UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

Emprendedorismo

TRENCH

Docente: Virginia Santos

Alumnos:

- Menel Angelo - 1804789
- Garza Leandro - 2012580
- Vietto Santiago - 1802890

Facultad: Ingeniería

Año: 2023

TRENCH

Storytelling

Tu Guardaespaldas Digital

Hace algún tiempo, en un mundo lleno de conexiones digitales, comenzaron a surgir amenazas invisibles. Todos escuchamos sobre esos engañosos ataques de phishing en WhatsApp y Gmail. Fue entonces cuando en la materia “Seguridad y Auditoría Informática” dictada por el Ing. Gaiero, con un grupo de amigos interesados en el ámbito, decidimos hacer algo al respecto, aprovechando los conocimientos adquiridos.

El grupo surgió cuando vimos en el aula quiénes éramos los interesados en el proyecto. En este caso tenemos a Santiago Vietto, quien a lo largo de su trayectoria como estudiante de ingeniería en sistemas también desarrolló numerosos cursos sobre Telecomunicaciones, redes Cisco, bases de datos y algoritmos. Otro de los miembros del grupo es Leandro Garza, quien cuenta con conocimientos avanzados sobre el hacking ético y ciberseguridad. Finalmente se sumó al equipo Angelo Menel y su especialidad en programar en Python.

Ahora es cuando entra en escena TRENCH, nuestro guardaespaldas digital. Imagina a Trench como el guardián silencioso que defiende tu celular, junto tus datos personales, contra las amenazas cibernéticas.

Si bien teníamos la parte técnica del proyecto bajo control, nos dimos cuenta de que debíamos aprender sobre la tarea crucial de buscar apoyo financiero. Necesitábamos entender cómo presentar nuestro proyecto a inversores, cómo comunicar la esencia de TRENCH a personas interesadas que pudieran colaborar invirtiendo en el mismo. Fue justo cuando, entre todos los integrantes del equipo, comenzamos con la materia “Emprendedorismo”, en la cual pudimos aprender todo lo mencionado y más.

La historia de TRENCH es la historia de simplificar la ciberseguridad. Sabemos que no todos somos expertos en tecnología, pero todos merecemos sentirnos seguros en línea. TRENCH es como el amigo que siempre está alerta, detectando esos intentos de ataques antes de que se conviertan en problemas reales.

La interfaz de TRENCH es como un mapa claro en tu viaje digital, mostrándote dónde hay peligros y cómo sortearlos. Es tu cómplice en la lucha contra los ciberdelincuentes. Y cuando se trata de esos ataques que escuchamos

en las noticias, TRENCH no solo detecta, ¡también responde automáticamente para mantenerte a salvo!

Propuesta de valor

Trench es una aplicación mobile que tiene como objetivo monitorizar los compromisos del sistema operativo del teléfono celular, mediante la recopilación de metadatos de la red en tiempo real, para detectar y analizar amenazas o incidentes, y de esta manera proteger los activos, prevenir nuevos ataques y ofrecer al cliente seguridad, facilidad de uso, transparencia y alto rendimiento.

Creemos que todas las personas que son usuarios de sistemas comunes y corrientes, en específico usuarios de dispositivos móviles deberían poder operar la ciberseguridad con velocidad y precisión. Por ende, TRENCH es una solución integral y flexible, que ayuda a las personas a comprender si hay actividad adversa en su teléfono celular, con datos contextuales, sobre cuando se ha producido actividad maliciosa y como está impactando en dicho usuario.

Por ende buscamos lograr que operar con ciberseguridad no sea complicado, detectar compromisos o ataques de forma inteligente, responder de forma automática y visualizar los incidentes con una aplicación mobile.

En este caso, Trench está diseñado para que los usuarios hagan uso del mismo en diferentes sistemas operativos, tales como IOS y Android.

