HEROIC
.com

# La cybersécurité alimentée par l'intelligence artificielle et la blockchain

L'équipe de HEROIC.com
Février 2018

# Abstract

HEROIC.com renforce l'avenir de la cybersécurité avec l'intelligence artificielle et la blockchain pour se protéger contre les cyber-menaces actuelles et de prochaines générations.

Alors que les cybermenaces augmentent à un rythme exponentiel, les solutions modernes de cybersécurité sont réactives, dépassées et inefficaces. (1) La grande majorité des données sur les menaces est contrôlée par les grandes entreprises et les gouvernements, ce qui rend difficile et coûteuse la mise au point de solutions de nouvelle génération qui améliorent la protection. Les avancées récentes en matière de protection contre les menaces basées sur l'intelligence artificielle sont prometteuses, mais les solutions sont presque exclusivement déployées dans les grandes entreprises, ce qui met la technologie hors de portée des personnes les plus vulnérables aux attaques.

HEROIC.com adopte une nouvelle approche de la protection contre les menaces assistées par IA. Utilisant le "big data", l'intelligence artificielle et la blockchain, combinés avec une plateforme décentralisée P2P de protection contre les menaces, HEROIC.com changera la cybersécurité telle que nous la connaissons et rendra les solutions de prochaines générations librement accessibles à tous. HEROIC.com permettra et incitera les développeurs et les entreprises à créer la prochaine génération de cybersécurité grâce à l'écosystème HEROIC.com, qui comprend un échange ouvert de renseignements sur les menaces appelé "HEROIC Arc Reactor™", une plateforme unifiée de gestion de la sécurité appelée "HEROIC Guardian™", et un environnement de recherche et de développement. La motivation à la collaboration au sein de cet écosystème va être incités par la blockchain et par l'utilisation de la cryptomonnaie de HEROIC.com, le HRO (prononcez héro).

Cet article présente de multiples technologies nouvelles et uniques spécifiques à l'écosystème HEROIC.com, y compris "Threat Mining™", "Cyberlytics™" et le protocole "Proof-of-Threat™". Nous prévoyons des milliers d'applications potentielles pour lesquelles les données fournies peuvent être utilisées. Un écosystème de cybersécurité ouvert, alimenté par une blockchain, débloquera l'énorme opportunité de protection contre les menaces de la prochaine génération, éliminer les tensions et les coûts des intermédiaires tiers et assurer un monde plus sûr.

Nous croyons que la combinaison de données sur les cyber-menaces intégrées à l'intelligence artificielle et à la blockchain est l'avenir de la cybersécurité alimentée par l'intelligence artificielle. L'écosystème HEROIC.com et le token HRO deviendront un nouveau standard utilisé dans toute l'industrie de la cybersécurité pour assurer globalement la sécurité, la confidentialité et la confiance.

Avis : Ce document est à titre d'information seulement et ne constitue pas une offre ou une sollicitation de vente d'actions ou de titres de HEROIC.com ou de toute société ou organisation liée ou associée. Une telle offre ou sollicitation ne sera faite qu'au moyen d'un mémorandum d'offre confidentiel et conformément aux conditions de toutes les lois sur les valeurs mobilières et autres lois applicables.

Avis : Ce document est fourni à titre d'information seulement et ne constitue pas une offre ou une sollicitation de vente d'actions ou de titres de HEROIC.com ou de toute société ou organisation liée ou associée. Une telle offre ou sollicitation ne sera faite qu'au moyen d'un mémorandum d'offre confidentiel et conformément aux conditions de toutes les lois sur les valeurs mobilières et autres lois applicables.

# Table des Matières

# Le problème des solutions actuelles de cybersécurité

Une grande partie de notre vie repose sur la confiance dans la technologie : Croire que lorsque le feu devient vert, il est sûr de démarrer ; que lorsque nous mettons notre argent dans une banque ou un magasin en ligne, c'est sûr. Presque tout ce que nous utilisons chaque jour repose sur la technologie, depuis les réveils et les grille-pain jusqu'aux jouets et aux voitures des enfants. On estime que d'ici 2020, il y aura plus de 30 milliards d'appareils connectés à Internet. (2)

Avec l'augmentation exponentielle de la technologie, le monde assiste à une augmentation similaire des attaques malveillantes. (3) À mesure que les dispositifs deviennent de plus en plus intelligents et interconnectés, des risques importants en matière de protection de la vie privée et de sécurité sont introduits. Non seulement nos appareils sont vulnérables aux attaques, mais les détails les plus importants de notre vie sont stockés sur ces appareils et les services cloud connexes. Ces détails vont de nos dossiers médicaux à nos renseignements bancaires en passant par les communications privées avec la famille et les amis.

Les informations privées qui tombent entre de mauvaises mains peuvent avoir des conséquences catastrophiques. Ginny Rometty, PDG d'IBM, a déclaré : "Nous croyons que les données sont le phénomène de notre époque. C'est la nouvelle ressource naturelle du monde. ....la cybercriminalité, par définition, est la plus grande menace pour chaque profession, chaque industrie, chaque entreprise dans le monde". (4)

Le niveau universel d'insécurité et les coûts réels associés aux atteintes à la protection des données et à la cybercriminalité sont stupéfiants : "72 % des grandes entreprises ont signalé un cyber-incident au cours de l'année écoulée et près de la moitié (47 %) de toutes les entreprises américaines en ont connu deux ou plus ". (5) En 2016, plus de trois milliards de dossiers personnels ont été volés et ont fait l'objet de fuites sur le Dark Web et plus de 100 millions d'Américains se sont fait voler leur dossier médical. (6) Presque toutes les personnes connectées à Internet dans le monde ont été touchées par une ou plusieurs atteintes liées à la protection des données.

L'augmentation continue des menaces ne montre aucun signe de ralentissement à court terme. Dans un article de Forbes, Steve Morgan de CSO Online a déclaré : "De 2013 à 2015, les coûts de la cybercriminalité ont quadruplé, et il semble qu'il y aura un autre quadruplement de 2015 à 2019. Juniper Research a récemment prédit que la numérisation rapide de la vie des consommateurs et des documents de l'entreprise augmentera.

le coût des atteintes à la protection des données atteindra 2,1 trillions de dollars à l'échelle mondiale d'ici 2019, soit près de quatre fois le coût estimé des atteintes en 2015 " (7).

