PERCEPTION POINT

Perception Point

Diferenciadores clave

DSA
DISTRIBUIDORA DE SERVICIOS ANTIVIRUS, S.L.

Diferenciadores clave

Perception Point se centra únicamente en la ciberseguridad y ofrece seguridad para proteger contra las amenazas provenientes de distintos tipos de contenido (URL, archivos, distintos tipos de texto, etc.). La empresa ha desarrollado un enfoque único hacia la protección de las empresas a través de los siguientes canales: el correo electrónico, los navegadores web y las apps en la nube. Así, ha ganado una posición de liderazgo en el mercado.

Entre los diferenciadores clave que permiten que Perception Point destaque en comparación con otras soluciones en el mercado se encuentran:

Detección de última generación

Perception Point proporciona siete capas de detección avanzada contra cualquier tipo de ataque en forma de contenido, lo que da como resultado la protección más efectiva, no solo la mejor tasa de detección del mercado, sino también la tasa de falsos positivos más baja. El valor añadido de Perception Point incluye motores *anti phishing* únicos basados en ML e IA, prevención avanzada de ataques provenientes de archivos, utilizando tecnología dinámica rápida de última generación y capacidades BEC avanzadas para evitar la suplantación de identidad en forma de texto. Es importante tener en cuenta que Perception Point es compatible con todas las implementaciones de seguridad de correo electrónico, incluidas las implementaciones locales, en la nube e híbridas.

Prevención 0-days

Perception Point ha desarrollado una tecnología patentada que ninguna otra empresa puede ofrecer. Utiliza datos a nivel de CPU, tomados de la fuente misma de la CPU para evitar ataques 0-days de manera determinista. Esta tecnología avanzada ha revolucionado el mundo del escaneo dinámico y supera cualquier sandboxing u otra tecnología APT (como CDR) en el mercado.

Motores anti-evasión

Perception Point ha creado una tecnología innovadora para descubrir cualquier intento de ocultar/ocultar intenciones maliciosas. Los algoritmos exclusivos de la empresa, junto con la arquitectura en la que se basa la tecnología, permiten que Perception Point escanee todo el contenido en varias formas y métodos para garantizar que se descubra la intención maliciosa. Otras soluciones simplemente no tienen tales capacidades, lo que deja a la organización propensa a ser víctima de este tipo de ataques.

Respuesta a incidents

Además de informar al usuario final, con la combinación de algoritmos automatizados basados en ML y decisiones impulsadas por humanos, Perception Point garantiza la optimización continua del sistema, el control total de FP y FN y el análisis profundo de incidentes. El equipo de respuesta a incidentes de Perception Point está compuesto por expertos en ciberseguridad altamente calificados que garantizan una respuesta rápida a cualquier solicitud. El servicio proporciona informes e información de alta calidad. No es

solo una opción de "salir de la cuarentena" como en otros servicios, sino un equipo de soporte completo y una extensión del equipo SOC del cliente.

Análisis dinámico del 100 % del tráfico

A diferencia de otros proveedores de seguridad de contenido y correo electrónico, Perception Point analiza el 100 % del contenido de forma dinámica. Esto significa que Perception Point escanea cada dato que se transfiere para validar que el contenido es seguro, sin atajos ni cambios. Ninguna otra empresa puede ofrecer eso, y esto es aún más relevante para las empresas a gran escala.

Velocidad

La tecnología Perception Point proporciona el tiempo de demora promedio más bajo para la entrega de correo electrónico que incluye escaneo dinámico. Con un tiempo de escaneo promedio de 10 segundos, el servicio de Perception Point garantiza la mejor experiencia de usuario y la mejor entrega de correo electrónico a sus clientes. Perception Point recomienda encarecidamente que los clientes tengan en cuenta este atributo al elegir el proveedor adecuado para sus necesidades. La experiencia del usuario es clave en la entrega soluciones a los usuarios finales.

