CYBER SECURITY ECOSYSTEM AND UTILITY TOKEN

Whitepaper

August 28, 2018

Shawn R. Key and David Donnenfeld

Cybrtoken.io
shawn.key@cybrtoken.io
david.donnenfeld@cybrtoken.io

"…the solution is a forward-thinking, disruptive technology that addresses the issue of illicit file activity (IFA) within the enterprise. Every organization is facing this advanced persistent threat and the associated reputation risk, and this specialized threat and assessment solution is a must-have for any government, commercial, education and non- profit."

Chad Fulgham, former CIO of the FBI

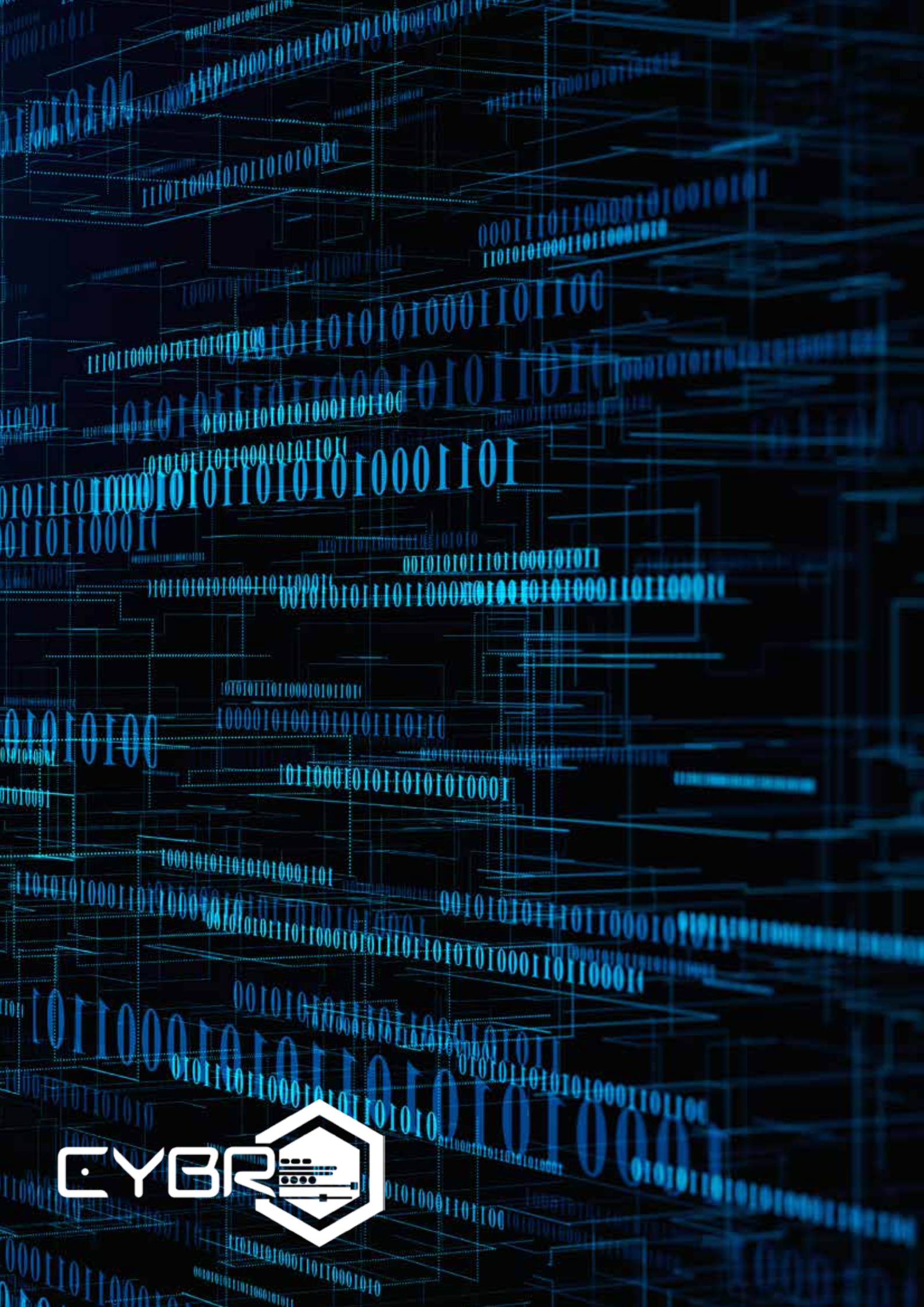

CYBR

Table of contents

Executive Summary

A Stolen Horse

I grew up in Virginia, so I am often reminded of an expression Southerners use:

"You don't lock up the stable after the horse has been stolen."

When weighing the need for cyber security in the blockchain space, this old adage could not apply more nor be more appropriate.

An Abbreviated History

The parabolic rise and volatile nature of cryptocurrencies portends the enormity of its potential impact. There is widespread speculation. Some pundits predict a cashless society in less than a decade and the more outspoken supporters of Bitcoin predict a price that will eventually crest seven figures. The detractors, irrespective of authority and stature, utter a single word in dismissing the viability of widespread adoption. And that word is "scam". Not a pretty word. While it certainly speaks to the level of threat the old guard senses from the emergence of crypto and decentralized systems, it also smacks of a fundamental concern that these "monies" can be taken as easily as they can be created.

While swindlers and charlatans can be found in all businesses, if digital assets and virtual currencies cannot be secured, they can not be adopted. And the irony is that crypto and blockchain technologies have garnered public support as a result of a collective distrust for our existing governments, monetary policies and FIAT currencies on the whole. Certainly there is compelling evidence that points to governing corruption across the globe. What can be said about crypto? Consider the following:

- In June 2016, DAO, Decentralized Autonomous Organization, had US $50 million stolen. Running on the Ethereum network, written in the language of Solidity, a simple flaw was responsible.
- In 2014 Mt. Gox filed for bankruptcy claiming it had lost 750,000 Bitcoin.
- In January 2018, Coincheck, a Japanese cryptocurrency exchange was hacked for approximately US $534 million.
- After being hacked in April 2017, South Korean Exchange Youbut stated, it did its "best to improve the security, recruitment and system maintenance."
- In December 2017, Youbut was hacked again, losing 17 per cent of its total crypto holdings. Parent company Yapian filed for bankruptcy.

- Bancor raised US $153 million in June 2017 to develop a decentralized liquidity network, i.e. a decentralized exchange of the highest order. In July it was hacked for US $23.5 million*
- On the same day as Bancor, a hack on a popular VPN compromised "My Ether Wallet (MEW)," a widely used service to manage Ethereum network cryptos.

The list could go on. Still, it would be remiss not to mention the astonishing number of individuals who have been hacked or scammed out of their crypto. The laundry list continues as high-profile ICOs have been victimized by phishing attacks. There has been no shortage of exit scams in the space. Even simple human error can be costly as one unfortunate individual learned when he inadvertently spent 50 Bitcoin in transferring fees.[1]

Hacking and Internet-based crimes are not unique nor confined to crypto. A 2017 Norton Report stated that US $172 was hacked from nearly a billion consumers worldwide. More than half the adult population online can count themselves as victims of cyber crime and mainstream stories like the Equifax breach have grabbed headlines. However, the nascent asset class that is crypto and distributed ledger technologies (DLT) is acutely vulnerable. Nothing can destroy a revolutionary overhauling of a monetary system faster than a plague of theft.

Stateside Measures

Security has become such a concern that congress introduced the "hack back" bill, allowing businesses to attack their attacker's computers or networks.

- Active Cyber Defense Certainty Act introduced this amendment to the Computer Fraud and Abuse Act anti-hacking law.