Les solutions actuelles sont incapables de suivre l'augmentation du nombre et de l'intelligence des menaces qui s'attaquent à nos systèmes. Les systèmes de détection des menaces basés sur les signatures couramment utilisés aujourd'hui ne parviennent pas à détecter de nouvelles menaces inédites. Bien qu'efficaces si le vecteur de menace est connu et que les signatures sont entièrement mises à jour, ces solutions réactives ne peuvent pas nous protéger contre la prochaine génération d'attaques intelligentes. Qu'il s'agisse de voitures auto-propulsées, d'implants médicaux ou

d'intelligence artificielle générale (IA), l'avenir des logiciels malveillants et des systèmes intelligents commencera à attaquer la technologie à laquelle nous confions notre vie et la vie de ceux que nous aimons. Ces dernières années, des progrès importants ont été réalisés grâce à la protection contre les menaces par l'IA, mais cette technologie n'a pas encore atteint les masses. Les solutions de la prochaine génération se concentrent presque exclusivement sur la résolution de problèmes pour l'entreprise, avec très peu d'attention aux utilisateurs individuels, aux familles ou aux petites et moyennes entreprises.

En plus de se concentrer sur l'entreprise, les données sur les cyber-menaces, qui sont le composant central nécessaire pour construire des algorithmes intelligents, sont principalement contrôlées et stockées par les gouvernements et les grandes entreprises. L'accès à ces données est primordial mais d'un coût inabordable, ce qui rend difficile pour les développeurs et les petites organisations de construire la prochaine génération de solutions alimentées par l'intelligence artificielle.

Il est clair que l'amélioration progressive n'est pas suffisante pour protéger contre le danger à notre porte. Une innovation radicale est impérative.... quelque chose d'HEROIC.

# Aperçu de l'écosystème

L'écosystème HEROIC.com (l'"écosystème") est un écosystème de cybersécurité ouvert, intelligent et incitatif basé sur lablockchain, qui protège contre les cyber-menaces actuelles et de prochaine génération. Les principales composantes de l'écosystème sont les suivantes :

1) une plateforme décentralisée de renseignements sur les cyber-menaces appelée ***HEROIC Arc Reactor™***
2) un système unifié de gestion des menaces dans le cloud appelé ***HEROIC Guardian™***
3) Un ***Environnement de recherche et développement*** ("Environment R & D ) pour que les développeurs puissent développer et tester leurs propres algorithmes sur une plateforme sécurisée et hébergée. Ces trois éléments clés font partie intégrante de l'écosystème.

Il s'agit d'une approche unique pour créer un écosystème à long terme, durable et en constante évolution pour la protection contre les cyber-menaces. Une fois pleinement opérationnel, l'écosystème fournira les ressources nécessaires pour se protéger intelligemment contre les menaces actuelles et de prochaine génération.

## 2.1 Arc Reactor

HEROIC Arc Reactor™ est un système ouvert et décentralisé d'échange de renseignements sur les menaces à la cybersécurité, alimenté par la blockchain. Le but d'Arc Reactor est de fournir un dépôt ouvert de renseignements sur les cyber-menaces, un accès programmatique simple aux données et un marché efficace pour les données.

Les fournisseurs de données comprennent, sans toutefois s'y limiter, les mineurs, les fournisseurs de renseignements sur les menaces de sources ouvertes, les organisations de toutes tailles et les partenaires de données. Les données collectées passent par un processus d'extraction pour récupérer les attributs pertinents qui sont ensuite normalisés et sauvegardés dans une base de données distribuée. Les données recueillies ainsi que leurs attributs sont alors prêtes à être utilisées pour former des algorithmes d'apprentissage machine qui permettront en fin de compte la cotation et la classification des échantillons.

L'accès aux échantillons collectés et à leurs attributs sera disponible par le biais d'API et de SDK conformes aux formats standard de l'industrie.

Arc Reactor deviendra plus intelligent et plus robuste à mesure que davantage d'utilisateurs, d'organisations et de fournisseurs de données se joindront à l'écosystème. Nous nous attendons à ce que les données fournies par Arc Reactor alimentent de nombreux produits liés à la cybersécurité et deviennent à terme le plus grand dépôt de renseignements sur les cyber-menaces au monde.

Un échange décentralisé et ouvert de renseignements sur les menaces fera tomber les barrières d'entrée lors de l'élaboration de solutions de cybersécurité alimentées par l'intelligence artificielle et permettra de distribuer les données sur les menaces pour le bénéfice de tous.

Le marché pour les données fournies par Arc Reactor est exclusivement alimenté par le token HRO et ses contrats intelligents.

## 2.2 Guardian

HEROIC Guardian™ est une plateforme de cybersécurité unifiée, basée sur le cloud. Il s'agit d'une simple interface en ligne pour les utilisateurs individuels, les familles et les entreprises pour gérer toutes les pièces du puzzle de la cybersécurité. Guardian utilise les données de menace du réacteur Arc et les combine avec l'intelligence artificielle pour prédire et prévenir les cyber-attaques.

Guardian permettra aux développeurs de logiciels et aux organisations de développer des intégrations et des applications supplémentaires qui se connectent avec Guardian et sa couche de données. Ces intégrations permettront aux développeurs de développer et de monétiser leurs créations, conduisant à une plateforme de cybersécurité encore plus robuste et holistique.

Guardian est fourni en tant que service gratuit avec des intégrations supplémentaires et des services de tiers fournis à un coût supplémentaire. Les utilisateurs peuvent payer pour des services premium à l'aide de tokens HRO ou de monnaie fiduciaire. Guardian fournira également l'accès à un portefeuille sécurisé pour gérer les tokens HRO.

