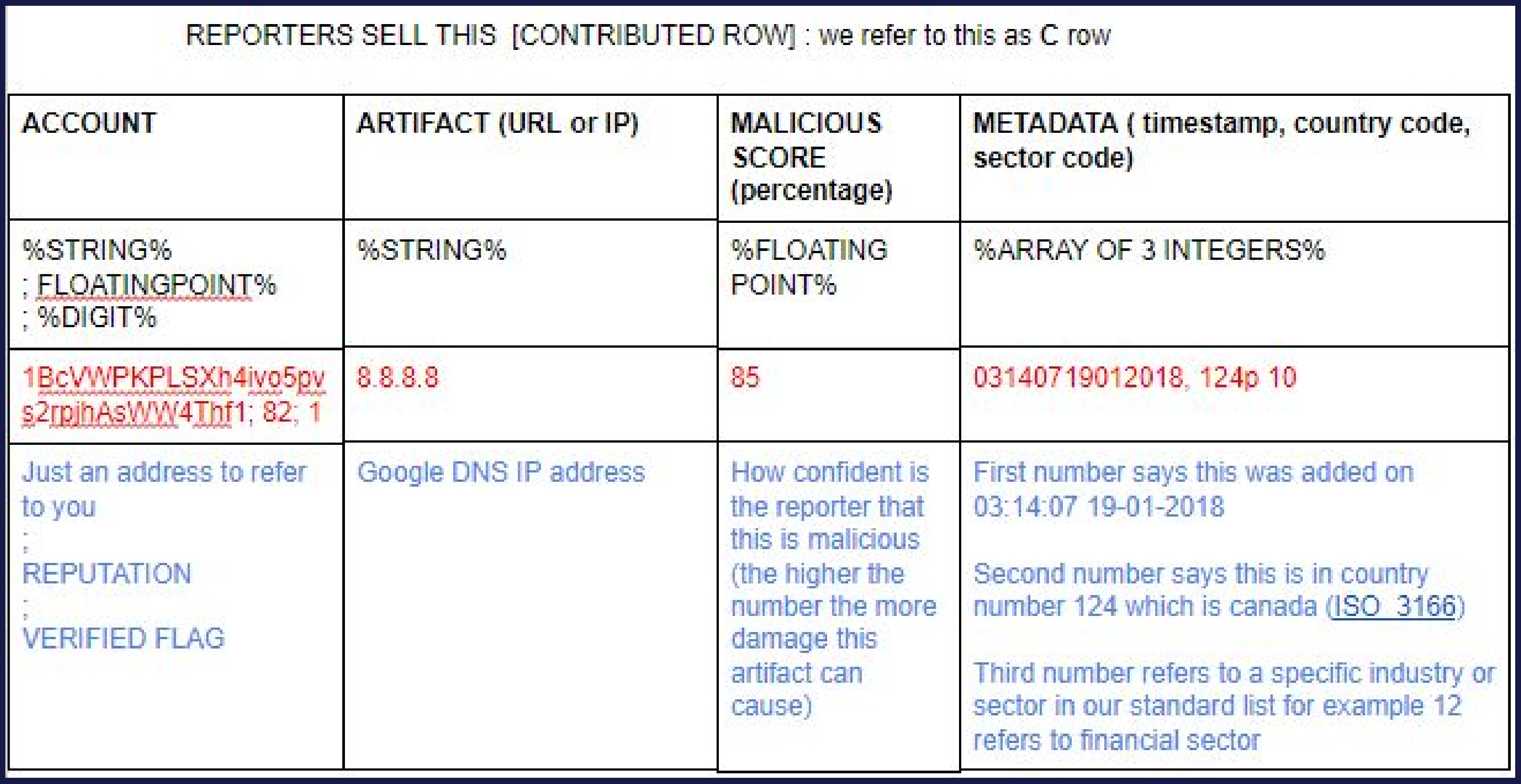
Sharing threat intelligence is currently an extremely inefficient and ineffective process. Customers depend on many security vendors and other users (who risk bad PR if they were hacked themselves (ex:Bank saying they got hit with a zero day virus to warn others from it)) to provide the intelligence but they end up with duplicates, bad data, raw data, and tedious lengthy process to acquire the information with different formats, and lags from different enterprises and groups. Also they have to completely trust their sources to check and validate their information in realtime before sending it out. There is no clear way to evaluate threat intelligence vendors since their effectiveness is not directly compared to each other and security sensitive customers (ex:Large corporations and governments) in this market end up buying everything they think they need (including duplicated information), wasting big money, communication and processing time to crunch all the different formats with little return, just to make sure they aren't missing anything important. Current solutions have tried to open source threat intelligence for everybody for free on a certain website. This ends up being a single failure point (that can be taken down by for ex: a DDOS attack) that no enterprise can depend on specially if they don't trust the moderators of such website since if they are compromised their attackers can manipulate the data feeds that everybody is using. We propose a decentralised threat intelligence database, that 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 so that you dont buy it again, and you make money of 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 database is resilient, almost impossible to take down or manipulate, immutable, distributed, and 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). We also offer buyers a more resilient, safe, secure way that they can actually rely on for their threat intel. Today's enterprises rely on an ad-hoc mixture of security solutions subscriptions, threat intelligence feeds, and assorted dynamic analysis engines to defend against evolving adversarial cyber activity. Users must weigh the benefits and drawbacks presented by each solution and decide on the least-worst fit for their environment.