El sistema busca ayudar a detectar todos y cada uno de los contactos con el atacante, lo que permitirá actuar con decisión para mitigar esos incidentes y los efectos potencialmente catastróficos que pueden causar.

Dentro de las funcionalidades que podemos visualizar en la interfaz son:

- Homepage: brinda una vista general de cómo se ataca a nuestro sistema. Podemos comprender nuestro estado de compromiso y la actividad de incidentes en un alto nivel.
- Vista de incidentes: brinda un desglose detallado de la cantidad de incidentes, tipos de ataques, cuando se produjeron los incidentes y los activos afectados. A su vez, cada incidente se puede visualizar individualmente para obtener más detalle del mismo.
- Redes sociales: el usuario tendrá la posibilidad de vincular a TRENCH sus cuentas de WhatsApp e Instagram, para que estén permanentemente monitorizadas y de esta forma prevenir intrusiones en estas, como hackeos o intento de robo de credenciales.
- Email: al igual que con las redes sociales, el sistema permite vincular su cuenta de email para controlar la casilla de correo electrónico de phishing o spam.
- Archivos de descarga y páginas web: la aplicación puede monitorizar la red, cualquiera sea el navegador, para evitar la descarga de archivos corruptos o el acceso a páginas comprometidas.

- Defender: opción de agregar APIs creadas por otras empresas de ciberseguridad para automatizar la respuesta ante un ataque.

Una red que está comprometida se comporta de manera diferente que otra que no lo está, es por eso que los metadatos de la red proporcionan la fuente definitiva de verdad. TRENCH recopila metadatos de la red a través de múltiples métodos para la recopilación de datos, lo que hace que el proceso sea fácil y simple.

Todos los ataques exitosos tienen un denominador común: el ciberdelincuente debe usar la red. Es por eso que los metadatos de nuestra red son la única fuente de verdad para medir y comprender de manera continua e intencional el compromiso. Nuestro dispositivo genera enormes cantidades de metadatos, comenzando con consultas de DNS, flujos de red, proxy logs, firewall logs, etc.

Esta correlación de metadatos proporciona inteligencia invaluable sobre los intentos de ataques y los patrones de ataques. Por eso, la idea es recopilar las diferentes piezas de metadatos, de diferentes orígenes, en tiempo real, y que dicha información sea procesada por los IoCs, para que en una interfaz amigable y fácil de utilizar, se pueda realizar un seguimiento de posibles amenazas, medir el impacto de uno o varios incidentes, mitigar ataques, todo esto gracias a la lectura, análisis y monitoreo que se realiza por detrás. Todo esto con el fin de proteger los activos del cliente y la integridad del sistema.

Marco teórico

Conceptos

Metadatos: Datos que describen otros datos, grupo de datos que describen el contenido informativo de un objeto al que se denomina recurso. Ayudan a calificar y encontrar datos.

Consultas DNS: Los servidores DNS convierten las solicitudes de nombres en direcciones IP, con lo que se controla a qué servidor se dirigirá un usuario final cuando escriba un nombre de dominio en su navegador web. Estas solicitudes se denominan consultas.

Flujos de red: Un flujo de red es una serie de comunicaciones entre dos puntos finales que están limitadas por la apertura y el cierre de sesiones. Hay una gran cantidad de datos en flujo.

Proxy logs: Un servidor proxy es un equipo que intercepta y administra el tráfico entre dos dispositivos, redes o protocolos. Los proxies son pasarelas que actúan como intermediarios entre su equipo y los sitios web y servicios de Internet que

utiliza. Retransmite el tráfico entre nuestro dispositivo y la Web, con lo que evita que nuestro navegador esté en contacto directo con los sitios que visita. Sus solicitudes web pasan primero a través del servidor proxy, a continuación, este envía su solicitud al servidor web correspondiente y reenvía la respuesta a su dispositivo. Al actuar como intermediarios, los proxies ayudan a proteger su privacidad y a reforzar la seguridad de su red local.