## 2.3 Environnement de recherche et développement

L'environnement de R & D fournira aux développeurs, aux organisations et aux entreprises un emplacement central pour interagir visuellement et programmatiquement avec les données sur les menaces en temps réel et historiques fournies par Arc Reactor.

Les développeurs peuvent effectuer des recherches, développer et tester leurs propres algorithmes dans un environnement sécurisé et hébergé. L'environnement permettra également d'accéder aux algorithmes et logiciels fournis par la communauté.

d'analyser et de bloquer les menaces, avec la capacité de transformer des données écrasantes et disparates en informations et renseignements exploitables.

HEROIC.com se consacre à fournir les données, les outils et les logiciels nécessaires pour construire la prochaine génération de cybersécurité alimentée par l'intelligence artificielle. Nous contribuerons à faciliter et à encourager le développement de solutions logicielles libres selon les besoins, la première d'entre elles étant la protection contre les menaces liées à l'intelligence artificielle.

L'accès aux données et aux ressources sur l'environnement de R & D se fera exclusivement par l'intermédiaire du token HRO.

# 3 Participants de l'écosystème

## 3.1 Individus (utilisateurs et mineurs de Menaces)

Les personnes qui participent à l'écosystème recevront un logiciel multifonctionnel qui comprend une protection contre les menaces alimentée par l'IA, une fonctionnalité d'extraction des menaces, un portefeuille sécurisé pour les tokens HRO et une connexion à l'écosystème.

Non seulement les utilisateurs pourront protéger leurs appareils avec le logiciel, mais ils gagneront également des tokens HRO au fur et à mesure que leur système trouve, analyse et partage des données anonymes sur les menaces. Au fur et à mesure que de plus en plus d'utilisateurs rejoignent l'écosystème, de plus grandes quantités de données peuvent être analysées par les algorithmes d'apprentissage machine de la communauté, ce qui rend tout le monde plus en sécurité.

Le logiciel sera disponible pour la plupart des appareils, y compris les ordinateurs de bureau, les ordinateurs portables, les smartphones et les appareils IoT. La gestion du logiciel est assurée par Guardian. La puissance de calcul, le stockage des données et les données apportées à l'écosystème sont compensés par le token HRO et passent à travers un bouclier d'anonymat qui les prive de toute information d'identification personnelle (PII).

Les mineurs de Menaces sont les individus qui permettent à leurs appareils de faire partie de l'écosystème de façon anonyme, formant un puissant collectif d'appareils individuels et de puissance de calcul. Les dispositifs qui participent activement à l'exploitation des mines de menace reçoivent une compensation libellée en HRO pour l'information et les renseignements minés.

HEROIC.com facilitera la participation des utilisateurs sans avoir à comprendre le fonctionnement de la technologie sous-jacente et offrira des cours en ligne dans le cadre de la plateforme Guardian.

## 3.2 Développeurs

Les développeurs auront un accès ouvert à l'ensemble de l'écosystème. Le principal avantage pour les développeurs est l'environnement de R & D, qui offre la possibilité de faire de la recherche, de développer, de tester et de distribuer leurs propres logiciels et algorithmes.

Les développeurs seront rémunérés pour leurs créations, qui peuvent inclure des algorithmes intelligents, des outils logiciels et des systèmes logiciels complets. La compensation de l'écosystème se fait exclusivement par le biais du token HRO.
Parmi les autres avantages, mentionnons

- Accès à l'un des plus grands dépôts de renseignements sur les cyber-menaces en open-source.
- Une solide communauté de développeurs axés sur la cybersécurité et l'intelligence artificielle.
- La capacité d'effectuer des recherches visuelles et programmatiques, de construire et de tester des algorithmes propriétaires à l'aide de données historiques et en temps réel sur les menaces.

- Des sources de revenus légitimes pour les développeurs et les experts en sécurité.
- Compensation via le token HRO pour la participation aux données et les algorithmes de blocage des menaces les plus efficaces.
- La capacité de télécharger et d'utiliser les données pour les développeurs de leurs propres recherches et produits de cybersécurité.
- Compensation pour la construction d'applications décentralisées (Dapps) qui interagissent avec l'écosystème.

Nous prévoyons que l'écosystème incitera des personnes talentueuses partout dans le monde à écrire des algorithmes de cybersécurité et à élaborer des solutions pour le bien commun.