We are proposing a threat intelligence market, which enables sharing & validating threat intel in real time. Including incentivized sharing of new artifacts that helps vendors get access to premium feeds reliably cheaply. Can have anonymous sharing also.

The Market & 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. SEC is a coin used in these transactions in the market. The THRINTEL MARKET will essentially 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.

The Contributed Row will look like this:



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%
1BcVWPKPLSXh4ivo5pvs2rpjhAsWW4Thf1; 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

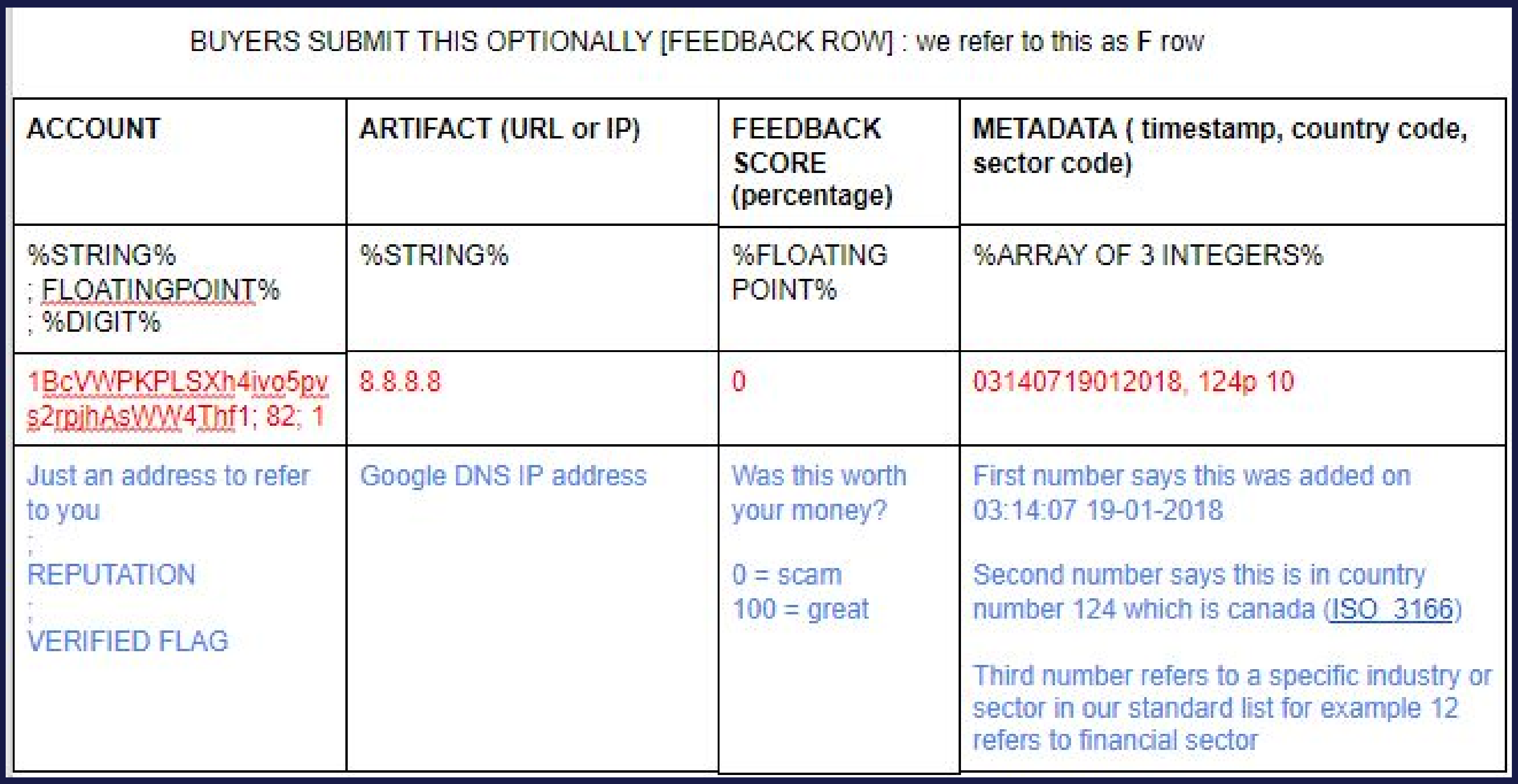
Under ACCOUNT you have an ADDRESS, A REPUTATION SCORE, and a VERIFIED FLAG. This represents you, your current reputation on the market, and whether you have a verified account or not (verified accounts are for branding purposes by security firms).

