GBMSTECH

SECURED BUSINESS CONTINUITY

Accumulus Threat Shield

Consensus-based blockchain driven cybersecurity threat protection

WHITEPAPER

Accumulus Threat Shield

GBMS Tech Ltd whitepaper:

Accumulus Threat Shield

Consensus based blockchain driven Cyber Security threat protection.

A breakthrough cybersecurity platform for everyone built with blockchain technology and incentivised onboarding through token rewards.

"Prevention is better than cure"

– Desiderius Erasmus

Abstract:

In an ever more technical world, the cyber threats we face are becoming more diverse and more advanced. To provide a sustainable level of protection organisations need to pool resources and change approach in order to find solutions which really make a difference.

We know that traditional cyber security methods of scanning for threats will never be 100% effective because even with heuristic technology which enables systems to identify previously unknown threats there will always be new threats which go undetected and can effortlessly bypass all security protocols.

GBMS Tech Ltd ('GBMS Tech') has developed a new cyber security as a service offering which uses a paradigm shift in cybersecurity and works inversely to the scan/detect/remediate model.

By combining this already developed product and expanding it with a hive mind, using the data integrity of blockchain and a new incentivised adoption method to ensure penetration we aim to put an end to breaches.

To bring about this global shift in cybersecurity we needed to bring together key technological ingredients that up until now simply weren't available.

- A breakthrough product recently developed and in use (by GBMS Tech).
- A revolutionary threat detection system.
- A hacking and manipulation proof threat/reputation system using decentralised blockchain technology.
- AI-driven threat analysis.
- An incentive system to drive adoption using cryptocurrency/token rewards delivered via algorithmic microtransactions.

Now that these technologies are available GBMS Tech will develop the Accumulus Threat Shield which will not only offer superior protection and threat blocking but through its Spartan AI-powered hive mind (secured through blockchain technology) and monetary incentives to drive adoption, will cause organic passive effects like herd immunity effect and the disincentification of nefarious activity.

Who we are:

GBMS Tech is a UK-based global cybersecurity company founded on the principle that in a world of increasing cyber attacks, preventing breaches is a far better option than curing them.

GBMS Tech secured business continuity technologies provide proactive cybersecurity protection that is radically different to traditional reactive cybersecurity technologies available today.

We design cybersecurity systems which not only eliminate the risk of a failure to regularly update the threat management systems, (in most cases this is human error) by changing the paradigm and creating a new kind of protection which does not rely on the identification of malicious code.

Our technologies protect the host from all 'unknown' and 'zero day' viruses, unlike existing traditional anti-virus software.

The concept is simple: if a virus and malware are rigorously stopped from infecting the host system, they cannot spread and infect, if hackers cannot enter the platform they cannot disrupt it. GBMS Tech Secured Business Continuity technologies integrate fully into the Microsoft Windows operating systems and

provide preventative protection capability.

GBMS Tech prevents all malware; including crime-ware, ransom-ware, spyware, phishing and web robots from infecting the host by using a proprietary non-scan based protection methodology to secure the host and a unique internal and external threat detection process to shut the door on employee data theft and network attacks. Please see case studies; https://www.gbmstech.com/cyber-securitycase-studies-success-stories-of-gbms-tech/

GBMS Tech has been tested by the cyber security underwriters for Lloyds syndicate and proven so successful that they offer a significant discount on cyber security policies for companies that adopt GBMS Tech protection.

Our technology also reduces processor load, ensures systems run at peak performance and saves energy, which is why it has been chosen as a partner for Cool DC data centres... innovative new eco-friendly data centres.

The problem

Anti-virus systems and traditional products that scan and identify malicious code are not effective at stopping new threats and the efficiency drops significantly when their systems are not properly maintained or simply through human error.

The bad news about cyber security breaches just keeps coming:

October 2017; 3 Billion Yahoo accounts hacked. source

$2.4 million - Average cost of malware attack spend and the top cost to companies. source

2017 Cryptojacking Attacks Explode by 8,500 Percent from 2016 source

Cyber-attacks are the third most likely global risk for 2018, behind extreme weather conditions and natural disasters. source

Over 169 million personal records were exposed in 2015, stemming from 781 publicised breaches across the financial, business, education, government and healthcare sectors.

– "ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC source

The median number of days that attackers stay dormant within a network before detection is over 200.
– "Microsoft Advanced Threat Analytics" | Microsoft

74 percent of CISOs are concerned about employees stealing sensitive company information.
– "SANS 2015 Survey on Insider Threats" | SpectorSoft

We think it's time the Cyber security segment gets in front of threats instead of reacting to them and such an achievement needs a total rethink of how things are implemented.