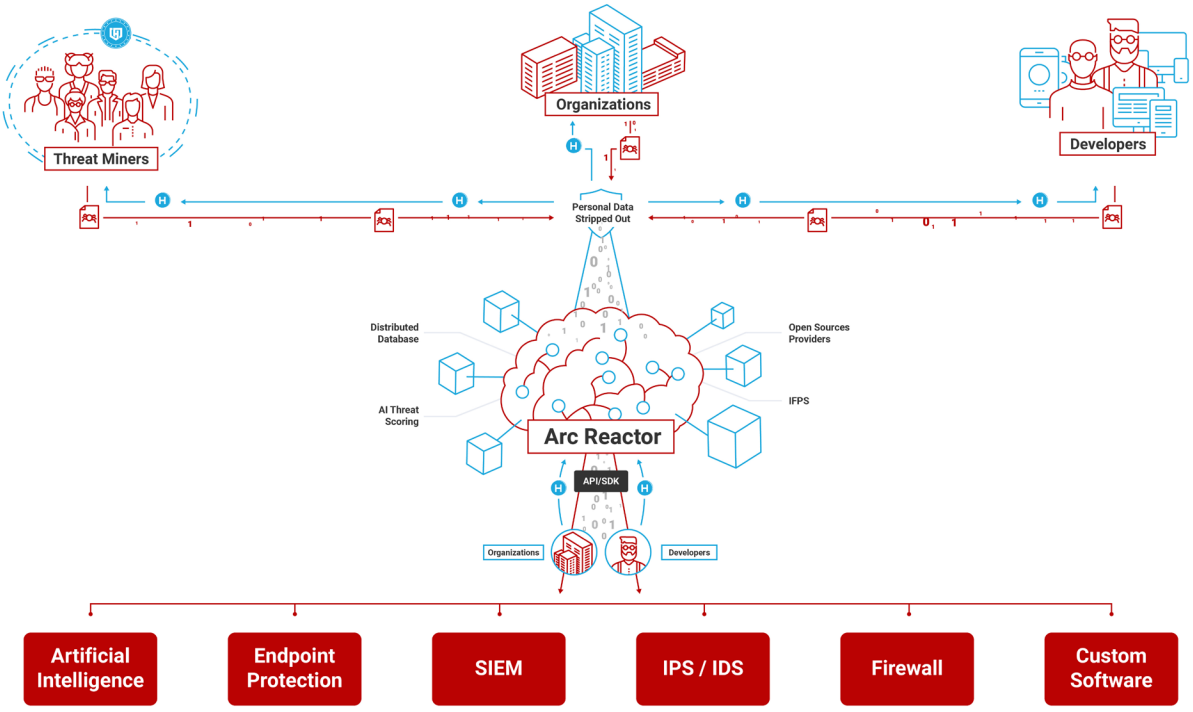
## 3.3 Organisations

Comme les développeurs, les organisations auront également un accès ouvert à l'ensemble de l'écosystème pour protéger leurs propres données, recevoir une compensation pour les données fournies et les intégrer à des produits et services appartenant à des tiers.
Les organisations sont un élément important de l'écosystème, car elles contribueront à fournir de grandes quantités de données qui aideront à protéger l'ensemble de l'écosystème et fourniront un marché efficace
de données sur les menaces. Les organisations peuvent comprendre des entreprises, des écoles, des organisations sans but lucratif, des pools de mineurs, des gouvernements et autres.
En utilisant les méthodes de distribution standard de l'industrie, les organisations seront en mesure de consommer les données pour les utiliser avec les systèmes de cybersécurité interne et de construire leur propre logiciel.
Les avantages pour les organisations comprennent :

- Accès à l'un des plus grands dépôts de renseignements sur les cyber-menaces en open-source.
- Compensation pour la participation aux données et contributions aux algorithmes de blocage des menaces.
- La possibilité de télécharger des données sur les menaces pour améliorer leurs propres produits de cybersécurité.
- Compensation pour la construction d'applications décentralisées (Dapps) qui interagissent avec l'écosystème.

# Aperçu de la technologie

Comme décrit ci-dessus, l'écosystème HEROIC.com se compose de trois projets de base qui se combinent pour former une solution de sécurité efficace au bénéfice de tous les types d'utilisateurs, y compris les utilisateurs individuels, les développeurs et les organisations. Il a été conçu pour fournir de multiples niveaux d'accès, de valeur et de soutien afin de stimuler la recherche accélérée, le développement et l'intégration des technologies avancées de cybersécurité, en plus d'assurer l'accès universel à ces technologies. Plus l'écosystème grandit, plus il sera fort.



## 4.1 Arc Reactor

Arc Reactor est une plateforme ouverte et décentralisée de renseignements sur les menaces de cybersécurité qui offre trois fonctions principales. Il s'agit de la collecte, de la transformation et de la distribution de données sur les menaces, à utiliser avec des systèmes d'intelligence artificielle et de cybersécurité. Nous considérons chacune des trois fonctions ci-dessous.

### Collecter

Les données sur les menaces sont recueillies auprès de nombreuses sources, y compris les mineurs de menaces, les sources de menaces ouvertes, les fournisseurs de renseignements commerciaux sur les menaces, les renseignements sur les menaces fournis par la collectivité et le partage des menaces par les organisations. Chaque source participant à l'écosystème est un agent autonome, capable d'effectuer ces actions avec une interaction humaine limitée.

Les participants à l'écosystème disposeront d'agents logiciels et d'un accès programmatique pour fournir un flux constant de données sur les menaces. Les données recueillies passent à travers un bouclier d'anonymat pour s'assurer qu'aucune information d'identification personnelle n'est partagée.

### Transformer

Les données recueillies sur les menaces passent par un processus de nettoyage qui comprend la vérification, la normalisation, la déduplication et l'enrichissement. Ces données nettoyées sont ensuite stockées dans un réseau de stockage distribué à l'aide d'IPFS, et les métadonnées sont stockées dans une base de données distribuée.

Une fois stockées, les données sur les menaces passeront par des processus supplémentaires qui associent, classifient et évaluent les données à l'aide de l'intelligence artificielle. Ces métadonnées supplémentaires associées à l'échantillon sont ensuite fusionnées avec les métadonnées de la base de données distribuée.

### Distribuer

De multiples sources de données sur les menaces seront fournies aux participants de l'écosystème, notamment : Détails du fichier, domaine, URL et données IP, données du Dark Web, IOC et données communautaires. L'accès aux flux de données sera fourni programmatiquement en utilisant les normes de l'industrie par le biais d'API et de SDK. Ces normes peuvent inclure YARA, STIX, TAXII, CybOX et d'autres.

Arc Reactor fournit le "big data" et les incitations nécessaires pour alimenter l'intelligence artificielle qui peut finalement être utilisée pour se protéger contre les menaces. Nous prévoyons que les données sur les menaces seront utilisées pour de nombreuses applications différentes, y compris la protection des points finaux alimentée par l'IA, les systèmes de détection des intrusions/prévention des intrusions, la gestion des informations et des événements de sécurité (SIEM), la détection des réseaux de bots et la détection et la prévention de l'hameçonnage.

## 4.2 Guardian

De multiples couches de sécurité sont nécessaires pour protéger la technologie d'un utilisateur. Ces couches comprennent les logiciels antivirus, la surveillance des brèches de données, la protection contre le vol d'identité, la gestion des justificatifs, les sauvegardes, les DNS et bien d'autres systèmes. Chez HEROIC.com, nous appelons souvent ces couches le puzzle de la cybersécurité.

Guardian est une plateforme de cybersécurité unifiée et basée sur le cloud qui fournit une interface simple pour les utilisateurs individuels, les familles et les organisations pour gérer toutes les pièces du puzzle de la cybersécurité.