Under ARTIFACT you have an IP or URL. This is what you are submiiting 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 will look 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

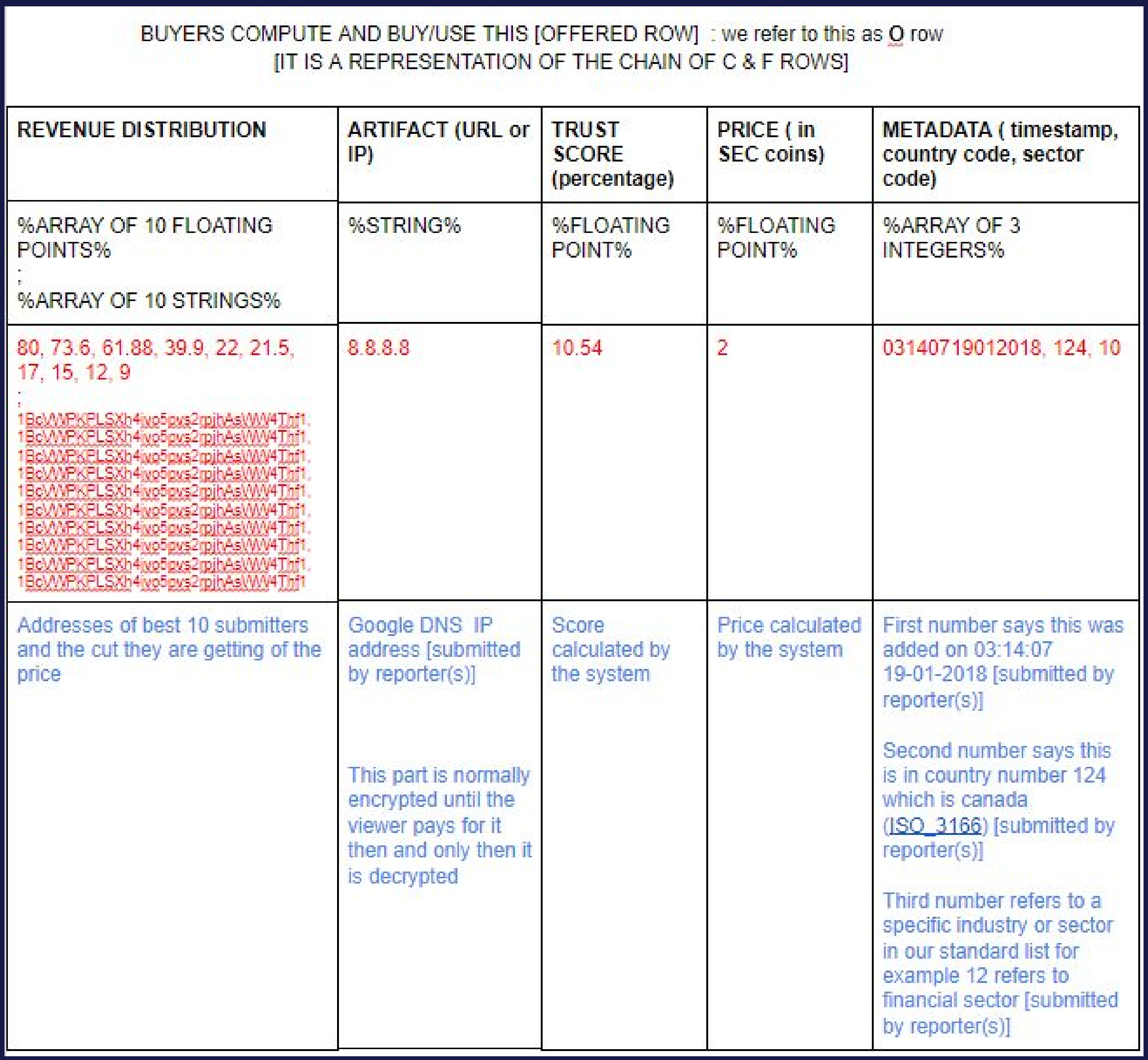
Under ACCOUNT you have an ADDRESS, A REPUTATION SCORE, and a VERIFIED FLAG. This represents you, your current reputation on the market, and whether you have a verified account or not (verified accounts are for branding purposes by security firms).

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 centres, 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 ; 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1, 1BcWMPkPLSXh4ivo5pvs2rpjhAsWW4Tnf1	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 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 addreses 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 # of reporters, submissions timestamps, malicious scores, reporters reputations.