Un servidor proxy web puede enmascarar nuestra dirección IP, lo cual dificulta al servidor web rastrear su ubicación física. No obstante, al ocultar la dirección IP no se cifra el tráfico de Internet, esto quiere decir que sus solicitudes de datos, incluidos los nombres de usuario, las contraseñas y otros datos de las cuentas, no están protegidas ni ocultas.

Firewall logs: Un firewall es un sistema diseñado para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet. Estos pueden ser de tipo hardware o software, o una combinación de ambos. Los firewall protegen nuestro dispositivo, o una serie de dispositivos en una red, de los sitios web llenos de malware o de los puertos de red abiertos vulnerables. Ayudan a detener a los posibles atacantes antes de que puedan causar algún daño. Los firewall de red pueden encontrarse en empresas, hogares, escuelas e intranets, las cuales son redes privadas dentro de una organización. Además, pueden configurarse para impedir el acceso a usuarios de la red a sitios web externos.

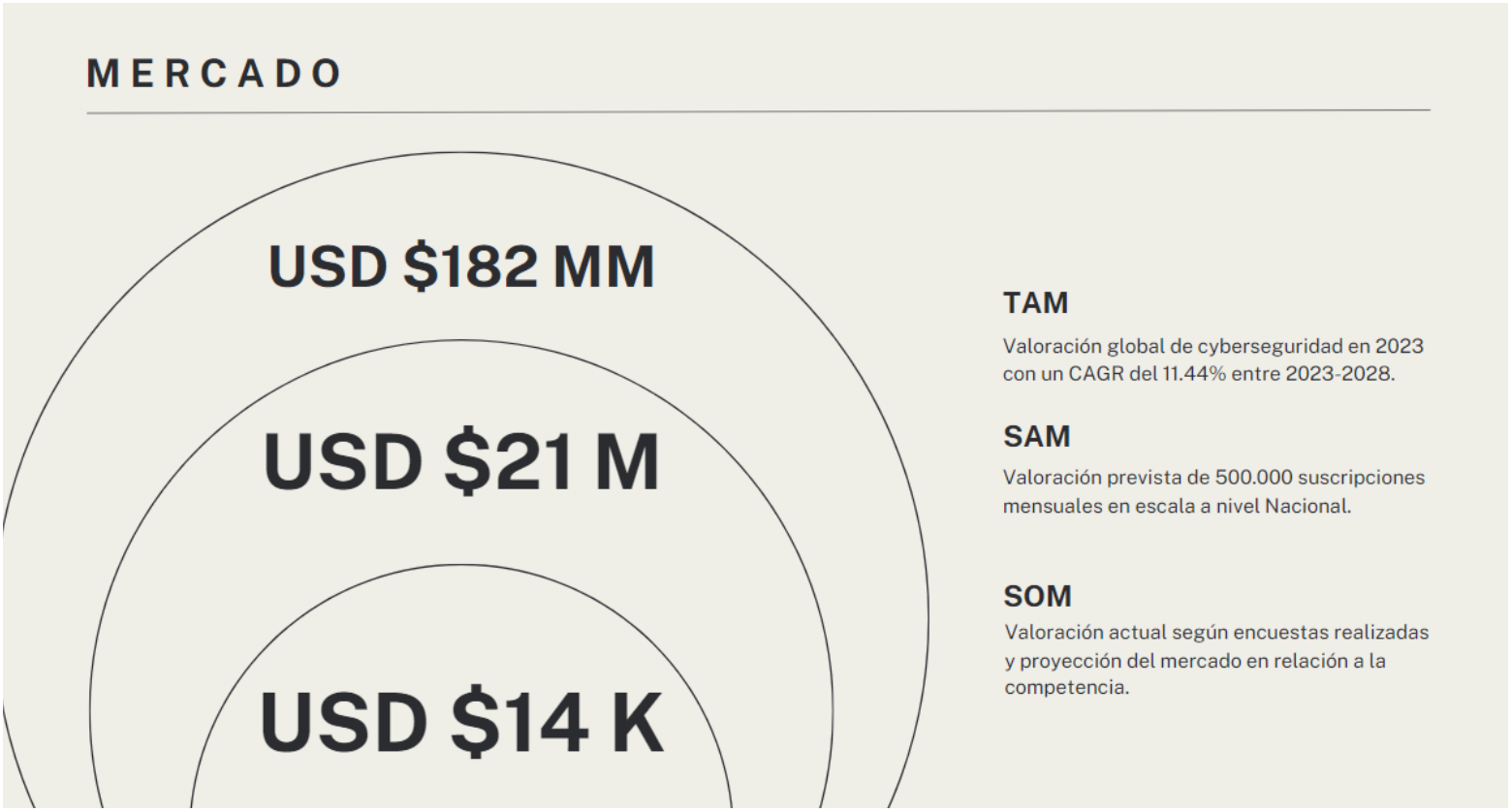
Indicadores de compromisos: Un Indicador de compromiso (IOC) es un conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. Toda aquella información relevante que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.