The foundation of a new solution

Any ambitious project needs a solid foundation. In this white paper, we'll discuss the fulfilment of the goal by using blockchain technology to expand on a paradigm shift in cyber security which has already been developed and proven in the marketplace.

The product is Trident CMP (developed by GBMS Tech). It uses a different approach to successfully provide a high level of protection through a combination of AI and man-monitored services which accurately provide network protection against threats and can efficiently lockdown a system to prevent breaches and attacks.

Our technology offers best in class security and facilitates data protection regulation compliance through a unique combination of features which allow administrators to quieten attack noise and block unwanted traffic, even if they break through a firewall or aren't recognised by antivirus.

Blockchain will allow expansion of the functionality of Trident to create a platform which protects all participant systems and allows people to benefit from a 'hive mind' where each device benefits from the discoveries made by the others.

Expanding via blockchain and open source

In this Whitepaper, we outline a case for the improved speed and certainty of the development of our solution, because it is mostly composed of technology that is newly developed (already available) and proven past the concept stage.

GBMS Tech Ltd has developed and deployed an enterprise-grade cybersecurity service which includes a proprietary network monitoring device with best in class accuracy and combines it with host protection for complete security. This service is designed to scale from start-up customers to the largest enterprises.

GBMS Tech Ltd will take this breakthrough cybersecurity service and expand its capability by creating a free and open source service able to provide increased cybersecurity to everyone. This means that all device users benefit through consensus-based authentication, made possible by a distributed blockchain ledger of identified threats.

After two and a half years of product development, testing, and proven commercial application, we can draw upon this technology to create a professional paid service offering superior security to clients whose efficiency is magnified by the assistance of both free and open-source users of consumer devices who received commercial grade security and potential rewards. The free consumer version will only omit the monitoring, compliance and remediation services that professional users require.

Realising maximum effect through a charitable attitude

In the eyes of today's connected world, there is much to benefit from a selfless attitude towards the greater community of users. There is a synergy involved with providing an exceptional commercial product which encompasses the compliance and reporting features businesses need but also supports the development of a consumer version available to all.

One of the biggest places cybersecurity can win is by reducing the profitability of hacking by increasing the difficulty & cost on every device. With a community-based approach to cybersecurity, we can achieve the goal of better protection, wider adoption and a demised profitability for hackers which will organically encourage these smart and creative people into any myriad of more lucrative legitimate pursuits.

Product expansion and implementation, Developing the next step: The Accumulus Threat Shield Ecosystem

Accumulus Threat watch is the next step in the cybersecurity development by GBMS Tech, our initial product offering Trident CMP (Cybersecurity Monitoring Platform) is a breakthrough because it offers a level of efficacy so high, as to be being considered by any reasonable measure impenetrable. By using a paradigm shift in the approach to cybersecurity and ensuring the scan, detect and remediate model for a system level block, that simply thwarts the execution of any unauthorised code. This is coupled with a man-monitored threat detection service which locates both external and internal threats (employee data theft) with the protection and reporting required in a GDPR world.

As a stand-alone system, it is limited in that the information stored is segregated per client. While we feel that segregating the data is important in this age of data breaches, consensus-based blockchain will afford us the ability to expand the product so that multiple nodes can crowdsource threat detection and the resulting distributed threat repository will be integrity-protected through a decentralised ledger.

Our development team understands that there are ways to share data between client data stores to create a broader fundamental picture of the cybersecurity landscape. To use the adage 'one client by itself is dumb, but 10,000 clients grouped together sharing, correlating, fixing, and hardening systems are smart'.

The key ingredient to making this possible is the verification of data integrity afforded by blockchain technology.

GBMS Tech will create a cybersecurity ecosystem protected at the core through blockchain, that will not only be reactionary but will also be preventative to the point of anticipating potential attacks.

Protecting against human inefficiencies

Hackers are continually relying on human error to gain access to their systems, systems administrators tend to create weak passwords, forget to update secure systems, use unauthorized devices, and many other tasks that go against cybersecurity 101. While administrators are not being remiss in their duties, being short-staffed, overworked and constant demands can cause strain on the ability to achieve a successful cybersecurity foundation and structure.

Revenue and Business Model

GBMS Tech will use a subscription-based revenue model in order to engage with SME, Large Enterprises, Nation States, and any other entities that may have a need for enhanced cyber security.