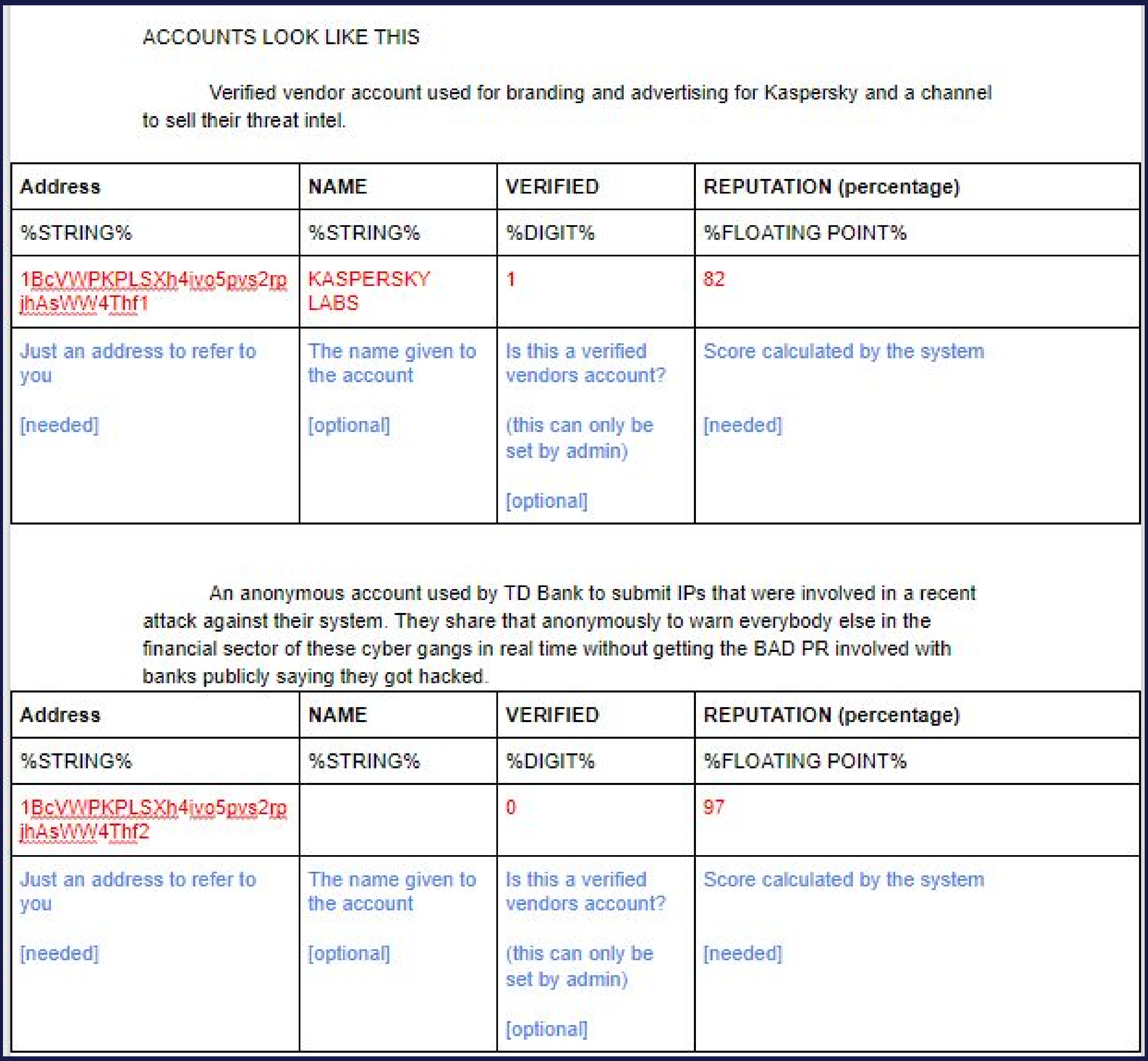
Under ARTIFACT you have the IP or URL you are buying but of course it is encrypted until you buy the key that unlocks it only for you (the key would only work with your account).

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, you have a timestamp, a country code, and a sector code. This gives context to the artifact.

On the Platform everybody has an account. Accounts come 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. More to that later. Anonymous accounts are an asset for banks getting hacked and wanting to report on an artifact leading on the APT group attacking them to warn others. This may sound familiar as Obama's administration was working towards something like this. But this leads to bad PR for the reporting bank for instance. So the current channels are only between selected banks or partners, leaving many out of the news. 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%
1BcVWPKPLSXh4ivo5pvs2rp jhAsWW4Thf1	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%
1BcVWPKPLSXh4ivo5pvs2rp jhAsWW4Thf2		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]

The verified flag on accounts is only to be set by an Admin, admins are to be selected early on before launching the network. They shall be trusted 3rd parties in different parts of the world, a paper will follow on the selection process and the voting system leading to it. But essentially security firms will reach out to the admin prove that they are indeed the firm and register the account officially to their name, and then get the flag set by the admin, the holder of the private key to set the flag, that everybody else is able to verify using the public key.

The Market feeds on few concepts engineered it into it and it makes the market truly special. They are as follows.

1. You may want to upload your data to make sure you are not buying it, this also makes you money

2. you view metadata, trust, price, before paying then after you pay the artifact is decrypted

3. people upload metadata and artifact; we assign a trust and price and give them, reputation and coins

4. TIM is the exchange, SEC is the coin they both use blockchain differently

5. blockchain is giving anonymity, decentralization, ddos protection, inventiveness, immutability

6. security devices can make you money that can get spent on keeping it updated automatically.