Guardian fournira initialement les couches centrales du puzzle de la cybersécurité tout en permettant aux développeurs et aux organisations de contribuer aux intégrations avec l'App Store Guardian et d'être compensés pour ces intégrations. Guardian Apps utilisera des API de développement pour interagir avec les données de l'écosystème. Ces éléments combinés permettront d'unifier et de simplifier la gestion de la cybersécurité.

Guardian combine l'intelligence artificielle avec les données de ses applications interconnectées.

et Arc Reactor pour prédire et prévenir les cyber-attaques. Les utilisateurs Guardian ne bénéficieront pas seulement de l'intelligence globale fournie par l'écosystème, mais ils auront également leur propre IA personnelle dédiée à la protection de leurs appareils et services cloud. Au fur et à mesure que de nouvelles données seront analysées, le système continuera à devenir plus intelligent et à mieux se protéger contre les attaques.

La pile (stack) logicielle Guardian se compose des technologies suivantes :

- Gestion de la cybersécurité unifiée et basée sur le Cloud
- Agents logiciels et capteurs de données
- Gestion des noeuds terminaux
- API pour les développeurs
- App Store pour les intégrations de tiers
- Moteurs d'IA spécifiques à l'utilisateur
- Gestion des transactions blockchain

## 4.3 Environnement de Recherche et Développement

L'environnement de R & D fournit un accès simple aux données de menace d'Arc Reactor combinées à de solides capacités de recherche et de développement de logiciels.
Les développeurs peuvent s'informer sur l'intelligence artificielle et la cybersécurité grâce à nos tutoriels et conférences. En utilisant ces informations, ils peuvent construire et tester leurs propres créations par rapport à des données historiques et en temps réel dans un environnement de développement interactif (IDE). Les développeurs seront également incités à construire les meilleurs algorithmes de protection contre les menaces et à vendre leur technologie sur le marché en échange d'HROs.

La plateforme de R & D permettra à une communauté de développeurs et de chercheurs d'acquérir les connaissances et les ressources nécessaires pour construire la prochaine génération de protection contre les menaces.
L'environnement de R & D se compose des technologies suivantes :

- Accès aux données historiques sur les menaces
- API pour les développeurs
- SandBox de test de logiciels
- Outils logiciels
- intelligence artificielle et communauté de la cybersécurité
- Marché alimenté par les HROs
- Gestion des transactions de la blockchain

## 4.4 Autres technologies

### 4.4.1 Agent Logiciel

L'agent logiciel peut être installé sur des dispositifs individuels et fournit une variété de fonctions, y compris le minage des menaces, les connexions à l'écosystème, la protection des terminaux, un portefeuille HRO sécurisé et une gestion simple du système.

L'agent logiciel sera disponible pour plusieurs appareils, y compris les ordinateurs de bureau, les ordinateurs portables, les téléphones portables et les appareils IoT. On s'attend à ce qu'un agent logiciel  soit développé pour tous les systèmes d'exploitation populaires.

Chaque agent individuel surveille activement les actions et les changements de fichiers, le trafic de l'écosystème, le comportement des utilisateurs et les attributs de fichiers. Les agents peuvent identifier de manière indépendante les anomalies et les menaces, les valider et prendre les mesures appropriées. Cette surveillance assure la protection de l'utilisateur et de ses données.

La communication au sein de l'écosystème est effectuée entre les agents, l'Arc Reactor et la blockchain afin de caractériser les menaces validées, d'accroître l'intelligence du système et d'organiser la compensation pour les menaces minées. Cette communication facilite également l'identification et la validation des menaces et assure une vaccination en temps réel contre les attaques actives.

Les données vérifiées sur les menaces sont anonymisées et envoyées à l'écosystème pour aider d'autres systèmes à prévenir les menaces futures et pour que les développeurs construisent leurs algorithmes de protection contre les menaces.

Une fois entièrement développé, le logiciel de l'agent peut agir en tant que protection primaire du terminal d'un dispositif pour identifier et bloquer les menaces en plus de fournir une puissance de traitement et de stockage à l'écosystème pour la surveillance et l'identification à distance des menaces.

## 4.4.2 Intelligence artificielle (Cyberlytics®)

HEROIC.com utilise l'intelligence artificielle comme terme général pour décrire les nombreux systèmes et processus intelligents qui seront utilisés dans l'écosystème.

L'intelligence artificielle au sein de la cybersécurité englobe de nombreux domaines d'étude, notamment les mathématiques, l'apprentissage automatique, les réseaux neuronaux, la reconnaissance de motifs, la détection d'anomalies et plus encore.

Cyberlytics® est le moteur intelligent d'intelligence artificielle de HEROIC.com, utilisé pour prédire et prévenir les cyber-attaques avant qu'elles ne se produisent. Le moteur Cyberlytics analyse d'énormes quantités de données complexes sur les menaces provenant d'Arc Reactor afin de créer de puissantes informations qui sont utilisées pour protéger automatiquement votre technologie, vos données et, en fin de compte, vous.

## 4.4.3 Logiciel Blockchain

HEROIC.com utilise les contrats intelligents Ethereum pour les transactions ce qui facilite les paiements directs entre les utilisateurs, les organisations et les développeurs de logiciels. En utilisant une blockchain sécurisée, HEROIC.com offre la possibilité d'acquérir, de maintenir et de transférer des HROs. Nous encouragerons et indemniserons continuellement les utilisateurs qui contribuent à l'écosystème, y compris en effectuant et en recevant des paiements pour la distribution et l'utilisation de données sur les menaces.

Notre algorithme de consensus est la preuve du travail basé sur le protocole de preuve du travail d'Ethereum, qui deviendra éventuellement le nouveau protocole Proof-of-Threat™ d'HEROIC.com.

## 4.4.4 Proof-of-Threat™

Le nouveau protocole Proof-of-Threat™ de HEROIC.com sera éventuellement utilisé comme méthode principale pour quantifier le travail accompli par chaque nœud, et fournira un score à l'équipe de HEROIC.com pour chaque échantillon de menace. Au lieu de gaspiller de l'énergie et des ressources précieuses pour calculer les hashes, le protocole Proof of Threat permettra aux mineurs de contribuer leurs ressources informatiques à l'analyse et à la notation des menaces potentielles, et d'être récompensés proportionnellement pour ce travail.

