HEROIC
.com

Ciberseguridad Impulsada por Inteligencia Artificial y Blockchain

Equipo HEROIC.com

Febrero 2018

Resumen

HEROIC.com pretende impulsar el futuro de la ciberseguridad, respaldado por las vanguardistas tecnologías de inteligencia artificial y blockchain, para brindar protección contra las amenazas cibernéticas actuales y de próxima generación.

Mientras las amenazas cibernéticas crecen a un ritmo exponencial, las soluciones modernas de ciberseguridad se limitan a ser reactivas, quedan obsoletas y han dejado patente su ineficacia. (1) La inmensa mayoría de los datos sobre amenazas está controlada por grandes empresas y gobiernos, dificultando y encareciendo la creación de soluciones de próxima generación que enriquezcan el nivel de protección. Las novedades en cuanto a protección contra amenazas basadas en la inteligencia artificial son prometedoras, aunque dichas soluciones parecen relegarse exclusivamente para grandes corporaciones, es decir la tecnología queda fuera del alcance de las personas más vulnerables a ser atacadas.

HEROIC.com aplica un novedoso enfoque para la protección contra amenazas, dirigido por IA. La combinación de ingentes cantidades de datos, inteligencia artificial y blockchain, con una plataforma descentralizada de protección contra amenazas P2P, HEROIC.com hará un lavado de cara del concepto actual de ciberseguridad, brindando soluciones de próxima generación disponibles a título gratuito para cualquiera. HEROIC.com dirigirá la capacitación e incentivará a desarrolladores y empresas, con el propósito de crear la próxima generación de ciberseguridad mediante el Ecosistema HEROIC.com. Dicho Ecosistema integra un mecanismo público de intercambio de información sobre amenazas, el denominado HEROIC Arc Reactor™. Se trata básicamente de una plataforma integral, la cual fusiona la administración de seguridad -denominada HEROIC Guardian™-, con un entorno de investigación y desarrollo. El incentivo a la colaboración dentro de este Ecosistema provendrá del blockchain y del uso de la criptomoneda de HEROIC.com, el HRO (héroe según la pronunciación inglesa).

El presente documento hace una presentación de variadas y vanguardistas tecnologías, exclusivas para el Ecosistema HEROIC.com, como por ejemplo: Threat Mining™, Cyberlytics™ y el protocolo Proof-of-Threat™. Anticipamos miles de aplicaciones potenciales para darle utilidad a los datos provistos. Dispondremos de un ecosistema de ciberseguridad abierto, impulsado por el blockchain, el cual representará una alternativa para la protección contra amenazas de próxima generación, además de aliviar los inconvenientes y sobrecostes de terceros intermediarios, que en última instancia redundará en un mundo más seguro.

Estamos convencidos de que la integración de datos de amenazas cibernéticas, con inteligencia artificial y blockchain, sentará los cimientos del futuro de la ciberseguridad. Tanto el ecosistema de HEROIC.com, como su token HRO marcarán el nuevo estándar para el sector de la ciberseguridad, que garantice seguridad, privacidad y confianza, a escala mundial.

Aviso: Eel presente documento tiene propósitos exclusivamente informativos y no supone oferta o solicitud alguna para vender acciones o valores en HEROIC.com o cualquier compañía u organización relacionada o asociada. Cualquier tipo de oferta o solicitud de este tipo se gestionaría solo a través de un memorando confidencial de dicha oferta, de conformidad con los términos legales respecto a valores y resto de leyes aplicables.

IMPORTANTE:
El presente documento tiene propósitos exclusivamente informativos y no supone oferta o solicitud alguna para vender acciones o valores en HEROIC.com o cualquier compañía u organización relacionada o asociada. Cualquier tipo de oferta o solicitud de este tipo se gestionaría solo a través de un memorando confidencial de dicha oferta, de conformidad con los términos legales respecto a valores y resto de leyes aplicables.

ÍNDICE

El Problema de las Soluciones Actuales de Ciberseguridad..... 4
- 2.1 Arc Reactor..... 6
- 2.2 Guardian.....7
- 2.3 Entorno de Investigación y Desarrollo..... 7

Participantes del Ecosistema..... 8
- 3.1 Individuos (Usuarios y Mineros de amenazas)..... 8
- 3.2 Desarrolladores 8
- 3.3 Organizaciones..... 9

Descripción Tecnológica General..... 10
- 4.1 Arc Reactor..... 11
- 4.2 Guardian..... 12
- 4.3 Entorno de Investigación y Desarrollo..... 12
- 4.4 Otras Tecnología 13
- 4.4.1 Software de Agente..... 13
- 4.4.2 Inteligencia Artificial (Ciberlítics®)..... 14
- 4.4.3 Software de Blockchain..... 14
- 4.4.4 Proof-of-Threat™ 14
- 4.4.5 Fijación de Precios de los Datos (Algoritmo Dinámico de Fijación de Precios).. 15

Detalles del Token..... 16
- 5.1 El Token HRO..... 16
- 5.2 Incentivos y Beneficios del Token..... 16
- 5.3 Mercado de Tokens..... 16
- 5.4 Fondo de Crecimiento de Usuarios..... 16

Privacidad y seguridad..... 17

Otras tecnologías de HEROIC.com 18
- 7.1 HEROICO DarkHive™..... 18
- 7.2 HEROICO EPIC™..... 18

Trabajos de Cara al Futuro 19
- 8.1 Trabajo Actualmente en Curso 19

Agradecimientos..... 20

Apéndice..... 21

Glosario..... 21

Referencias..... 23

El Problema de las Soluciones Actuales de Ciberseguridad

Una gran parte de nuestra vida es directamente dependiente de la certidumbre respecto a la tecnología: confiar por ejemplo, en la seguridad de cruzar, cuando la luz se pone en verde; confiar en que al poner nuestro dinero en un banco o comprar online, estamos seguros. Casi todo lo que hacemos en nuestra vida rutinaria, depende de la tecnología, desde relojes-despertadores, tostadoras o juguetes para niños. Se pronostica que llegados al año 2020 existirán más de 30 billones de dispositivos conectados a Internet.(2)

Junto a este aumento exponencial de la tecnología, se aprecia paralelamente un aumento similar de ataques maliciosos por todo el mundo. (3) Mientras los dispositivos se vuelven más inteligentes e interconectados, aparecen mayores riesgos para la privacidad y la seguridad. Nuestros dispositivos no son simplemente vulnerables a los ataques, sino que además exponemos los detalles más importantes de nuestras vidas en los dispositivos y servicios en la nube relacionados con los mismos. Dichos detalles abarcan desde nuestro historial médico, hasta nuestra información bancaria, aparte de comunicaciones privadas con familiares o amigos.