The Market feeds on few calculations that are performed by all nodes as well. These calculations are to be optimized during development cycles leading to the launch of the network software. This software will come in classes of varying accuracy, a class for embedded systems with low to average computing resources (Firewalls, routers, switches), a class for data centers and servers with highly available computing resources, and a class for average resources (PCs, endpoints). These solutions are to run through the calculations and do the trading based on the user settings. Hence keep on updating everybody on what it sees, making money, spending it on buying more signatures or cashing it out to its owners to pay for its electricity or upgrades. The core calculations are listed below, and they are functions of few variables:

1- TRUST SCORE (# of reporters, malicious score, reporters reputations, feedback

2- PRICE CALC (trust score, metadata)

3- REVENUE DISTRIBUTION (# of reporters, submissions timestamps, malicious scores, reporters reputations)

4- REPUTATION CALC (# of artifacts, feedback, malicious scores, submissions timestamp, # of buyers)

FORMATS:

It is important to note that the market is supporting the full STIX Taxonomy, TAXII, CYBoX. A graph network representation is also developed to make it easier for Threat Intelligence analysts and shall follow in a another paper.

DATA:

It is worth noting that most artifacts are to expire and experience a price dip on the market after 2-3 weeks given the type of data shared, so the amount of data traded on the exchange makes it a fertile ground for big data analysis and would introduce more insights on hacker groups and would provide deeper analysis of their behaviours and targets. In theory this may lead to predicting their next operations with accuracies up to 90%.

Blockchain:

Given the existence of acts like the US patriot act and in spirit of NET NEUTRALITY, a decentralized solution is needed in the security industry. Also given the sophistication of sponsored state hackers and how they are known to take down OSINTs during operations to kill threat feeds to everybody in the world while they are progressing on their targets and causing damage we need to have a DDOS proof database. These groups and other APTs were also reported to hack into databases and remove data leading to their assets which introduces the need for IMMUTABILITY. With governments, large corporations, large financial organizations making most victims of these groups we develop a need for anonymous reporting to avoid bad PR and backlash. All mentioned points and more are to be provided by the THRINTEL MARKET and to be facilitated by the technology referred to as block chain.

Why?

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 what6 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 securtiy industry and hence lead to all the failures or “hacks”/”breaches”/”scandals” that affect the economy negatively pulling more than 2 TRILLION USD by 2019 to cybercrime, according to the Forbes. We need to start rewarding researchers that actually develop results regardless where they are, what company they work for, or what their work is sold as. The THRINTEL MARKET makes sure you get the money and the reputation points for your work if its valued by the community. The buyer also circumvents all the sales, the markups, the process, the desks, and gets right from the source. Hence it has full integration between threat pools, security devices detecting zero days, security devices intelligent enough to find new patterns, security devices not so smart that rely on feeds from analysis engines, security researches, threat hunting operations, threat intelligence analyst, intelligence officers tracking down hacking groups, law enforcement tracing certain online threats and threat actors, and more.

A

Community

A community is to be born. The community of Cyber Security Researchers, Threat Intelligence Analysts, Security Architects, Threat Hunting Ops, Intelligence Officers, Big Data Engineers, Machine Learning Researchers, Security Operations, penetration testers, Security Vendors, Security Firms, Networking Appliances Vendors, Enterprises with huge networks, Corporations of great scale, White Hat Hackers, and more. These are to plug in to the market and trade on it as described per the section THE MARKET & THE COIN. They just install the software set the settings for autonomous trading or disable it and execute manual trading and that is it. The community is to be monitored by few selected 3rd parties for verified accounts and local support. These parties are to be selected via a voting process to be announced in a following paper. The community generally shall be accessed via the threatintelligence.community website for support and more. While the software the plugs into the blockchain is to be found on threatintelligence.market. The online version of the representation and reports are to be found on the threatintelligence.market, so you would be able to monitor the network and read reports and analysis of current movements.