La score de la menace donne une valeur numérique à chaque menace individuelle. Le score indique la probabilité que l'échantillon soit une menace. Plus le score est élevé, plus il est probable qu'il s'agisse d'une menace.

La notation des échantillons est bénéfique car elle permet aux systèmes de mieux contrôler s'il faut ou non bloquer la menace, au lieu de fournir une simple valeur binaire indiquant si quelque chose est ou n'est pas une menace.

Un score de menace est basé sur un certain nombre de facteurs et utilise une moyenne arithmétique pondérée pour produire un score de zéro à 100. HEROIC.com adopte une approche d'apprentissage machine, avec un score initial pour chaque échantillon sur un nœud, puis en utilisant les données de Arc Reactor pour valider le score initial et apprendre des données.

Le score de la preuve de la menace sera calculé à l'aide de certains ou de tous les systèmes suivants:

- Pré-exécution
  - Moteur propulsé par intelligence artificielle HEROIC Cyberlytics
  - Comparaison du hachage d'artefact avec les menaces connues dans Arc Reactor
- Post-exécution
  - Analyse heuristique d'artefact qui observe le comportement ou les caractéristiques d'un fichier ou d'un processus, ce qui peut indiquer qu'il est suspect.
  - Analyse de la Sandbox

Le protocole Proof-of-Threat™ et le moteur de score des menaces seront open-source et accessibles à tous. Un livre blanc plus complet sur la mise en œuvre initiale de Proof-of-Threat™ sera publié ultérieurement.

## 4.4.5 Tarification des données (algorithme dynamique)

La tarification des données sur les menaces est l'un des aspects les plus importants de l'écosystème, car le système doit motiver les utilisateurs à fournir des données avec sa structure de tarification tout en ne détournant pas les consommateurs des données parce que les coûts sont trop élevés.

Au lieu de fournir un système de tarification des offres et des demandes de prix qui ajoute des complications inutiles pour les utilisateurs, nous construisons un algorithme de tarification automatisé en temps réel qui motive les fournisseurs de données en maximisant la rentabilité et motive les consommateurs des données sur les menaces en fournissant des prix hyper-compétitifs. Ce système est similaire à ce qu'Uber utilise pour fournir des prix à ses coureurs et conducteurs, car il n'y a pas besoin de choix de l'utilisateur ou de transparence explicite dans la façon dont les prix sont déterminés.

L'algorithme fournit une tarification dynamique basée sur l'offre et la demande pour les données fournies. Il prend en compte des aspects tels que l'âge et la taille des données, leur type et leur importance potentielle, la taille totale de l'ordre, la cote de menace et les autres conditions du marché.

Au fur et à mesure que nous recevrons les commentaires des utilisateurs de l'écosystème et que notre compréhension de la valeur des données augmentera, nous mettrons continuellement à jour l'algorithme et intégrerons l'apprentissage machine afin d'offrir un marché toujours plus efficace.

Voici un exemple de la notion mathématique actuelle qui sera mise en œuvre.

$$F = M\left(\frac{X}{M + .BN + .CP}\right) + .BN\left(\frac{X}{M + .BN + .CP}\right) + .CP\left(\frac{X}{M + .BN + .CP}\right)$$

**F = total des revenus mensuels pour chaque mineur de menace.**
**M = Type de données 1 (évalué à A %) (tel que déterminé par d'autres facteurs)**
**N = Type de données 2 (évalué à B %) (tel que déterminé par d'autres facteurs)**
**P = Type de données 3 (évalué à C %) (tel que déterminé par d'autres facteurs)**
**X = revenu gagné auprès des consommateurs de données pour ce mois.**

# 5 Details des Token

## 5.1 Token HRO

Dans le cadre du développement de l'écosystème HEROIC.com, nous introduisons le token HRO (prononcez héro), qui sera utilisé comme une forme d'autorisation, d'incitation et de règlement entre les participants de l'écosystème, et pour d'autres services connexes.

Un approvisionnement fixe de HROs sera créé dans le cadre de la vente de tokens, avec des contrats intelligents appropriés et un registre blockchain qui suivra la norme ERC20. Le registre constituera une méthode sûre pour les détenteurs de HROs afin de les conserver et de les transférer à d'autres utilisateurs.

Alors que HEROIC.com a l'intention de développer le logiciel initial et les contrats intelligents qui alimentent l'écosystème, nous nous attendons à ce que le HRO soit une nouvelle norme utilisée dans tout l'écosystème de la cybersécurité et dans d'autres industries.

## 5.2 Incitatifs & avantages des Tokens

L'écosystème a été conçu pour fournir de multiples niveaux d'accès, de valeur et de soutien afin de stimuler la recherche accélérée, le développement et l'intégration de technologies de pointe en matière de cybersécurité et d'assurer la disponibilité de ces technologies pour tous. Les mesures incitatives sont gérées par l'utilisation des tokens HRO, l'écosystème étant multi-transactionnel, permettant à la fois les achats et les paiements entre n'importe quelle combinaison de participants HEROIC.com, y compris les utilisateurs finaux, les développeurs et les organisations.

## 5.3 Marché des Tokens

HEROIC.com est en train de construire un marché robuste pour les données de menace, alimenté par le token HRO. Les HROs peuvent être achetés en utilisant Bitcoin (BTC), Ethereum (ETH), d'autres cryptomonnaies populaires, ou monnaie fiduciaire.

Les utilisateurs qui possèdent des HROs peuvent utiliser leurs tokens pour acheter des services existants et futurs directement de HEROIC.com et d'autres partenaires de l'écosystème.

Le token sera disponible sur certaines bourses de cryptomonnaie. Les participants de l'écosystème recevront chacun un portefeuille sécurisé avec lequel ils pourront gérer leurs tokens HRO.

## 5.4 Fonds de croissance des utilisateurs

Un fonds de croissance des utilisateurs sera mis en place pour inciter les utilisateurs à participer aux différents aspects de l'écosystème. HEROIC.com encouragera et facilitera également le développement de services supplémentaires liés à la cybersécurité qui peuvent être échangés contre des tokens HRO.