Two clichés come to mind when I see this: "sometimes the cure is worse than the disease," and "an ounce of prevention is worth a pound of cure."

- Identifying a hacker often takes time and analysis.
- Ordinary researchers are not capable of performing such analysis.
- Hackers often leave clues in the code and spoof that evidence, e.g. leaving code from known hacking organizations in malware.
- The amendment only applies within the United States.
- Most attacks come from abroad.

- Those that don't come grom abroad are often routed through servers that come from overseas.

Governing bodies have already enacted a number of stops on the "hack back" amendment:

- Before taking action against attackers, the National Cyber Investigative Joint Task Force (NCIJTF) must be alerted.
- Prying into hacking networks may be an obstruction to ongoing investigations and non-permitted retaliation is potentially criminal.

The NCIJTF is led by the FBI and the FBI defense review is worried that actions taken by private organizations could effectively trigger our government's international legal responsibilities.

As DLT wends its way into the mainstream, the stakes are rapidly being raised. Quantifying prevention is not easy but it is easy to overlook. When Equifax hackers made off with the private information of 143 million people, who is responsible for what amounts to an en masse modern-day home invasion? Is it a victimless crime if insurance pays?

The reality is that the ultimately accountable Equifax is not held liable and as of now, no one is reimbursing lost crypto. If the last four digits of our social security numbers can be sold on the dark web, in what stead should we hold the security of digitized currency?

Digital assets are currently being used as mediums of exchange, as stores of value, and more. They are the equivalent of money, bartering tools, precious metals as well as the lifeblood of emerging ecosystems. Make no mistake, horses have been stolen and many more thieves are coming. We can no longer overlook the clear and present threat to the technologies that are poised to reshape our world. It is time to secure the blockchain.


CYBR

Enter CYBR

Good Cyber Threat Intelligence (CTI) is continuously refined information that hones in on potential or current attacks that can threaten any system.

CYBR is an ever-expanding compendium of information combined with state-of-the-art software that will be optimized for the blockchain. CYBR is a holistic security solution that will endeavor to secure wallets, smart contract transactions and related activities that take place in the blockchain space.

Unlike most token generation events (TGEs), where a theoretical idea is presented and implementation is to follow, much of the CYBR solution is already built and being utilized in traditional environments.

To this point, it is safe to say there is a truly pressing need for top-flight cybersecurity in the realm of crypto. However, there are very few parties qualified to provide the needed level of security. With that in mind, let us momentarily stray from the traditional structure of a white paper. Thus far, the "why" has been addressed. Now, let us the broach the most critical component of such an undertaking "the who."

The Vision And The Visionary

"We invest in people, not ideas." – A maxim of venture capitalists.

CYBR's founder, Shawn Key (detailed biography and related links under "Team" at cybrtoken.io) is a cybersecurity veteran of some notoriety. He is attributed as the person first described as an "ethical hacker," based on an article in a governmental trade magazine.[2] The term presaged the popular "white hat hacker," by more than a decade after Shawn successfully found his way into numerous federal networks in 1999.

Shawn's facility and acumen in the field were widely noted and his early contributions to "information security" aka "information assurance", were seminal. A few years later, the industry would become known as "cyber security."

Some of his early work included one of the first patch management solutions, which was acquired by a company that eventually sold to IBM for some US $500 million. He quickly garnered a reputation as someone who could "see around the corner."

Over the last ten years Mr. Key's cyber services company has maintained a flawless reputation and is a subcontractor to Raytheon (see cybrtoken.io under "Partners"). Raytheon has the distinction of earning the largest cyber security contract awarded in US history of US $1.115 billion.

In recent years, Shawn's focus has been on the underlying solution that makes up the CYBR Ecosystem: BlindSpot. The software solution has gone through its share of iterations and pivots but the concepts of detecting malicious code and associated bad actor activity were consistent themes throughout his numerous grants and awards received for his work. These include, but are not limited to:

- Mach37 Cyber Accelerator: awarded US$150,000 in grants via Mach37 and the Center for Innovative Technology (CIT).
- Dell Founders 50 Club: recognized Shawn's technology as one of the top 50 most disruptive technologies in the world.
- Tandem NSI, associated with the National Security Agency (NSA): recognised Mr. Key for creating one of the best technologies in the D.C. metro area.

Mr. Key was intrigued by cryptocurrency and with each passing hack, this interest morphed into the central preoccupation in his life. He quickly found that many of the exploitations were similar to "traditional" attacks. What he dealt with in every day enterprise systems mirrored the methodologies used in the majority of reported hacks. He determined that BlindSpot was applicable to the blockchain and it became his mission to optimize it for cryptocurrencies in securing smart contracts and associated transactions. Although it poses some unique challenges and there are inherent differences, Mr. Key realized that his experience could improve the security posture of the world of crypto. The last year has been solely focused on what has evolved into CYBR.

Welcome to the CYBR Security Ecosystem and Utility Token.

Enter CYBR

Not Your Father's Antivirus

While antivirus (AV) software hasn't sounded relevant for a long time, threat detection and eradication has remained at the fore for government and many private sector organizations. Sensitive data and the protection of these assets have grown in scope, commensurate with our advancements in technology. Unfortunately, the general public has not benefited from this growth and the displays of negligence in corporate America provide unimpeachable evidence to this point.

There have been numerous data breaches of sensitive information and despite the headlines they have captured, it has ceased to be a priority to those responsible for securing said data. Society pays the cost for the mishaps of Target, Equifax and similar, while specialized agencies have continually evolved against growing threats.

As crypto takes hold and drives towards critical mass, the need for a gold standard of security and an attendant solution has never been greater.

Elegant, Robust

CYBR, like good CTI itself, is a two-fisted attack that provides real-time safeguards, countermeasures, threat intelligence and secures transactions via two distinct methods:

- BlindSpot: A proprietary software that powers a potentially borderless landscape of threat identification.
- Portal: CYBR utilizes a real-time, pedigreed data feed heretofore not available to the general public.

Identifying a threat is one thing, removing it another and still another to prevent its return. Standard issue solutions can tell you something is wrong but can't necessarily eradicate the problem nor detect the evolution of threats. They are simply obsolesced by current malware.

Work-a-day antivirus software is nothing more than a compilation of known threats with basic search capabilities. Today's malware has adapted and can morph into a slightly different version of known viruses. The result is that malicious code is no longer identifiable by standard AV software. The permutations of known viruses that can continually plague networks are known as advanced persistent threats (APTs) and standard software has no solution for it.

BlindSpot not only detects, "bad actor," associated illicit file activities and APTs, it disrupts them. The three primary tenets of risk management in relation to CTI and ensuring data are as follows:

1. Confidentiality
2. Integrity
3. Availability

BLINDSPOT

BlindSpot captures attack signatures by deploying a combination of machine learning in concert with artificial intelligence. Whence identified, this information is distributed to the protected community via the blockchain. To augment the supporting data that runs concurrently with BlindSpot, one of the CYBR's token initiatives is to reward community members for identifying suspicious activities.

Being Smarter

Smart contracts are a protocol that executes the terms of a contract. The potential efficiencies it offers are myriad and game changing. It is a revolutionary time saver that can considerably reduce expenses and sidestep legal entanglements and associated costs. The applications for smart contracts are growing by the day and they are the lifeblood of distributed ledgers. The Company believes that the primary stumbling block for mass adoption of blockchain technology is security and aims to establish a "best practices" standard. Any executor of code is aware of the inherent issues but unfortunately, even the most outspoken and vocal leaders of the blockchain neglect to properly acknowledge this growing risk.

