INSTITUTO TECNOLÓGICO DE BUENOS AIRES – ITBA

ESCUELA DE (TECNOLOGÍA - GESTIÓN)

Sistema integral de Ciberseguridad para Pequeñas y Medianas Empresas en Argentina

AUTOR: Abastante Santiago Nicolás (Leg. Nº 104572)

DOCENTE: Pedro del Campo

TESIS PRESENTADA PARA LA OBTENCIÓN DEL TÍTULO DE ESPECIALISTA / MAGÍSTER EN DIRECCIÓN ESTRATÉGICA Y TECNOLOGÍA.

BUENOS AIRES

PRIMER CUATRIMESTRE, 2022

Resumen Ejecutivo

La transformación digital ha llegado a nuestras vidas para quedarse principalmente debido al cambio de normalidad introducido por el COViD-19. La democratización de la tecnología ha impulsado a todas las empresas a abrazar la transformación digital como herramienta principal para materializar sus operaciones de negocio.

El gran problema es que la tecnología se comporta como una espada de doble filo, puesto que además de ser un gran facilitador del negocio, también introduce grandes cantidades de riesgos de seguridad que, si no son tomados seriamente, pueden afectar considerablemente, no siendo pocas las organizaciones que han cesado sus operaciones por ataques informáticos, en la gran mayoría de los ataques, los cibercriminales no diferencian entre objetivos y utilizan las mismas técnicas, ataques y amenazas.

En la República Argentina existen 602.805 pequeñas y medianas empresas (Ministerio de Producción y Trabajo de la Nación, 2018), las que, en su mayoría, no pueden afrontar los costos de implementación de un sistema de ciberseguridad. Esto se debe a que l**os competidores existentes centran sus servicios sobre aquellas empresas que pueden adquirir sistemas complejos y muy costosos**. A su vez requieren ciertas capacidades operativas existentes para poder aprovechar el valor de sus servicios. **Es aquí donde Solidarity brilla, ofreciendo una alternativa económica y a la medida para empresas que no disponen de estas capacidades.**

Es por esto que hemos adoptado un modelo de negocios B2B (Business to Business), ofreciendo servicios de soporte estructural a las operaciones de todas las organizaciones que utilicen sistemas informáticos. **Podemos aportar valor agregado a todas las industrias y sectores y, al tratarse de un sistema SaaS (Software as a Service), podemos**

ofrecerlo sin importar la ubicación geográfica del cliente. De todas maneras, en esta primera etapa enfocaremos nuestros esfuerzos sobre aquellas provincias de la República Argentina con mayor densidad empresarial.

Para capturar estos clientes, **nuestra estrategia competitiva se basará en una solución de bajo coste, de suscripción mensual y sin requerimientos de inversiones iniciales.** Ofreceremos capacidades de elevar el nivel de seguridad de todas las empresas por igual, sin importar su capacidad de inversión. **Esto podrá lograrse gracias a una conjunción entre servicios freemium y una estrategia de "Pay as You Go",** permitiendo a los clientes adaptar sus mecanismos de detección en función de su capacidad de pago. Es así que haremos valer nuestra Propuesta de Valor "Defensa ante ciberamenazas, al alcance de todos."

El personal trabajará completamente a distancia, no dispondremos de oficinas físicas de ningún tipo. Esto permite reducir ampliamente los costos de operación y circunscribir los costos variables a aquellos asociados directamente con la infraestructura cloud requerida. Teniendo en cuenta que **los recursos utilizados escalan automáticamente en función de la demanda, ofrecen la capacidad de disponer de una infraestructura elástica.** La suite tecnológica se basa principalmente en tres elementos:

1) **Solidarity** - "Discovery": Un software gratuito y open source diseñado para ser configurado en la red de la empresa y diagnosticar el estado de situación. Dispone de una aplicación que automáticamente ofrecerá un informe detallado de los desvíos, configuraciones y vulnerabilidades que la empresa debe resolver. Está diseñado para quien gestione los recursos informáticos de la empresa sin necesidad de conocimientos técnicos específicos de seguridad.
2) **Zener SaaS**: La versión paga del Solidarity, complementa las capacidades ofrecidas anteriormente con la posibilidad de disparar alertas ante la detección de anomalías, correr chequeos rutinarios de detección y hasta implantar un centro de monitoreo,

detección y respuesta a incidentes. De esta manera permite generar información accionable para los recursos de IT e implementar controles detectivos y preventivos de seguridad.

3) **Contenido Multimedia de Información**: Desarrollo web gratuito donde quien requiera conocer la solución a algún problema de seguridad encontrará explicaciones detalladas y concisas. El objetivo es unificar el conocimiento ya existente y esparcido en la internet, traducido al idioma castellano que en muchos casos suele ser una limitante para los recursos de IT.

Teniendo en cuenta la alta demanda existente, la falta de competencia en este sector particular y el exponencial aumento de la consciencia de los empresarios respecto al riesgo que introduce la cibercriminalidad en sus operaciones, y basados en las proyecciones elaboradas (las que serán abordadas más adelante), consideramos que podemos alcanzar una facturación de 33 millones en los próximos 5 años, con una unidad neta acumulada que ronde los 77 millones, esperando recuperar la inversión a los 3 años de haber comenzado con la operación. Es por esto, y teniendo en cuenta tanto el valor actual neto como la tasa interna de retorno, podemos afirmar que el proyecto es rentable.

Índice

Índice de Figuras

Índice de Tablas

Introducción

Ya debe ser un cliché mencionar que estamos atravesando tiempos de mucha incertidumbre. El contexto global es por demás complejo, teniendo en cuenta el drástico cambio en lo que consideramos como normal debido a la pandemia de COVID-19.

Con esta variable de entorno marcando nuestro contexto, tanto a nivel mundial como regional, las organizaciones han tenido que adaptarse rápidamente para poder sobrevivir, adelantando el abrazo a la transformación digital de manera improvisada, desencadenando una serie de acontecimientos sistémicos que posicionan a las organizaciones en circunstancias poco favorables, dependiendo absolutamente de la tecnología para operar. A su vez, estas no son conscientes de los riesgos que esta introduce, pudiendo quedar fuera del negocio en un abrir y cerrar de ojos.

¿Por qué sucede esto? El principal problema es que la tecnología elimina las fronteras físicas de protección que ofrecen los estados, si tenemos en cuenta lo referido en (LACNIC, 2020) *"Los ciberdelincuentes entienden la debilidad y las restricciones de los diferentes países y sus agencias de aplicación de la ley. Saben que, si colocan el contenido malicioso fuera de sus jurisdicciones, disminuirá la velocidad con la que pueden investigar las naciones respetuosas de la ley."*.

En nuestro país esto se traduce directamente en el aumento de ciberataques, como refiere el Director Nacional de Ciberseguridad de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros, Gustavo Sain. *"Durante la cuarentena por COVID-19, establecida por el Gobierno argentino en 2020, aumentaron las denuncias de delitos informáticos"* (Sputnik News, 2021). En ese mismo orden de cosas, la investigadora del InFo-Lab Sabrina Lamperti dijo que en 2020, cuando empezó la pandemia, creció exponencialmente

el ciberfraude, *"en función de la masificación del uso de la tecnología para efectuar operaciones bancarias y financieras"* (Sputnik News, 2021).

Como dato de color, Lamperti agregó que Entre 2019 y 2020 se ha visto un incremento del 600% en este tipo de ciberfraude, *"tendencia que continúa durante lo que va del 2021", agregó Lamperti.*

Desde el lado de las empresas, **Pedro Adamović**, Director de Seguridad de la Información (CISO) de Banco Galicia y docente de Ekoparty Hackademy, comenta que *"hubo un aumento exponencial de los riesgos y ataques cibernéticos producto de la pandemia, lo que acrecentó la demanda de talento calificado por parte de las organizaciones."* (ITware Latam, 2021).

Si abordamos algunos conceptos teóricos detrás de un ataque informático, podemos comprender que todo se trata de qué tan expuestos estamos a los riesgos y cómo nos ocupamos de gestionarlos.

El riesgo es la posibilidad de que un daño ocurra. La gestión de riesgo se basa en identificar y reducirlo hasta un punto aceptable. **No existe un ambiente 100% seguro."**

Cuanto más vulnerable es nuestra infraestructura, a mayor riesgo nos exponemos. Todo lo construido por humanos es vulnerable a algo. Los sistemas de información, en particular, están plagados de vulnerabilidades hasta en los casos mejor protegidos.

Como si todas estas circunstancias no fueran lo suficientemente graves, la República Argentina no tiene la reputación de gestionar adecuadamente sus riesgos y vulnerabilidades. En el siguiente gráfico se puede observar el nivel de posicionamiento de nuestro país en el contexto regional:

Figura 1 - (Valiente, 2021)

Todo esto se potencia en gran medida por la falta de personal capacitado en materia de ciberseguridad, lo que pone en riesgo a empresas de todo el mundo, según Laércio Cosentino (Cosentino, 2021). A nivel regional, el contexto es igual de preocupante *La industria IT se encuentra en alerta por la escasez de talento en un área donde cada vez más personas son requeridas, la de ciberseguridad. En 2020 se publicaron más de 166,000 búsquedas de analistas de seguridad y se espera que este sector crezca un 28% en la próxima década, según un informe de Randstad* (ITware Latam, 2021).

Todo esto deviene en que para lograr implementar una estrategia de ciberseguridad básica se requieren grandes inversiones, independientemente del tamaño de la empresa.

Solidarity

Solidarity nace en este contexto **ofreciendo una alternativa de seguridad integral al alcance de todos**. Nuestro principal objetivo es generar ciber-resiliencia, es decir, ofrecer a las empresas la capacidad de adaptarse y continuar con sus funciones y su trabajo en situaciones de riesgo, **democratizando el acceso a los servicios de seguridad informática** independientemente del tamaño o capacidad de compra de quien lo requiera.

Para lograrlo, comenzamos con la **creación de contenido técnico específico**, pero a su vez altamente pedagógico, **tendiente a capacitar a los recursos de IT de todas las organizaciones** en el tema que nos compete, ofreciendo tutoriales y guías para implementar soluciones gratuitas y así elevar el nivel de seguridad de su organización.

De todo lo aprendido, creamos lo que se convirtió en el corazón de la empresa, un **software de análisis de seguridad integral** y Open Source.

En su versión gratuita, **ofrece a las empresas la capacidad de entender su estado de situación, comprendiendo los desvíos que deben corregir.**

Para quienes quieran ir más allá, ofrecemos una versión paga, Zener SaaS, que luego de una **suscripción altamente accesible** permite automatizar una gran cantidad de tareas básicas relativas a la Seguridad de la Información, elevando aún más las defensas. Esta oferta de gestión progresiva de riesgo ofrece visibilidad y contexto a las empresas.

Nuestra plataforma se encuentra completamente desplegada en la nube, ofrecida a través de un sistema SaaS (Software as a Service). Contamos con los más altos estándares de calidad, puesto que cumplimos con los requerimientos establecidos por la Cloud Security Alliance, una organización sin ánimo de lucro cuyo objetivo es "promover el uso de prácticas recomendadas para ofrecer garantías de seguridad en el ámbito de la informática en la nube, así como proporcionar información sobre los usos de la informática en la nube a efectos de ayudar a proteger todas las demás formas de la informática" (Amazon Web Services, 2021).

Creemos que la ciberseguridad debe ser considerada un derecho y no un privilegio. Sentimos que nuestro aporte a la sociedad va a generar un impacto real en los próximos años, y trabajamos fuertemente con las tecnologías más modernas para lograrlo.

Demanda

Demanda Potencial

La empresa en cuestión utiliza un modelo de negocios B2B (Business to Business), es decir que ofrece servicios a otras empresas o compañías. Dentro de esta modalidad comercial, apuntamos a empresas de diferentes tamaños (En lo que a capacidad de ventas se refiere), principalmente micros, pequeñas y medianas de tramo 1, pudiendo alcanzar en alguna medida empresas medianas de tramo 2, pero no siendo el principal objetivo de momento. Esto se debe a que la principal diferencia entre las empresas medianas de tramo 1 y las empresas medianas de tramo 2 es el volumen de ventas anual y la cantidad de empleados. (Ministerio de Producción y Trabajo de la Nación, 2018)

Visto y considerando que el servicio ofrecido cumple funciones de soporte estructural a las operaciones de todas las organizaciones que utilicen sistemas informáticos en alguno de sus procesos, y siempre teniendo en cuenta que la meta es elevar el nivel de seguridad de aquellas que no suelen ser conscientes de su estado, es decir, que poseen una madurez baja en lo que respecta a la gestión y el gobierno de sus recursos informáticos, creemos firmemente que **es posible aportar valor agregado en todas las industrias y sectores**.

En lo que respecta a la ubicación geográfica objetivo, el sistema de entrega SaaS (Software as a Service) nos ofrece la capacidad de distribuir nuestra solución en cualquier parte del país. En lo que respecta a la oferta de servicios profesionales, limitaremos el alcance a las principales ciudades de la República Argentina, hasta que dispongamos de la capacidad operativa de ampliarnos y cubrir mayores superficies de territorio.

Teniendo en cuenta un análisis realizado por el Ministerio de Producción de la Nación, en su informe de Distribución de empresas y empleo, por tamaño. Año 2017,

(Ministerio de Producción y Trabajo de la Nación, 2018) podemos afirmar que la demanda potencial es de 602.824 empresas:

Demanda	**%**	**Cantidades**
Total	100%	605.854
Empresas entre 1 y 9 personas	85%	514.976
Entre 10 y 49 personas	12%	72.702
entre 50 y 200 personas	2,50%	15.146
más de 200 personas	0,60%	3.635
Demanda Potencial		**602.825**

Tabla 1: Demanda Potencial - (Elaboración Propia, en base a datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

La propuesta de valor de la empresa permite ofrecerle a estas entidades la capacidad de identificar, entender, ponderar y remediar los desvíos de seguridad informática existentes en su infraestructura, capacidad que resulta extremadamente necesaria en los tiempos modernos donde *los ataques informáticos a escala mundial dirigidos a entidades públicas, privadas y personas aumentaron un 70 por ciento en la primera mitad del 2020* (Telam, 2020).