# Privacité & sécurité

Avec un projet de l'ampleur et de l'importance de l'écosystème de HEROIC.com, une déclaration sur l'importance et l'application de la protection de la vie privée et de la sécurité est nécessaire.

La protection de la vie privée est d'une importance capitale pour nous. Nous nous efforcerons de maintenir la conformité avec les règlements connexes, y compris la prévention des pertes de données (DLP), les lignes directrices du NIST, les exigences du GRDP et d'autres pratiques exemplaires en matière de cybersécurité. En tant que tel, les outils, processus et systèmes de protection des données sont primordiaux pour assurer la confidentialité des clients de HEROIC.com, et toutes les données stockées qui y sont conservées.

HEROIC.com s'efforce d'utiliser les dernières technologies et normes de cybersécurité, et continuera d'évoluer et d'être transparent sur la technologie qu'il utilise. Les politiques de HEROIC.com sont conçues pour s'assurer que les données stockées ne sont pas mises à la disposition de personnes ou d'organisations non autorisées.

Dans le cadre de notre plan de cybersécurité, nous maintiendrons un programme de primes aux bogues pour tous les aspects de notre architecture, avec des récompenses libellées en tokens HRO. Il est important de noter que notre objectif est d'héberger tous les aspects de l'écosystème sur une architecture sans connaissances.

Afin de faire respecter les normes d'utilisation éthique, tout participant ou utilisateur qui cause délibérément des dommages à l'écosystème, aux plateformes ou aux applications, ou qui utilise les données à des fins non éthiques, peut se voir refuser l'accès de façon permanente et perdre l'accès à ses tokens HRO.

# 7 Autres technologies HEROIC.com

HEROIC.com est une spin-off d'une entreprise deux fois présente dans le Inc. 500 spécialisée dans la cybersécurité d'entreprise et le développement de logiciels, et a été fondée avec pour mission de protéger intelligemment l'information dans le monde. Avec cette mission, HEROIC.com a été activement impliqué dans le développement d'un certain nombre de produits de cybersécurité. Les produits suivants sont actuellement disponibles et sont utilisés par de grandes organisations.

## 7.1 HEROIC DarkHive™

HEROIC DarkHive est l'une des plus grandes collections au monde de fuites d'informations d'identification d'utilisateur compromises. HEROIC.com utilise la technologie intelligente et les analystes de la cybersécurité pour fouiller le deep web et le dark web à la recherche de piratage, de fuites et de toute autre source de données compromises.

Le DarkHive inclut à la fois des données de piratage détaillées et des données sommaires, pour une utilisation dans les entreprises du monde entier. Le DarkHive est le grand dépôt de données qui alimente EPIC (voir ci-dessous).

## 7.2 HEROIC EPIC™

HEROIC EPIC aide à découvrir, à corriger et à prévenir l'utilisation d'informations d'identification volées trouvées dans des brèches et des fuites de données de tiers.
En 2016, plus de 3,3 milliards d'enregistrements, y compris les adresses électroniques, les noms d'utilisateur et les mots de passe de plus de 1 700 atteintes à la protection des données, ont été divulgués sur le dark web. Une fois rendus publics, les pirates informatiques et autres parties peuvent obtenir et utiliser ces enregistrements pour se frayer un chemin par la force dans les systèmes et les écosystèmes des organisations, afin de mener des attaques ciblées. EPIC découvre les vulnérabilités et prévient les attaques en obtenant les mêmes bases de données divulguées sur le Web et en avertissant les organisations si les données de leurs employés ou clients ont été compromises. Cela donne aux professionnels de la sécurité l'occasion de réparer les connexions volées avant qu'elles ne soient utilisées contre leurs propriétaires.

# 8 Travaux futurs

L'équipe de HEROIC.com croit que pour réaliser notre mission de fournir la cybersécurité de prochaine génération à tous, le rythme actuel de développement est insuffisant pour éclipser le rythme des cyber-menaces, et nécessite donc une expansion significative et un développement accéléré.

Comme indiqué dans l'abstract, nous prévoyons qu'il y aura littéralement des milliers d'applications potentielles pour lesquelles les données fournies par l'écosystème HEROIC.com peuvent être utilisées. Nous n'avons pas l'intention de construire la grande majorité de ces applications, mais de faciliter et de motiver les autres acteurs de l'écosystème à construire ces systèmes.

Les fonds collectés grâce à la vente de tokens seront appliqués aux projets énumérés dans le présent document, la priorité initiale étant de compléter l'écosystème HEROIC.com afin de fournir aux utilisateurs une plate-forme décentralisée pour gérer tous les aspects de leurs besoins en matière de cybersécurité.

Le présent document établit un cheminement clair et cohérent vers la construction de l'écosystème. Cependant, nous considérons également qu'il s'agit d'un point de départ pour de futures recherches sur les logiciels de cybersécurité alimentés par l'intelligence artificielle.

La recherche active est continue, et de nouvelles versions de ce document apparaîtront sur HEROIC.com. Pour tout commentaire ou suggestion, veuillez nous contacter à l'adresse contact@HEROIC.com.

## 8.1 Travaux en cours

Les sujets suivants représentent les travaux pertinents en cours qui devraient apporter des bénéfices significatifs à l'écosystème HEROIC.com.