We can ill afford to analyze vulnerabilities after an attack. While open source is inspired and will pave the way for innovation, there must be a standard. Auditing can go a long way but ultimately, the safe harbor that CYBR can provide will raise the bar and be the benchmark by which security on the blockchain will be measured.

For example, smart contract programming in Ethereum is known to be error prone and many of these common errors are known quantities. The DAO hack for example, was the result of a recursive calling vulnerability. Essentially, hackers with an initial minimum balance were able to repeatedly withdraw that balance. There was no fallback function and thus, repeated withdrawals were made, as balances were not updated in real time. Such gaffs are imminently avoidable. This contract would not have met any security expert's minimum standards, yet some US$ 50million was heisted.

Enter CYBR

To summarize, CYBR is an advanced cyber security solution that deploys its proprietary software, BlindSpot and layers it with a comprehensive data feed to proactively identify hackers.

Mission Critical

There is a pressing need to dramatically reduce the average time of detection in identifying and contending threats. Without this, the adoption of DLT hangs in the balance. The implementation of a proactive defensive as well as preventive approach to cybersecurity is sorely lacking in the space. CYBR seeks to solve that problem.

CYBR's mission is to provide a seamless continuum of threat security and establish a gold standard of cybersecurity on the blockchain.

Governance, Risk Management and Compliance (GRC)

In traditional cybersecurity, the term GRC is a buzzword. The acronym stands for Governance, Risk (Management) and Compliance. Currently, an enormous number of vendors are providing this service in integrated, point solutions or domain specific capacities.

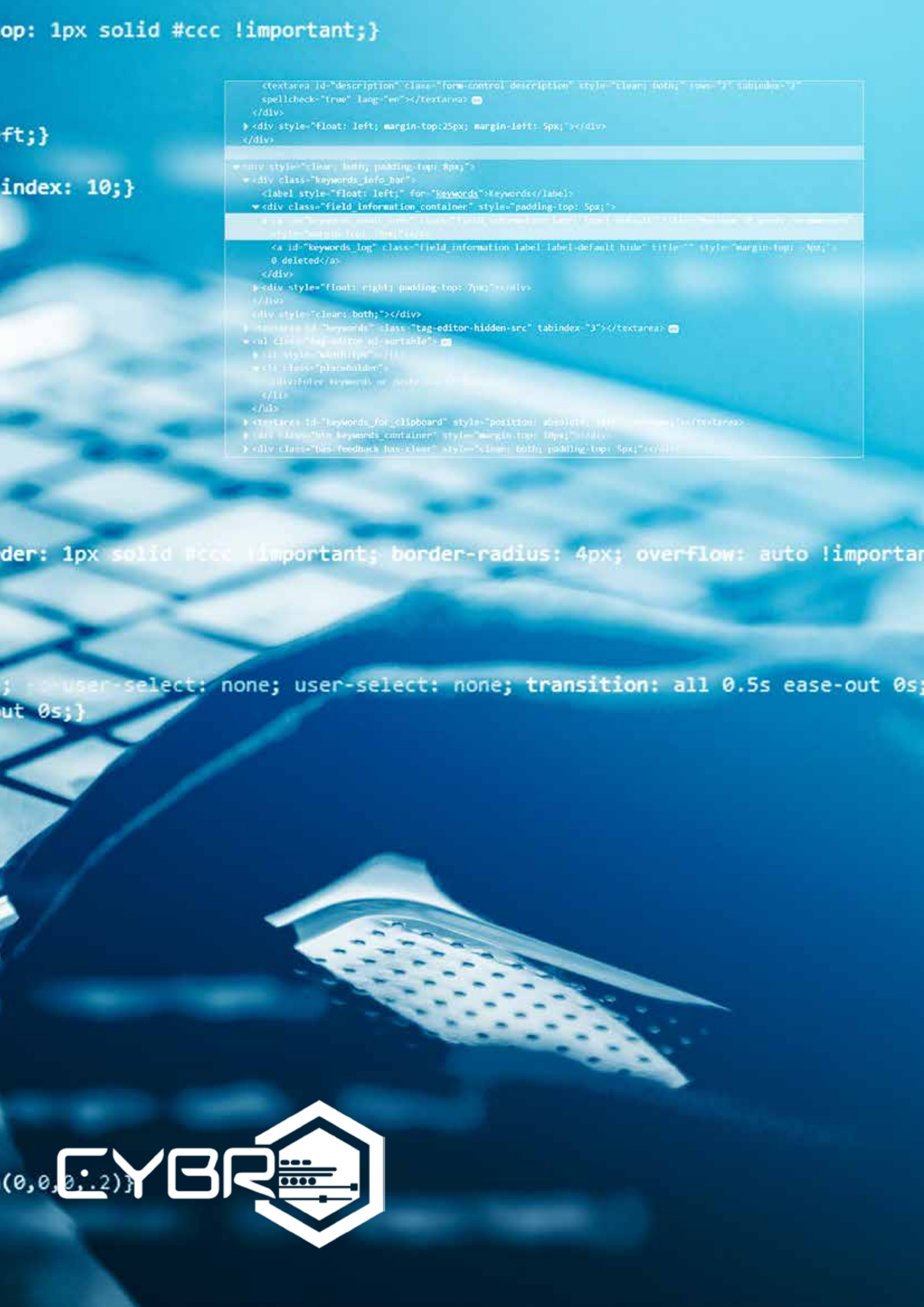
Each of the core disciplines is comprised of four basic characteristics: processes, technology, strategy and people. Dependent upon an organization's risk tolerance, company policies and any external regulations are what determine the level of engagement. Once identified and assessed, operational rules or parameters that the GRC "quotient" supports are integrated or merged holistically across an organization.

As nebulous as it sounds, the field is rapidly growing and its efficacy remains unquestioned. What this translates to for CYBR is the need to establish a robust community, as their input creates the checks and balances for a decentralized world. GRC implemented into security is the voice of a unified whole that lacks central authority but compensates with efficiency and consensus. Although the world of crypto is an evermoving target, establishing best practices, attracting key opinion leaders (KOLs) as well as supporters is paramount. The CYBR token itself shall derive much of its utility by the provision of tokens to active members who can successfully identify and report threats. From a business standpoint, this "open-sourcing" of security creates an enviable dataset and encyclopedia of intelligence.

All this leads CYBR to lay claim to an overused buzzword. Although the word "ecosystem" is bandied about in tech circles, let us remember what the definition actually states:

Ecosystem *a biological community of interacting organisms and their physical environment. (In general use) a complex network or interconnected system* and this is precisely what CYBR's governance is:

- CYBR offers incentives to subscribers whom:
  - o Successfully identify threats
  - o Provide actionable intelligence
  - o Offer needed fixes
  - o Detect and report threat-related activities
- Intel is then verified
  - o If criteria are met, data is analyzed, and ranked.
- Ranking is based on risk factor as determined by programmed AI algorithms.
- Done in real-time with signature lists updated automatically.
- Once processed and identified, the information is disseminated to subscribers.


op: 1px solid #ccc !important;}
ft;}
index: 10;}
der: 1px solid #ccc !important; border-radius: 4px; overflow: auto !importa
user-select: none; user-select: none; transition: all 0.5s ease-out 0s;
ut 0s;}
(0,0,0,.2)}
CYBR

Digital File Fingerprints

Any File Type, Any Language, Anywhere

BlindSpot can see through the polymorphic camouflage used by the world's most advanced hackers. Utilizing digital file fingerprints and leveraging an adaptive brain, BlindSpot locates partial matches within the files on endpoints including systems, servers, laptops, desktops, USB drives, and even mobile devices. BlindSpot is also designed to monitor traffic flowing through the network (available in subsequent release).