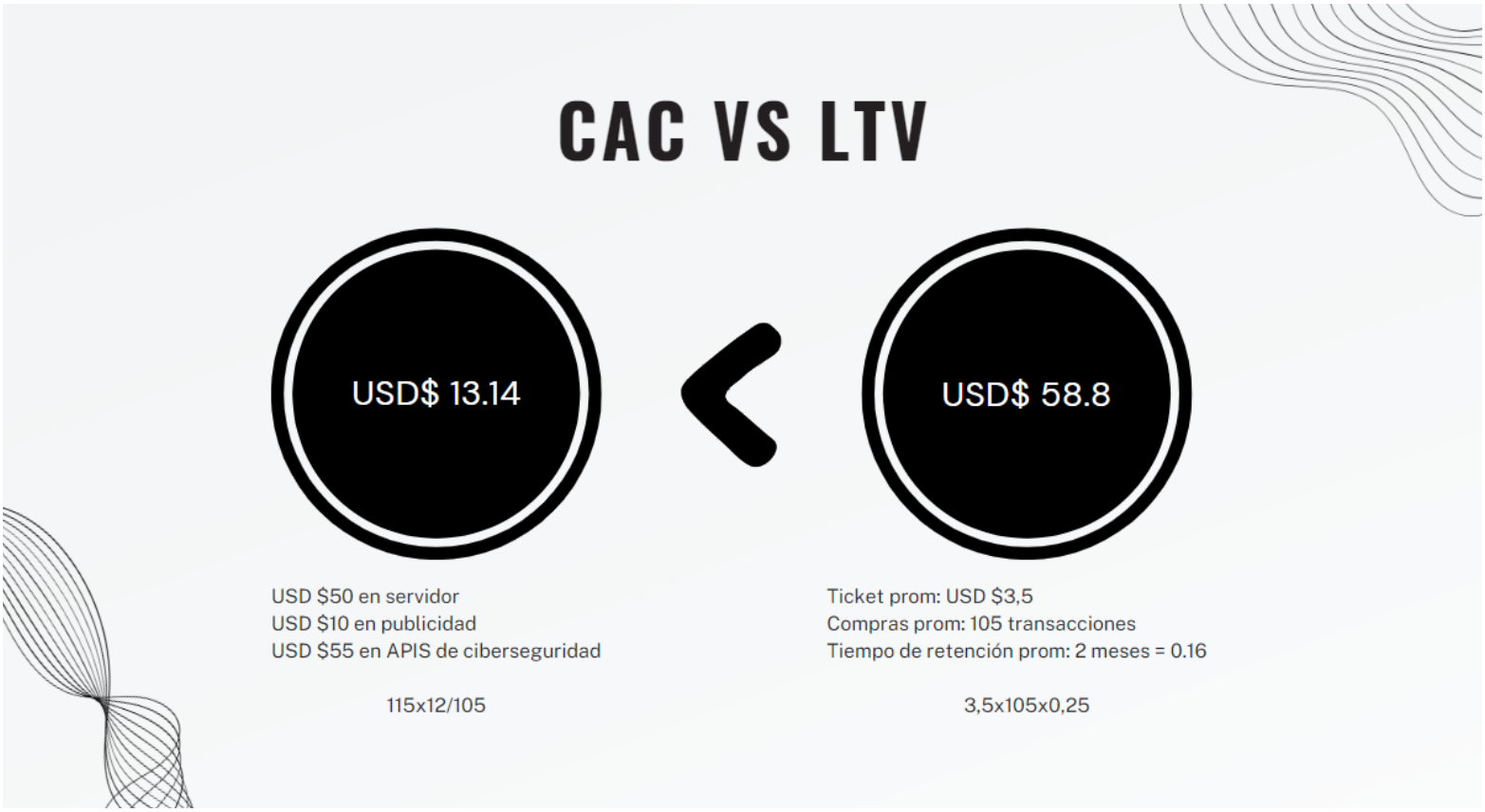
Malware: proviene del inglés malicious software, y en español significa software malicioso. Es un software que tiene como objetivo infiltrarse en el sistema y/o dañar la computadora sin el conocimiento de su dueño. Hay muchos tipos de malware, ya que es un término muy genérico, por ende nombramos los más conocidos en el ámbito de dispositivos móviles:

- Adware: Muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo.
- Keylogger: Programa espía que registra todas las pulsaciones del teclado para robar claves e información sensible del usuario. Puede ser hardware pero por lo general es software.
- Pharming: Es engañar al ordenador suplantando lo que es el servicio de DNS mediante el archivo hosts local, dirigiendo así al usuario a un sitio distinto del que cree estar abriendo, y así engaña al ordenador.

- Phishing: Consiste en obtener información confidencial engañando al usuario con páginas o correos que se hacen pasar por entidades a las que normalmente uno accede o utiliza, para cargar un malware por ejemplo, y cuanto más convincente son mayor éxito tienen. Básicamente es mandar un mensaje al usuario que lo preocupe, que lo haga abrir un archivo o ir a un enlace y así poder ser engañado.
- Spam: Es correo electrónico masivo no deseado con fines publicitarios. Spyware: Son aplicaciones que recopilan información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet. Al fin y al cabo cualquier red social es un gran spyware, pero donde uno es consciente y acepta para poder utilizarlo.
- Troyano: Es un programa o conjunto de programas relacionados que bajo una apariencia inofensiva se ejecuta de manera oculta en el sistema y permite el acceso remoto de un malware o usuario no autorizado al sistema. Este viene bajo el concepto de caballo de Troya, donde por fuera es algo y por dentro otra.
- Virus: Software malicioso que se adhiere a un archivo ejecutable, macro, correo, etc. Tiene la capacidad de auto-replicarse infectando otros archivos, y generalmente se utiliza como un vector para transferir troyanos o backdoors. En fin este se adosa a archivos y se replica a través de estos.
- Worm (gusano): Es un tipo de virus, pero que se replica de un sistema a otro en forma automática a través de la red. Este se adosa a la red.

Análisis del mercado





Business Model Canvas

TRENCH

SOCIOS CLAVE

- *CISCO*
- *Fortinet*
- *Red Hat*
- *Mc Safe*
- *Hornetsecurity*

ACTIVIDADES CLAVE

- *Análisis del mercado y competencia.*
- *Desarrollo de pagina web y red social como estrategia de marketing del producto, incluyendo el pago de publicidad.*
- *Análisis y obtención de requerimientos en base a encuestas.*
- *Diseño de la aplicación.*
- *Construcción de la aplicación.*
- *Implementación, testing, y despliegue.*
- *Modulo de pago en funcionamiento.*
- *Promocionar el uso de la herramienta durante 30 días de forma gratuita.*
- *Medios de contacto disponibles para atender consultas.*

RECURSOS CLAVE

Personal
Ingenieros en sistemas especializados en ciberseguridad y telecomunicaciones

Capital
Inversión privada

Infraestructura
Mobile

Tecnología
IoCs, Cloud, Proxy Firewall, SpamBox, Netflows, DNS & Social networks.