El principal objetivo de Solidarity es elevar el nivel de seguridad de todas las empresas, puesto que entendemos que es la única manera real de enfrentar la cibercriminalidad de manera efectiva. Es por esto que ofrecemos una versión del software que hemos desarrollado de manera gratuita. Ahora bien, quienes quieran contar con todas las funcionalidades del mismo podrán hacerlo inscribiéndose a un servicio de pago mensual.

En ese orden de cosas, aquellos que deseen ir un paso más allá, y contar con el asesoramiento específico de nuestros servicios profesionales podrán hacerlo también.

Seduciendo y construyendo la Demanda

Para construir y seducir la demanda, trabajaremos sobre aquellas personas encargadas de realizar el mantenimiento de los sistemas informáticos de las empresas. Las empresas más grandes poseen personal con dedicación exclusiva a tales efectos, mientras que las más chicas pueden optar por tercerizar el servicio.

Para captar a estas personas, trabajamos en diferentes flancos:

Primeramente, disponemos de un sitio web con contenido técnico específico, tutoriales y recomendaciones de buenas prácticas completamente gratuitas. Esto ofrece un nivel de confianza sobre nuestra marca e imagen.

Por otro lado, disponemos de una serie de videos tutoriales en Youtube, que siguen los lineamientos del sitio web mencionado ut-supra, pero con explicaciones didácticas para resolver problemas cotidianos. El objetivo es cubrir contenido que, normalmente, solo puede ser obtenido a través de medios de pago o en idioma extranjero.

De manera activa, contamos con un equipo comercial que trabajará sobre las consultoras de TI y sobre aquellas pymes que posean un equipo de TI conformado.

Para finalizar, participamos activamente en la comunidad de tecnologías de la información, dando disertaciones y charlas en conferencias. Estas comunidades son muy unidas y reconocen el expertise de un expositor, permitiéndonos captar la atención de una gran porción del público objetivo.

Fidelización

El principal factor de fidelización es la oferta de valor con respecto al bajo costo de la solución, el hecho de ofrecer un servicio de seguridad integrado a través de pagos recurrentes y sin requerir grandes inversiones iniciales desde ya es un diferencial.

A pesar de los bajos costos, trabajamos con un servicio de muy alta calidad, que permite cumplir con todos los estándares de seguridad existentes en el mercado (ISO 27001, NIST, etc.).

En lo que respecta a la atención al cliente, disponemos de un centro de atención especializado, ofrecemos SLAs más que competitivos y trabajamos con un trato personalizado, puesto que, con su debida autorización, recolectamos información de contexto de la infraestructura del cliente, lo que nos permite realizar un análisis mucho más metódico y específico de los problemas que pudieran suceder.

Finalmente, todo nuestro software es Open Source, por lo que es completamente auditable. De esta manera garantizamos la transparencia en nuestras operaciones.

Oferta

Actualmente en la República Argentina existen tres tipos de competidores diferentes que ofrecen servicios muy disímiles en materia de Seguridad Informática.

1. Grandes Competidores

Los grandes competidores del mercado ofrecen servicios de la más alta calidad, ejemplos del caso son las empresas Checkpoint, Palo Alto, Fortinet, Trend Micro, entre otras.

Estas empresas disponen de suites de soluciones completas, permitiendo cubrir cualquier necesidad del cliente.

Naturalmente, los orígenes de capitales son extranjeros, a pesar de tener presencia nacional y suelen operar a través de canales especializados, por lo que no realizan ventas directas.

Su segmento objetivo son grandes empresas, aquellas con un área de seguridad informática conformada que entiende las necesidades de la organización y puede trabajar en conjunto con sus especialistas para el dimensionamiento, implementación, mantenimiento y operación de las plataformas.

En lo que respecta a la postventa ofrecen capacidades variadas, aunque principalmente el servicio es ofrecido también a través del mismo canal.

A pesar de contar con los principales avances y la más alta tecnología, sus costos son prohibitivos para el 99% del mercado nacional, por lo que no disponen de la capacidad de ofrecer servicios a las empresas objetivo de Solidarity.

2. Consultoras

Siguiendo la línea de pensamiento del punto anterior, las consultoras son aquellas empresas que ofrecen servicios profesionales únicamente, es decir, cuentan con personal técnico especializado en diferentes soluciones para asesorar a las organizaciones que así lo requieran.

Existen de diversos tamaños, pero coinciden con los grandes competidores en que tienen como objetivo empresas con equipos de seguridad de la información ya conformados, que pueden entender el valor agregado de tamaño repertorio de talentos. Es por esto que sus clientes son empresas de gran tamaño.

Estas empresas ofrecen casi en su totalidad servicios, y utilizan la metodología de venta directa, sin necesitar intermediarios para alcanzar sus objetivos. A su vez, el servicio post-venta suele ser implementado siguiendo la misma metodología, pero atado a la adquisición de paquetes de horas de consultoría o servicios profesionales.

La principal debilidad que poseen es la burocracia requerida para poder ofrecer el servicio, no pudiendo demostrar el valor agregado ofrecido de manera inmediata, a diferencia de Solidarity.

3. Profesionales independientes

Los profesionales independientes son recursos humanos altamente capacitados en materia de seguridad de la información que ofrecen sus servicios de manera particular.

Operan en la República Argentina de manera directa, concentrados en su mayoría en el AMBA, y apuntando a empresas pequeñas y medianas de tramo 1 y 2.

A pesar de que ofrecen sus servicios de manera directa, tienen la capacidad de implementar soluciones de seguridad como los grandes competidores como así también horas

de consultoría de manera inmediata, por lo que, en principio, los vuelve un competidor directo para Solidarity.

Teniendo esto en cuenta, su principal fortaleza es su debilidad. Al tratarse de personas altamente especializadas, fallan en cubrir todo el abanico de habilidades requeridas para brindar un servicio integral de ciberseguridad.

Mercado

Teniendo en cuenta lo informado por el Ministerio de Producción de la República Argentina, *"la actividad de las empresas está concentrada territorialmente: el 70% de las empresas se localiza en 4 jurisdicciones: Capital Federal, Buenos Aires, Córdoba y Santa Fe."* (Ministerio de Producción y Trabajo de la Nación, 2018), aunque cabe aclarar que *"Parte de la alta concentración en CABA tiene que ver con que las empresas registran allí su domicilio fiscal o su oficina central aunque mantengan operaciones en otras regiones."*

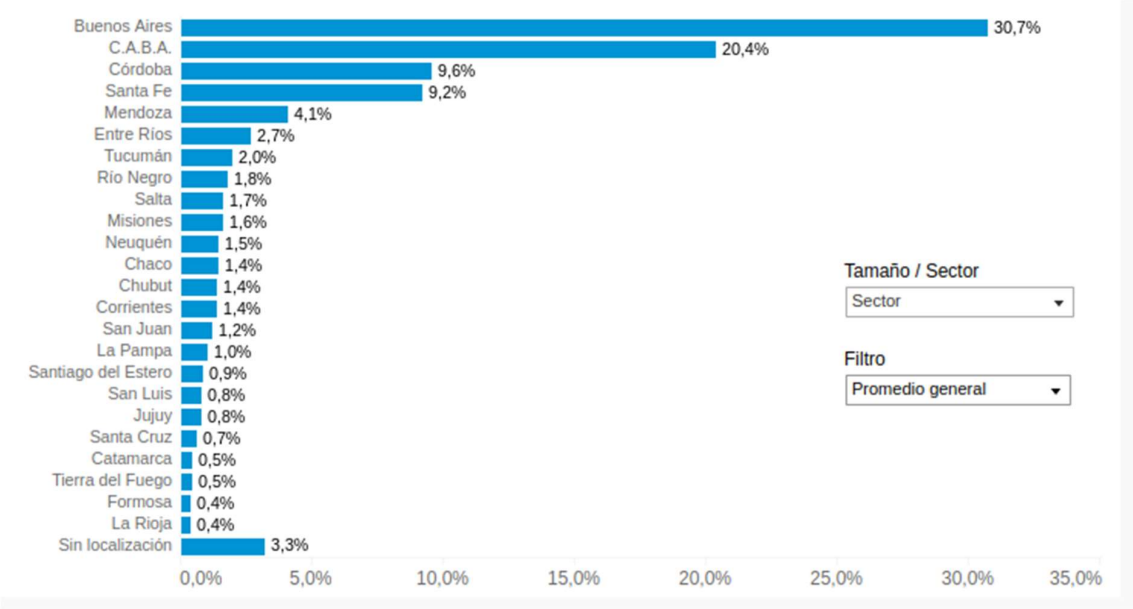

Figura 2 - (Ministerio de Producción y Trabajo de la Nación, 2018)

Si tomamos en cuenta el porcentaje de concentración con el total de empresas objetivo mencionado anteriormente, y segmentamos en las zonas del país sobre las que enfocaremos nuestro esfuerzo inicial, obtenemos el siguiente desglose:

Localización	*Tamaño*	SUM de Empresas
Buenos Aires	Entre 1 y 9	160.364
	Entre 10 y 49	21.471
	Entre 50 y 200	4.537
	Más de 200	872

Total Buenos Aires		187.244
C.A.B.A.	Entre 1 y 9	99.858
	Entre 10 y 49	18.988
	Entre 50 y 200	4.043
	Más de 200	1.391
Total C.A.B.A.		124.280
Córdoba	Entre 1 y 9	50.901
	Entre 10 y 49	5.917
	Entre 50 y 200	1.184
	Más de 200	221
Total Córdoba		58.223
Mendoza	Entre 1 y 9	21.265
	Entre 10 y 49	3.145
	Entre 50 y 200	563
	Más de 200	114
Total Mendoza		25.087
Santa Fe	Entre 1 y 9	48.398
	Entre 10 y 49	6.200
	Entre 50 y 200	1.313
	Más de 200	247
Total Santa Fe		56.158
Suma total		**450.992**

Tabla 2: Distribución de Mercado Objetivo en Argentina (Elaboración Propia, en base a datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

Crecimiento de Mercado

En lo que respecta al crecimiento de mercado, teniendo en cuenta el Reporte del Ministerio de Producción, *"Entre 2007 y 2017 la cantidad de empresas activas aumentó 7,6%, a un ritmo de 3.900 empresas adicionales por año."*, puesto que *"Entre 2007 y 2016 nacieron*

por año cerca de 70.500 empresas y cerraron 69.000. Así, el stock de empresas creció en términos netos." (Ministerio de Producción y Trabajo de la Nación, 2018). De todas maneras, *"en los últimos años la cantidad de nacimientos se redujo y los cierres se mantuvieron relativamente constantes, dando lugar a una caída neta en el total de empresas activas."*

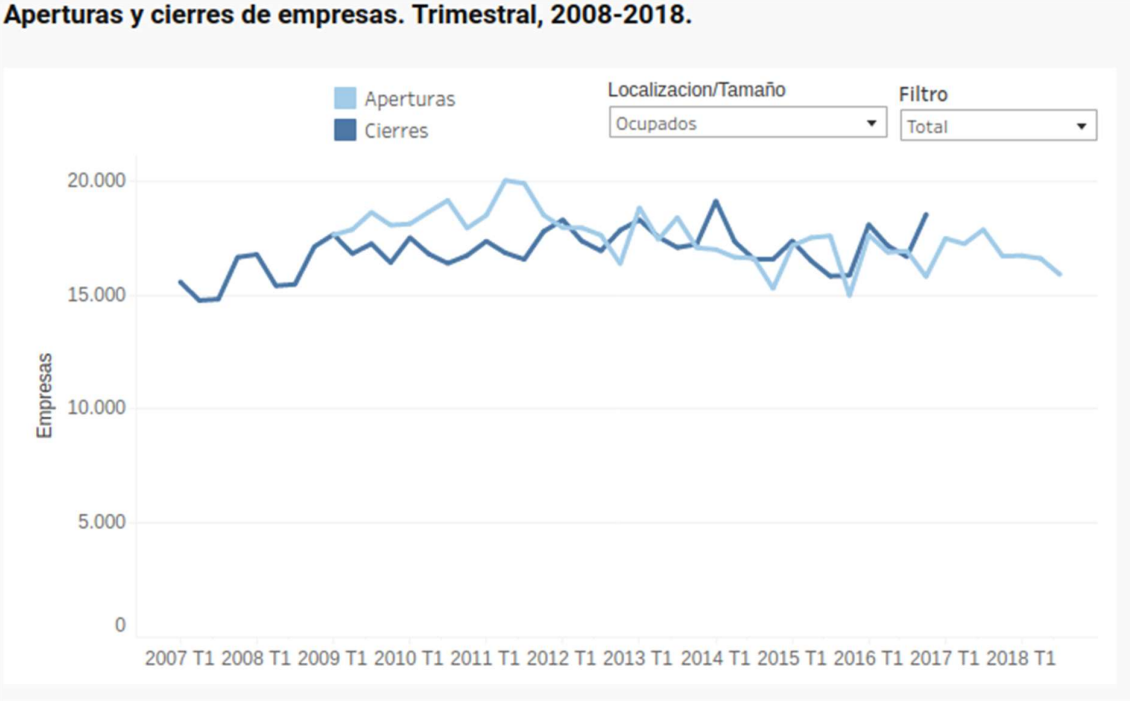

Figura 3 - (Ministerio de Producción y Trabajo de la Nación, 2018)

Modelo de Competencia

Como prioridad, el servicio ofrecido debe ser adquirible por las empresas del segmento al que apuntamos, ofreciendo una muy buena relación costo/beneficio.

El servicio se ofrecerá a través de un desarrollo SaaS (Software as a Service), permitiendo aprovechar las ventajas competitivas que ofrecen los entornos Cloud, como ser el rápido aprovisionamiento, la utilización inmediata, el pago por uso y la capacidad de suscribirse a un consumo mensual sin necesidad de altos costos iniciales.

El desarrollo en cuestión contará con altos estándares de calidad, siguiendo el Consensus Assessment Initiative Questionnaire (CAIQ) v3.1 ofrecido por la Cloud Security Alliance.