Protección transversal de canales

La oferta de productos de Perception Point incluye una amplia gama de soluciones de protección. La tecnología de Perception Point se utiliza para proteger todos y cada uno de los portales de colaboración de contenido, lo que garantiza una comunicación segura entre la empresa y sus partes interesadas externas. Las principales aplicaciones en la nube cubiertas son OneDrive, SharePoint, Teams, Blob Storage, Salesforce, aplicaciones compatibles con ICAP y más. Además, Perception Point también ha desarrollado una API altamente personalizada que permite a la empresa y sus clientes integrarse fácilmente con cualquier aplicación construida internamente.

Escala y rendimiento nativos de la nube

Perception Point proporciona soluciones verdaderamente nativas de la nube, a diferencia de las soluciones que “han migrado a la nube”, pero cuya arquitectura y tecnología se construyeron originalmente como una solución local. Como solución nativa de la nube, Perception Point puede adaptarse a cualquier escala y tráfico de la organización, asegurando un escaneo dinámico completo, evitando cuellos de botella y proporcionando siempre niveles de rendimiento altos y optimizados.

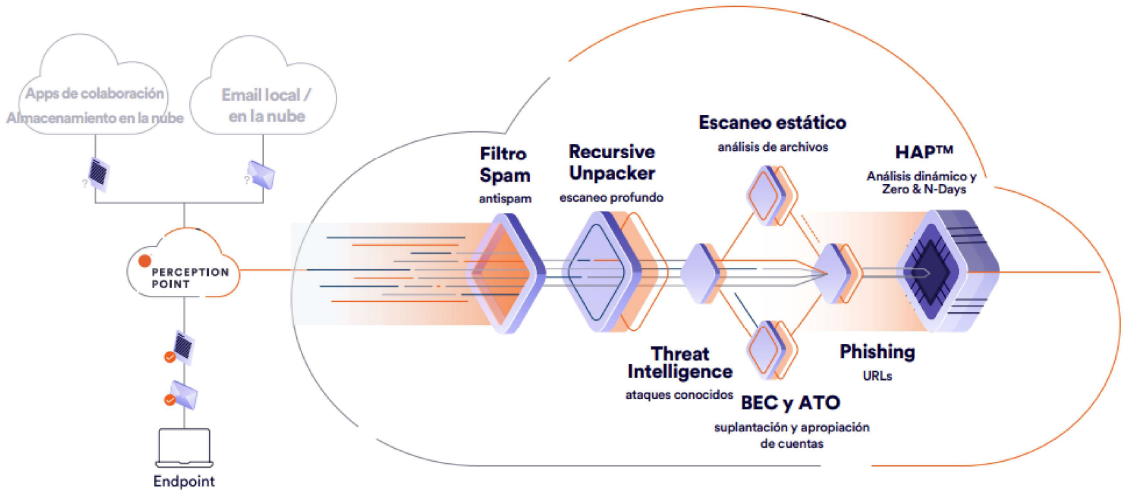
Implementación

Las soluciones de Perception Point se implementan de manera fácil y nativa con Office 365. Los clientes pueden decidir cómo desean implementar Perception Point, ya sea en el SEG o como una solución integrada que complemente a otros SEG, incluido FireEye. En el último caso, la implementación de Perception Point permitirá al cliente conservar las reglas existentes, evitar el cambio de registro MX y beneficiarse de la protección de la oferta de Microsoft además de la solución de Perception Point.

Estas capacidades se han traducido en una sólida posición de mercado en el mercado de la seguridad del correo electrónico. También nos gustaría remitirlo a la respuesta a la pregunta 4 en el Excel de soporte que destaca diferencias adicionales entre Perception Point y SEG y Agari de FireEye.

1. Resumen de tecnología y productos

Advanced Email Security de Perception Point cuenta con la tecnología de una plataforma de 7 capas que identifica e intercepta cualquier ataque cibernético basado en contenido, aprovechando tecnologías dinámicas y estáticas patentadas que se ejecutan rápidamente en todos los archivos, URL y texto libre:



Mecanismo general

Decisiones y reglas: proporciona una política avanzada y una gestión del tráfico de contenido específico compartido por cada cliente y los clientes de Perception Point. El mecanismo de "Decisiones" de Perception Point incluye algoritmos automatizados basados en IA y decisiones impulsadas por humanos que se acumulan continuamente para decidir inteligentemente si el contenido es malicioso o no. Las decisiones incluyen un amplio conjunto de opciones para incluir en la lista de permitidos/bloquear en función de la IP, el dominio o la URL del remitente, lo que impulsa reglas complejas basadas en los diferentes atributos específicos de la fuente.