La información privada puede tener consecuencias catastróficas, en el caso de caer en las manos equivocadas. Ginny Rometty, Director Ejecutivo de IBM, dijo: "Estamos convencidos de que los datos son un fenómeno relevante de nuestra época. Constituyen un nuevo recurso natural del mundo. ...el cibercrimen, supone en su definición más amplia, la mayor amenaza para cada profesión, sector o empresa del mundo." (4)

El nivel a escala universal de inseguridad, de los costes reales asociados a la violación de datos y el ciberdelito, han alcanzado cotas espeluznantes: "Un 72% de las grandes empresas, informaron de algún incidente cibernético durante el pasado año, mientras casi la mitad (47%) de todas las compañías en USA sufrieron dos o más". (5) En 2016, más de tres billones de registros personales fueron robados y filtrados a la denominada Red Oscura, mientras a 100 millones de estadounidenses les sustrajeron sus historiales médicos. (6) Casi cualquier persona del mundo, al estar en conexión a Internet, se ha visto inexorablemente afectada por alguna filtración de datos, o incluso varias.

El incremento incesante de las amenazas no muestra signo evidente de que vaya a ralentizarse en el futuro inmediato. Un artículo de Forbes publicado por Steve Morgan, de CSO Online, afirmaba: "De 2013 a 2015, los costes de los ciberdelitos se multiplicaron por cuatro, y todo apunta a una nueva cuadruplicación para le periodo de 2015 a 2019. Juniper Research ha pronosticado hace poco que la rápida digitalización de las vidas de los consumidores y los registros de las compañías, incidirán en un aumento del coste de las filtraciones de datos a $2,1 billones a nivel mundial para 2019, equivalente a unas cuatro veces el coste estimado de las filtraciones en 2015" (7).

Las soluciones actuales carecen de potencial para abordar el ritmo del creciente número y sofisticación de las amenazas que atacan nuestros sistemas. Los habituales sistemas de detección de amenazas basados en firmas, ampliamente utilizados hoy en día, no son

capaces de detectar nuevas amenazas nunca vistas antes. A pesar de ser eficaces en caso de conocerse el vector de amenaza y si las firmas son completamente actualizadas, dicho carácter reactivo de las soluciones, nos deja vulnerables a la próxima generación de ataques inteligentes. Abarcando desde coches autodirigidos, implantes médicos o inteligencia artificial en general (IA), el futuro del malware y de los sistemas inteligentes, se enfocarán en atacar la tecnología a la que confiamos nuestras vidas y las vidas de nuestros más allegados. Durante los últimos años, se han producido desarrollos significativos respecto la protección contra amenazas impulsada por IA, no obstante dicha tecnología aún dista de ser ampliamente adoptada por las masas. Las soluciones de próxima generación se enfocan casi únicamente en la solución de problemas corporativos, obviando a los usuarios individuales, familias o PYMES.

Aparte de dirigirse a la empresa, los datos de las ciberamenazas -los cuales constituyen la piedra angular para la generación de algoritmos inteligentes-, quedan sobre todo bajo el control y a buen recaudo de gobiernos y grandes empresas. El acceso a dichos datos se vuelve esencial, aunque desgraciadamente a un coste desorbitado, lo cual dificulta a desarrolladores y a pequeñas organizaciones la creación de soluciones de próxima generación impulsadas por IA.

Se ha evidenciado que una mejora gradual es insuficiente para protegernos el peligro que se avecina. Por todo lo mencionado, se ha vuelto imperativo contar con una innovación radical ... algo HEROIC-O.

Descripción General del Sistema

El Ecosistema HEROIC.com (a partir de ahora, el "Ecosistema") constituye un entorno de ciberseguridad abierto, inteligente y sobre incentivos, respaldado en blockchain, el cual se encarga de brindar protección frente a las ciberamenazas actuales y de próxima generación. Sus componentes esenciales son:

- una plataforma descentralizada de inteligencia ante ciberamenazas, denominada HEROIC Arc Reactor™ ("Arc Reactor")
- un sistema unificado de gestión de amenazas basado en la nube, denominado HEROIC Guardian™ ("Guardian")
- un Entorno de Investigación y Desarrollo ("R&D Environment") donde los desarrolladores creen y pongan a prueba sus propios algoritmos en una plataforma segura. Dichos tres componentes clave son integrales y forman el Ecosistema

Se trata de un enfoque exclusivo para crear un ecosistema a largo plazo, sostenible y que evolucione continuamente con el propósito de proteger contra las ciberamenazas. En cuanto esté plenamente operativo, el ecosistema proveerá de los recursos necesarios para protegerse de forma inteligente contra amenazas tanto presentes, como futuras.

2.1 Arc Reactor

HEROIC Arc Reactor™ constituye un sistema abierto y descentralizado de intercambio de información sobre amenazas de ciberseguridad, respaldado en blockchain. Su objetivo es dotar de un repositorio público de inteligencia ante amenazas cibernéticas, una puerta de enlace programática sencilla a los datos y un mercado eficiente para la negociación de dichos datos.

Entre los proveedores de datos encontramos entre otros, amenazas de mineros individuales, proveedores de inteligencia de amenazas de código abierto, organizaciones de cualquier tamaño, y socios de datos. Los datos recopilados, son gestionados por un proceso que determina las características relevantes de los mismos, posteriormente se analizan y pasan a almacenarse en una base de datos distribuida. El conjunto de datos acumulados, así como los respectivos atributos de estos, serán especialmente útiles en la capacitación de algoritmos de aprendizaje automático, a partir de los cuales pueda determinarse una calificación y clasificación de las muestras.

Se podrá acceder a las muestras recopiladas y a sus atributos, de forma programática, mediante el uso de APIs y SDKs adaptadas al formato característico del sector.

Arc Reactor se irá enriqueciendo, volviéndose más inteligente y sólido, mientras más usuarios, organizaciones y proveedores de datos se incorporen al ecosistema. Los datos acumulados por Arc Reactor serán el germen de muchos productos relacionados con la ciberseguridad, los cuales con el tiempo, se convertirán en el mayor repositorio mundial de inteligencia sobre ciberamenazas.