Con estos atributos, se diferenciará de la competencia, puesto que aquellas pymes que quieran contratar el servicio podrán hacerlo de manera inmediata, con bajos costes de ingreso y gran valor agregado, elevando su visibilidad e identificando puntos de mejora de manera prácticamente inmediata.

Modelo de Marketing

Segmentación

- Empresas Micro, pequeñas y medianas de tramo 1;
- Que utilizan tecnología para sus operaciones;
- En las principales ciudades de la República Argentina.

Estrategia Competitiva:

- Bajo coste;
- Suscripción mensual, sin inversión inicial;
- Eleva el nivel de seguridad;
- SaaS (Software as a Service);
- Estándares de calidad de la Cloud Security Alliance;
- Rápidos resultados.

Política de Precios:

- Estrategia “Pay as you go”, el cliente paga sólo lo que utiliza;
- Recursos gratuitos;

- Software Open Source, transparencia;
- Servicios profesionales bajo demanda.

Política de Comunicación:

- El servicio debe ser conocido por todos los responsables de IT;
- El valor agregado debe ser claro;
- Oferta de recursos gratuitos para resolver problemas comunes;
- Oferta de software Open Source para que se familiaricen con el mismo;
- Charlas y ponencias en conferencias de alto renombre para la comunidad.

FODA

- Fortalezas:
    - Bajo coste;
    - Suscripción mensual, sin inversión inicial;
    - Servicio Integral de Ciberseguridad;
    - Eleva el nivel de seguridad;
    - SaaS (Software as a Service);
    - Estándares de calidad de la Cloud Security Alliance;
    - Rápidos resultados.
- Oportunidades:
    - Falta de servicios similares;
    - Terreno sin explorar por otras empresas;
    - Gran aumento de ciberataques y ciberamenazas;
    - Mayor conciencia respecto a los riesgos de seguridad;
    - Mayor utilización de las tecnologías por el contexto mundial;

- Transformación Digital acelerada.

- Debilidades:
  - Terreno sin explorar en demasía;
  - Requiere alcanzar cierto nivel de masa crítica para ser redituable;

- Amenazas:
  - Contexto de volatilidad natural de la República Argentina;
  - Cierran más empresas de las que abren;
  - Falta de personal técnico especialista en Ciberseguridad para realizar las tareas de servicios profesionales;
  - El personal técnico especialista en Ciberseguridad presenta una alta tasa de volatilidad y poca permanencia en las compañías.

Matriz de Stakeholders

s	*Stakeholder*
Azul	Gobiernos Municipales
	Gobiernos Nacionales
	Gobiernos Provinciales
	Proveedores
	Sociedad en general
Negro	Clientes del servicio free
	Comunidad Open Source
	De IT
	De Seguridad Informática
	Empleados administrativos
Rojo	Clientes del producto básico
	Clientes del servicio de consultoría
	Directivos
	Socios
Verde	Accionistas
	Analistas
	Consultores
	Empresas de capacitación en materia de seguridad informática

Azul: Con poco poder y poco interés, en este caso nos limitaremos a monitorizar los, ir viendo cuál es su estado para detectar cambios de actitud o percepción respecto al proyecto.

Negro: Con poco poder pero bastante interés, este será un «grupo amigo», tienen interés en lo que hacemos, nos pueden aportar feedback, y nos apoyarán pero no disponen de poder suficiente como para ofrecernos un impulso al proyecto, por lo tanto simplemente les mantendremos informados.

Rojo: Con interés y mucho poder, interesados con los que debemos conectar y hacer un esfuerzo para involucrarnos al máximo en el proyecto y mantenerlos satisfechos.

Verde: Con poder y menor interés, estos son

	Empresas de Seguridad Informática tradicionales Instructores Proveedores de productos pagos de seguridad informática	los más «peligrosos» ya que puede llegar a afectar muy negativamente al proyecto, por lo tanto es vital involucrarnos cuanto antes y gestionarlos activamente, mantenerlos informados en todo momento, con el objetivo de que vean con buenos ojos nuestro proyecto.
Suma total		

Tabla 3 – Matriz de Stackeholders - (Elaboración Propia basada en conocimiento de la industria.)

Tipo	**Grupo**	**Stakeholder**	**Tipo de Impacto**
Primarios	Accionistas	Accionistas	Beneficio
Primarios	Solidarity	**Empleados administrativos**	Beneficio
Primarios	Solidarity	Consultores	Beneficio
Primarios	Solidarity	Instructores	Beneficio
Primarios	Solidarity	Analistas	Beneficio
Primarios	Solidarity	Directivos	Beneficio
Primarios	Solidarity	Socios	Beneficio
Primarios	Proveedores	Proveedores	Beneficio
Primarios	**Comunidad Open Source**	**Comunidad Open Source**	Beneficio
Primarios	**Clientes**	**Clientes del servicio free**	Beneficio
Primarios	**Clientes**	Clientes del producto básico	Beneficio
Primarios	**Clientes**	Clientes del servicio de consultoría	Beneficio
Secundarios	Competidores	Empresas de Seguridad Informática tradicionales	Perjuicio
Secundarios	Competidores	Empresas de capacitación en materia de seguridad informática	Perjuicio

Secundarios	Competidores	Proveedores de productos pagos de seguridad informática	Perjuicio
Secundarios	Administración pública	Gobiernos Municipales	Beneficio
Secundarios	Administración pública	Gobiernos Provinciales	Beneficio
Secundarios	Administración pública	Gobiernos Nacionales	Beneficio
Secundarios	Comunidades	**De Seguridad Informática**	Beneficio
Secundarios	Comunidades	**De IT**	Beneficio
Secundarios	Sociedad en general	Sociedad en general	Beneficio

Tabla 4 – Matriz de Stackeholders - (Elaboración Propia basada en conocimiento de la industria.)

Tecnología

Como ya hemos visto en puntos anteriores, el proyecto está completamente basado en tecnología. Siendo una empresa de base tecnológica, utilizamos diferentes desarrollos y soportes de tecnologías de la información para implementar técnicas y tácticas específicas de seguridad de la información y así alcanzar los objetivos.

Arquitectura de la Solución

1. Solidarity

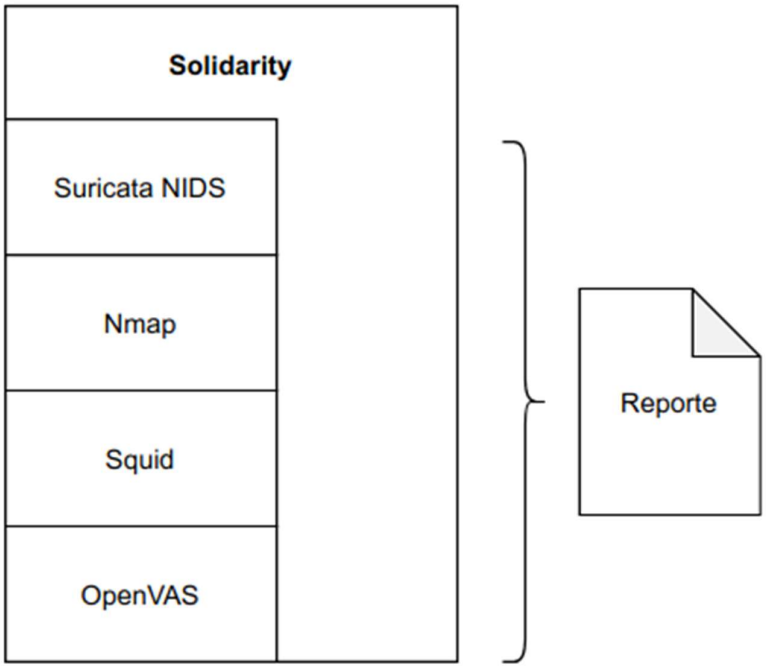

Figura 4 – Diseño de Arquitectura Ideado Para la Solución

2. Zener

Zener				
Discovery	**Detect**	**Protect**	**Alert**	**Event Handling**
Suricata NIDS	Suricata NIDS	Wazuh	Email	TheHive
Nmap	Wazuh	Suricata NIPS	Slack	Defect Dojo
Squid	Squid		Telegram	MISSP
OpenVAS	OpenVAS		Webhook	CORTEX

Figura 5 – Arquitectura de la Solución - Elaboración Propia

3. Gestión de eventos

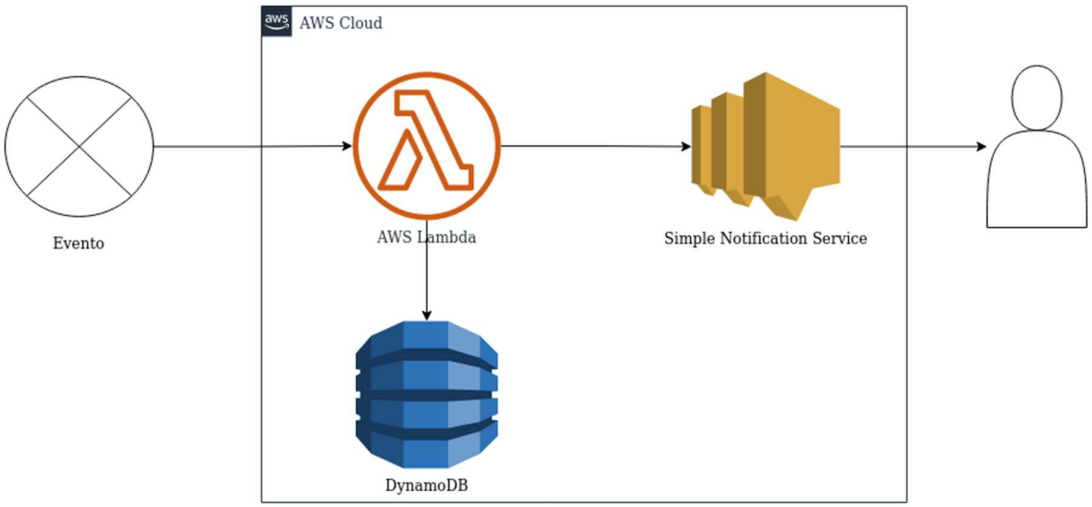

Figura 6 – Arquitectura de la Solución - Elaboración Propia

Tecnologías Implementadas

Módulos

Como puede apreciarse en la arquitectura de la solución, utilizamos una estructura modular compuesta por múltiples piezas, cumpliendo cada una una función específica.

Describiremos cada uno de los módulos enunciados ut-supra considerando sus beneficios, consideraciones, limitaciones, problemas, alternativas y su aplicabilidad en nuestro mercado.

1. Nmap

Nmap ("Network Mapper" - https://nmap.org/) es una herramienta de escaneo y auditoría de red, gratuita y open source. Utiliza paquetes IP de diferentes maneras para determinar qué activos están disponibles dentro de una red, qué servicios están ofreciendo, qué sistemas operativos utilizan, qué tipos de filtros de paquetes o firewall están implementados, entre otras funcionalidades.

Esta herramienta es el estándar de facto para realizar acciones de reconocimiento de red, según versa el siguiente artículo (Ferranti, 2018). Una de sus principales bondades es su flexibilidad y capacidad de integración con otras herramientas, como en nuestro caso siendo parte fundamental de Solidarity.

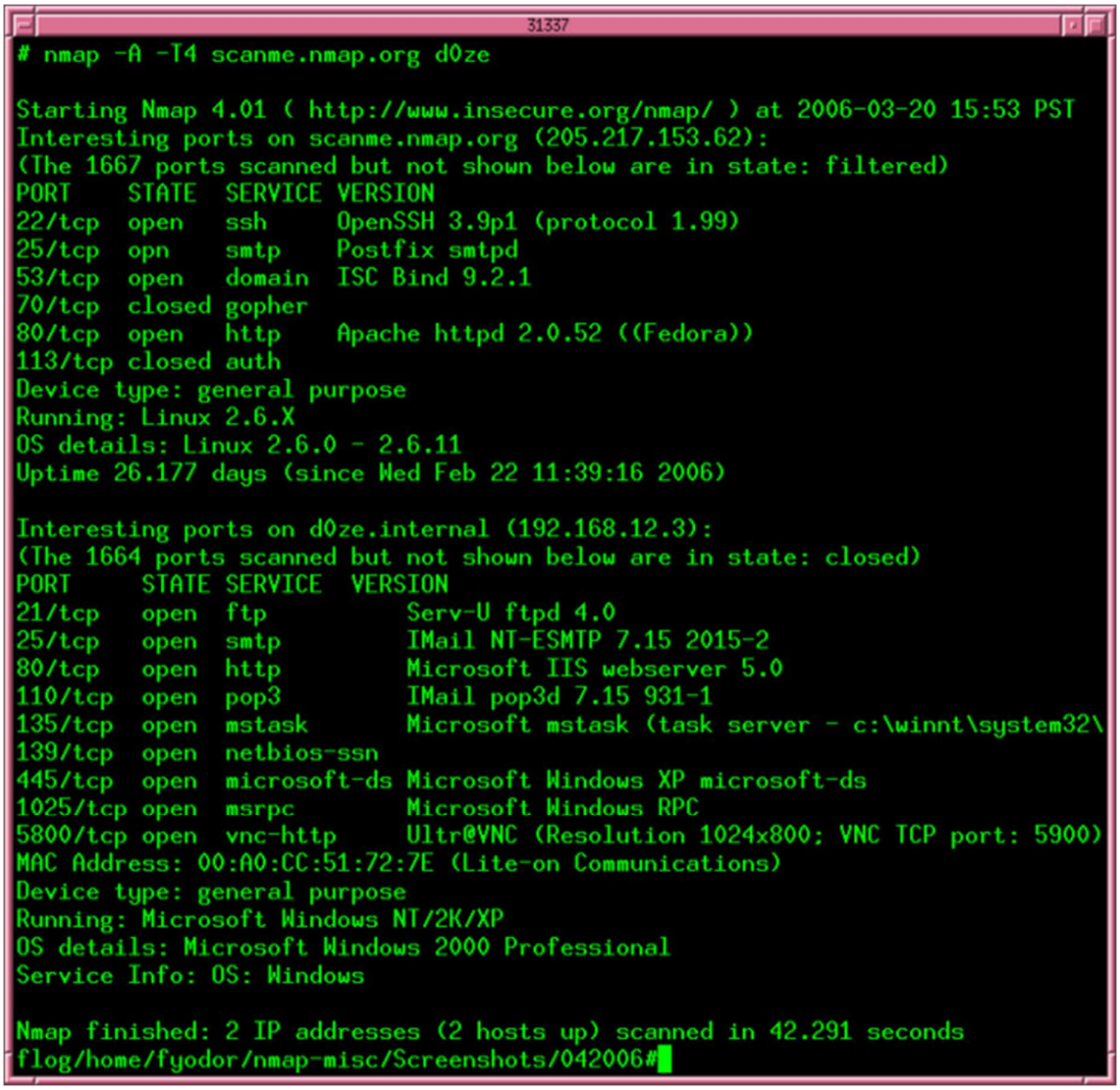

Figura 7 - https://nmap.org/

En nuestro contexto en particular, utilizaremos Nmap para realizar reconocimiento dentro de la red, identificar activos existentes dentro de la organización y entender qué servicios están corriendo, pudiendo de esa manera comprender si existen vulnerabilidades o desvíos de seguridad que pudieran ser usados para comprometer a la organización. Ejemplos de estos son:

- Servers vulnerables a Eternal Blue (https://es.wikipedia.org/wiki/EternalBlue);
- Servers vulnerables a HeartBleed (https://heartbleed.com/);
- Servers exponiendo el protocolo Telnet;

- Servers exponiendo protocolo RDP.Sur

2. Suricata

Para entender lo que hace suricata, primero debemos adentrarnos en el concepto de Network Intrusion Detection and Prevention Systems (IDPS).