Capa 1

Antispam: evita que las campañas de spam pasen al proveedor ubicado en el MX, p. ej. *FireEye*. Entre los muchos algoritmos de AI/ML desarrollados internamente en esta capa se encuentran la identificación de contenido simulado, similitudes de metadatos de correo electrónico y las verificaciones basadas en la reputación. Todos están en constante evolución y autoaprendizaje sobre las tendencias y ataques actuales. Además, esta capa

también proporciona un antivirus básico basado en la reputación para identificar rápidamente los correos electrónicos maliciosos.

Capa 2

Anti-evasión (el "*Recursive Unpacker*"): descubre ataques que utilizan técnicas de evasión, incluida la incorporación de contenido malicioso en archivos y URL. El Recursive Unpacker y los algoritmos de soporte descubren URL y archivos maliciosos ocultos dentro de otros objetos para garantizar que ninguna técnica de evasión engañe al servicio. La capa busca recursivamente archivos y URL, los extrae y los escanea por separado en sus diversos motores. Esta capacidad le permite al cliente mejorar sus políticas; por ejemplo, el cliente puede extender la política de bloqueo de manera recursiva (por ejemplo, bloqueando un archivo .exe archivado en un archivo .rar u oculto detrás de una carpeta o URL de Dropbox).

Capa 3

Inteligencia de amenazas: detecta e identifica *malware* básico generalizado, direcciones URL maliciosas y campañas de ataque. Perception Point administra una base de datos de inteligencia de amenazas que recopila múltiples listas de URL maliciosas y archivos de terceros, además de una base de datos interna que recopila información de clientes protegidos, prospectos y de la naturaleza. La base de datos se actualiza cada minuto y se agregan diariamente millones de URL y archivos únicos.

Capa 4

Firmas AV estáticas: detecta la ejecución de código malicioso en archivos mediante firmas conocidas y otros métodos de análisis estático. La capa combina los mejores motores antivirus basados en firmas de su clase para identificar ataques maliciosos con una herramienta patentada, el "Disector", que identifica firmas altamente complejas.

Capa 5

Anti-phishing: detecta páginas web de phishing enviadas en forma de URL por correo. Esta capa se compone de muchos motores y tecnologías únicos, que incluyen:

- Reconocimiento de imágenes: un motor patentado que identifica la suplantación de marca y los ataques de phishing al aprovechar la visión artificial con capacidades de IA. El motor valida que todas las URL son realmente legítimas. El motor es completamente dinámico e identifica intentos de suplantar activos de ambas marcas conocidas (por ejemplo, Microsoft, WeTransfer)
- Gráfico de la cadena de suministro: uso de capacidades de IA/ML para monitorear constantemente y proporcionar comentarios sobre la reputación y la puntuación de riesgo de cualquier metadato de correo electrónico, incluidos dominios, URL, IP y más.
- Análisis léxico de URL: análisis de la estructura de URL y búsqueda de similitudes con URL maliciosas utilizando AI/ML.
- Reputación de URL: además de aprovechar los recursos de terceros, el motor también analiza múltiples parámetros de cada contenido entregado, centrándose

en los activos del remitente y el destinatario, para identificar el intento de phishing del empleado.
- Escaneo avanzado de páginas web: utiliza ML para identificar la suplantación de identidad y el robo de contraseñas en sitios que se sabe que roban credenciales (por ejemplo, Google Form, incluida cualquier evasión en esta plataforma).
- Escaneo de URL o archivos html para la identificación de kits de phishing.
- Algoritmos de similitud: búsqueda y comparación de indicadores de phishing para ataques similares utilizando AI/ML.