Services can be paid for using ATS Tokens or FIAT currency.

Revenue Stream	Description
Monthly Accumulus Threat Watch License	A monthly recurring license to use the Accumulus Threat Shield at a location that is dependant on the number of computers/assets to be monitored.
Threat Feed API	A Monthly license fee to access the Accumulus Threat Reputation System.
SOC Monitoring	A Monthly license fee to monitor SIEM and other products that are not part of GBMS Tech brand as an outsourced 3rd Party support.
Professional Services and Consulting	Professional Services and consulting fees to implement security systems, validate current security posture, or do post-breach follow up.

An opportunity exists to fill a real gap in the SME market. Typically most cyber security vendors have targeted Large Enterprise organizations while the SME has been largely ignored due to the cost of implementing systems. The Accumulus Threat Shield combined with a proper channel partner program creates a market opportunity to attract a large number of monthly recurring customers in the SME market.

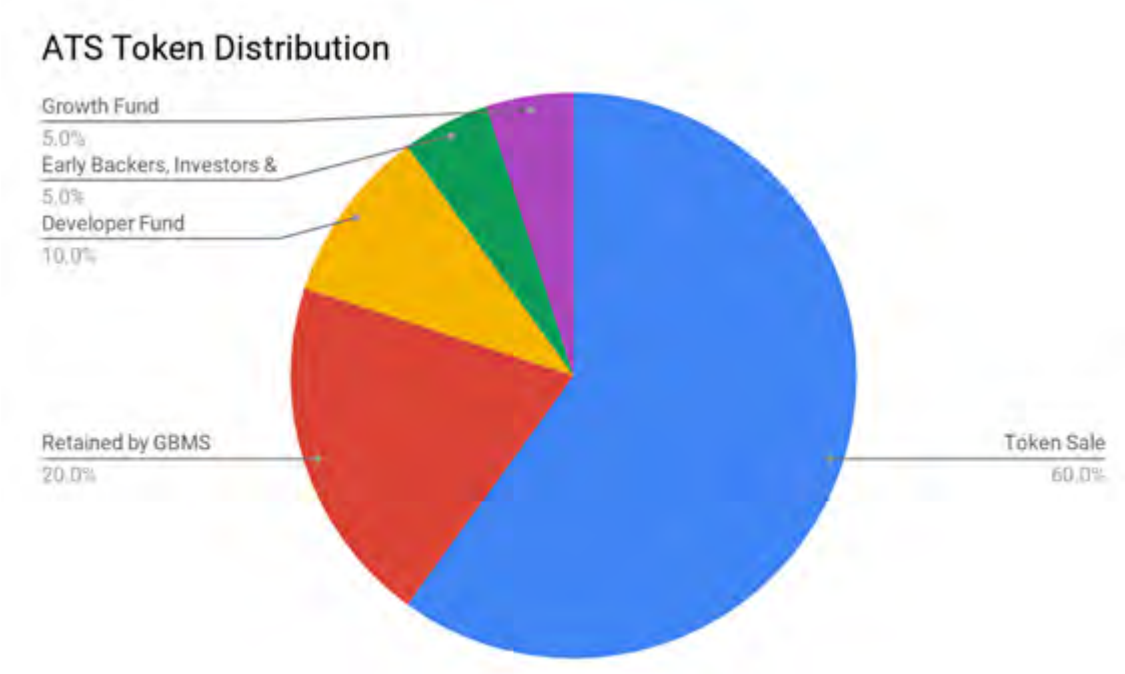
GBMS Tech has the ability to supplement this income by leveraging these channels and end-user relationships to provide professional services and consulting to a large number of SMEs who are poised to purchase services from a trusted expert.

GBMS Foundation

All tokens that are used to pay for services are paid to the GBMS foundation, a percentage share is given back to GBMS, which are burnt. The foundation is set up a DAO with a strict structure for governance that defines the rewards for the Hoplites.