Un sistema de detección y prevención de intrusiones de red es un programa que analiza el tráfico de red, es decir, los paquetes enviados y recibidos buscando anomalías que pudieran significar un comportamiento malicioso.

Esto puede ser logrado de diferentes formas, dentro de las que podemos describir la validación de las direcciones IP de origen y destino, corroborando si han sido agregadas a listas negras mantenidas por grandes industria; otro ejemplo sería el análisis del contenido de los paquetes, buscando encontrar firmas o indicadores que se relacionen con familias específicas de malware.

Gracias a estas técnicas, Suricata analiza del tráfico de red de la organización objetivo, permitiéndonos descubrir anomalías altamente críticas como ser:

- Equipos PC comprometidos con Malware intentando comunicarse a Centros de Comando y Control;
- Servidores siendo atacados a través de la red, aprovechando vulnerabilidades existentes o desvíos de configuración;
- Comportamiento inapropiado de los usuarios, como ser descargas utilizando servicios P2P;
- Acceso a los equipos a través de plataformas de administración remota como ser TeamViewer;
- Intentos de fuga de información, detectando grandes volúmenes de datos siendo infiltrados de un equipo.

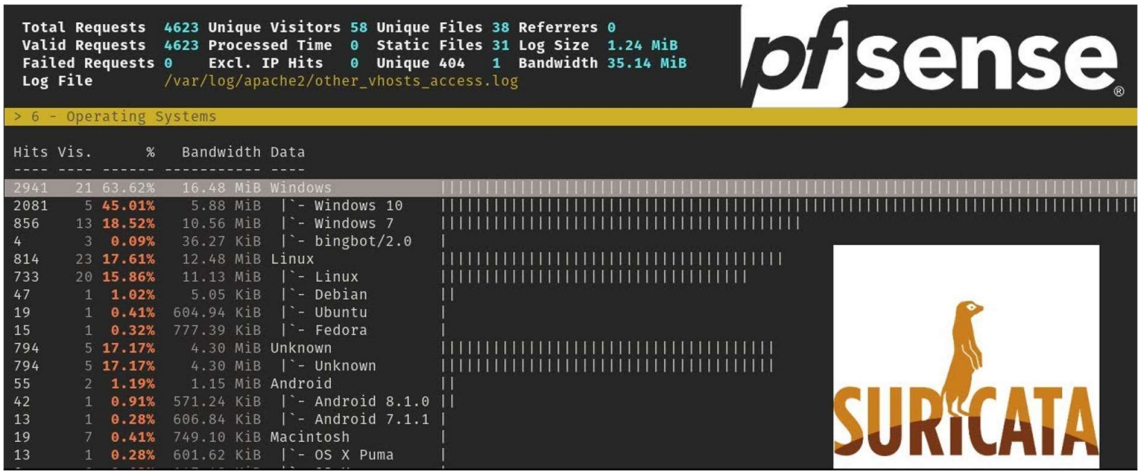

Figura 8 - https://suricata.readthedocs.io/en/suricata-6.0.3/

3. OpenVAS

OpenVAS es un escáner de vulnerabilidades completo, es una herramienta que permite analizar los equipos críticos de la red en búsqueda de desvíos de configuración, software desactualizado, vulnerable, que pueda ser comprometido por actores maliciosos.

Dentro de sus capacidades incluye la habilidad de hacer pruebas sin autenticación, pruebas sobre protocolos de red, internet e industriales y la habilidad de realizar escaneos altamente performantes para grandes entornos.

Como todas las soluciones utilizadas en Solidarity, es gratuita y Open Source. Dentro de nuestra integración, nos permite obtener un nivel de visibilidad muy certero respecto de las vulnerabilidades existentes en la infraestructura del cliente, principalmente por disponer de un módulo de clasificación en función de la criticidad de la vulnerabilidad detectada.

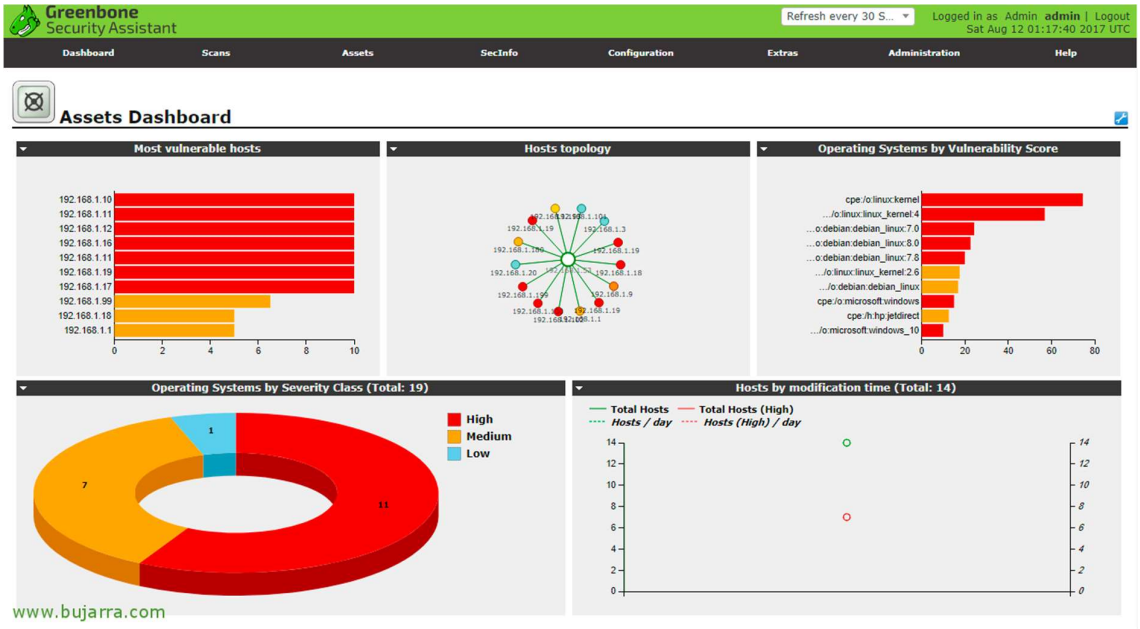

Figura 9 - (Herrero, 2017)

4. Squid

Squid es el proxy open source por excelencia en el mercado, por lo que, para comenzar a hablar de Squid, debemos explicar el concepto de proxy primero.

Un servidor proxy es un software que se utiliza como puente entre el origen y el destino de una comunicación, encauzando todas las comunicaciones de red a través de un proxy nos permite tener un control mucho más granular de nuestros equipos.

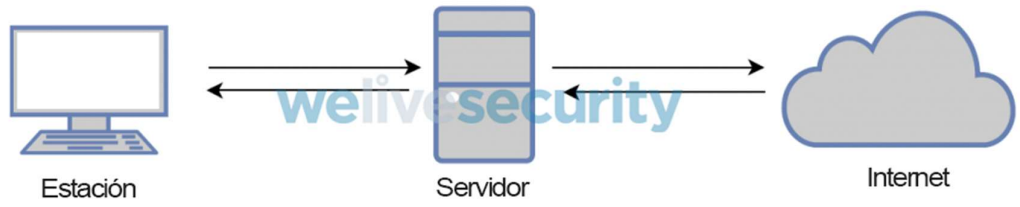

Figura 10 - (Barbosa, 2020)

De esta manera, implementando un servidor proxy como Squid, podemos identificar cierto comportamiento que no es malicioso de por sí, pero que, según nuestras necesidades de negocio pueden ser indeseadas.

Ejemplos de los controles que podemos implementar usando un servidor proxy son:

- Filtro de contenido, por ejemplo podemos evitar que los usuarios se conecten a Facebook;
- Detección y protección contra fuga de información, podemos detectar cuando un usuario se conecta a una plataforma de almacenamiento remota como ser Google Drive, Onedrive, Dropbox, etc;
- Restricción del ancho de banda, limitando acceso a plataformas de alto consumo de ancho de banda (Streaming, por ejemplo), podemos permitirle a la organización utilizar su red de manera más eficiente para las actividades de negocio.

5. Wazuh

Wazuh es una solución gratuita, open source y del más alto nivel para realizar tareas de detección de incidentes, monitoreo de integridad, detección de amenazas y respuesta.

Dentro de nuestra implementación, Wazuh nos permite instalar agentes en los equipos PC y servidores de la organización que deseamos proteger, monitoreando en tiempo real el estado de seguridad en búsqueda de anomalías de diferente tipo.

Estamos hablando de una plataforma con diferentes módulos, cada módulo ofrece una capacidad extra de seguridad, dentro de los que no podemos dejar de nombrar:

- Análisis de Seguridad: Permite recolectar información de los equipos en búsqueda de intrusiones, amenazas y comportamientos inusuales;
- Detección de intrusiones: Los agentes de Wazuh escanean los equipos buscando malware, rootkits y actividades maliciosas;

- Análisis de Logs: Los agentes de Wazuh revisa los logs de sistema y los envían de manera segura a un servidor para realizar análisis basados en reglas y así detectar posibles compromisos;
- File Integrity Monitoring: Wazuh monitorea el sistema de archivos identificando cambios críticos, pudiendo detectar, por ejemplo, un compromiso por malware.
- Detección de Vulnerabilidades: El sistema realiza un escaneo de vulnerabilidades sobre el host, identificando posibles desvíos de configuración y software desactualizado.
- Consejos de Configuración: El agente escanea el sistema e identifica configuraciones inseguras que posea el host.
- Respuesta ante incidentes: Es posible habilitar la ejecución de scripts dentro del sistema, permitiendo a Wazuh responder ante la detección de algún tipo que haya sido detectado a través de los módulos mencionados anteriormente.

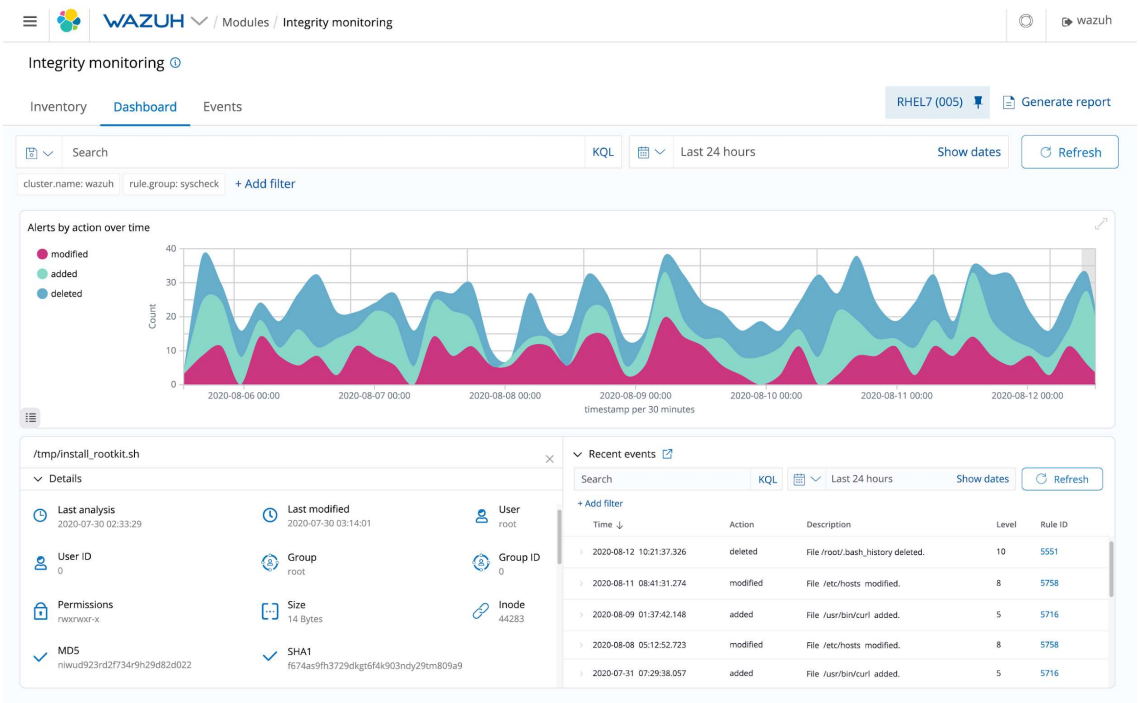

Figura 11 - https://wazuh.com/

6. The Hive

The Hive es un producto gratuito y Open Source dedicado exclusivamente a la gestión de la respuesta a incidentes. Su principal característica es su habilidad de integrarse con MISP y Cortex, dos soluciones que veremos más adelante.