PROPUESTA DE VALOR

Aplicación mobile que tiene como objetivo monitorizar los compromisos del sistema operativo del teléfono celular, mediante la recopilación de metadatos de la red en tiempo real, para detectar y analizar amenazas o incidentes, y de esta manera proteger los activos, prevenir nuevos ataques y ofrecer al cliente:

- *Seguridad*
- *Facilidad de uso*
- *Transparencia*
- *Alto rendimiento*

RELACIÓN CLIENTES

La relación con los clientes es del tipo asincronico ya que se recopilara información desde:

- *Canales de comunicación.*
- *Atención al cliente.*
- *Página web de la empresa.*

CANALES

Los canales de comunicación y visualización serán:

- *Redes sociales*
- *Teléfono*
- *Email*
- *Página web*

SEGMENTO CLIENTES

El sistema estará dedicado a todas las personas (usuarios comunes) que deseen operar ciberseguridad de manera sencilla mediante su dispositivo mobil.

Sera viable tanto para usuarios de:

- *IOS*
- *Android*

COSTES DE ESTRUCTURA

- *Programadores*
- *Expertos en ciberseguridad*
- *Expertos en telecomunicaciones*
- *Administradores Linux*
- *Equipo de marketing*
- *Impuestos*
- *Gastos operativos (servidores, APIs, hardware)*
- *Mantenimiento*

FUENTES DE INGRESO

La principal fuente de ingreso será mediante el pago de la licencia de la aplicación, a modo de suscripción, de manera mensual, por parte de nuestros clientes (suscriptores)

Métodos de pago:

- *Tarjeta de crédito/debito*

Sombreros

Sombrero Negro (logico-negativo): Como integrante con el sombrero negro, me surgieron algunas preguntas con respecto a Trench: ¿Qué pasa si no detecta correctamente los malware inyectados?, ¿Qué pasa si Trench detecta como amenazas actividades normales? ¿Estás seguro que las pymes van a poder costear el precio del producto? cómo van a procurar adaptarse a cada uno de los malwares recientes? (ya que estos se actualizan constantemente), ¿Vamos a tener los fondos necesarios para costear a los empleados?

Sombrero Amarillo (lógico-positivo): En un principio, considero viable la realización de la herramienta, ya que contamos con profesionales especializados en el área de ciberseguridad, el equipo posee una base sólida de fundamentos teórico-prácticos para encarar el proyecto, la probabilidad de adquirir una primera inversión por parte del seno familiar es casi un hecho, y se nota un claro entusiasmo y compromiso por parte de los integrantes hacía con la idea final.

Sombrero Rojo (pasional): Mi misión en esta vida es que todo el mundo esté a salvo, es por eso considero a Trench como la solución óptima, para que todas las personas comunes y diferentes empresas, le hagan frente al ciberataque, con una herramienta intuitiva y fácil de usar.

Sombrero Blanco (objetivo): Como entusiasta de los datos objetivos y claros, quisiera saber cual es el porcentaje de acierto en cuanto a la detección de amenazas por parte de Trench. Además me gustaría ver algunos de los casos ejemplos en los cuales Trench haya ayudado a detectar o mitigar.
Finalmente, si Trench hace una recopilación de los metadatos que se encuentran en la red, esto lo hace cumpliendo con las distintas políticas de privacidad que existen?