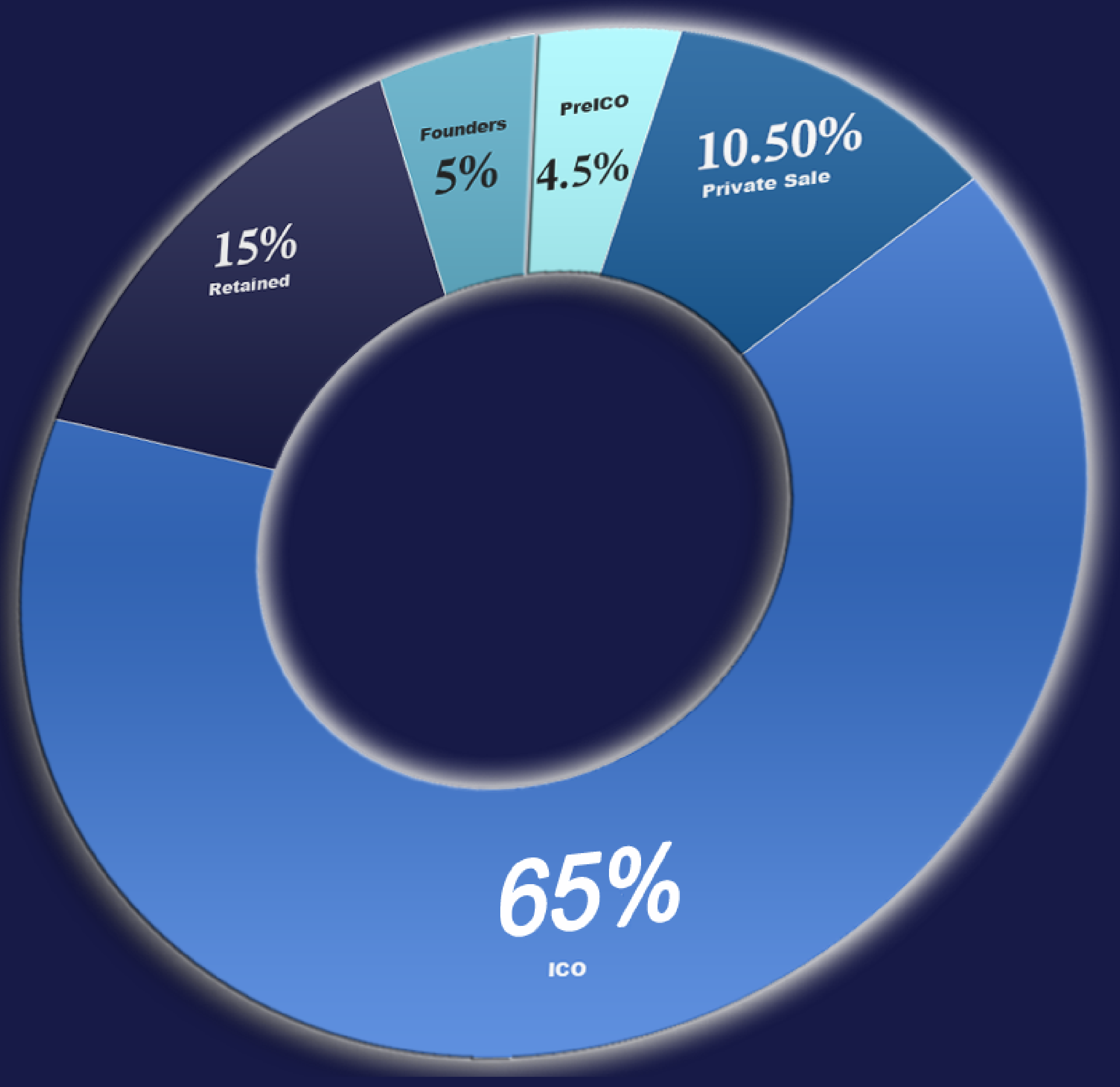
Threat Pools

Threat pools exist, and many are giving us there data for free. Some need something in return however. A list of feeds we get for free is to be attached below for your reference but it is huge. However some pools are interested in a data exchange. It is based on ratio. They give us 10% of our threat pool in fresh new data we didn't have, we give them 15% of our market of data they didn't have 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 allow for integration of multiple threat pools easily into the THRINTEL MARKET.

\

Coin Details

THE SECURE COIN is a crypto coin built on top of ethereum (ERC20).. PoS/Pow. The THRINTEL MARKET uses the SECURE (SEC) COIN in all its transactions. It goes by the ticker SEC. There are only 2,000,000,000 SEC Coins. There is a limited supply but an increasing demand as the network goes live and transactions start hence the coin will be of rising value. The SEC Coin is kind of like Bitcoin, however it is ultra secure. It is also ultra fast. It is open source.