Este producto se integra perfectamente dentro de la suite puesto que nos permite centralizar todas las detecciones halladas por las soluciones mencionadas en los puntos anteriores, de forma tal que los analistas que tengan que resolver los desvíos solo tengan que acceder a una única consola centralizada.

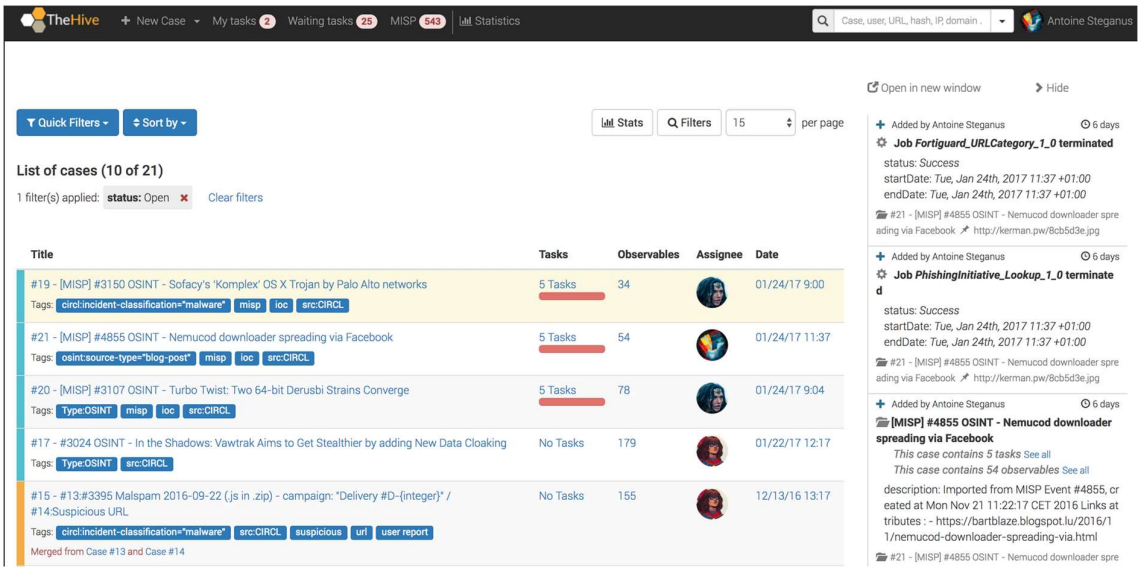

Figura 12 - https://thehive-project.org/

7. Defect Dojo

Defect Dojo es una solución gratuita y Open Source que nos permite centralizar las vulnerabilidades encontradas en un solo lugar, de la misma manera que The Hive nos permite centralizar los incidentes.

El objetivo de tener una herramienta como esta dentro de la integración es ofrecer a las partes de la organización que mantienen los sistemas, infraestructura, IT, desarrolladores, visualizar las fallas de seguridad existentes, clasificarlas y documentar sus remediaciones.

Es una gran herramienta para monitorear SLAs (Acuerdos de Nivel de Servicio) pudiendo notificarnos cuando una vulnerabilidad lleva demasiado tiempo sin ser resuelta.

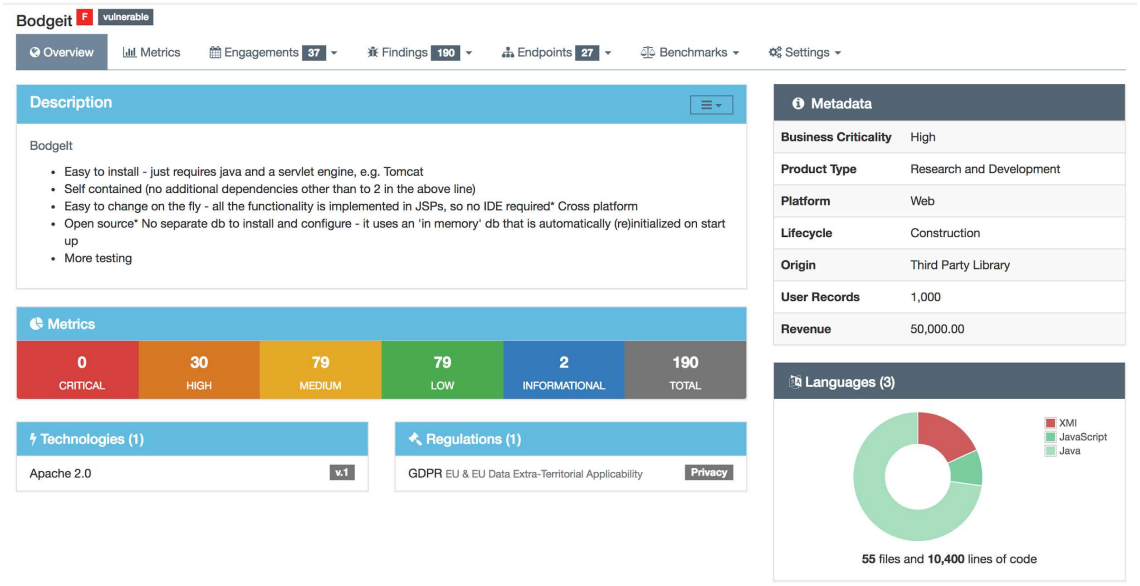

Figura 13 - https://www.defectdojo.org/

8. Cortex

Cortex es una herramienta Open Source y gratuita que permite centralizar una serie de herramientas utilizadas para analizar observables ante un incidente.

Para poder entender esto debemos adentrarnos un poco en el concepto de respuesta ante incidentes.

Cuando alguna de las soluciones mencionadas anteriormente detecta un desvío de seguridad, por ejemplo un servidor siendo atacado, genera un evento en The Hive. Este evento cuenta con información generada automáticamente por la solución que lo detectó, el problema

es que muchas veces esa información no es suficiente para poder dar una respuesta efectiva al ataque.

Es en este punto donde Cortex entra en juego, permitiendo al analista realizar transformaciones sobre la información existente, generando nuevos registros de información que le van a dar el contexto necesario para tomar una decisión adecuada.

Un ejemplo claro de uso de cortex es un intento de ataque a un servidor, donde producto de Suricata podemos identificar la IP atacante, Cortex nos permite realizar una transformación sobre esa IP para entender si se encuentra dentro de una lista negra.

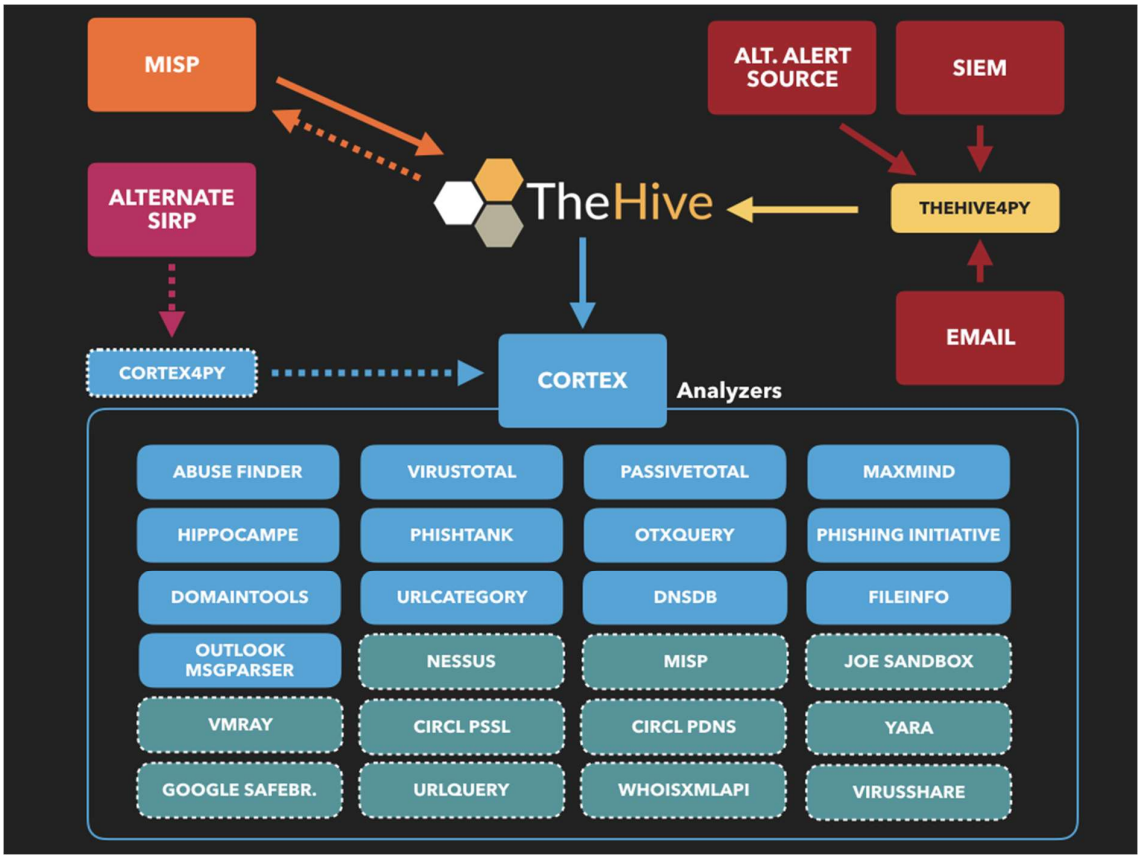

Figura 14 - https://github.com/TheHive-Project/Cortex

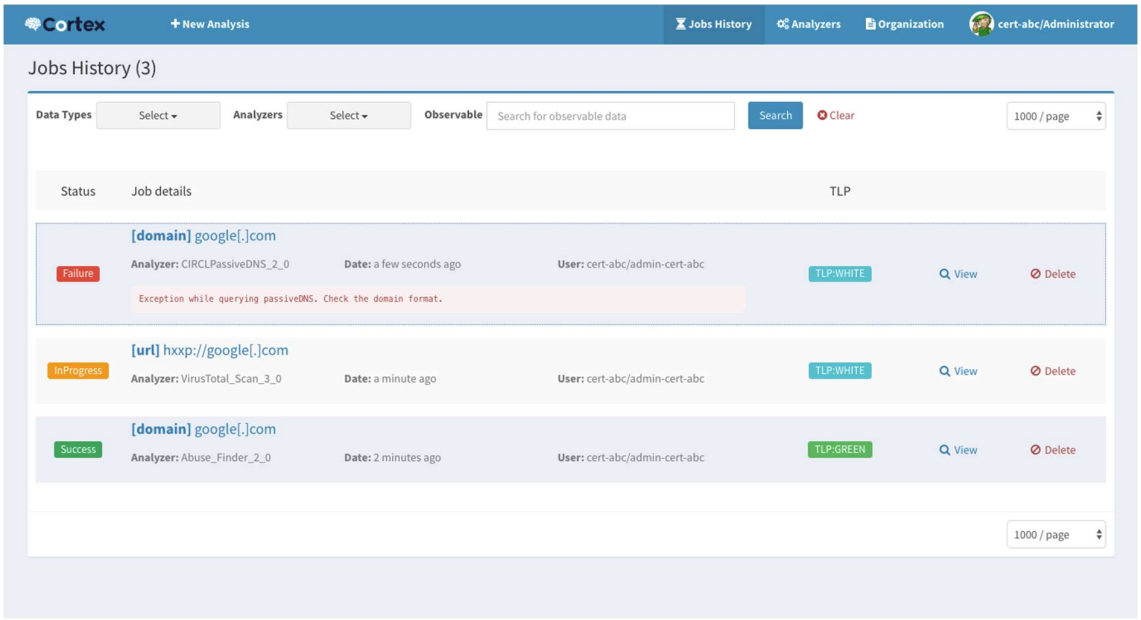

Figura 15 - https://github.com/TheHive-Project/Cortex

9. MISP

MISP es una plataforma de análisis de inteligencia Open Source. Es el estándar por defecto para compartir eventos de interés, indicadores de compromiso y fuentes de inteligencia entre diferentes equipos.

Como vimos anteriormente, todas las soluciones descritas se basan en información para entender qué comportamientos son maliciosos y cuáles no. Es por esto que es tan importante la generación de inteligencia, para estar actualizado constantemente respecto de nuevas técnicas, tácticas y procedimientos utilizados por los cibercriminales.

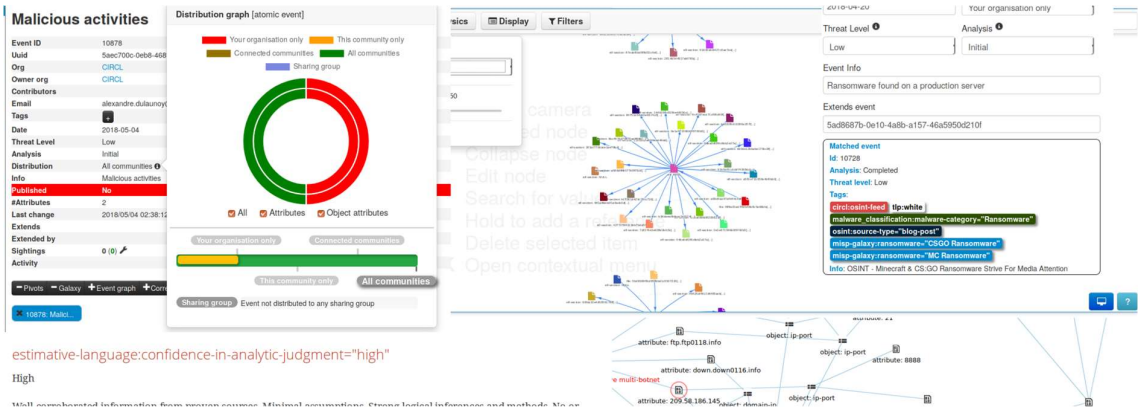

Figura 16 - https://github.com/TheHive-Project/Cortex

Tecnología de Soporte

Ahora bien, para poder entregar estos componentes a los clientes, nos basamos principalmente en un repositorio en GitHub donde alojamos los componentes relativos a Solidarity para que sean descargados por quien así lo desee. De la misma manera, contamos con otro repositorio privado donde alojamos los componentes correspondientes Zener SaaS, dándole acceso solamente a quienes hayan abonado la suscripción.