Most attacks happen weeks or even months after initial penetration. Even the simplest attacks tend to have a fuse that is typically several days. To map out a system, probe for information, and obtain or forge credentials takes time. However, the moment malicious tools land on a network, BlindSpot sees them even if the files are not copied to your systems. BlindSpot is preventive as it identifies and alerts of merely potential illicit activities before Zero Day.

BlindSpot reveals concealed hacking tools, even fragments of more complete sets.

The software continuously monitors file activities from an endpoint searching for digital fingerprints. Whenever it finds partial matches of any file type, in any language, it is reported back and kept in perpetuity on a temporal repository. The constantly updated database of known malicious files and hacking tools locates and alerts subscribers to any indication of hacking, malicious files, or illicit activity.

Just like with humans, once a fingerprint has been taken, you no longer need the person to identify them. Even a partial print is enough, and sometimes a smudge will do. Once BlindSpot has taken a digital fingerprint of a file, the file is no longer needed to identify it. And they are tiny even a multi-gigabyte file has a digital fingerprint that is no larger than 10KB.

BlindSpot can identify matching files even when the digital fingerprint is only partially there. With advanced processing capabilities, file fragments, recovered data from a hard drive, partially downloaded documents, damaged files (both intentional and accidental) and other incomplete file structures can be properly fingerprinted in a way that still allows matches to be found.

CYBR Real World Application

System Compliance

All Government systems go through Certification and Accreditation. BlindSpot offers malicious code protection, for both security considerations and required compliance. Guidelines found in NIST 800-53 Revisions 3+ Security Requirements for System Integrity, SI-3 Malicious Code Protection, state that malicious code protection mechanisms must be employed at information system entry and exit points, including workstations, notebook computers, and mobile devices, to detect and eradicate malicious code. BlindSpot's continuous monitoring and updating of its known malicious file repository, provides the required real-time and monthly re-scans of files. It also alerts appropriate staff when malicious code is found, provides reports on potential malicious files, illicit activity, and offers follow-up with brief false positive reports (less than 0.01 per cent). BlindSpot helps organizations meet the mandated security requirements while ensuring continued compliance.

Intellectual Property Protection

Track sensitive information as it changes and moves around the enterprise.

Government entities and corporations are addressing the issue of monitoring documents. Files that contain sensitive information or intellectual property can no longer be safely stored on a secure server with the only requirement for access being perfunctory credentials. People either unwittingly or with malicious intent copy and paste parts of documents, move files to USB drives, transfer files onto a laptop, share them with co- workers, or exfiltrate confidential information to outside networks and systems. BlindSpot carefully guards networks, and can even track USB drives. BlindSpot can send alerts regarding questionable activity with specified documents/files, with specific computers or even individual activity.

It is a sensitive information watchdog that catches both unintentional and malicious exposure to non-secure systems. BlindSpot will create a set of digital file fingerprints that can track across networks and systems, ensuring the proprietary and sensitive information for organizations, 365 days of the year, 7 days a week, 24 hours a day.


CYBR

CYBR Ecosystem Overview

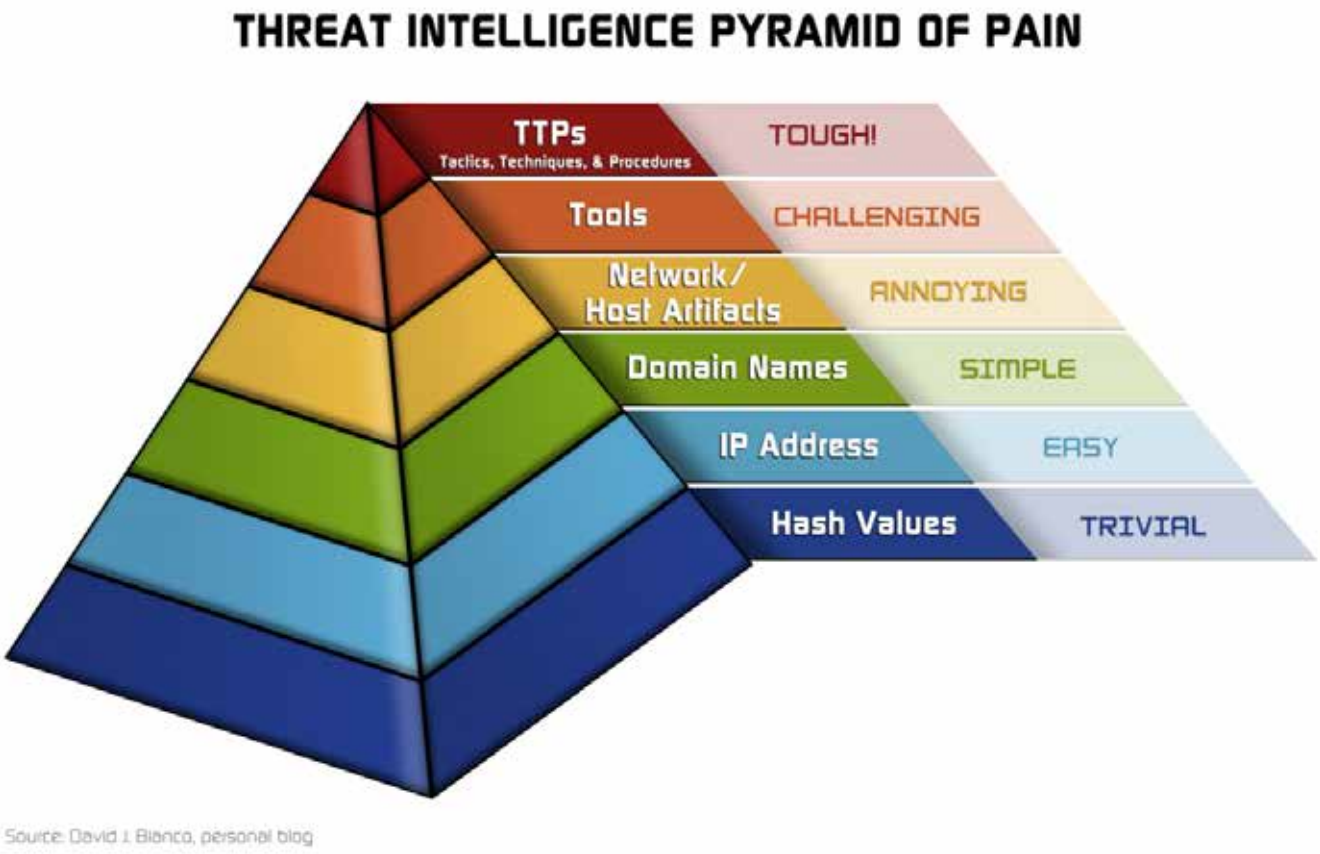
Information technology systems face danger every day, as do smart contract transactions and any blockchain project in existence. Hackers work around the clock in an effort to infiltrate systems, steal tokens, take control of systems, and perpetuate and other of the litany of nefarious motives the mind can conjure. Most importantly perhaps, they seek to steal investments from wallets and exchanges.

The CYBR Ecosystem is holistic; arithmetic from part to whole. Via a portal that provides real-time safeguards, countermeasures and threat intelligence coupled with Blindspot, it is a proprietary, powerful cyber security engine that identifies and disrupts bad actor and associated illicit file activity. It essentially identifies anything that seeks to affect the confidentiality, integrity and availability of crypto smart contract transactions.

CYBR Ecosystem:

- Identifies and disrupts evolving threats to blockchain-based transactions.
- Detects advanced and polymorphic threats that seek to circumvent detection by existing safeguards and countermeasures.
- Ensures safe transactions by vetting token addresses.
- Near synchronous feed of information: emerging threats, new attacks, phishing sites, bad actors and more.
- Two years of development with current product sales .
- Automated and scalable.