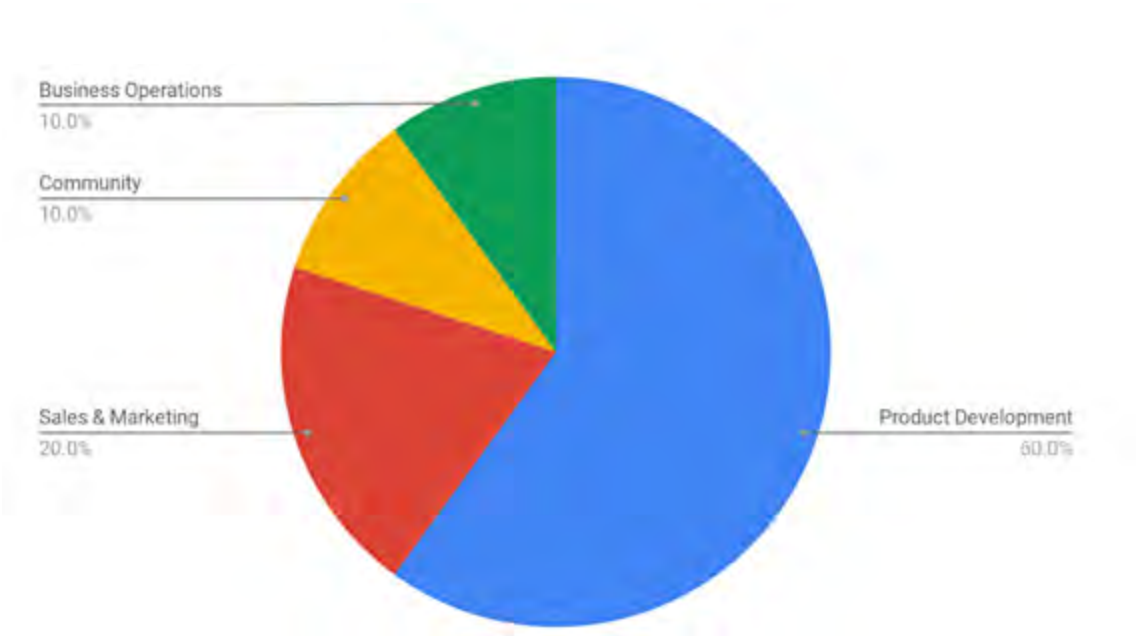
Token Sale

GBMS Tech will be conducting a token sale to raise funds to continue product development and bring to the commercial market. The maximum raise is $15,000.000 USD.



Developer Fund	10%	Used to incentivise and attract outside developers to be part of the ecosystem.
Retained by GBMS	20%	These tokens will be used for rewarding Hoplites who find and validate new threats in the Accumuls Threat Shield System.
Token Sale	60%	ATS Token offered for sale to be used on the Accumulus Threat Shield offering.
Early Backers	5%	Early token holders and advisors who have worked to help develop the technology and ICO offering.
Growth Fund	5%	Used to grow the community around Accumulus Threat Shield.

Fund Distribution



PRODUCT DEVELOPMENT	60%	Used to develop the product, build the product development staff and allow for continual updates.
SALES & MARKETING	20%	Sales & Marketing costs to include trade shows, advertising, PR, lead generation, and webinars.
BUSINESS OPERATIONS	10%	Costs of running business operations and overhead to include legal, compliance, and accounting.
COMMUNITY	10%	Capital needed to drive membership and create a global community around Accumulus Threat Shield.

TOKEN NAME	ATS (Accumulus Threat Shield)
TYPE OF TOKEN	Ethereum ERC-20 Format
USE OF TOKEN	● Externally Tradable ● Used to purchase services from GBMS Tech ● Used for rewarding Hoplites for finding or validating new threats, vulnerabilities.
TOKEN CHARACTERISTICS	Industry standard format used by the majority of tokens. Running on the ethereum network.

The Accumulus Threat Shield Token

Accumulus Threat Shield Ecosystem

The Accumulus Threat Shield compliments the IT infrastructure and provides dependable actionable cyber security intelligence, reporting and action.

The Accumulus Threat Shield ecosystem is not comprised of one product, but a collection of services and products that when combined form a true cybersecurity ecosystem that is unrivalled.