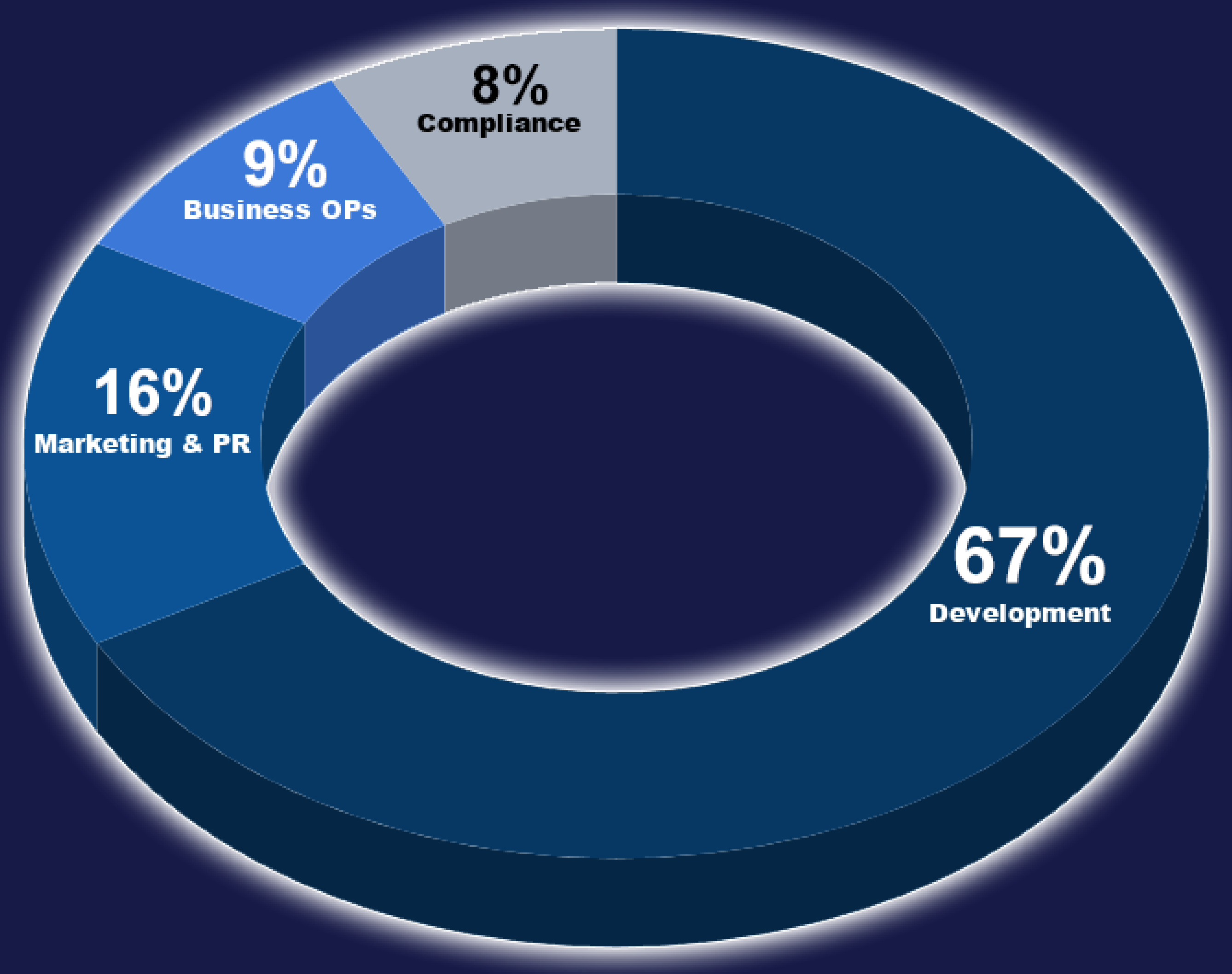


69.5% of the coin will be released to the public during the PRE ICO & ICO rounds of token sale. 10.5% are sold privately to selected investors in the THRINTEL MARKET circle. 15% are retained for outreach and promotional activities. 5% are to be given to the founders.

Token Sale

PRE ICO (Initial Coin Offering) is MARCH 12 - MARCH 18 2018. ICO (Initial Coin Offering) is scheduled for JULY 2018. 3 weeks After Pre ICO SEC Coins are to be issued. Bonus rates up to 37.5%. Rewards (BOUNTY) program worth 10,000,000 SEC Coins.

YOU MAY NOT BE PERMITTED TO BUY SEC COINS IN:
CANADA
CHINA
SINGAPORE
United States (Accredited Only)
US Virgin Islands (Accredited Only)
US Minor Outlying Islands (Accredited Only)



Platform: Ethereum (ERC-20 Token)

Start of token sale: 12 March

Soft cap: 300 ETH

Hard cap: 3 000 ETH

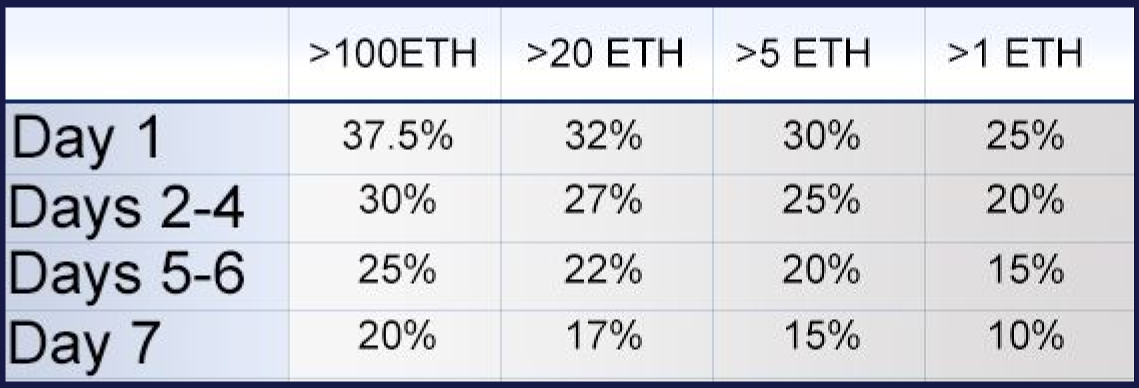
Tokens offered in PreICO: 90 000 000 SEC