In the world of cyber security, associated threats and necessary solutions are typically described in what is commonly referred to as the “threat intelligence pyramid of pain” as pictorially represented below (Figure 1):



The keys to a viable cyber security solution includes four core components:

1. Holistic: infrastructure protection in totality.
2. Countermeasures and safeguards provide proactive security.
3. Timely threat identification.
4. Immediate transition from data to actionable intelligence.

The Blindspot software and CYBR Portal offer the technological capability to meet these requirements.


CYBR

The CYBR architecture primarily consists of two (2) key components:

1. Web Portal
2. BlindSpot

Web Portal

The CYBR Web Portal serves as the CYBR Community User Interface (UI) for the Ecosystem solution. It offers a holistic solution that ensures the cyber security of smart contract associated transactions and its threat intelligence can be used to contribute to the security of the blockchain. There are numerous features and capabilities associated with the CYBR Web Portal. At a high level, they include:

1. Threat Intelligence
2. Verification
3. Token Sending/Receiving Capability
4. Downloads
5. Support Page

These are currently broken down into subset capabilities, which include:

1. Threats
   a. New Threat Advisories
   b. Search Threat Intelligence Database
   c. Threat Intelligence Feeds
      i. CYBR
      ii. Partner Feeds
2. Verification
3. Verify Token Address
4. Verify Website
5. Send/Receive
   a. CYBR Wallet Details
   b. Send Tokens
6. Download BlindSpot
   a. Windows
   b. OSX
   c. LINUX
   d. IOS
   e. Android
7. Support
   a. FAQ
   b. Knowledge Base
   c. Contact Us

CYBR Wallet

The CYBR Portal also offers a proprietary CYBR Wallet, which incorporates a Token Name Service ("TNS"). The unique TNS feature resolves and reduces public addresses to common names. This provides users the ability to send tokens to known, vetted persons and entities without the concern of sending to incorrect or bogus addresses.

The wallet also includes a facial recognition and biometric (fingerprint) capability, which allows smart contract transactions (send/receive) to occur without the need to enter the private key or the incorporation of a mask (e.g. Metamask). Private keys are NEVER compromised when executed in this fashion.

This capability is exclusive to the CYBR Ecosystem.

BlindSpot

Hackers share and use a variety of tools and techniques to gain and maintain access to crypto and similar associated systems. The most noteworthy and effective technique are advanced persistent threats.

As mentioned earlier, APTs exploit vulnerabilities in systems that traditional cyber security technologies are ill-equipped to deal with. Hackers can now actively camouflage their tools by changing known malware signatures into new files. Without known signatures, this poly-morphic malware exploits a gap in most current file detection systems, leaving enterprises open to exploitation.

Traditional signature-based systems simply can not compete, They are estimated to be only roughly 25 per cent effective in contending with APTs.

BlindSpot, even as the files morph and change, sees through it all. It is an adaptive security solution and the heart of the CYBR Ecosystem. It sees through the polymorphic camouflage used by the world's most advanced hackers.

Note: A deeper dive into the technical specifications can be found in the CYBR "Yellow Paper".


CYBR TOKEN
CYBER SECURITY ECOSYSTEM AND UTILITY TOKEN
CYBRTOKEN.IO
CYBR

CYBR – The Company

It is imperative that a company, crypto or otherwise, ensures the profitability of the company to give return on investment (RoI) for its investors and stakeholders. Stated bluntly, revenue counts. Too many "companies" in the crypto space today will fail because they will not be able to establish a profitable business model.

CYBR Past Performance

CYBR has existing, world-class partnerships in cyber security and blockchain. The company currently holds over US$6 million in task orders for the Department of Homeland Security (DHS) DOMino program, a US$1.115 billion Indefinite Delivery Indefinite Quantity (IDIQ) contract as a subcontract to Raytheon Corporation. CYBR's past and current clients/partners include but are not limited to:

Partners

1. Raytheon
2. General Dynamics Information Technology (GDIT)
3. Lockheed Martin Federal Systems (LMFS)
4. Dell
5. Hewlett Packard Enterprise (HPE)
6. ManTech
7. Science Applications International Corporation (SAIC)
8. XYO Network
9. UNICOM (formerly GTSI)
10. DEI
11. EdgeSource
12. American Systems
13. 21CT
14. Paragon
15. Channel Systems
16. Trigent Solutions
17. Stratford University
18. Eastern Michigan University

19. Western Kentucky University.
20. MKM Global
21. Cognizant
22. Campbell and Company (Abu Dhabi)

Customers

1. Department of Homeland Security (DHS)
2. Department of Defense (DoD)
3. Department of Transportation (DoT)
4. Department of Energy (DoE)
5. Department of Interior (DoI)
6. Federal Bureau of Investigations (FBI)
7. Joint Terrorism Task Force (JTTF)
8. Internal Revenue Service (IRS)
9. U.S. Mint
10. Office of the Comptroller of the Currency (OCC)
11. Federal Reserve Board (FRB)
12. Federal Reserve Bank (FRb)
13. Health Resources and Services Administration (HRSA)
14. Accenture
15. DMR
16. BioMerieux
17. CareFirst Blue Cross and Blue Shield
18. Stratford University

As a result of these relationships, CYBR is able to apply for grants and funding which are not insubstantial, often into the millions of dollars. Such funding will allow CYBR to create and update a word class cyber security solution that can transcend the blockchain and potentially disrupt the entire cyber security industry.

Ultimately though, CYBR believes it can help the individual, especially in the blockchain space. Crypto wallets are at risk, mobile devices running crypto apps are fraught with peril as evidenced by a recent US$224 million lawsuit against AT&T regarding the alleged theft of some US$24 million via a mobile device. Even two-factor authentication does little to mitigate these risks. The company believes that establishing itself in the B2B market will pave the way for consumer adoption.

Additionally, the company is involved with numerous global consortiums and recognizes the importance of proof of concept. CYBR will endeavor to provide protection for crypto organizations and enterprises through current solutions and emerging technologies, provided by an Internal Research and Development (IR&D) and Center of Excellence (CoE).

Core Competencies

There are almost as many potential types of hacks as there are hackers. Among the better known are simple web defacement, flooding, brute force attacks, SQL injection attacks, and OS command. The need for intrusion detection is commensurate with the traffic and diversity of the network itself. Irrespective of size, scope, breadth, and depth, BlindSpot's proprietary capabilities coupled with a real time data feed and bolstered by communal support (the open source factor), ensures there is no job beyond the company's scope.

CYBR shall endeavor to be known as the "guardians of the blockchain" and below is a highlight list of existing capabilities.


CYBR

CYBR Functionality

Aerial Overview

- CYBR threat intelligence protects subscribers from malicious attacks.
  o Guards against Zero Day attacks and advanced persistent threats.
- CYBR can incorporate with existing networking, be it customized or out of the box, with limited configuration changes.
- CYBR's threat landscape meets regulatory and compliance standards.
- CYBR's B2B partners provide proof of concept to individual users.
- CYBR is poised to deliver a B2C solution to "normies" entering the space.

Community and Token:

- CYBR's community are global watchdogs for the network.
- CYBR's community provides a key utility for the CYBR token.
- Contributors can earn CYBR tokens for identifying verified, evaluated risks.
- Allocations are contingent upon "degree of difficulty," and level of threat.

Holistic

- CYBR's BlindSpot, data feed and community shall prevent, detect and respond to qualified threats.
- CYBR's compendium of threat intelligence shall be continuously updated and deployed to subscribers.
- CYBR's solution a seamless continuum of threat detection that integrates with existing networks, irrespective of customization.