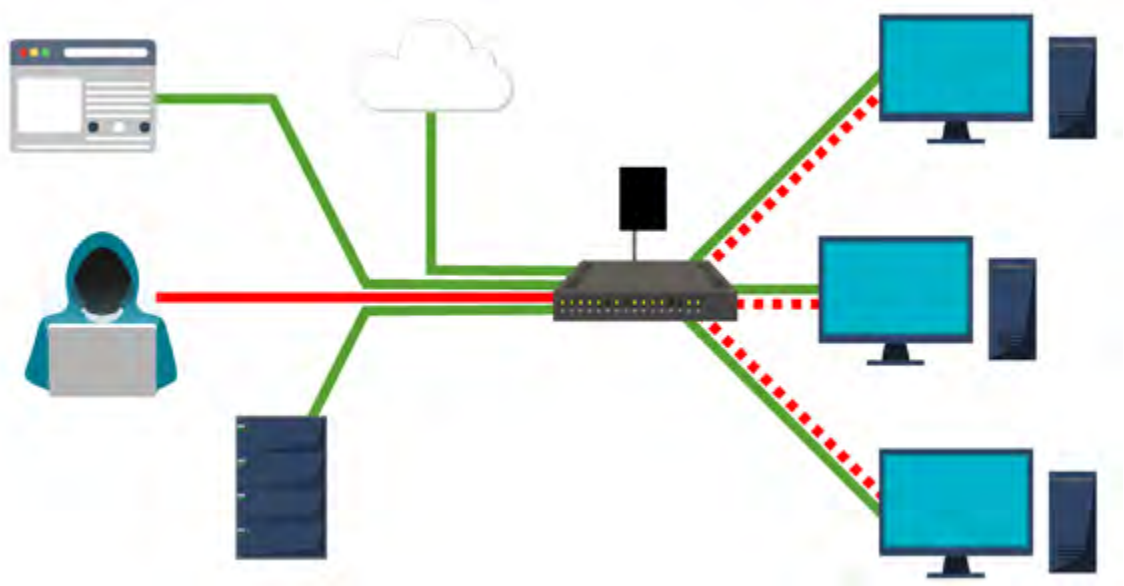
The components of the Accumulus Threat Shield are as follows and described in further detail further in this paper:

- Trident Network Protection and Monitoring.
- The Kraken Firewall.
- The Accumulus Threat Reputation System.
- Spartan AI.
- Token Based Participation Reward System.

Each security component works individually but they will combine to create a product designed to protect and be widely adopted.

Trident Network Protection and Monitoring

Trident Network Protection and Monitoring is the flagship product of GBMS Tech Ltd, consisting of our data collection appliance, dashboard, threat feeds, and security operations portal and is the starting point for the Accumulus Threat Shield.



Components of Trident Network Protection and Monitoring

Appliance: Consists of a deploying physical or virtual appliance that sits on a customer network typically attached to a network span port or tap. Appliance acts as a data collector and ingestion engine at the client site for network data to be analysed. Current physical appliances are based on either small form factor appliances, 1U Rack Server or virtual appliance for cloud readiness.

Dashboard: End-user dashboard that allows clients to view their security devices and the current events, alerts, and metrics related to their network and hosts.

Threat Feed Engine: Hourly curated list of threat feeds ingested into the Trident CMP system.

Database and Rule Engine: Proprietary database schema and rule engine developed to store and correlate security data ingested by the appliance.

The Shield Core

The shield core is a repository of data used by the MESH and Accumulus data that is rendered immutable with blockchain. This information integrity is guaranteed by the decentralisation of the data through a semi-private blockchain maintained by machines across a secure private network.

Blockchain will allow the data to be immune to manipulation either by any kind of wilful alteration from an authorised person (personnel corruption) or through unauthorised access (system breach). Because this is a cybersecurity product all the systems which form part of the blockchain for the purpose of maintaining data integrity will be vetted and approved cybersecurity companies, SOC's, specialists and partners of GBMS Tech Ltd. Of course, all systems involved in the maintenance of the Shield Core data integrity will use Trident CMP to lock down the system.

Overview of the Shield Core

Kraken Next Generation Managed Physical/Virtual Firewall

From small office to enterprise networks worldwide each network has an ingestion point to where the public internet traffic meets the internal network.

The Kraken FW brings in a new era of SOC managed firewalls by combining the firewall with the Phalanx Secure Solutions Trident CMP product. Business often places a firewall in their environment and it ends with the firewall. What they often fail to recognise is that the firewall needs to be updated, the logs must be monitored, and changes need to be made to the firewall on a day-by-day basis, and sometimes in real time requiring significant human resources.

The Managed Kraken FW's are updated so that each FW in the ecosystem is preventing, blocking and learning from each other via the secured blockchain ledger. Using the Kraken FW, GBMS Tech brings in all the components of the Accumulus Threat Shield to keep it hardened.

Trident Network Protection and Monitoring– By sending all the FW traffic and logs into the Trident Network Protection and Monitoring system the Kraken FW is sharing its data so that the human and the Spartan AI SOC team at GBMS Tech Ltd can continuously check for new, old, or potential threats.