El surgir de un mercado descentralizado y público de información sobre las amenazas, demolerá las tradicionales barreras de entrada, gracias a la posibilidad de crear soluciones de ciberseguridad impulsadas por IA, las cuales posibiliten una distribución de los datos sobre amenazas, que redunden en un beneficio universal.

El mercado de los datos proporcionados por Arc Reactor, girará en exclusiva, en torno al token HRO y contratos inteligentes relativos al mismo.

2.2 Guardian

HEROIC Guardian™ conforma una plataforma unificada de ciberseguridad basada en la nube. Proporciona un interfaz simple online, eficaz para usuarios individuales, familias y empresas, que les permitirá administrar todos los aspectos relacionados con la ciberseguridad. Guardian se basa en los datos de amenazas provenientes de Arc Reactor, incorporados a un proceso que emplea inteligencia artificial, especialmente destinado a predecir y prevenir ciberataques.

Guardian posibilita que tanto desarrolladores de software y como empresas, puedan desarrollar complementos y aplicaciones extra, acoplables a Guardian y su capa de datos. Gracias a dichas integraciones, los desarrolladores estarán en disposición de crecer y sacar rentabilidad de sus creaciones, generando una plataforma de ciberseguridad holística y de mayor robustez.

Guardian en principio será brindado como un servicio gratuito, aunque incluirá complementos adicionales y servicios de terceros con un coste extra. Los usuarios pueden satisfacer estos servicios premium pagando con tokens HRO o fiat. Guardian también proporcionará acceso a una cartera segura para administrar los tokens de HRO.

2.3 Entorno de Investigación y Desarrollo

El entorno de I+D es de vital interés para desarrolladores, organizaciones y empresas, al contar con un punto de encuentro donde interactuar visual y programáticamente con los datos de amenazas en tiempo real, así como los datos históricos recopilados y provistos por el Arc Reactor.

Los desarrolladores pueden centrar sus esfuerzos en investigar, desarrollar y poner a prueba sus propios algoritmos en un entorno seguro. El entorno también dispondrá de acceso a los algoritmos y software proveniente de la aportación comunitaria, para analizar y bloquear amenazas, con capacidad de convertir una ingente cantidad de datos dispares, en información e inteligencia con la que interactuar.

HEROIC.com se encargará de brindar los datos, herramientas y software necesarios para dar forma a la próxima generación de ciberseguridad impulsada por IA. Facilitaremos y alentaremos el desarrollo de soluciones de software de código abierto según se requiera, priorizando la protección respaldada en IA, contra amenazas de código abierto.

El acceso a los datos y recursos en el entorno de I+D estará también disponible en exclusividad mediante el token HRO.

3 Participantes del Ecosistema

3.1 Individuos (Usuarios y Mineros de Amenazas)

Quienes participen en el Ecosistema serán provistos de un software multifuncional, el cual integrará un sistema de protección contra amenazas impulsado por IA, función de minería de amenazas, una cartera segura para los tokens de HRO, además de conexión con el Ecosistema.

Los usuarios además de mantener protegidos sus dispositivos con nuestro software, se beneficiarán al obtener tokens HRO, mientras su sistema encuentra, analiza y comparte datos anónimos sobre amenazas. Cuanta mayor cantidad de usuarios formen parte del Ecosistema, mayor cantidad de datos pueden analizarse por los algoritmos de aprendizaje automático de la comunidad, enriqueciendo con ello la seguridad de la misma.

El software será operativo en la inmensa mayoría de los dispositivos, como ordenadores de sobremesa, portátiles, teléfonos inteligentes y dispositivos IoT. El software es gestionado mediante Guardian. La potencia de computación, el almacenamiento de datos y la información (datos) provistos del usuario al ecosistema, son recompensados con tokens de HRO, por medio de un mecanismo de filtrado que permite el absoluto anonimato capaz de ocultar cualquier información que pudiera conducir a una identificación personal (PII).

Denominamos mineros de amenazas a aquellos individuos, cuyos dispositivos pasan anónimamente a formar parte del Ecosistema, dando forma a un poderoso conjunto de dispositivos individuales, que colectivamente tienen un enorme poder de computación. Los dispositivos participantes activamente en la minería de amenazas, son recompensados en tokens HROs por la información e inteligencia minera aportada.

HEROIC.com posibilitará que puedan participar incluso aquellos usuarios sin conocimiento técnico sobre la tecnología subyacente, los cuales dispondrán de la posibilidad de recibir formación técnica mediante cursos online impartidos por la plataforma Guardian.

3.2 Desarrolladores

Los desarrolladores dispondrán de pleno acceso a todo el ecosistema. Como principal beneficio para los desarrolladores, destaca el entorno I+D, donde desplegar labores de investigación, desarrollo, ensayo y distribución de su propio software y algoritmos. Los algoritmos inteligentes, herramientas de software y sistemas de software integrales de los desarrolladores, serán recompensados exclusivamente en tokens HRO.

Entre los beneficios adicionales cabe señalar:

- Acceso a uno de los mayores repositorios -en código abierto- de inteligencia sobre ciberamenazas
- Una comunidad robusta de desarrolladores, particularmente enfocada en la ciberseguridad e inteligencia artificial
- Capacidad de investigar de modo visual y programático, construyendo y probando algoritmos patentados, con una amplia gama de datos de amenazas en tiempo real e histórico.

- Flujos de ingresos legítimos tanto para desarrolladores, como para expertos en seguridad
- Recompensas en tokens HRO por la contribución con datos y algoritmos de bloqueo de amenazas más efectivos
- Posibilidad de descargar y hacer uso de los datos, enriqueciendo así la investigación propia y creación de productos de ciberseguridad por los desarrolladores.
- Recompensas por crear aplicaciones descentralizadas (DApps), las cuales interactúen con el ecosistema.

Esperamos que el Ecosistema sirva de inspiración a personas con talento en cualquier parte del mundo, incentivándolos a crear algoritmos de ciberseguridad y soluciones para el bien del público general.

3.3 Organizaciones

Del mismo modo que los desarrolladores, las organizaciones también disfrutarán de un acceso pleno al ecosistema, empleándolo para proteger sus propios datos, mientras son recompensados por los datos contribuidos, los cuales van siendo incorporados a productos y servicios de marcas de terceros.