CYBR's Heartbeat

CYBR's BlindSpot software is currently powered by a fuzzy logic engine that will also incorporate the latest in AI and machine learning technologies to maximize pattern matching and heuristics capabilities.

- Fuzzy logic guards against APTs and identifies threats using proprietary weighted algorithms. (Much like a drone were it properly used)
- Support Vectors/Predictive Modeling
  o Vectors of attack continuously change

While understanding yesterday's attack can be helpful, it does not guard us against tomorrow's. Thus the need for technologies that can "time travel."

Platforms

Blindspot will be available for the following Operating Systems (OSs):

1. Windows (10 and up)
2. OSX
3. Linux
4. IoS
5. Android

Note: BlindSpot is also available as a Software as a Solution (SaaS) and Client/Server solution. Customized development is available upon request.

Application Plug-In (API) and Indictor of Compromise (IoC) Funnel

BlindSpot can also be customized for existing platforms and frameworks. The data feeds can leverage existing delivery mechanisms (i.e. AV) and function as:

1. API
2. IOC Funnel

Not So Neural Intuitive Networks

Artificial neural networks are comprised mostly of simple processing nodes that provide a feed-forward, which transmits data in a single direction. A unilateral process is actually quite limited. Although the name sounds compelling, BlindSpot's fluid exchange is much more dynamic and ultimately effective. Additionally, the network is continuously being entrained to all new verified information and is more representative of a developing system.

BlindSpot acts as the cell body, signaling the data feed and community, which serve as "dendrites," delivering and receiving information to and from BlindSpot via a synaptic highway. BlindSpot would also signal the "axon" to deliver validated information to subscribers.

CYBR Functionality

Demonstrating Efficacy

CYBR's intelligence portal shall receive high volume data that relies on an ability to quickly detect and assess threat agents. This information is sent to subscribers in order to prevent systems from being compromised. A "best-of-breed" threat intelligence engine is mission critical. CYBR's existing relationships in the field can assure subscribers that their data feed will be nonpareil.

Assessing Efficacy

Much like a truth verification algorithm in oracles, threat intelligence data must be received from multiple sources and interpreted. Machine learning, AI, and experience are great tools to convert information into actionable intelligence. For many security concerns, though, it is also the proverbial bane of their existence.

Assessment and understanding still belongs in the realm of human thinking and nothing can take the place of experienced personnel. Parsing through information and high traffic data feeds from virtual security checkpoints in an effort to identify and determine intrusions can be likened to attempting to find a white rabbit in a snowstorm. Optimizing systems for threat identification and continually compiling and archiving data are best practices, but lesser practitioners and solutions will overlook vital information.

The Company's experience in managing threat intelligence platforms and their unrivaled access to robust data feeds, normally reserved primarily for government agencies and Fortune level companies, offers a leg up on its competition.


CYBR

CYBR Team

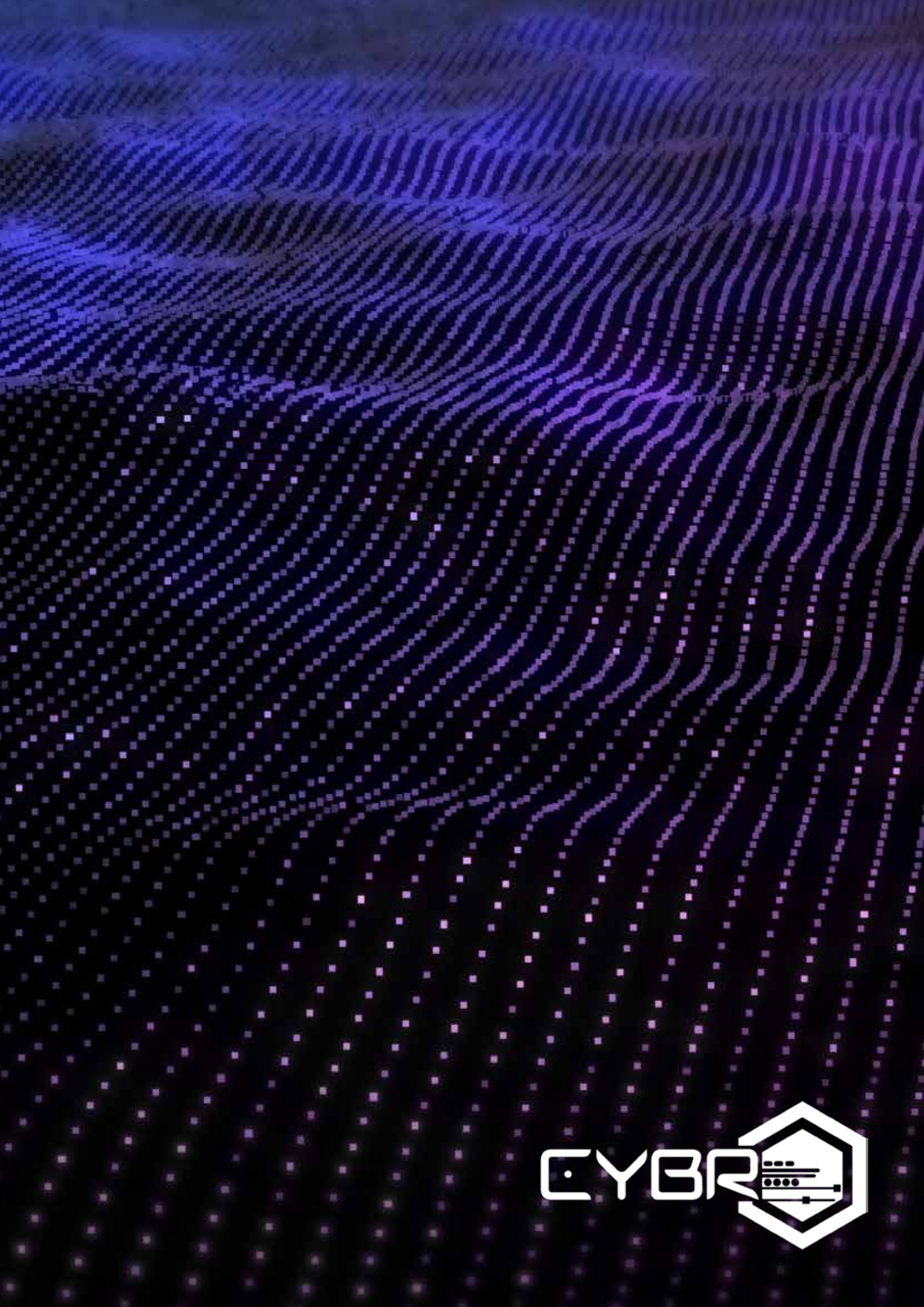
CYBR's team of executives, staff and advisors bring combined 125 years of cyber security, blockchain and information technology experience. Complete bios and profile information can be found on the main website (cybrtoken.io).