MESH Threat Reputation System: All threats recognized by the Kraken FW and the Trident CMP are ingested into the MESH Threat Reputation system which also gathers information from over 100 other online threat repositories, allowing a complete sharing of data.

Spartan AI - Threat Scoring System: The Kraken FW uses the Spartan AI - Threat scoring system to generate its list of potential threats that are potentially a threat.

Spartan AI - Threat Hardening System the Kraken FW uses the Accumulus Threat Hardening system to block ports, countries, IP, rules, or bad actors from passing traffic through the firewall. Once the Accumulus Threat Scoring system trips to a bad actor level, the AI in the hardening system will work to create a rule for all Kraken FW or appliances with the Accumulus Threat Shield Integration system in the mesh network.

MESH Threat Reputation System

The MESH Threat Reputation System (MTRS) handles many problems that are faced in cybersecurity with the two largest problems primarily being security firms keeping centralised proprietary databases of threats and bad actors, and the second being zero-shared resources amongst security vendors to stop threats faster.

The MESH Threat Reputation System will comprise two components the free community version accessible to all via the blockchain and the paid premium version accessible to subscribers with additional benefits and services.

Reputation cannot be determined via one or two sources, to determine the reputation of potential cyber actors one must consider many sources such as Virus Total, Sophos Labs, etc. The problem is when one of these sites has mistakenly identified the traffic as bad/malicious it tends to create false positives that could result in legitimate traffic being blocked or made inaccessible.

The MESH reputation system works using the blockchain ledger to allow entries of bad traffic to the ledger. Once in the ledger, the AI algorithms will then start to form a reputation factor for that item.

To gain the correct information Phalanx Secure Solutions will need to gain the support of existing threat feeds already in action, it will then be required to build an API that will allow this threat feeds to automatically send their data to the community/paid system based on their level of input and ability.

The system will also gain by allowing those same feeds to read the data from the ledger along with other cyber companies building products. The premium version of the MESH Threat Reputation System will comprise of a read-only AI that will allow for the licensing of third-party applications to view and gather threat data for their existing or new applications.

Spartan AI - Threat Scoring System

Reputation alone does not indicate the level of threat to the system. The Spartan AI - Threat Scoring System will use a proprietary algorithm based on the MESH Threat Network, type of asset being attacked, type of attack, and the number of occurrences to create a score for that attack.

Scoring is done in real time using the AI engine and is done with each attack. The score results in the potential to block or let traffic pass through the firewall/agent designated to read the score and determine its meaning.

The score will be based on a 1-10 designation with 1 being the lowest, meaning no real threat to 10 being the highest and setting the bar for the most extreme attacks such as large-scale ransomware, DDOS or botnet attacks.

To use the scoring engine, an organisation must have access to the Spartan AI - Threat Hardening System.

Spartan AI - Threat Hardening System

Cyber threats are now a fact of life in business. Every day your network is exposed to thousands of internet connection points and any one or many of them could potentially be a potential breach waiting to happen. Reactionary systems are no longer capable of preventing cyber attacks as many attacks are occurring at a rate of speed that reactionary systems can no longer keep up with.

The Spartan AI - Threat Hardening System enhances your security posture by using its AI machine learning algorithms to track the MESH Threat Reputation System and the Accumulus Threat Scoring system to learn whether traffic is potentially good or bad traffic. Once traffic has been identified as bad traffic the Accumulus Threat Hardening System automatically blocks that traffic using the Kraken FW or an agent for any commercially available firewall that agents are available for. As of the writing of this White Paper, GBMS Tech plans to create agents for the following firewall products to use the Spartan AI - Threat Hardening System:

- Sophos UTM
- Sophos Next Generation Firewall
- Barracuda Firewall
- Fortinet
- SonicWall

The Accumulus Threat Hardening System also blocks and updates rules on each firewall/agent that is in the GBMS Tech ecosystem, thereby using a herd/mesh topology to harden systems across the globe instantly.

Now, when the Spartan AI - Threat Hardening System at 'company A' detects a bad actor and blocks that traffic, it will signal the remaining agents and firewalls in the ecosystem to block that traffic potentially preventing a large-scale cyber attack by ransomware, botnets, worms, viruses etc.

Accumulus Threat Shield Features

Blockchain Sponsored Threat Detection and Monitoring

The ATS tokens (ethereum erc20 compatible tokens), created during the ICO, will be used for the operation of reward system which pays Hoplites who, through the simple adoption of the security product, passively participate in the automatic crowdsourcing of threat detection.