Las organizaciones constituyen parte esencial del ecosistema, porque hacen acopio de un cuantioso volumen de datos -el cual es de vital importancia para brindar protección a todo el ecosistema- y además generan un mercado eficiente de datos de amenazas. Tales organizaciones vienen representadas por empresas, colegios, ONGs, grupos de minería, gobiernos y otros.

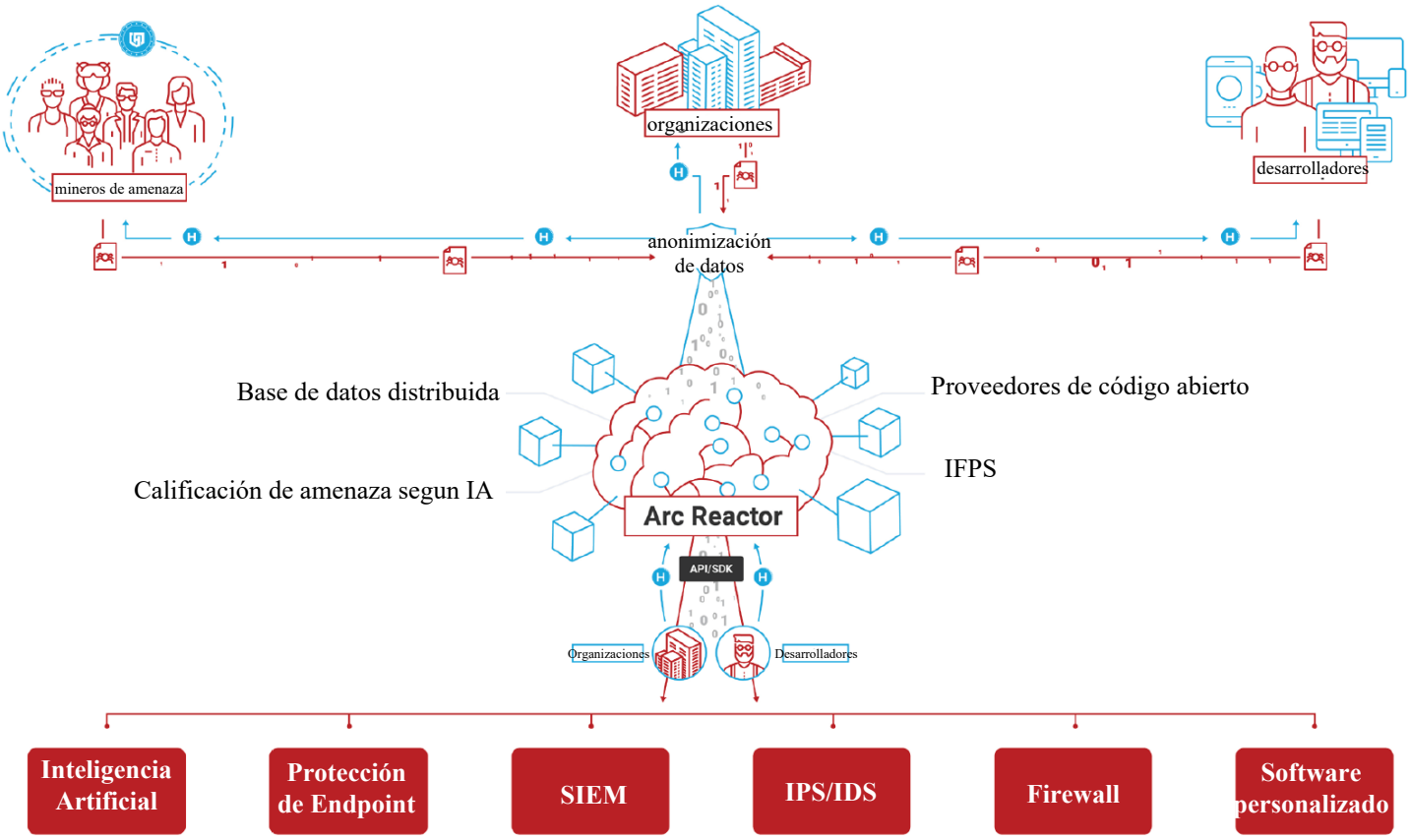
Empleando los métodos de distribución habituales del sector, las organizaciones podrán respaldarse en los datos recopilados, que permitan ser empleados por sus sistemas internos de ciberseguridad, moldeando su propio software.

Entre las ventajas de las organizaciones podemos destacar:

- Acceso a uno de los mayores repositorios -en código abierto- de inteligencia sobre ciberamenazas
- Recompensas por colaborar en la aportación de datos a algoritmos de bloqueo de amenazas
- Capacidad de descargar datos de amenazas, las cuales permitan enriquecer sus productos de ciberseguridad propios.
- Recompensas por dar forma a DApps (aplicaciones descentralizadas) que interactúen con el ecosistema.

4 Descripción Tecnológica General

Tal como ya hemos comentado, el Ecosistema de HEROIC.com está compuesto en esencia por tres proyectos principales combinados para dar forma a una solución de seguridad efectiva, la cual otorga beneficios a cualquier tipo de usuario, independientemente de su condición de individuo, desarrollador u organización. Su diseño parte de un sistema integrador de múltiples niveles de acceso, valor y apoyo, el cual alienta a la investigación, el desarrollo y la integración de tecnologías avanzadas de ciberseguridad, así como garantiza un acceso generalizado a dichas tecnologías. Cuanto más grande sea el ecosistema, más fuerte será.



4.1 Arc Reactor

Arc Reactor representa a una plataforma abierta y descentralizada de inteligencia de amenazas de ciberseguridad, la cual provee básicamente tres funciones: recopilación, transformación y distribución de datos respecto de amenazas, para su despliegue en sistemas de inteligencia artificial y ciberseguridad. Veamos a continuación de forma detallada cada una de éstas tres funciones:

Recopilar

Los datos sobre amenazas provienen de diversas fuentes, entre las que se encuentran los mineros de amenazas, la fuente de amenazas de código abierto, los proveedores de inteligencia sobre amenazas comerciales, la inteligencia sobre amenazas provista por la comunidad y las amenazas compartidas por las organizaciones. Toda fuente participante en el ecosistema, lo hace en calidad de actor autónomo, ejecutando dichas acciones con una interacción humana restringida.