Por otro lado, contamos con infraestructura desplegada en AWS donde soportamos las operaciones. El hecho de utilizar una plataforma Cloud para alojar nuestros servicios nos permite escalar rápidamente a medida que la demanda crece, como así también reducir nuestros costes en caso de que la misma merme.

Plan de Negocio

Ventaja Competitiva

La ventaja única y sostenible que posee Solidarity respecto a sus competidores es el software desarrollado, el que habilita a la empresa a ofrecer un servicio integral de seguridad y primera calidad a un coste mucho menor.

Propuesta de Valor

“Defensa ante ciberamenazas, al alcance de todos.”

La pregunta no es si los cibercriminales van a atacarte, el asunto es ***cuando***. Solidarity te permite elevar tu seguridad desde el día cero, pagando solo por lo que usas.

- Diseñado específicamente para pequeñas y medianas empresas Argentinas;
- Servicio de seguridad integral, visualización, detección, monitoreo y respuesta a incidentes de seguridad;
- Capacidades modulares, pagas solo por lo que usas;
- Homologado por los más altos estándares;
- Servicio de atención al cliente personalizado.

Factores Claves de Éxito

Los factores críticos de éxito son puntos clave que definen y garantizan el desarrollo y crecimiento de una empresa y su negocio, logrando sus objetivos. En tal sentido, los factores claves de éxito de Solidarity son:

- **Capacidad de innovación**, implementando constantemente nuevos procesos y tecnologías al servicio del cliente.

- **Impacto Social,** ya que con su versión Open Source permite a todas las empresas elevar su nivel de seguridad.
- **Al alcance de todos**, gracias a sus bajos costes y operaciones SaaS.
- **Facilidad de uso**, puesto que el servicio está pensado para ser automatizado en su totalidad.
- **Integración con la comunidad**, participando de conferencias de alto renombre en el territorio como ser Ekoparty.

Servicio

Solidarity busca brindar una respuesta a la creciente oleada de ciberataques que afecta a la República Argentina. Para lograrlo, ofrecemos un servicio modular, basado en tecnología cloud, respaldado por un gran equipo de profesionales y al alcance de todos.

Propuestas

El servicio mencionado en el apartado anterior puede ser contratado de maneras diferentes según los requerimientos del cliente, como veremos a continuación:

1. Solidarity, Open Source:

Solidarity ofrece las principales capacidades de su software completamente gratuito (Módulo Discovery), a través de una implementación Open Source que puede ser descargada de su sitio web.

El objetivo de este desarrollo es alcanzar a todas las empresas y organizaciones, sin importar su poder adquisitivo. Tomamos esta decisión basándonos en experiencias previas en entes estatales, donde a pesar de ser conscientes de la necesidad manifiesta de reforzar la seguridad de la organización, no era posible adoptar medidas por falta de presupuesto.

2. Zener SaaS:

Zener SaaS es la versión propietaria de Solidarity. Adquiriendo este servicio de pago mensual habilita a la organización acceder a todas las capacidades del software completo. Cabe destacar que dentro de Zener SaaS existen diferentes módulos, los cuales pueden ser adquiridos de manera independiente o en su totalidad, según los requerimientos de la organización.

3. Tutoriales técnicos:

Se trata de una propuesta complementaria, basada en buenas prácticas de seguridad y guías de implementación, en formato escrito como así también en video, que permitan a las organizaciones elevar su nivel de seguridad sin requerir inversiones. El objetivo principal de esta medida es posicionar el nombre Solidarity en el mercado, como una empresa que busca, sobre todo, el bienestar social independientemente del lucro.

Módulos

1. Discovery

Es el módulo principal del sistema, una vez configurado realiza un gap analysis de la infraestructura del cliente y genera un reporte detallado informando su estado de situación. Como parte del escaneo, realiza las siguientes validaciones:

- **Seguridad de red:** Analiza el tráfico de red para identificar comportamientos maliciosos, como ser equipos infectados con malware intentando comunicarse con centros de comando y control.
- **Seguridad Perimetral de Hosts:** Analiza los diferentes equipos de la red, como terminales, PCs, servidores o equipos de networking, buscando puertos abiertos que puedan significar un riesgo potencial para la organización.
- **Vulnerabilidades Internas:** Realiza un escaneo de vulnerabilidades sobre toda la infraestructura, buscando software explotable por actores maliciosos. Esta información

permite identificar problemas de configuración, software obsoleto o pendiente de actualizaciones y vectores de ataques directos.

- **Vulnerabilidades Externas:** Realiza un escaneo de vulnerabilidades sobre los servidores expuestos a internet por la empresa, principal blanco de ataque de actores maliciosos. Permite identificar vulnerabilidades críticas fácilmente explotables por terceros puesto que aquello que está expuesto a internet es público y accesible.

Luego de correr esta serie de evaluaciones, confecciona automáticamente un informe compuesto de tres partes:

- **Resumen ejecutivo:** Se trata de una carilla con el estado de situación de la organización, sin contenido técnico pero con métricas e indicadores que permiten entender el nivel de exposición y criticidad.
- **Informe técnico:** Este informe es mucho más completo, ofrece información para ser analizada por los responsables de TI con los desvíos existentes, recomendaciones de remediación priorizadas según criticidad y esfuerzo, pudiendo entender, además de su estado de situación, el plan de remediación.
- **Detalles:** Aquí se expresa toda la documentación referente a los hallazgos, sirve como registro de auditoría pudiendo entender los pormenores de los desvíos. Ofrece mayor información que el informe anterior, siendo de gran utilidad para entender los motivos e identificar posibles falsos positivos.

2. Detect

Módulo complementario con Discovery, el cual permite monitorear en tiempo real el comportamiento de diferentes partes de la infraestructura, pudiendo detectar ataques o compromisos posteriores a la ejecución del Discovery. Se basa principalmente en 3 funciones:

- **Monitoreo de Hosts:** Se deberá instalar un software de EDR (Endpoint Detection and Response) provisto por la empresa en cada uno de los equipos que se desee monitorear,

ya sean equipos PC, servidores, etc. El software analizará el comportamiento, buscando patrones maliciosos que suelen significar un intento de ataque hacia el sistema.

- **Monitoreo de Red:** El análisis de tráfico continuará trabajando de manera ininterrumpida, generando eventos de seguridad ante la detección de comportamientos maliciosos, como ser el intento de conexión de un equipo a una dirección IP de conocida mala reputación.
- **Monitoreo de Vulnerabilidades:** Los escaneos de vulnerabilidades correrán de manera periódica, una vez por día, analizando la infraestructura de manera constante contra nuevas vulnerabilidades.

3. Protect

El módulo Protect agrega dos capacidades extra a Detect, permitiendo realizar respuesta ante incidentes en tiempo real en dos de sus principales funciones, monitoreo de host y red. Ante la detección de un comportamiento malicioso, Protect bloqueara el origen del ataque, actuando como primer respondiente ante la amenaza.

4. Alert

Este componente permite encauzar todas las notificaciones generadas por los otros módulos hacia diferentes medios de comunicación, a elección del cliente, a través de webhooks. El servicio por defecto es a través de email, pero permite también crear bots en plataformas como Telegram o Slack.

5. Event Handling

El módulo de Event Handling ofrece la capacidad de gestionar y remediar los hallazgos identificados por Discovery o detectados por Detect, de una manera centralizada y eficiente. Consta principalmente de dos componentes:

- **Gestión de Vulnerabilidades:** Ofrece una plataforma donde coleccionar todas las vulnerabilidades detectadas, priorizarlas según su criticidad, asignarle un SLA, es decir, la fecha para la cual se espera que la vulnerabilidad este arreglada, y asignarle un dueño para su remediación. Permite integrarlo a través de Alert con otras plataformas para dar seguimiento de manera sencilla.
- **Gestión de Incidentes:** Ofrece una plataforma para tratar los incidentes de seguridad identificados por Discovery y Detect. Permite realizar procesos de inteligencia sobre los mismos, pudiendo entender fácilmente si se trata de un falso positivo o de un hecho real que requiere atención inmediata.

Arquitectura Organizacional

La organización se basa completamente en la tecnología, buscando automatizar todos los procesos posibles, reduciendo la cantidad de personal requerido para sus operaciones al mínimo exponente. Es por esto que consideramos que la estructura más eficiente, especialmente en esta etapa, es la Arquitectura Lineal.

Estrategia

La estrategia de la firma es ofrecer un servicio integral de seguridad a Pymes a través de un servicio SaaS. Para lograrlo, debe contar con una base tecnológica robusta, eficiente y a prueba de fallas, respaldada por personal técnico altamente capacitado y preparado para mantenerla y escalarla.

Teniendo en cuenta la volatilidad del mercado, la empresa dedica grandes esfuerzos en la fidelización del personal, buscando retenerlos generando un ambiente de trabajo sólido.

Estructura

Al ser una organización lineal, las decisiones se basan en el principio de la jerarquía. De todas maneras, creemos en la pluralidad de voces, por lo que abrimos el juego a la totalidad de los empleados, principalmente con el objetivo de que se sientan escuchados.

En este sentido, las decisiones estratégicas son tomadas por la Dirección, delegando fuertemente las decisiones operativas en los respectivos jefes de cada sector.

Recompensas

Se paga a los empleados el salario acorde al valor de mercado, priorizando en la selección aquellos que son motivados por desafíos más allá de lo económico.

La recompensa se complementa fuertemente con capacitaciones, desafíos laborales de gran magnitud, horario flexible y un gran ambiente laboral.

Personas

Dentro de las políticas asociadas a los empleados, creemos firmemente en la retención del personal para generar un ambiente de seguridad en toda la firma. Utilizamos mecanismos de feedback continuo y capacitamos a los líderes en el arte de la escucha activa y la capacidad de detección temprana de posibles problemas.

El área de Recursos Humanos es vital para la organización, y trabajan fuertemente en la selección de talento que pueda adaptarse a la cultura de la organización.

Trabajamos fuertemente en capacitar al personal, complementándolo con la asignación de desafíos cada vez más complejos que justifiquen esa capacitación. Es una manera de mantener los recursos activos, motivados y a gusto con su performance.

El personal trabaja completamente a distancia, la empresa no tiene oficinas físicas.

Organigrama

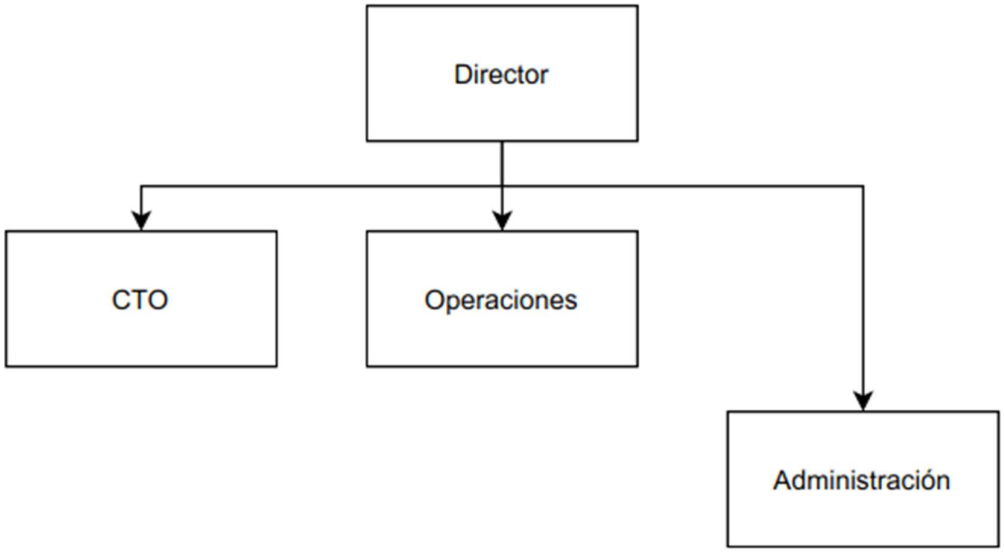

Figura 16

Recursos Requeridos

1. Management

El management consta de un director, encargado de los aspectos económicos, financieros y contables de la organización. Al director le reportan dos gerentes, el de Operaciones y el CTO, y la administración.

El gerente de Operaciones tiene la responsabilidad de llevar adelante las tareas técnicas operativas de la organización, como ser los servicios profesionales, soporte, respuesta a incidentes y la creación de nuevos contenidos.

Por otro lado, el CTO es responsable de implementar, mantener y escalar los desarrollos y sistemas.

2. Personas

	Management	Colaboradores	Total
Director	1	0	1
Operaciones	1	4	5
CTO	1	2	3
Administración	0	1	1
Total	3	7	10

Tabla 5

3. Tecnología

- Repositorio de GITHUB para alojar el código fuente del sistema;
- Plataforma en AWS para establecer la estructura del SaaS;
- Sitio web para distribución de contenido.

4. Conocimientos

Operaciones

- Seguridad de la Información
- Respuesta ante Incidentes
- Consultoría
- Atención al cliente
- Creación de contenido
- Pedagogía

CTO

- DevOps
- AWS
- Nmap
- Suricata

- Wazuh
- The Hive
- Cortex
- MISP
- OpenVAS
- GitOps
- Linux

5. Equipamiento

	Macbooks	Monitores	Sillas	Mouse	Headset
Director	1	1	1	1	1
Operaciones	5	5	5	5	5
CTO	3	3	3	3	3
Administración	1	1	1	1	1
Total	10	10	10	10	10

Tabla 6 – Equipamiento - (Elaboración Propia.)

6. Tercerización

Teniendo en cuenta el tamaño de la organización, hemos decidido tercerizar la selección de personal, los esfuerzos de marketing, las relaciones públicas y el soporte legal.