Each user or organisation , along with receiving the ability to protect their systems, will be participant threat detectors (Hoplites). Any activity seen as suspicious by automatic processes will be passed to a combination of automatic, AI-driven and manual testing dependent on the threat severity and level of urgency required.

Through the use of smart contracts (a function that allows a set of predetermined actions), GBMS Tech will be able to issue tokens to any Hoplites who discover or validate a new threat in the the community.

Any threats that are found in the ecosystem are automatically sent by a Hoplite would be checked against the current threats in the MESH Threat Reputation system to ensure that there are no existing threats with the same characteristics.

Other Corporate or Individual Hoplites have the ability to review the threats that are in the MESH queue and validate it, in order for a new threat to be validated as active it should have up to 8 Hoplites validate it. Rewards will be assigned to the Hoplite that discovers the threats along with the up to 8 Hoplites who validated the threat. Rewards are determined based on the severity of the threat, the scope of potential targets, and breach type to be listed on the Accumulus Hoplite portal.

Much like mining cryptocurrencies, the user is rewarded, but in this case, the computational resources required are so negligible as to be considered almost zero and the reward potential could be higher than mining. We see this as an attractive incentive not just for the crypto community but for all users.

Definition of all parties within the GBMS Ecosystem

A. **GBMS** – Developer of the ecosystem.
B. **Corporate Hoplites** – Partner Companies in the system who act as detectives (finding the threats) or as consensus confirming nodes (checking another Hoplites reported threats). The system will start with these partner companies as the trusted hoplites.
C. **Whitehat Hoplites** – Individuals security professionals who act in the same manner as corporate hoplites, but only act as an individual.
D. **End User Corporate and Business** – Organisations both large and small who benefit from GBMS security products, which in turn rely on a multi-validated distributed threat database on the blockchain.

The reward structure is in place to pay the 'workers'(i.e. the Hoplites) in the system on a proof of work basis.

There are 3 variables for the number of tokens that are awarded to each threat, each variable has its own role in the gamification of the system.
The number of tokens that are awarded are based on:

- Severity of the Threat: The Threat Scoring systems using a scale of 1 to 10 to determine threat levels based on several factors such as:

  - Scale of Attack
  - Type of Attack
  - Type of Target

- Role played:

  - Finder - Did you find the threat and have it reported to the Accumulus Threat Shield System.
  - Verifier - Did you verify the threat for another Hoplite.

- Position of Accumulus Threat Watch Leaderboard

Hoplites that find and report new threats are rewarded with 1,000 to 10,000 tokens upon successful verification of a new threat added to the threat feed and verified by at least 4 finders.
Hoplites that assist in the verification of new threats are rewarded with 100 to 1,000 tokens upon successful verification of a new threat added to the threat feed.

Accumulus Threat Watch AI - Spartan

The Accumulus Threat Watch AI, named Spartan provides a real-time interface for reviewing public threat feeds, incoming GBMS Tech client data, incoming 3rd party data, community data and filtering all of the noise in order to validate real actual alerts that need to be acted upon.

The Spartan AI will ingest all of the data in its raw format and outputs actionable data that can be used to identify real threats.

Accumulus Threat Shield System Architecture and Operations

- The current Accumulus Threat Shield API engine runs as a multi-layer pipeline hosted on GBMS Tech owned servers located in secret data centres around the world.
- Deployment is handled using Ansible
- Data is encrypted at rest and in transit between client devices, core servers, databases, and long-term storage.
- User and client non-security data are stored on a clustered MySQL instance.
- All communication is handled using the JSON Format.
- Most code is python, with all web features created using the React framework.

Community Version of Accumulus Threat Shield

The Accumulus Threat Shield will contain a free community component which will give superior protection through limited Accumulus Thread Shield technology and also increased threat detection by crowdsourcing the detection process and use a blockchain secured hive mind to disseminate the security information.

To achieve the maximum onboard efficacy, the product will be comprised of two simple (but compelling) incentives:

- Unbeatable security for free.
- Automatic token rewards for participating in threat detection.

The first of these should be compelling enough. The same breakthrough cybersecurity as the GBMS Tech professional products without the monitoring and compliance reporting required for a business to comply with new regulations. We believe that this new product will be so essential for home users that the word will quickly spread and drive unprecedented adoption.

Accumulus Threat Shield Benefits

Any assessment of the potential of a product of this magnitude would not be complete without observing the additional passive effects like the ability to disincentivise bad actors of malicious behaviour which would hopefully encourage smart minds to seek legitimate technological pursuits and the herd immunity effect which all security products contribute to.