Los participantes del ecosistema serán provistos de agentes de software y acceso programático, de manera que puedan colaborar con un flujo constante de datos acerca de amenazas. Los datos acumulados son procesados a través de un filtro de anonimato, el cual garantiza que ninguna información de identificación personal quede expuesta y por tanto comprometida.

Transformar

Los datos de amenazas recogidos, pasan a ser cribados -verificación, normalización, eliminación de duplicidades y enriquecimiento-, y tras dicho pulido, almacenados en una red de almacenamiento distribuido utilizando IPFS, mientras los metadatos se incluyen en una base de datos distribuida.

Tras guardarse, los datos de amenazas son sometidos a procesos adicionales de asociación, clasificación y calificación por medio de inteligencia artificial. Estos metadatos adicionales vinculados a la muestra, se acoplan con el resto de metadatos de la base de datos distribuida.

Distribuir

Existirán múltiples fuentes de datos de amenazas para los participantes en el Ecosistema, como: detalles del archivo, dominio, url y datos de la IP, datos de la Dark Web, IOC, y datos de la comunidad. El acceso a las fuentes de datos es programático, siguiendo el modelo habitual del sector mediante APIs y SDKs, cuyos estándares pueden incluir YARA, STIX, TAXII, CybOX y más.

Arc Reactor provee los macro datos e incentivos requeridos para impulsar la inteligencia artificial que en resumidas cuentas desarrollará protección contra las amenazas. Contamos con que los datos respecto a amenazas se utilicen para variados fines distintos, como protección de Endpoints respaldada por IA, sistemas de detección/prevención de intrusiones, gestión de eventos e información de seguridad (SIEM), detección de botnets, así como detección y prevención de suplantación de identidad.

4.2 Guardian

Para proteger la tecnología de un usuario, son necesarias múltiples capas de seguridad, las cuales hacen referencia a software antivirus, seguimiento de violación de datos, protección contra robo de identidad, gestión de credenciales, copias de seguridad, DNS y muchos más sistemas. HEROIC.com denomina a dichas capas como puzle de la ciberseguridad.

Guardian es una plataforma unificada de ciberseguridad basada en la nube, la cual brinda una interfaz simple mediante la cual un individuo, una familia o una organización sería capaz de manejarse con todas las piezas de este puzle de la ciberseguridad.

En un principio, Guardian proporcionará las capas esenciales del puzle de ciberseguridad, mientras posibilita que desarrolladores y organizaciones contribuyan y sean recompensados por medio de integraciones con la tienda de aplicaciones de Guardian. Las aplicaciones de Guardian usarán APIs de desarrolladores para interactuar con los datos del ecosistema. Dicho conjunto de piezas aunará y hará más sencilla la gestión de la ciberseguridad.

Guardian combina inteligencia artificial con los datos provenientes de sus aplicaciones interconectadas y Arc Reactor, lo cual les permitirá detectar y prevenir ciberataques. Los usuarios de Guardian sacarán partido no solo de la inteligencia general facilitada por el Ecosistema, sino además de su propia IA personal, especialmente pensada para brindar protección a sus dispositivos y servicios en la nube. Cuantos más datos sean analizados, mayor capacitación del sistema, mayor inteligencia y protección frente ataques.

El paquete de software Guardian incorpora las siguientes tecnologías:

- Gestión de ciberseguridad unificada basada en la nube
- Agentes software y sensores de datos
- Gestión de Endpoints
- APIs para desarrolladores
- Tienda App Store para integraciones de terceros
- Motores IA específicos del usuario
- Gestión de transacciones en blockchain

4.3 Entorno de Investigación y Desarrollo

El Entorno de I+D permite acceder de forma simple a los datos respecto amenazas recopilados por Arc Reactor, gracias a la fusión de capacidad de investigación integral y desarrollo de software.

Disponemos de tutoriales y conferencias, para que los desarrolladores se formen en los campos de inteligencia artificial y ciberseguridad. A partir de dicha información, pueden generarse y posteriormente ser puestas a prueba sus propias creaciones basadas en datos históricos y en tiempo real, dentro de un entorno de desarrollo interactivo (IDE). Los desarrolladores serán incentivados además, para crear los mejores algoritmos de protección contra amenazas y con la posibilidad de vender su tecnología en el mercado a cambio de tokens HRO.

La plataforma de I+D propulsa a la comunidad de desarrolladores e investigadores, proveyéndolos de los conocimientos y recursos requeridos para moldear la próxima generación de protección contra amenazas.

El entorno de I+D abarca las tecnologías siguientes:

- Acceso a datos históricos de amenazas
- APIs para desarrolladores
- Sandbox (entorno de pruebas para software)
- Herramientas de software
- IA y comunidad de inteligencia sobre ciberseguridad
- Mercado impulsado por tokens HRO
- Gestión de transacciones en blockchain

4.4 Otras Tecnología

4.4.1 Software de Agente

El software de agente puede instalarse en dispositivos individuales, lo cual le dotará de diversas funcionalidades, como minería de amenazas, conexiones de ecosistema, protección de Endpoints, cartera segura para tokens HRO y una gestión sencilla del sistema.

El software del agente será compatible con una amplia gama de dispositivos, como: ordenadores de sobremesa, portátiles, teléfonos móviles y dispositivos IoT. Pretendemos desarrollar software de agente para los sistemas operativos más populares.

Cada agente individual estará en disposición de realizar un seguimiento activo de las acciones y cambios en: los archivos, tráfico del ecosistema, comportamiento de los usuarios y atributos de archivos. Los agentes pueden identificar de manera individualizada, cualquier irregularidad o amenaza, verificarla y emprender las medidas oportunas, garantizando con ello, la protección del usuario y de sus datos.

La comunicación dentro del ecosistema se realiza entre los agentes, el Arc reactor y el blockchain, para detectar las amenazas verificadas, incrementar la inteligencia del sistema y definir una recompensa por las amenazas identificadas. Dicha comunicación es útil para identificar y validar las amenazas, asistiendo con información en tiempo real sobre los ataques activos.

Los datos de amenazas verificados se transforman en informes anónimos, que una vez recibidos por el ecosistema, son de utilidad para que otros sistemas puedan evitar amenazas futuras y para que los desarrolladores elaboren algoritmos de protección contra amenazas, apoyándose en dicha información.