Marketing

Basados en la segmentación realizada, acotaremos nuestros esfuerzos principalmente a las empresas micro, pequeñas y medianas de tramo 1 (Ministerio de Producción y Trabajo de la Nación, 2018), con base tecnológica y ubicadas en las principales ciudades de la república argentina:

Intentaremos capturar estas oportunidades a través de diferentes canales, como ser el contacto directo, los tutoriales, la participación en conferencias y la generación de contenido

en redes sociales como Linkedin e Instagram. Estimamos que el impacto generado por estos en las diferentes industrias nos permitirá definir los siguientes objetivos de Marketing

Empresa por Región			Canal	2022	2023	2024	2025	2026
				Estimado	Estimado	Estimado	Estimado	Estimado
Buenos Aires	Micro	160364	Cont. Dir.	0	0	0	0	0
	Micro	160364	Tutoriales	327	245	164	98	98
	Micro	160364	Conferencias	327	245	164	98	98
	Micro	160364	Linkedin	981	736	491	294	294
	Micro	160364	Instagram	654	491	327	196	196
	Pequeñas	21471	Cont. Dir.	0	0	0	0	0
	Pequeñas	21471	Tutoriales	44	33	22	13	13
	Pequeñas	21471	Conferencias	44	33	22	13	13
	Pequeñas	21471	Linkedin	219	164	110	66	66
	Pequeñas	21471	Instagram	88	66	44	26	26
	Mediana tramo 1	4537	Cont. Dir.	19	14	9	6	6
	Mediana tramo 1	4537	Tutoriales	46	35	23	14	14
	Mediana tramo 1	4537	Conferencias	9	7	5	3	3
	Mediana tramo 1	4537	Linkedin	28	21	14	8	8
	Mediana tramo 1	4537	Instagram	0	0	0	0	0
	Mediana tramo 2	872	Cont. Dir.	0	0	0	0	0
	Mediana tramo 2	872	Tutoriales	2	1	1	1	1
	Mediana tramo 2	872	Conferencias	2	1	1	1	1
	Mediana tramo 2	872	Linkedin	0	0	0	0	0
	Mediana tramo 2	872	Instagram	0	0	0	0	0

Tabla 7 – Esfuerzo de Marketing Buenos Aires - (Elaboración Propia basada en datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

Empresa por Región			Canal	2022	2023	2024	2025	2026
				Estimado	Estimado	Estimado	Estimado	Estimado
CABA	Micro	99858	Cont. Dir.	0	0	0	0	0
	Micro	99858	Tutoriales	204	153	102	61	61
	Micro	99858	Conferencias	204	153	102	61	61
	Micro	99858	Linkedin	611	458	306	183	183
	Micro	99858	Instagram	407	306	204	122	122
	Pequeñas	18988	Cont. Dir.	0	0	0	0	0
	Pequeñas	18988	Tutoriales	39	29	19	12	12
	Pequeñas	18988	Conferencias	39	29	19	12	12
	Pequeñas	18988	Linkedin	194	145	97	58	58
	Pequeñas	18988	Instagram	77	58	39	23	23
	Mediana tramo 1	4043	Cont. Dir.	16	12	8	5	5
	Mediana tramo 1	4043	Tutoriales	41	31	21	12	12
	Mediana tramo 1	4043	Conferencias	8	6	4	2	2
	Mediana tramo 1	4043	Linkedin	25	19	12	7	7
	Mediana tramo 1	4043	Instagram	0	0	0	0	0
	Mediana tramo 2	1391	Cont. Dir.	0	0	0	0	0
	Mediana tramo 2	1391	Tutoriales	3	2	1	1	1
	Mediana tramo 2	1391	Conferencias	3	2	1	1	1
	Mediana tramo 2	1391	Linkedin	0	0	0	0	0
	Mediana tramo 2	1391	Instagram	0	0	0	0	0

Tabla 8 - Esfuerzo de Marketing CABA - (Elaboración Propia basada en datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

Empresa por Región			Canal	2022	2023	2024	2025	2026
				Estimado	Estimado	Estimado	Estimado	Estimado
Cordoba	Micro	50901	Cont. Dir.	0	0	0	0	0
	Micro	50901	Tutoriales	104	78	52	31	31
	Micro	50901	Conferencias	104	78	52	31	31
	Micro	50901	Linkedin	312	234	156	93	93
	Micro	50901	Instagram	208	156	104	62	62
	Pequeñas	5917	Cont. Dir.	0	0	0	0	0
	Pequeñas	5917	Tutoriales	12	9	6	4	4
	Pequeñas	5917	Conferencias	12	9	6	4	4
	Pequeñas	5917	Linkedin	60	45	30	18	18
	Pequeñas	5917	Instagram	24	18	12	7	7
	Mediana tramo 1	1184	Cont. Dir.	5	4	2	1	1
	Mediana tramo 1	1184	Tutoriales	12	9	6	4	4
	Mediana tramo 1	1184	Conferencias	2	2	1	1	1
	Mediana tramo 1	1184	Linkedin	7	5	4	2	2
	Mediana tramo 1	1184	Instagram	0	0	0	0	0
	Mediana tramo 2	221	Cont. Dir.	0	0	0	0	0
	Mediana tramo 2	221	Tutoriales	0	0	0	0	0
	Mediana tramo 2	221	Conferencias	0	0	0	0	0
	Mediana tramo 2	221	Linkedin	0	0	0	0	0
	Mediana tramo 2	221	Instagram	0	0	0	0	0

Tabla 9 - Esfuerzo de Marketing Cordoba - (Elaboración Propia basada en datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

Empresa por Región			Canal	2022	2023	2024	2025	2026
				Estimado	Estimado	Estimado	Estimado	Estimado
Santa Fe	Micro	48398	Cont. Dir.	0	0	0	0	0
	Micro	48398	Tutoriales	99	74	49	30	30
	Micro	48398	Conferencias	99	74	49	30	30
	Micro	48398	Linkedin	296	222	148	89	89
	Micro	48398	Instagram	197	148	99	59	59
	Pequeñas	6200	Cont. Dir.	0	0	0	0	0
	Pequeñas	6200	Tutoriales	13	9	6	4	4
	Pequeñas	6200	Conferencias	13	9	6	4	4
	Pequeñas	6200	Linkedin	63	47	32	19	19
	Pequeñas	6200	Instagram	25	19	13	8	8
	Mediana tramo 1	1313	Cont. Dir.	5	4	3	2	2
	Mediana tramo 1	1313	Tutoriales	13	10	7	4	4
	Mediana tramo 1	1313	Conferencias	3	2	1	1	1
	Mediana tramo 1	1313	Linkedin	8	6	4	2	2
	Mediana tramo 1	1313	Instagram	0	0	0	0	0
	Mediana tramo 2	247	Cont. Dir.	0	0	0	0	0
	Mediana tramo 2	247	Tutoriales	1	0	0	0	0
	Mediana tramo 2	247	Conferencias	1	0	0	0	0
	Mediana tramo 2	247	Linkedin	0	0	0	0	0
	Mediana tramo 2	247	Instagram	0	0	0	0	0

Tabla 10 - Esfuerzo de Marketing Santa Fe - (Elaboración Propia basada en datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

Empresa por Región			Canal	2022	2023	2024	2025	2026
				Estimado	Estimado	Estimado	Estimado	Estimado
Mendoza	Micro	21265	Cont. Dir.	0	0	0	0	0
	Micro	21265	Tutoriales	43	33	22	13	13
	Micro	21265	Conferencias	43	33	22	13	13
	Micro	21265	Linkedin	130	98	65	39	39
	Micro	21265	Instagram	87	65	43	26	26
	Pequeñas	3145	Cont. Dir.	0	0	0	0	0
	Pequeñas	3145	Tutoriales	6	5	3	2	2
	Pequeñas	3145	Conferencias	6	5	3	2	2
	Pequeñas	3145	Linkedin	32	24	16	10	10
	Pequeñas	3145	Instagram	13	10	6	4	4
	Mediana tramo 1	563	Cont. Dir.	2	2	1	1	1
	Mediana tramo 1	563	Tutoriales	6	4	3	2	2
	Mediana tramo 1	563	Conferencias	1	1	1	0	0
	Mediana tramo 1	563	Linkedin	3	3	2	1	1
	Mediana tramo 1	563	Instagram	0	0	0	0	0
	Mediana tramo 2	114	Cont. Dir.	0	0	0	0	0
	Mediana tramo 2	114	Tutoriales	0	0	0	0	0
	Mediana tramo 2	114	Conferencias	0	0	0	0	0
	Mediana tramo 2	114	Linkedin	0	0	0	0	0
	Mediana tramo 2	114	Instagram	0	0	0	0	0

Tabla 11 - Esfuerzo de Marketing Mendoza - (Elaboración Propia basada en datos obtenidos de la Distribución de empresas y empleo, Ministerio de Producción y Trabajo de la Nación, 2018)

Costos y Gastos

Costos Variables

Los costos variables están asociados directamente con la infraestructura cloud requerida para sustentar las operaciones. Teniendo en cuenta que los recursos utilizados escalan automáticamente en función de la demanda, ofrecen la capacidad de disponer de una infraestructura elástica.

Recurso	U$S	Pesos	Detalle
Lambda	$0,000000	$0,000000	primer millon por mes
	$0,000200	$0,020000	por mil extra
DynamoDB	$0,000000	$0,000000	Primeros 25GB
	$0,000900	$0,090000	por MB
SNS email	$0,000000	$0,000000	Primeros 1000 email
	$0,002000	$0,200000	por 1000 emails
SNS Webhook	$0,000000	$0,000000	Primeros 100.000 notificaciones
	$0,000600	$0,060000	Por mil extra

Tabla 12 – Costos Variables - (Elaboración propia basada en costos asociados a los recursos necesarios para implementar la solución).

Costos Variables por año en función a la Demanda Potencial:

Año	Año 2022	Año 2023	Año 2024	Año 2025	Año 2026
Clientes	**3961**	**2971**	**1980**	**1188**	**1188**
Lambda	$79.217,30	$59.412,98	$39.608,65	$23.765,19	$23.765,19
DynamoDB	$35.647,79	$26.735,84	$17.823,89	$10.694,34	$10.694,34
SNS email	$792.173,04	$594.129,78	$396.086,52	$237.651,91	$237.651,91
SNS Webhook	$237.651,91	$178.238,93	$118.825,96	$71.295,57	$71.295,57
Costos Variables	**$1.144.690,04**	**$858.517,53**	**$572.345,02**	**$343.407,01**	**$343.407,01**

Tabla 13 – Costos Variables en función de la demanda potencial - (Elaboración propia basada en costos asociados a los recursos necesarios para implementar la solución.)

Sueldos y Salarios

En Solidarity los sueldos de los empleados están por encima del mercado, en particular teniendo en cuenta que trabajamos con profesionales muy requeridos por las diferentes industrias. Es por esto que el cuadro de compensaciones se alinea de la siguiente manera:

Sueldos	Empleados	Pesos	Total
Director	1	$700.000,00	$700.000,00
Managers	2	$700.000,00	$1.400.000,00
Ingenieros	2	$250.000,00	$500.000,00
Operaciones	4	$300.000,00	$1.200.000,00
Administrativos	1	$50.000,00	$50.000,00

Tabla 14 – Tabla de Sueldos y Salarios – (Elaboración Propia basada en estimaciones de salarios del mercado de IT.)

Costos Fijos

Teniendo en cuenta que la totalidad de la infraestructura se encuentra hosteada en entornos cloud, y que la empresa se desempeña completamente de manera remota, se reducen en gran medida los costos fijos requeridos para operar.

De esta manera, es que tendremos en cuenta aquellas tareas que tercerizamos, como ser las campañas de Marketing, el talent scouting para reclutamiento de personal y la gestión de relaciones públicas.

Costos Fijos	Q1	Q2	Q3	Q4
Marketing/Publicidad	$600.000,00	$300.000,00	$300.000,00	$300.000,00
Soporte legal	$450.000,00	$450.000,00	$450.000,00	$150.000,00
Software de Gestion (ERP)	$150.000,00	$150.000,00	$150.000,00	$90.000,00
Talent Scout	$300.000,00	$300.000,00	$300.000,00	$300.000,00
RRPP	$600.000,00	$600.000,00	$600.000,00	$600.000,00
TOTAL	$2.100.000,00	$1.800.000,00	$1.800.000,00	$1.440.000,00

Tabla 15 – Costos Fijos - (Elaboración Propia basada en estimaciones.)

Análisis Económico Financiero

Estimación de venta, pricing.

Es importante destacar que el precio de los servicios a ofrecer impactará directamente en el flujo de caja de la empresa, basados principalmente en los márgenes de ganancia y volúmenes de venta.

En los capítulos anteriores nos hemos familiarizado con los clientes objetivo, la competencia y las características del mercado y hemos logrado identificar cuales son las características más importantes para nuestros clientes objetivo.

Siguiendo esa línea de pensamiento, hemos analizado los objetivos comerciales siguiendo la máxima prioridad de respetar la visión de Solidarity, es decir, elevar el nivel de seguridad de todas las organizaciones independientemente de su poder adquisitivo.

Es por todo esto que hemos decidido adoptar la estrategia de precios Freemium para la plataforma Solidarity, muy común en la industria del software, mediante la cual ofreceremos parte del servicio en forma gratuita, pudiendo ser ampliado por un precio.

A su vez, utilizaremos una estrategia de precio de penetración para los servicios de consultoría, buscando atraer a más seguidores que, a su vez, podrán contratar los módulos de Solidarity.

Política de pagos y cobros

Todos los servicios serán adquiridos a través de nuestro portal, pudiendo suscribirse de manera completamente automática con la utilización de una tarjeta de crédito, metodología muy común en los servicios SaaS.

De esta manera, los consumos les serán debitados de manera mensual a los clientes. En caso de que no cumplan con los pagos, la plataforma se retraerá automáticamente a su versión gratuita.