Executives:

- Shawn R. Key – Founder
- Frank Corsi – Chief Technical Officer
- David Donnenfeld – ICO Advisor
- William "Todd" Helfrich – Cyber Security Advisor

Staff/Advisors:

- Dr. Amini – Advisor
- Dr. Mohammed Moussavi – Advisor for International Relations
- Adam Peterson – Director of Marketing
- Rich Berkley – Investor Relations/Social Media
- Mark Stanwyck – Ecosystem and Technology Advisor
- Gerald "Skip" Lawver – Cyber Security Advisor
- Darron Tate – Public Outreach
- Devin Leshin – Branding
- Simon van der Leek – Designer/Webdeveloper
- Kim Moyer-Crabtree – Public Relations
- Hunter Key – Economic Analyst


CYBR

Roadmap

2016-2017

2Q 2016 - 2Q 2018

- East Coast office opened (Virginia)
- BlindSpot Enterprise Solution is developed and rigorously tested
- Larger pilots are deployed
- Enterprise sales generate revenue

2018

2Q 2018

- The detailed design description for the CYBR Ecosystem is completed
- Over 30 Million unique, digital identifiers are added to the BlindSpot database
- The Software as a Service (SAAS) model is repurposed for the blockchain and the CYBR Ecosystem Testnet begins development
- CYBR utility tokens are generated

2018

3Q 2018

- CYBR Presale
- CYBR TGE (Token Generating Event.)
- CYBR Testnet will be completed and BlindSpot will be accessible by Windows, Mac and LINUX users
- CYBR will be listed on top exchanges for global trading
- Open West Coast Office

2018

4Q 2018

- IoS and Android client development will be completed
- Web App, API and IoC funnels development will be completed
- Web migration to Dreamweaver

Roadmap

2018

4Q 2018

- IoS and Android client development will be completed
- Web App, API and IoC funnels development will be completed
- Web migration to Dreamweaver

2019

1Q 2019

- CYBR Main Net will launch
- Open overseas office(s)

2019

2Q 2019

- Integration of numerous data intelligence feed providers; (some partnerships already in place)
- Integration of AI and Machine Learning platforms and frameworks into CYBR Ecosystem (some partnerships already in place)

2019

3Q - 4Q 2019

- CYBR will market globally to disrupt and dominate anti-virus and malicious code vertical marketplaces

2020

and beyond

- Assess technology posture/market conditions; drive CYBR into as many global market verticals as possible.

CYBR Token

CYBR Tokens are designed to incentivize and provide functionality for the three-pronged CYBR solution. Subscription services and the provision of blockchain related services will be solely transacted utilizing CYBR Tokens. Rewards for CYBR community members will be a determined allocation of CYBR Tokens. CYBR is a standard ERC20 smart contract-based token running on the Ethereum network and is implemented within the business logic set forth by the Company's developers.

CYBR Token Utility and Pricing Model

The CYBR utility token is redeemable for usage with BlindSpot and global threat intelligence feeds. The CYBR initiative provides protection to individual networks, SMEs and large-scale enterprise users. Intelligence feeds are based on risk scores; packaged in a series of products/services and delivered via a subscription model which can provide:

- Assessed zero-day global threat feeds o Json, CSV and XML formats
  o Utilizing IP tables firewall rules
  o Magento, Wordpress and related plugins
- Global threat intelligence reports
- Email alerts
- Mobile apps
- API key to access CYBR via apps/dapps

Data feeds will be based on number of user licenses, to be purchased on a yearly-based subscription model. Special needs assessments, customized solutions, or any appliance applications can be purchased at an additional cost.

The CYBR business model is simple: a subscription-based value-added service with recurring revenues. The company has identified a number of ancillary revenue streams, ranging from customized packages to the sale of propriety and modded hardware devices. However, it should be noted that the potent solution that is BlindSpot will drive our quest for adoption.

Threat Intelligence Community (TIC)

Individual users and companies interested in earning CYBR tokens, are welcome to join the CYBR Threat Intelligence Community (TIC).

CYBR tokens are required to access the CYBR portal which offers the official download for BlindSpot, CYBR's proprietary intrusion and malicious actor detection software.

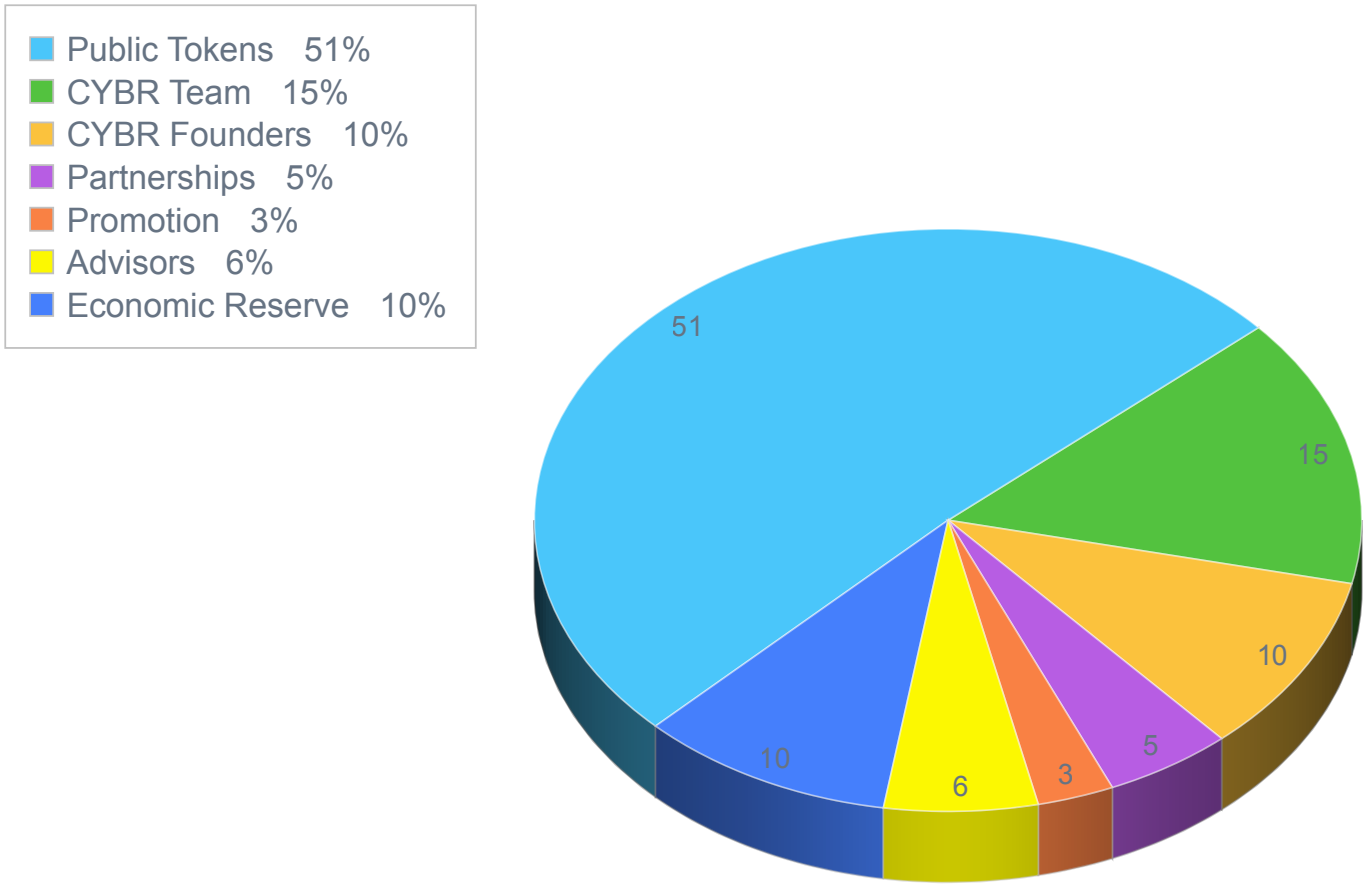
CYBR community members that have captured verified, evaluated risks, or threat, that is, information deemed valuable at the Company's discretion, and have shared said data with CYBR, may earn a reward.

Although no risk-scoring metrics are currently in place, the Company feels it is capable of assessing the information accurately. Thus, rewards shall be contingent upon "degree of difficulty," determined by the level and uniqueness of threat and/or intrusion.