En cuanto ha sido plenamente desarrollado, el software del agente actuaría como protección principal del Endpoint del dispositivo, permitiendo identificar y bloquear amenazas, además de servir dotando de capacidad de procesamiento y almacenamiento al ecosistema, para vigilar e identificar las amenazas de forma remota.

4.4.2 Inteligencia Artificial (Cyberlytics®)

HEROIC.com se vale generalmente de inteligencia artificial para describir los múltiples sistemas y procesos inteligentes empleados en el ecosistema.

La Inteligencia Artificial dentro de la ciberseguridad comprende diversas áreas de estudio, entre las que destacan: matemáticas, aprendizaje automático, redes neuronales, reconocimiento de patrones, detección de anomalías y mucho más.

Cyberlytics® es el motor inteligente basado en IA, el cual es empleado por HEROIC.com para predecir y prevenir ataques cibernéticos con anterioridad a su ocurrencia. El motor de Cyberlytics analiza un inmenso volumen de datos de amenazas complejas a partir de la información suministrada por Arc Reactor, dando lugar a revelaciones cruciales empleadas en la protección automática de su tecnología, datos y, por ende, de usted.

4.4.3 Software de Blockchain

HEROIC.com utiliza contratos inteligentes de Ethereum para las transacciones, los cuales permiten operaciones de pagos directamente entre usuarios, organizaciones y desarrolladores de software. Gracias a un blockchain seguro respaldado en un registro distribuido, HEROIC.com posibilita la adquisición, mantenimiento y transferencia de tokens HROs. Incentivaremos y recompensaremos de forma constante a aquellos usuarios que contribuyen al ecosistema, con las transferencias de pagos por la distribución y el uso de los datos de amenazas.

Nos basamos en un algoritmo de consenso de prueba de trabajo (PoW) basado en el protocolo de PoW de Ethereum, el cual en última instancia se convertirá en el novedoso protocolo de Prueba de Trabajo de HEROIC.com.

4.4.4 Proof-of-Threat™

El novedoso protocolo Proof-of-Threat™ (prueba de amenaza) de HEROIC.com se empleará de modo general para cuantificar el trabajo completado por cada nodo de la red, y otorgará una puntuación a cada muestra individual de amenaza. A diferencia del despilfarro de energía y recursos preciados que supone el cálculo de hashes, el protocolo de Prueba de Amenaza permitirá a los mineros contribuir con su capacidad de computación al análisis y calificación de amenazas potenciales, siendo compensados de acuerdo a dicho trabajo de forma proporcional.

La puntuación de amenazas califica individualmente con un valor numérico a cada amenaza, atendiendo a la probabilidad de que la muestra sea efectivamente una amenaza. A mayor puntuación, mayor probabilidad de amenaza.

La puntuación de las muestras es beneficiosa, dotando de mayor control al sistema, ya que al cuantificarse, es más sencilla la toma de decisión respecto de bloquear o no la amenaza, que si solo se dispusiera de un valor binario -es o no una amenaza-.

Para puntuar la amenaza se atiende a la media aritmética ponderada de determinados criterios, que resulta en un valor de cero a cien (0 a 100). HEROIC.com adopta un enfoque de aprendizaje automático, ya que en principio califica cada muestra en un nodo, mientras que posteriormente irá empleando los datos de Arc Reactor para validar la puntuación inicial y aprender sobre dichos datos.

La puntuación de Prueba de Amenaza se determina a partir de algunos o todos los sistemas descritos a continuación.

- Ejecución previa
  - Motor HEROIC impulsado por IA Cyberlytics
  - Comparación del hash de los items con amenazas conocidas en el Arc Reactor
- Ejecución posterior
  - Análisis de items heurísticos que abarcan el comportamiento o las características de un archivo/proceso, lo cual pueda ser identificativo de que sea sospechoso.
  - Análisis de entorno de pruebas (Sandbox)

El protocolo Proof-of-Threat™, así como el motor de puntuación de amenazas vinculado al mismo, serán de código abierto y estarán disponibles a todo el público. Más adelante se publicará un whitepaper con mayor énfasis en la implementación inicial del Proof-of-Threat™.

4.4.5 Fijación de Precios de los Datos (Algoritmo Dinámico de Fijación de Precios)

El precio de los datos sobre amenazas es uno de los puntos más sensibles del ecosistema, ya que el sistema, por una parte debe alentar al usuario para que aporten datos con su estructura de precios, y por otro lado tener en cuenta el rechazo a los consumidores de los datos porque los costes puedan ser muy altos.
En vez de contar con un sistema de precios de oferta y demanda innecesariamente poco fluido, incómodo y complejo para el usuario, creamos un algoritmo de precios automatizado y en tiempo real, el cual incentiva a los proveedores de datos al maximizar la rentabilidad, mientras los consumidores de los datos de amenazas se ven atraídos al proveerse precios muy competitivos. El sistema podría considerarse análogo al empleado por Uber para ofrecer precios a sus usuarios y conductores. En este caso no se requiere que el usuario elija o que haya transparencia explícita en el modo en que se determinan los precios.
El algoritmo provee un sistema dinámico de precios, de acuerdo a la oferta y demanda de los datos provistos. Prestará especial atención a detalles tales como la antigüedad/tamaño de los datos, el tipo y su relevancia potencial, el volumen total de la orden, la calificación de la amenaza y otras circunstancias del mercado.
Al recibir feedback por parte de los usuarios del ecosistema y variar nuestra comprensión acerca del valor de los datos, tendremos que actualizar de manera constante el algoritmo e integrar aprendizaje automático para proporcionar un mercado cada vez más eficiente.

A continuación se muestra un ejemplo de la noción matemática actualmente implementada.

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

F = total de ingresos mensuales por cada minero de amenaza
M = Tipo 1 de datos (valorado en A%) (condicionado por otros factores)
N = Tipo 2 de datos (valorado en B%) (condicionado por otros factores)
P = Tipo 3 de datos (valorado en C%) (condicionado por otros factores)
X = ingresos obtenidos por los consumidores de datos durante ese mes

5 Detalles del Token

5.1 El Token HRO

En el desarrollo del Ecosistema HEROIC.com se erige en torno al token HRO (pronunciado "jirou"), el cual se usará como modo de autorización, incentivo y liquidación entre los participantes del Ecosistema, aparte de para otros servicios vinculados.

Se emitirá un suministro fijo de tokens HRO como parte de la venta de tokens, con contratos inteligentes adecuados y un registro en blockchain compatible con el estándar ERC20. El registro constituirá un modo seguro para que cualquier titular pueda mantener o transferir sus tokens HRO.