Total Tokens issued: 2 000 000 000 SEC

Price: 1 ETH = 30,000 SEC

Payment method: ETH

Minimum contribution: 0.1 ETH



	>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%

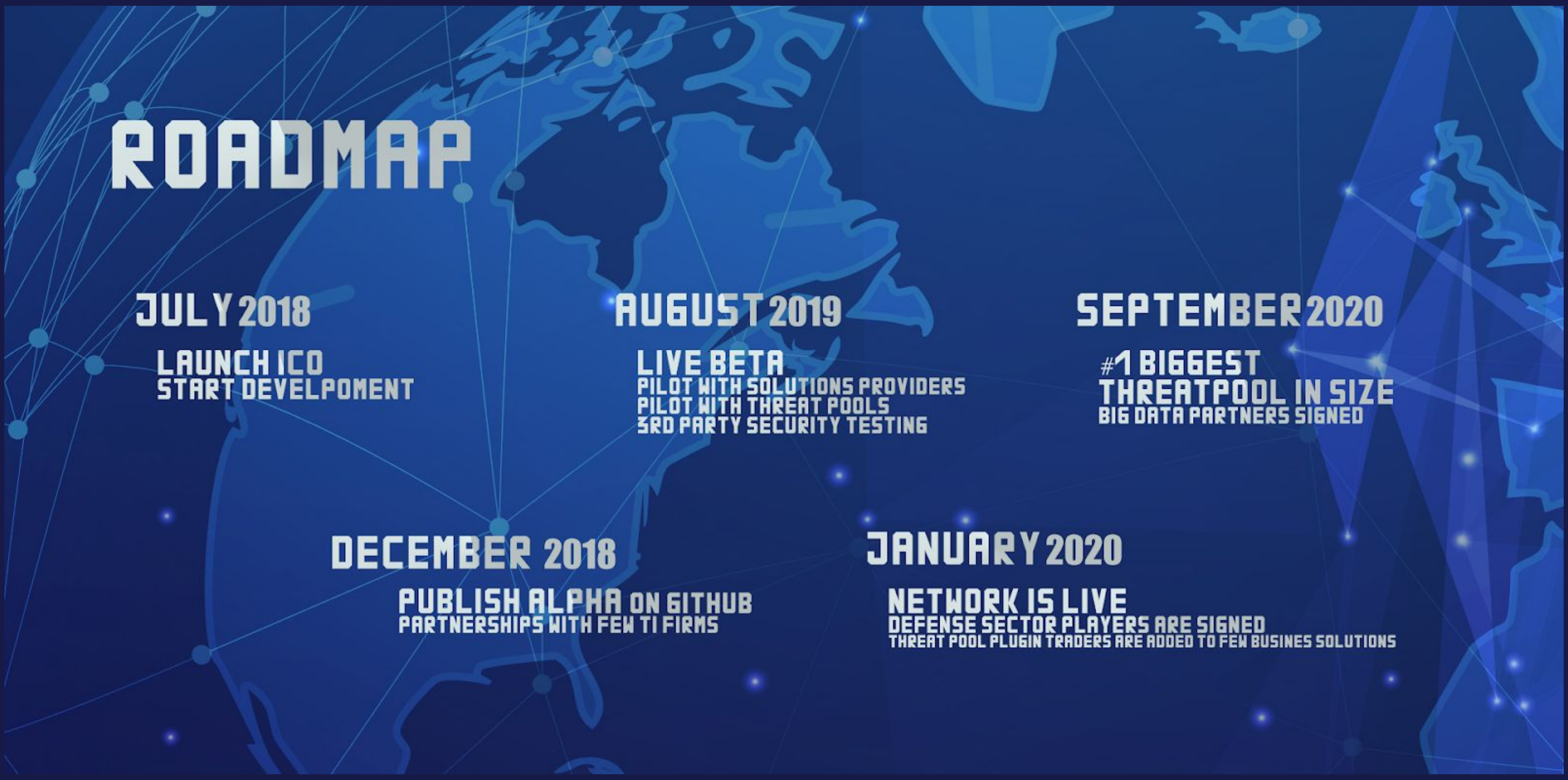
Weekly Air Drops

Our team would be airdropping various amounts of SEC tokens, proportional to your balance, to random wallets, on weekly basis, until the end of our full ICO (scheduled in Q3 2018).

Bounty / Rewards program: threatintelligence.market/bounty

Roadmap

Network goes live January 2020. ICO will be in JULY 2018.



ROADMAP

JULY 2018

LAUNCH ICO
START DEVELPOMENT

AUGUST 2019

LIVE BETA
PILOT WITH SOLUTIONS PROVIDERS
PILOT WITH THREAT POOLS
3RD PARTY SECURITY TESTING

SEPTEMBER 2020

#1 BIGGEST
THREATPOOL IN SIZE
BIG DATA PARTNERS SIGNED

DECEMBER 2018

PUBLISH ALPHA ON GITHUB
PARTNERSHIPS WITH FEW TI FIRMS

JANUARY 2020

NETWORK IS LIVE
DEFENSE SECTOR PLAYERS ARE SIGNED
THREAT POOL PLUGIN TRADERS ARE ADDED TO FEW BUSINES SOLUTIONS