CYBR tokens can also be earned by key opinion leaders, community leaders, or shared for promotional purposes. Others who submit suspicious network information may also qualify.

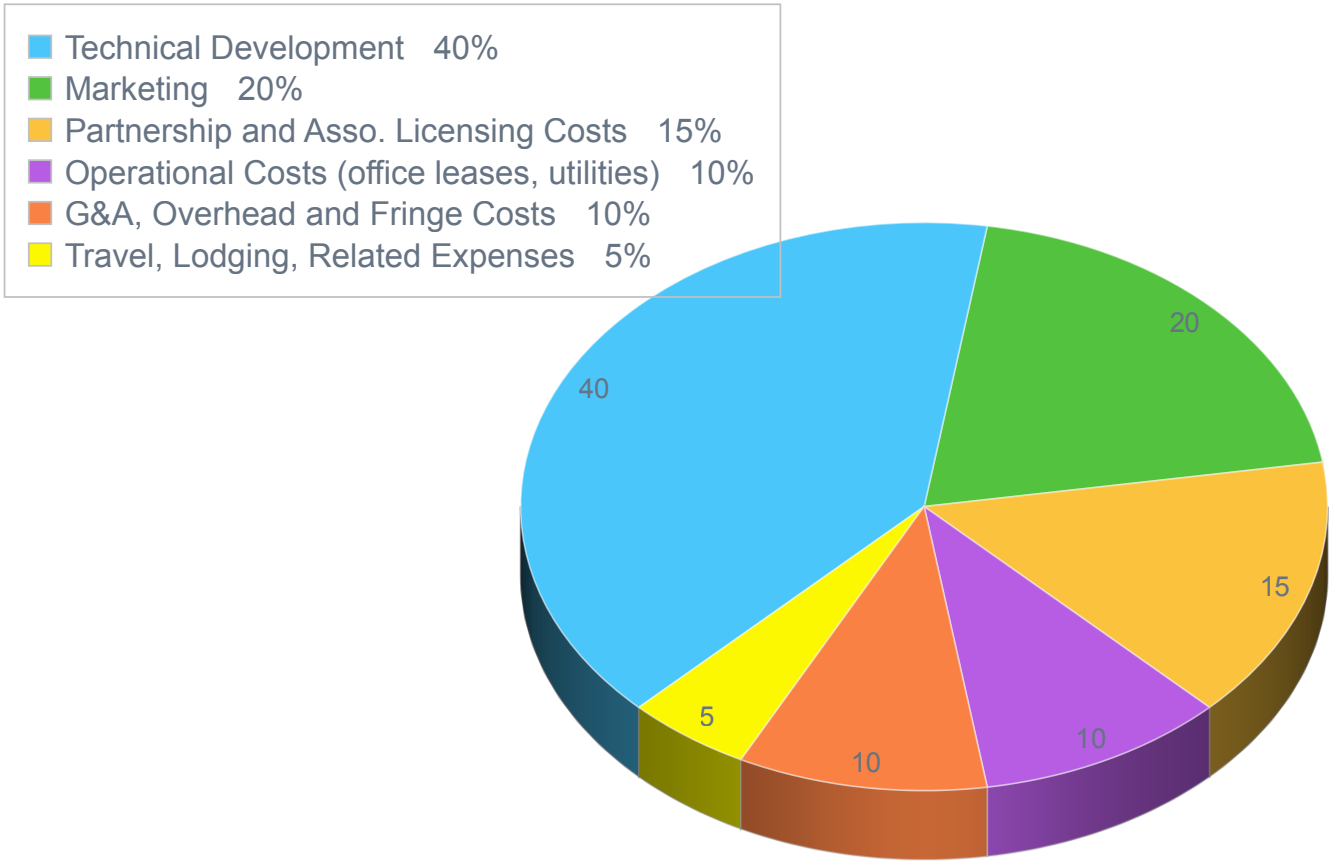
Tokenomics and Token Generation Event (TGE)

Equity Division



- CYBR has a total supply of one billion (1,000,000,000) tokens.
- The softcap is set at two million dollars (US$2 million) with an associated hardcap of fifteen million dollars (US$15 million).
- The CYBR token is priced at eight cents (US$0.08) per token.
- The TGE is slated to commence in October 2018.
- Founders' tokens will be locked for one year and large investors' tokens are locked for a minimum of six months.

Use of Proceeds



CYBR's Token Generation Event consists of a pre-sale and subsequent public event. The stated dates are estimates and and as subject to change, subject to extensions, and to early termination.

- The soft cap shall be US$2,000,000 (US$2 million) and the hard cap shall be US$15,000,000 (US$15 million), although CYBR reserves the right to seek additional funding.
- 1 CYBR Token = $.08*

*Structured bonuses and pooled allocations incentives are to be determined and announced.

Smart Contract Address BACK UP

The CYBR Smart Contract is: **0xb8ce3982d9b6757e27527f1f9b79ed5c299fe639**

Token Delivery BACK UP

CYBR tokens shall be distributed via a smart contract to the Ethereum address that was used to participate in the TGE. Upon completion of the event, the CYBR tokens shall remain locked to avoid any secondary market trading activities.

Ongoing Development BREAK

The continued development of the CYBR ecosystem is a considerable allocation of resources. Adapting BlindSpot and the key components of support may be assigned to the core CYBR team and remuneration shall be necessary. Temporary and full-time staff will likely be comprised of cyber security, engineers, developers (both blockchain and software), infrastructure architects, AI engineers, data specialists, customer service, support, marketing strategist, and so on.

Testing and Maintenance

Additional resources will be expended on the upkeep and testing of the CYBR platform. Given the nature of cyber security, testing is extremely thorough and often ongoing. Maintaining the integrity of our product offering is paramount and nothing will be released without taking needed precautions and assurances. There is also a relatively constant need to hone as well as maintain, and even upgrade, both software and hardware. These shall be part of operational costs.

Business Growth and Development

CYBR anticipates transitioning its focus from the B2B to the B2C sector. Certainly, the marketing and promotions of products and services is a notable consideration. The Company believes that the eventual adoption of crypto for individuals portends a market that will be underserved. Any sales and marketing is designed to support the manageable growth of the CYBR solution. CYBR feels poised to offer a cost effective, accessible platform that will appeal to the masses. Our focus on SMEs, blockchain projects, and public sector work will expand to include individual users. It is our goal to secure long term security contracts with these potential customers. CYBR is wholly confident in its ability to deliver a superior product to the end-users that will also provide a reduction in costs. Again, all transactions and subscriptions shall be made using CYBR tokens.

Token Generation Event (TGE) is subject to a Terms of Sale provision which will be published separately. Please refer to cybrtoken.io for further information. The website implements special features restricting access to TGE until all terms, conditions, and rules are explicitly and clearly accepted.

References

1. 50 BTC Mining Fees
   https://www.blockchain.com/btc/tx/d38bd67153d774a7dab80a055cb52571aa85f6cac8f35f936c4349ca308e6380
2. https://www.govexec.com/magazine/1999/04/information-insecurity/5989/
3. https://www.cnbc.com/2018/08/15/cryptocurrency-investor-sues-att-for-224-million-over-loss-of-digita.html

Disclaimer

CYBR IS NOT A SECURITY. THIS DOES NOT CONSTITUTE AN OFFER TO SELL OR A SOLICITATION OF AN OFFER TO BUY “CYBR” TOKENS. THE INFORMATION CONTAINED HEREIN IS PROVIDED FOR EDUCATIONAL PURPOSES ONLY.

CYBR is a utility token that is the exclusive form of payment that will be accepted to purchase services and subscriptions that CYBR offers.