HEROIC.com pretende a desarrollar en un principio el software y los contratos inteligentes encargados de dirigir el ecosistema, aspirando a convertir el HRO en el nuevo estándar empleado en cualquier entorno de ciberseguridad y expandiéndose en el futuro a otros sectores.

5.2 Incentivos y Beneficios del Token

El Ecosistema se diseñó para proveer distintos niveles de acceso, valor y apoyo, de modo que se fomente la investigación, el desarrollo y la integración de tecnologías avanzadas de ciberseguridad, además de garantizar el acceso universal a dichas tecnologías. Los incentivos se gestionan a partir del uso de tokens HRO, en un Ecosistema donde operan múltiples transacciones, bien se trate de compras o de pagos entre los diversos participantes de HEROIC.com -usuario final, desarrollador y organización-.

5.3 Mercado de Tokens

HEROIC.com está formando un mercado sólido -impulsado por el token HRO- donde negociar los datos de amenazas. Los tokens HRO se pueden comprar con Bitcoin (BTC), Ethereum (ETH), - además de otras de las criptomonedas más populares-, o fiat.

Aquellos usuarios que poseen HROs, pueden usar sus tokens para comprar servicios actuales y futuros, bien de HEROIC.com, como de forma directa a través de cualquier otro socio del Ecosistema.

El token será listado en los criptoexchanges más selectos. Todo usuario del ecosistema dispondrá de una cartera segura con la que podrá gestionar sus tokens HRO.

5.4 Fondo de Crecimiento de Usuarios

Crearemos un fondo de crecimiento de usuarios, el cual motive a los mismos para colaborar activamente en las distintas materias del Ecosistema. HEROIC.com también alentará y facilitará el desarrollo de servicios adicionales, vinculados con la ciberseguridad, y que puedan ser negociados a cambio de tokens HRO.

6 Privacidad y seguridad

Un proyecto de la magnitud e importancia del Ecosistema de HEROIC.com, exige una declaración expresa sobre la importancia, así como de aplicación de la privacidad y seguridad.

La privacidad es de vital importancia para nosotros, por lo que pondremos especial énfasis en actuar de conformidad con las regulaciones aplicables, como: Prevención de Pérdida de Datos (DLP), directrices del NIST, requerimientos del GRDP y resto de mejores prácticas del sector de la ciberseguridad. En consecuencia, prestaremos especial atención a las herramientas, procesos y sistemas de protección de datos, con el propósito de garantizar la privacidad de los clientes de HEROIC.com y de cualquier dato almacenado.

HEROIC.com se esforzará en la medida de lo posible, en implementar las últimas tecnologías y estándares de ciberseguridad, y proseguirá su evaluación, y su transparencia respecto la tecnología empleada. Las políticas de HEROIC.com se han previsto para garantizar que los datos almacenados no caigan en manos de personas u organizaciones no autorizadas.

Integrando parte intrínseca de nuestro plan de ciberseguridad, contaremos un programa de recompensas -en tokens HRO- de detección de errores en cualquier apartado del diseño de nuestro proyecto. Cabe destacar que nuestro propósito es al fin y al cabo, incorporar todos los aspectos del ecosistema en un diseño de conocimiento cero.

Partiendo de normas éticas, nos reservamos el derecho unilateral de negar el acceso a la plataforma -e incluso a sus tokens- a cualquier participante o usuario que dañe a conciencia al ecosistema, plataformas o aplicaciones, o bien emplee los datos para fines poco éticos.

7 Otras tecnologías de HEROIC.com

HEROIC.com proviene de la mejora de una empresa -incluida en dos ocasiones en el prestigioso índice “Inc. 500”- especializada en ciberseguridad corporativa y desarrollo de software, fundada con el propósito de proteger de modo inteligente la información mundial. Bajo esta premisa, HEROIC.com ha participado activamente desarrollando una amplia gama de productos de ciberseguridad, los cuales hoy en día están disponibles y son empleados por grandes organizaciones.

7.1 HEROIC DarkHive™

HEROIC DarkHive es una de las mayores recopilaciones del mundo en cuanto a credenciales de usuario filtradas y comprometidas. HEROIC.com se basa en tecnología inteligente y analistas de ciberseguridad que supervisan continuamente la Dark y Deep Web, a la caza de hacks, brechas y cualquier otra fuente de datos comprometidos.

Los datos de hacking provistos por DarkHive se encuentran tanto a nivel resumido como detallado, para ser usados por empresas a escala internacional. El DarkHive constituye un gran repositorio de datos que sirve de fuente a HEROIC EPIC (ver siguiente).

7.2 HEROIC EPIC™

HEROIC EPIC permite descubrir, afrontar y prevenir el uso de credenciales de acceso robadas, derivadas de brechas y filtraciones de datos de terceros.

Durante 2016, más de 3.300 millones de registros -entre los que se incluyen emails, nombres de usuario y contraseñas de más de 1.700 violaciones de datos-, fueron puestos a disposición en la Dark Web. En cuanto son publicados, los hackers pueden emplear dicha información para acceder por fuerza bruta en los sistemas y ecosistemas de las empresas, donde ejecutar ataques selectivos. EPIC alerta ante vulnerabilidades y previene ataques al acceder a las mismas bases de datos filtradas hacia la Dark Web, informando a aquellas organizaciones, cuyos datos de empleados o clientes han sido comprometidos. De esta manera, los responsables de la seguridad pueden realizar los ajustes para evitar los inicios de sesión robados y no autorizados, que puedan perjudicar a sus legítimos propietarios.

8 Trabajos de Cara al Futuro

El equipo de HEROIC.com está convencido de que para lograr el propósito de una ciberseguridad universal de próxima generación, la tasa de desarrollo actual es insuficiente para hacer frente al auge de amenazas cibernéticas, de modo que exige una expansión sustancial y mayor agilidad en el desarrollo.

Tal como se ha comentado en el resumen, pronosticamos la aparición de -literalmente- miles de aplicaciones potenciales, que puedan emplear los datos provistos por el Ecosistema de HEROIC.com. No nos encargaremos personalmente de crear la mayoría de estas aplicaciones, sino de procurar hacerlo más cómodo y motivar al resto de usuarios del Ecosistema, para que den rienda suelta a la generación de dichas aplicaciones.