Disincentivisation

If we can increase the difficulty and complexity that the hacker will encounter, it reduces the commercial incentive and encourage the talent pool of potential hackers to organically seek to apply their skills in increasingly more legitimate ways, many of which will also be created by the demand increase for talented coders which will be driven by the increasing adoption of blockchain, AI initiatives and other leading-edge technologies.

A unified cybersecurity platform which takes advantage of blockchain technology to ensure security, scalability, communication and distribution and is available to all, would go a long way to looking down systems in such a way that it diminished the potential for successful nefarious hacking.

Herd immunity

Herd immunity can be described as the protection non-immune organisms receive as a result of being distanced from a disease or pathogens through other organisms which have immunity.

Though the community-based rewards system to incentivise onboarding, the active security will be expanded passively to non-participant systems by the herd immunity effect. All active security systems will provide some degree of herd immunity but only a product with a significant improvement in effectiveness and a wide adoption will see a real result in the aspect of passive security.

This is a real boon for older legacy systems which may not be receiving regular updates. Worth noting here is that the GBMS Tech Trident CMP also effectively protects older Windows systems which no longer receive Microsoft updates.

Benefits to all parties within the GBMS Ecosystem.

A. **GBMS** – Improved multi validated threat detection system, increased HW sales, additional revenue from the foundation as GBMS acts as an Hoplite.
B. **Corporate Hoplite** – Additional revenue as a Hoplite, upside on holding tokens too.
C. **Whitehat Hoplites** – Additional revenue as a Hoplite, upside on holding tokens too.
D. **End User Corporate and Business** – As the system incentivises people to find bigger threats, they will benefit from faster patching and a more secure network.
E. **Token Holders** – the token circulation will progressively decrease, and as the subscription revenue's increase, the demand increases creating a positive price movement.

Roadmap

Miles Stones for Accumulus Threat Shield

Quarter 1

- Development of self-installed and monitored Trident Network Monitoring and Protection to continue.
- Development of Kraken Firewall to continue
- Development of Version 2.0 of Trident Network Monitoring and Protection Portal to continue

Total cost $ 209,858.75

Quarter 2
- Launch self-installed and monitored Trident Network Monitoring and Protection.
- Launch Kraken Firewall.
- Version 2.0 of Trident Network Monitoring and Protection Portal Launched
- Open Second SOC (Location Private)

Total cost $441,479.17

Quarter 3
- Start development of Threat Ingestion Feeds and Threat Scoring system
- Start development of Spartan AI Engine
- Start development of Version 1.0 of the Accumulus Threat Customer and Reseller Portal

Total cost $ 364,812.50

Quarter 4
- Establish the Shield Core Partner program to begin vetting trusted 3rd party resources to be part of The Shield Core trusted network of threat feed aggregators.
- Spartan AI Engine starts ingesting data to learn patterns and potential security issues.
- Version 1.0 of the Accumulus Threat Customer and Reseller Portal to be launched.

Total cost $ 364.812,50

Quarter 5
- Start development of community version of the “The Shield Core”.
- Start development of commercial version of the “The Shield Core”.

Total cost $ 364.812,50

Quarter 6
- Beta deployment of private blockchain code to contain MESH Threat Reputation System.
- Beta deployment of application code to non-GBMS Tech Ltd systems for access to The Shield Core. Integrate Accumulus Threat Scoring system with MESH Threat Reputation System to create accurate threat Reputation feed in the private blockchain.

Total cost $ 364.812,50

Quarter 7

- Integrate Accumulus Threat Hardening System with The Shield Core for real-time block traffic at devices, apps, and systems that are part of the Accumulus Threat Shield Ecosystem.
- Distribution of tokens for valid threat feed ingestion to begin.
- Launch Beta of MESH Threat Reputation System.
- Beta community version of The Shield Core to launch.
- Beta commercial version of the Shield Core to launch.

Total cost $ 352,742.08

Quarter 8

- All products into production, Accumulus Threat Shield live.
- Continual Updating to be started on Quarterly update schedule.

Total cost $ 364.812,50
Total development cost $ 2.828.142.50

Quarter 9+

- All products in update
- Product rollout to existing

ATST

GBMSTECH
SECURED BUSINESS CONTINUITY

ico@gbmstech.io
+44 (0) 207 096 0554
www.gbmstech.io
www.gbmstech.com
1Berkeley Street
London
W1J 8DJ