Sombrero Azul (control): En cuanto a mi deber como persona con sombrero azul, me surgieron algunas ideas de lo que debería ser importante prestar atención. Esto es, que al ser un servicio que opera en tiempo real, tenemos que garantizarnos que el proceso de recopilación de metadatos sea continuo y sin interrupciones. De otro modo, si hubiera interrupciones, ese tiempo sería vulnerable.
Como sombrero que básicamente tiene mucho cuidado del control, también creo que deberíamos hacer controles regulares sobre el correcto funcionamiento de la herramienta. En este tipo de controles o pruebas, pueden aparecer incidentes o resultados no queridos, para los cuales deberíamos tener un plan de respuesta

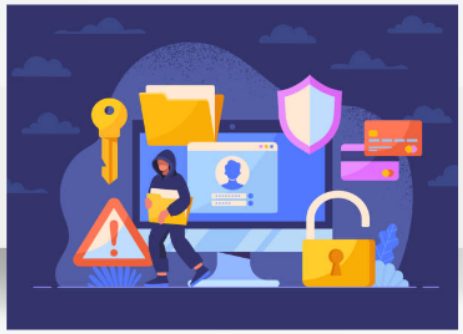
Sombrero Verde (creativo): Como integrante del equipo Trench, no puedo imaginar en otra cosa que no sea que los usuarios normales (sin tanto conocimiento sobre ciberseguridad) puedan entender la presentación de datos, todo esto facilitado por la herramienta.
Otra cosa que podría pensar es si Trench se puede utilizar en algún otro ámbito fuera de la ciberseguridad, que características adicionales podríamos agregarle a Trench para que su porcentaje de detección sea mayor o sí con todas las IA que estan saliendo, habrá alguna manera de que Trench pueda aprender solo de las nuevas formas de malware que se crean diariamente.

Pitch Deck

TRENCH

First line of defense

PROBLEMA/OPORTUNIDAD



SOLUCIÓN

MOBILE APP } CROSSPLATFORM

ANALIZA METADATOS EN TIEMPO REAL }

- PARA QUE EL USUARIO PUEDA:

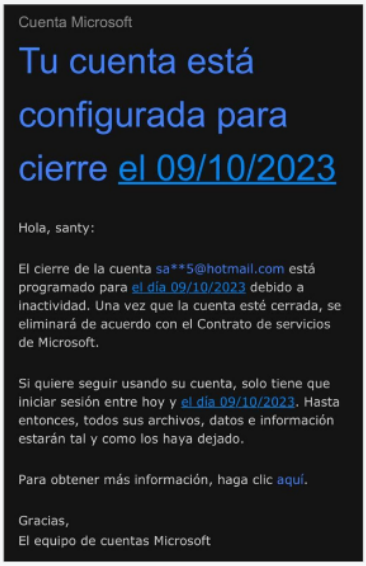
PREVENIR Y DETECTAR INTRUSIONES

MITIGAR ATAQUES

MEDIR EL IMPACTO DE INCIDENTES

FUNCIONAMIENTO

RECURSO


Cuenta Microsoft

Tu cuenta está configurada para cierre el 09/10/2023

Hola, santy:

El cierre de la cuenta sa**5@hotmail.com está programado para el día 09/10/2023 debido a inactividad. Una vez que la cuenta esté cerrada, se eliminará de acuerdo con el Contrato de servicios de Microsoft.

Si quiere seguir usando su cuenta, solo tiene que iniciar sesión entre hoy y el día 09/10/2023. Hasta entonces, todos sus archivos, datos e información estarán tal y como los haya dejado.

Para obtener más información, haga clic aquí.