Los fondos recaudados de la venta de tokens se destinarán a los proyectos mencionados en el presente Whitepaper, priorizando la creación del Ecosistema de HEROIC.com, para que los usuarios dispongan de una plataforma descentralizada donde administrar todos los aspectos de sus particulares requerimientos de ciberseguridad.

El presente Whitepaper marca de forma exhaustiva el camino que nos guiará a la construcción del Ecosistema. No obstante, también consideramos que supone la casilla de salida para investigaciones acerca de software de ciberseguridad impulsado por IA, en el largo plazo.

Al investigar continuamente, se irán publicando nuevas versiones de este documento en HEROIC.com. Si tiene cualquier comentario o sugerencia, por favor contáctenos enviando un email a contact@HEROIC.com.

8.1 Trabajo Actualmente en Curso

Las materias nombradas a continuación representan trabajos en curso, los cuales se estiman que redunden en sustanciales beneficios para el ecosistema de HEROIC.com.

- **Una especificaci·n del protocolo de Prueba de Amenaza completamente desplegable**
- **Investigaci·n de soluciones innovadoras de almacenamiento descentralizado**
- **Estimaciones detalladas de rendimiento y puntos de referencia para el Ecosistema HEROIC.com, as² como el resto de sus componentes**
- **Algoritmos de aprendizaje autom§tico para un mercado m§s eficiente de datos sobre amenazas**
- **An§lisis de teor²a de juegos respecto los incentivos de HEROIC.com**
- **Transacciones en milisegundos a trav®s de ecosistemas fuera de blockchain, an§logos a los respectivos de Bitcoin https://lightning.ecosystem/ o Ethereum Raiden https://raiden.ecosystem/**
- **Integraci·n con otros blockchains**
- **Sanciones a aquellos participantes o usuarios que causen da¶os al ecosistema o a cualquier aplicaci·n, o cuando empleen los datos con una finalidad incompatible con la ®tica**
- **Dise¶o de conocimiento cero**

9 Agradecimientos

Este trabajo deriva del esfuerzo continuo y prolongado de varios miembros que componen el equipo de HEROIC.com, y habría sido imposible sin la ayuda, feedback y evaluación de los colaboradores y asesores de HEROIC.com. Chad Bennett es el diseñador original del Ecosistema HEROIC.com. Él y David McDonald redactaron el presente whitepaper cooperando con el resto del equipo, con aportaciones significativas, feedback, evaluaciones y conversaciones. Tammy Bennett ayudó a mejorar la estructura y la redacción del documento, mientras que Wyatt Semanek se encargó de las ilustraciones y terminó de maquetar el texto. Para crear este documento se consultaron distintos Whitepapers relacionados con la criptografía, los cuales también se citan en las referencias bibliográficas (8), (9), (10) y (11). También queremos expresar nuestro agradecimiento a todos nuestros colaboradores y asesores por sus útiles conversaciones y apoyo.

10 Apéndice

[Ciberseguridad - Una Breve Historia]

Glossary

Impulsado por IA: Aquel software basado en inteligencia artificial o algoritmos de aprendizaje automático -en vez de requerir interacción humana- para enriquecer la inteligencia del software.

Algoritmo: Conjunto de reglas que permiten resolver un problema en un número finito de pasos, además de encontrar el máximo común divisor.

Inteligencia Artificial: Teoría y desarrollo de sistemas informáticos con la capacidad de ejecutar tareas, las cuales de forma habitual requieren interacción humana, tales como percepción visual, reconocimiento del habla, toma de decisiones o traducción de idiomas.

Macro Datos: Cluster de datos de inmenso volumen, el cual puede analizarse con potencia informática que permita poner de manifiesto patrones, tendencias y asociaciones, especialmente relacionadas con el comportamiento e interacciones humanas.

Blockchain: Véase https://HEROIC.com/blockchain-overview

Criptomoneda: Moneda digital encriptada y que incorpora métodos que rigen la generación de unidades monetarias y verificación de transferencia de fondos, en un entorno donde se ejecutan las operaciones, prescindiendo de un banco o autoridad central.

Ciberseguridad: Conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, ordenadores, programas y datos, frente a ataques, daños o accesos sin autorización.

Minería de datos: Proceso que permite descubrir patrones y relaciones interesantes y de utilidad a partir de ingentes cantidades de datos.

Descentralizar: Dispersar (algo) respecto de un área concentrada; crear algo pero prescindiendo de su restricción de control o uso a un grupo reducido.

Democratizar: Convertir en accesible y abierto de manera universal a cualquier individuo. El poder se transmite al pueblo, siendo ejercido directamente por el mismo.

Moneda Fiat: Moneda que un gobierno ha declarado como de curso legal, aunque no está respaldada por un bien físico. El valor del dinero fiat proviene de la relación entre oferta y demanda, en vez del valor del material que representa al dinero. Ejemplos de moneda fiat: dólar de USA, el euro, la libra esterlina, etc.

HEROIC Arc Reactor: Plataforma unificada de gestión de amenazas de HEROIC.com, diseñada para integrar la inteligencia, así como los datos provenientes del entorno de ciberseguridad.

Ecosistema HEROIC.com: El innovador sistema o red de partes interconectadas e interactivas, protege al mundo ante amenazas cibernéticas tan rápido como se crean, e incluso más rápido. El sistema está respaldado por tres nuevas plataformas que juntas crean un conjunto de soluciones universales de ciberseguridad rápidas, actualizadas y proactivas.

HEROIC Guardian: Una plataforma unificada y basada en la nube, creada por HEROIC.com para proteger a los usuarios de las amenazas cibernéticas, apoyándose en inteligencia artificial.

Aprendizaje automático: Habilidad de las computadoras para aprender sin ser programadas específicamente para tal efecto. Realiza predicciones a partir de los datos.

Minero de amenazas: Usuarios de software de minería de amenazas de HEROIC, los cuales se encargan de buscar, validar y distribuir informes sobre amenazas a la red.

Protección contra amenazas: un servicio o sistema implementado para brindarle protección a usted o a su empresa, frente a problemas o ataques maliciosos.

Diseño de conocimiento cero: Diseño de software, donde el almacenamiento de datos en los sistemas, es encriptado con pares de claves públicas y privadas, de modo que el proveedor de almacenamiento, carece de la posibilidad de desencriptar o visualizar los datos.

11 Referencias

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]