- Une spécification de protocole de preuve de la menace entièrement implémentable (Proof-of-Threat)
- Recherche de solutions de stockage décentralisées émergentes
- Des estimations détaillées des performances et des repères pour l'écosystème HEROIC.com et ses composantes.
- Algorithmes d'apprentissage machine pour un marché plus efficace pour les données sur les menaces.
- Analyse théorique des incitations de HEROIC.com.
- Transactions en millisecondes via des écosystèmes hors chaîne similaires au Bitcoin Lightning https://lightning.ecosystem/ ou Ethereum Raiden https://raiden.ecosystem/
- Intégration avec d'autres blockchain
- Pénalités pour les participants ou les utilisateurs qui causent intentionnellement des dommages à l'écosystème ou à toute application, ou qui utilisent les données à des fins non éthiques.
- Architecture zéro-connaissance

# Remerciements

Ce travail est l'effort cumulé de plusieurs personnes au sein de l'équipe de HEROIC.com, et n'aurait pas été possible sans l'aide, les commentaires et la révision des collaborateurs et conseillers de HEROIC.com. Chad Bennett est l'architecte original de l'écosystème HEROIC.com. Lui et David McDonald ont rédigé ce livre blanc en collaboration avec le reste de l'équipe, qui a fourni des contributions utiles, des commentaires, des révisions et conversations. Tammy Bennett a contribué à améliorer la structure et la formulation du document, tandis que Wyatt Semanek a créé les illustrations et finalisé le document. De multiples livres blancs sur la cryptographie ont été consultés lors de la préparation de ce travail et sont cités dans les citations (8), (9), (10) et (11). Nous remercions également tous nos collaborateurs et conseillers pour leurs conversations utiles et leur soutien.

# Annexe

Cybersécurité - Une brève histoire

## Glossaire

**Alimenté par l'IA:** Logiciel qui utilise l'intelligence artificielle ou des algorithmes d'apprentissage machine, au lieu d'un humain, pour rendre le logiciel plus intelligent.

**Algorithme:** un ensemble de règles pour résoudre un problème en un nombre fini d'étapes, comme pour y trouver le plus grand diviseur commun.

**Intelligence artificielle:** Théorie et développement de systèmes informatiques capables d'accomplir des tâches qui requièrent normalement l'intelligence humaine, comme la perception visuelle, la reconnaissance de la parole, la prise de décision et la traduction entre les langues.

**Big Data:** Des ensembles de données extrêmement volumineux qui peuvent être analysés par calcul pour révéler des modèles, des tendances et des associations, en particulier en ce qui concerne le comportement et les interactions humaines.

**Blockchain:** Voir https://HEROIC.com/blockchain-overview

**Cryptomonnaie:** Une monnaie numérique dans laquelle des techniques de cryptographie sont utilisées pour réglementer la production d'unités monétaires et vérifier le transfert de fonds, indépendamment d'une banque ou d'une autorité centrale.

**Cybersécurité:** Ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés.

**Minage de données:** Le processus de découverte de modèles et de relations intéressants et utiles dans de grandes quantités de données.

**Décentraliser:** Disperser (quelque chose) à partir d'une zone de concentration ; créer quelque chose sans limiter son contrôle ou son utilisation à un petit groupe.

**Démocratiser:** Rendre accessible et ouvert à tous. Le pouvoir est dévolu au peuple et exercé directement par lui.

**Monnaie Fiat:** Monnaie qu'un gouvernement a déclaré avoir cours légal, mais qui n'est pas soutenue par une marchandise physique. La valeur de la monnaie fiduciaire est dérivée de la relation entre l'offre et la demande plutôt que de la valeur du matériel dont l'argent est fait.

Les exemples de monnaie fiduciaire comprennent le dollar américain, l'euro, la livre sterling, etc.

**HEROIC Arc Reactor:** La plate-forme unifiée de gestion des menaces de HEROIC.com, conçue pour rassembler l'intelligence et les données du monde de la cybersécurité.

**Ecosystème HEROIC.com:** Le plus récent système ou réseau de composants d'interconnexion et d'interaction, pour aider à protéger le monde des cyber-menaces aussi vite qu'elles sont créées, ou plus vite. Le système utilisera trois nouvelles plateformes pour créer des solutions de cybersécurité rapides, à jour et proactives pour tous.

**HEROIC Guardian:** Une plateforme unifiée, basée sur le cloud, créée par HEROIC.com pour aider à protéger les utilisateurs contre les cyber-menaces, en utilisant l'intelligence artificielle.

**Apprentissage machine:** La capacité des ordinateurs à apprendre sans être programmés. Fait des prédictions sur les données.

**Mineur de menace:** Les utilisateurs du logiciel d'exploitation des menaces de HEROIC qui recherchent, valident et distribuent les menaces sur le réseau.

**Protection contre les menaces:** un service ou un système qui vous aide à vous protéger, vous ou votre entreprise, contre les problèmes ou les attaques malveillantes.

**Architecture sans connaissance:** Architecture logicielle où le stockage des données sur les systèmes est crypté à l'aide de clés publiques et privées de telle sorte que le fournisseur de stockage n'a pas accès au décryptage ou à la visualisation des données.

# 11 Citations


***1. BITSIGHT.*** Thousands of Organizations Run The Majority of Their Computers on Outdated Operating Systems, Nearly Tripling Chances of a Data Breach. Press Release. [Online] https://www.bitsighttech.com/press-releases/thousands-organizations-run-majority-of-computers-on-outdated-operating-systems.

***2. Claveria, K.*** 13 stunning stats on the Internet of Things. [Online] October 24, 2017. https://www.visioncritical.com/internet-of-things-stats/.

***3. Internet Security Threat Report. [Online] Symantec, April 2016.*** https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. Volume 21.

***4. Rometty, G. IBM Security Summit. . [Online] May 4, 2015.*** https://www.ibm.com/ibm/ginni/05_14_2015.html.

***5. Hiscox. The Hiscox Cyber Readiness Report 2017.*** [Online] 2017. http://www.hiscox.com/cyber-readiness-report.pdf.

***6. Graham, Luke. Cybercrime Costs the Global Economy $450 Billion." [Online]*** CNBC. https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

***7. Morgan, Steve. Cyber Crime Costs Projected to Reach $2 Trillion by 2019. [Online] Forbes, January 17, 2016.*** https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6923f2ff3a91.

***8. Protocol Labs. Filecoin: A Decentralized Storage Network.*** [https://filecoin.io/filecoin.pdf]

***9. Buterin, Vitalik. Ethereum Whitepaper.*** [https://github.com/ethereum/wiki/wiki/White-Paper]

***10. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.*** [https://bitcoin.org/bitcoin.pdf]

***11. block.one. EOS.IO Technical White Paper.*** [https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md]