Gracias,
El equipo de cuentas Microsoft

RECOPILACIÓN Y ANALISIS DE METADATOS

- Correos electrónico: Remitente y Destinatario
- Asunto
- Fecha y Hora
- Ruta de Entrega (Received)
- Dirección IP de Origen
- URL del enlace
- Lengua, ortografía y gramática
- Gráficos
- Archivos adjuntos

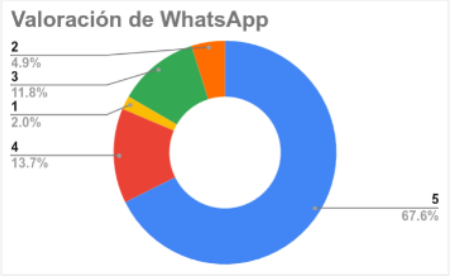
loc

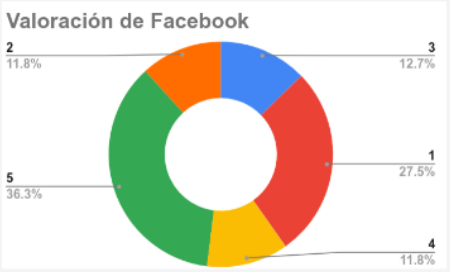
COMPARACIÓN CON BD DE FIRMAS DE MALWARE Y AMENAZAS O ATAQUES CONOCIDOS

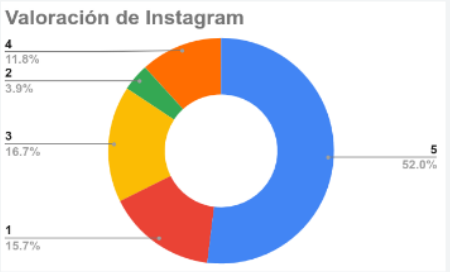
Obtención de resultados, generar alerta y sugerir acción de mitigación

DATOS DE ENCUESTA

- Cantidad de personas encuestadas: 102.
- Localidades: Córdoba, La Rioja y Neuquén.
- Resultados según la importancia de protección de datos en las siguientes aplicaciones:







MVP

WHATSAPP

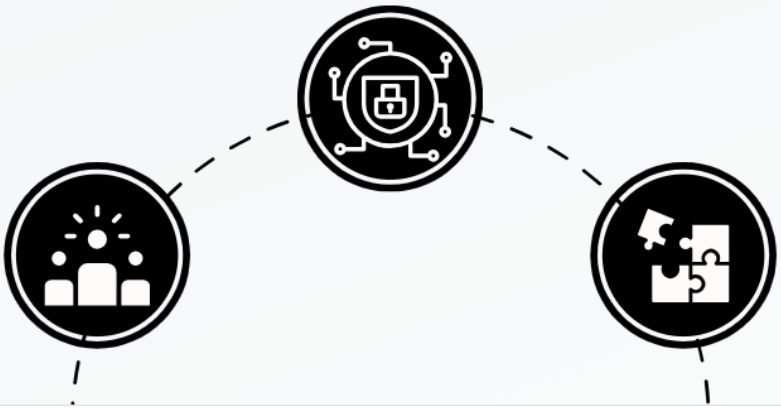
INSTAGRAM

EMAIL

APLICACIÓN

MTP

"Crear tu guardaespaldas digital"



MODELO DE NEGOCIO

PÚBLICO EN GENERAL

- APLICACIÓN MOBILE
- SUSCRIPCIÓN MENSUAL DE USD$ 3,5
- PROMOCIONES DE DESCUENTO POR N MESES

VERSIÓN DE PRUEBA GRATUITA POR 30 DIAS

EQUIPO

Santiago Vietto

CEO

Ingeniero en Sistemas - Analista en Ciberseguridad

Angelo Menel

Project Manager

Ingeniero en Sistemas - Fullstack Dev

Leandro Garza

Tech Lead

Ingeniero en Sistemas - DevSecOps

SOLICITUD DE INVERSIÓN

MERCADO

TAM	USD $182 MM
SAM	USD $21 M
SOM	USD $14 K

CAC - LTV

USD$ 13.14 < USD$ 58.28

USD $15.000