Flujo de caja, flujo de ingresos y egresos

Teniendo en cuenta el análisis de marketing, a partir del cual hemos sido capaces de identificar nuestro cliente persona, la demanda potencial y la cantidad estimada de clientes, y la estructura de costos y gastos abordados en los capítulos anteriores del presente documento, podemos establecer que nuestro flujo de cajas sería de la siguiente manera:

Año	Año 0	AÑO 1 - 2022	AÑO 2 - 2023	AÑO 3 - 2024	AÑO 4 - 2025	AÑO 5 - 2026
Clientes		**990**	**1683**	**2030**	**2134**	**2165**
Ventas		$19.804.326	$33.667.354	$40.598.868	$42.678.323	$43.302.159
Costos Variables		$286.173	$200.321	$100.160	$30.048	$9.014
cMG		$19.518.153	$33.467.033	$40.498.708	$42.648.274	$43.293.144
Costo Fijo		$16.598.715	$16.598.715	$16.598.715	$16.598.715	$16.598.715
EBIT		$2.919.438	$16.868.318	$23.899.993	$26.049.559	$26.694.429
Interes						
EBT		$2.919.438	$16.868.318	$23.899.993	$26.049.559	$26.694.429
Impuestos		$1.021.803	$1.021.803	$1.021.803	$1.021.803	$1.021.803
Inversion	-$17.138.715	-$2.919.438				
Utilidad Neta	$0	$1.897.635	$15.846.515	$22.878.189	$25.027.756	$25.672.626
Utilidad Acumulada	**-$17.138.715**	**-$15.241.080**	**$605.435**	**$23.483.624**	**$48.511.380**	**$74.184.006**

Tabla 16 – Cashflow - (Elaboración Propia basada en datos obtenidos previamente en este trabajo.)

Requerimientos de capital

Como puede apreciarse en el análisis realizado sobre el flujo de caja, se requieren $17.138.715 para iniciar con la operación y se comenzarán a percibir ganancias al finalizar el primer trimestre del 2do año.

Payback

En base al flujo de caja estipulado, se puede determinar que el período de Payback es de 2 Años.

VAN (Valor Actual Neto) y TIR (Tasa interna de Retorno)

Calculando el VAN y el TIR a partir de los flujos de caja estimados para los próximos 5 años de actividad, podemos determinar que:

El Valor Actual Neto es de $6.272.505, por lo que la inversión es aceptable.

Dada las condiciones económicas de la República Argentina, consultamos con una consultora externa especialista en finanzas para lograr determinar que la tasa de descuento habitualmente utilizada para este tipo de proyectos es del 50%.

En lo que respecta a la Tasa Interna de Retorno (66%), la misma es ampliamente mayor a la tasa de descuento esperada (50%) por lo que también se comprueba que la inversión es aceptable.

Desembolso Inicial	-$17.138.715,00			
Flujo de Caja Año 1	$1.897.635	K+1	150%	$1.265.090
Flujo de Caja Año 2	$15.846.515	(k+1)2	225%	$7.042.896
Flujo de Caja Año 3	$22.878.189	(k+1)3	338%	$6.778.723
Flujo de Caja Año 4	$25.027.756	(k+1)4	506%	$4.943.754
Flujo de Caja Año 5	$25.672.626	(k+1)5	759%	$3.380.757
Tasa de Descuento (K)	50%			
VAN (Valor actual Neto)	**$6.272.505**			
TIR (Tasa interna de Retorno)	**66%**			

Tabla 17 – (Elaboración Propia basada en datos obtenidos previamente en este trabajo.)

Para mayor ilustración, procedimos a simular la tasa interna de retorno en función de las siguientes cantidades de clientes supuestas para los primeros 5 años de operación:

Clientes	TIR
4501	21%
6752	49%
7202	53%
9003	66%
10803	77%
12604	86%

Tabla 18 – Simulación TIR en función de clientes (Elaboración Propia basada en datos obtenidos previamente en este trabajo.)

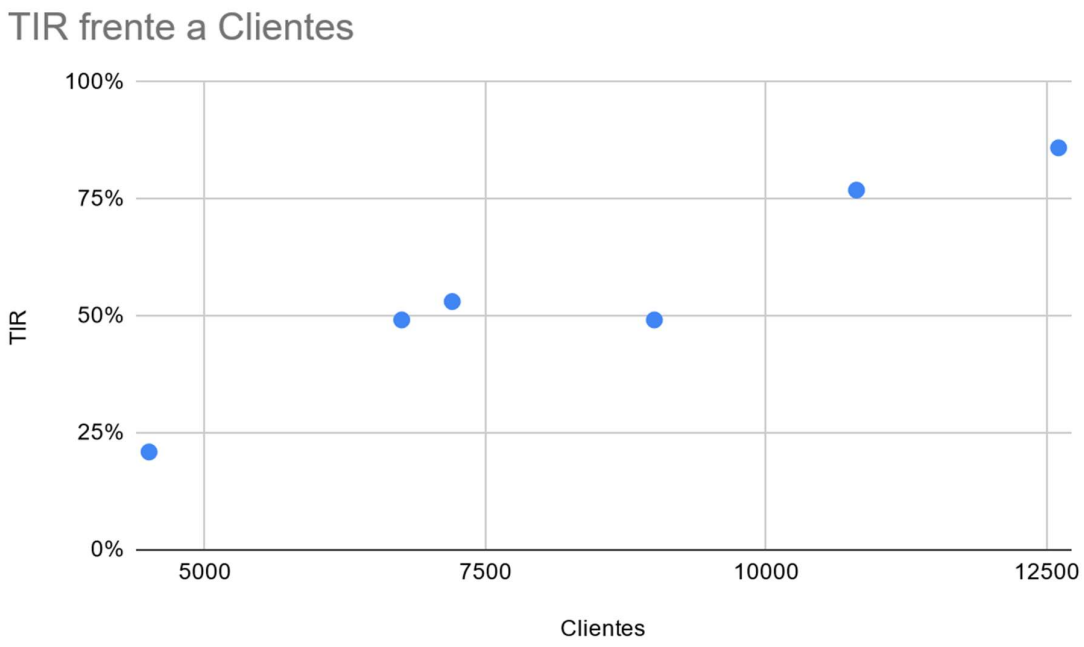

Tabla 19 – Simulación TIR en función de clientes 2 (Elaboración Propia basada en datos obtenidos previamente en este trabajo.)

Esta simulación nos permite comprender que, el proyecto sería rentable logrando adquirir 7200 clientes en los primeros 5 años de operación.

Financiación del proyecto

Teniendo en cuenta los montos requeridos para comenzar con la operación estudiadas en el apartado anterior, creemos conveniente financiar el proyecto con capitales propios.

Creemos que es la mejor forma de encarar este proyecto ya que es la que nos ofrece mayor independencia y rapidez, pudiendo prescindir de garantías o avales, dándonos la oportunidad de maximizar la rentabilidad al disminuir los gastos financieros.

Aspectos Jurídicos - Marcas

Dentro de los aspectos jurídicos, es importante considerar la protección de la marca Solidarity, es decir *"el amparo de una marca en relación a nuevas solicitudes de signos confundibles con el propio, o el de su protección con respecto a actos de terceros que mediante imitaciones o falsificaciones pretenden usufructuar el prestigio, reputación y éxito que ha adquirido su marca entre el público en general y el consumidor en particular."* (Dossier Net, 2014).

Para proteger la marca, utilizaremos una del tipo denominativa, es decir, *"aquellas marcas que identifican un producto o servicio a partir de una palabra o conjunto de palabras"* (Dossier Net, 2014), esto se fundamenta en que no se verán desactualizadas por aquellos cambios que pudieran surgir en el tipo de letra o color. Deberemos registrar la denominación por un lado y el logo por el otro.

Conclusiones

Como hemos señalado al iniciar con este proyecto, todas las organizaciones pueden ser afectadas por un ciberataque, ya sea por ser el objetivo específico de un grupo cibercriminal, como así también como un daño colateral de un ataque generalizado. Esta circunstancia se ve radicalmente agravada por el impacto de la transformación digital en todas las industrias, lo que se traduce en un gran problema, puesto que las bandas criminales elevan sus capacidades a diario, por lo que el riesgo al que se encuentran expuestas las diferentes entidades es cada vez mayor.

Como en toda carrera armamentística, los esfuerzos de ciberdefensa intentan seguir el ritmo de avance de los atacantes, especialmente de la mano de empresas dedicadas a ofrecer servicios de ciberseguridad. El gran inconveniente es que estos desarrollos son muy costosos, por lo que las empresas pequeñas y medianas de la República Argentina no disponen a la fecha de herramientas para elevar su postura de seguridad a un precio acorde a sus posibilidades.

Es en este contexto que nace Solidarity, con el simple objetivo de democratizar el acceso a la ciberseguridad, ofreciendo capacidades de manera gratuita a toda entidad que así lo requiera, pudiendo ampliarlas por una tarifa más que accesible en caso de creerlo necesario y contando con un equipo de consultores para potenciar y sumar aún más valor a los desarrollos.

La razón por la que es posible cumplir con estos objetivo se basa principalmente en la correcta implementación de tecnologías cloud que, como hemos visto a lo largo del desarrollo, nos permiten manejar los requerimientos de una manera elástica, es decir, utilizando los recursos justos, escalando horizontalmente conforme aumenta la demanda.

Siguiendo esta línea de pensamiento, desarrollamos una estrategia de marketing que nos permitirá alcanzar a nuestros clientes en las principales ciudades de la república argentina a través de diferentes canales, apoyándonos principalmente en la creación de

contenido de concientización y guías tutoriales que ayudarán a todas las personas del país a aumentar sus defensas, independientemente de que sean nuestros clientes o no, ofreciéndonos una imagen de marca gentil, dispuesta a colaborar y que refuerza nuestra visión. Queremos que todas las organizaciones puedan aumentar sus capacidades de seguridad.

A pesar de que el corazón del negocio funcionará de manera automatizada, contaremos con un equipo de profesionales que nos permitirán mantener los estándares de calidad que requerimos. Es aquí donde se presenta el mayor de los desafíos, puesto que el mercado de recursos humanos del sector es muy volátil y resulta muy difícil competir con la competencia, especialmente aquellas empresas extranjeras que pueden permitirse entregar salarios dolarizados.

Con esta batería de medidas podremos elevar el pobre nivel de seguridad existente en el país ampliamente, pero somos conscientes de que, para ayudar a nuestros clientes de la mejor manera, necesitamos un proceso de mejora continua que nos permite ofrecerles más servicios que sigan perfeccionando sus defensas. Es por esto que contaremos con un equipo de investigación y desarrollo, quienes serán responsables de crear nuevos proyectos que, con el tiempo, devendrá en nuevos productos.

En lo que respecta al análisis económico y financiero, es importante destacar que se espera alcanzar el payback a los 3 años de haber comenzado con la operación, habiendo alcanzado los 1683 clientes, indicando tanto el valor actual neto como la tasa interna de retorno que la inversión es aceptable.

La ciberseguridad es responsabilidad de todos, el impacto de un ciberataque no solo afecta a quien lo recibe, sino que también impide el funcionamiento de todas las entidades que dependen de esta. Es por esto que debemos poner nuestro granito de arena para ofrecer resiliencia a todas las organizaciones que estén dispuestas a abrazar el desafío, he aquí

Solidarity, nuestro aporte a la sociedad para democratizar el acceso a estas sofisticadas herramientas.

Bibliografía

Amazon Web Services. (2021, 1 1). *Cloud Security Alliance (CSA)*. Cloud Security Alliance (CSA). Retrieved 8 16, 2021, from https://aws.amazon.com/es/compliance/csa/

Barbosa, D. C. (2020, 1 02). *Qué es un proxy y para qué sirve*. Qué es un proxy y para qué sirve. Retrieved 8 16, 2021, from https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

Cosentino, L. (2021, 1 1). *Sí, vamos a hablar de ERP*. Sí, vamos a hablar de ERP. Retrieved 8 16, 2021, from https://recursos.evaluandosoftware.com/mercado/si-vamos-a-hablar-de-erp/

Dossier Net. (2014, 3 21). *Informe sobre aspectos legales para un correcto cuidado de las marcas*. Informe sobre aspectos legales para un correcto cuidado de las marcas. Retrieved 8 16, 2021, from https://www.dossiernet.com.ar/articulo/informe-sobre-aspectos-legales-para-un-correcto-cuidado-de-las-marcas/633

Ferranti, M. (2018, 8 17). *What is Nmap? Why you need this network mapper*. What is Nmap? Why you need this network mapper. Retrieved 8 16, 2021, from https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html

Herrero, H. (2017, 9 7). *Instalando y usando OpenVAS*. Instalando y usando OpenVAS. Retrieved 8 16, 2021, from https://www.bujarra.com/instalando-usando-openvas/

ITware Latam. (2021, 3 25). *La falta de especialistas en ciberseguridad preocupa a la industria*. La falta de especialistas en ciberseguridad preocupa a la industria.

Retrieved 8 16, 2021, from https://www.itwarelatam.com/2021/03/25/la-falta-de-especialistas-en-ciberseguridad-preocupa-a-la-industria/

LACNIC. (2020, 03 31). *La carrera contra el ciber crimen no tiene fronteras*. prensa.lacnic.net. Retrieved 08 16, 2021, from https://prensa.lacnic.net/news/ciberseguridad/la-carrera-contra-el-ciber-crimen-no-tiene-fronteras

Ministerio de Producción y Trabajo de la Nación. (2018, 1 1). *Panorama de empresas*. Panorama de empresas. Retrieved 8 16, 2021, from https://gpsempresas.produccion.gob.ar/datos-y-analisis/

Sputnik News. (2021, 4 2). *Aumentan en Argentina las denuncias por delitos informáticos en la cuarentena por COVID-19*. Aumentan en Argentina las denuncias por delitos informáticos en la cuarentena por COVID-19. Retrieved 8 16, 2021, from https://mundo-sputniknews-com.cdn.ampproject.org/c/s/mundo.sputniknews.com/amp/20210402/aumentan-en-argentina-las-denuncias-por-delitos-informaticos-en-la-cuarentena-por-covid-19-1110759794.html

Telam. (2020, 10 3). *Aumentaron un 70% los ciberataques durante la pandemia, según estudio privado de alcance global*. Aumentaron un 70% los ciberataques durante la pandemia, según estudio privado de alcance global. Retrieved 8 16, 2021, from https://www.telam.com.ar/notas/202010/530904-ciberataques-aumento-web.html

Valiente, J. (2021, 2 2). *Madurez de las estrategias nacionales de ciberseguridad en Latinoamérica*. Madurez de las estrategias nacionales de ciberseguridad en Latinoamérica. Retrieved 8 16, 2021, from https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/ciberseguridad-madurez-de-las-estrategias-nacionales-de-ciberseguridad-en-latinoamerica_20210202.html