Capa 6

Anti-BEC y Anti-ATO: detecta correos electrónicos que no necesariamente incluyen archivos/URL maliciosos y brinda protección a las partes interesadas y los activos de terceros. Esta capa también identifica cuentas comprometidas que se sospecha que han sido tomadas por un actor malicioso. Las tecnologías utilizadas en esta capa incluyen:

- Listas VIP y falsificación de nombres: evita los intentos de falsificación de nombres de empleados clave de la organización, incluida la identificación de direcciones de correo electrónico privadas.
- Suplantación de dominio (también conocida como "Suplantación de identidad perfecta"): tanto para los dominios del cliente como para los proveedores externos.
- Comprobaciones SPF, DKIM y DMARC.
- SPF interno: capacidad única que permite que Perception Point extraiga la IP de origen del correo electrónico, incluso si no se encuentra en el registro MX.
- Identificación similar al dominio: uso de IA para evitar intentos de ofuscar nombres de marca.
- Análisis léxico: análisis de texto, incluidas expresiones regulares y aprendizaje automático para identificar texto sospechoso. Esto incluye el análisis de correos electrónicos fraudulentos, sextorsión, fraudes con bitcoins y más.
- Mecanismo de puntuación: análisis de remitentes, dominios y otros vectores para identificar la actividad de los remitentes sospechosos.
- Aprendizaje automático de proveedores mediante IA/ML.

Para la detección de ATO, Perception Point analiza el registro de auditoría y utiliza varios algoritmos basados en IA para detectar comportamientos sospechosos de los usuarios. Dichas reglas pueden incluir la creación de reglas de bandeja de entrada sospechosas, viajes imposibles, realizar actividades de inicio de sesión sospechosas, reconocimiento de intenciones, detección de espionaje, detección de hilos secuestrados, detección de ataques dirigidos y más. Una característica adicional de esta capacidad es que una vez que se descubre un ATO potencial, el cliente recibe un correo electrónico con el asunto "URGENTE - ATO posible". El correo electrónico incluirá detalles de la presunta apropiación de la cuenta.

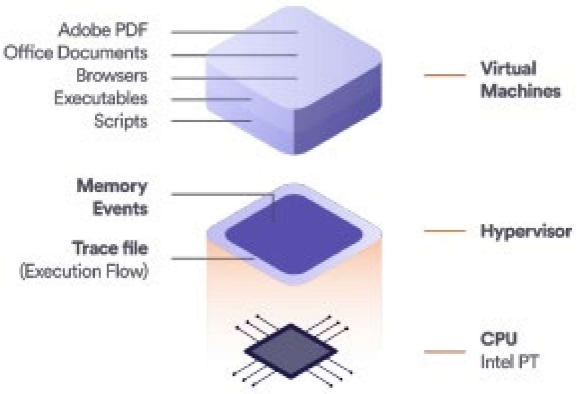
Capa 7

HAP™ (Plataforma asistida por hardware): este es el entorno limitado de última generación de Perception Point y el motor patentado más exclusivo que ha revolucionado la forma en que se realiza el escaneo dinámico. El HAP™ brinda prevención en tiempo real al

interceptar documentos maliciosos y URL que aprovechan: vulnerabilidades 0-days, vulnerabilidades N-days dirigidas a actualizaciones de software sin parches, ejecución de código malicioso en scripts y código malicioso en archivos ejecutables. El HAP sobresale en la velocidad de escaneo y, a diferencia de los sandbox tradicionales que toman minutos para cada escaneo, escanea en un promedio de 10 segundos por escaneo. El HAP™ se compone de algoritmos de software que utilizan datos a nivel de CPU para acceder a todo el flujo de ejecución, directamente desde el procesador. En solo segundos, puede interceptar de manera determinista técnicas de explotación previas al lanzamiento de malware.

El HAP™ incluye tres tipos de algoritmos:

- CFG: detecta exploits de corrupción de memoria de día cero y día N
- FFG - Detecta técnicas de explotación avanzadas
- Dropper: detecta errores lógicos y Droppers en aplicaciones, así como códigos maliciosos en secuencias de comandos. Además, HAP™ es único en el sentido de que proporciona escaneo dinámico para computadoras macOS, lo que permite a una organización proteger tanto sus PC como las computadoras y portátiles Apple.



2. El servicio

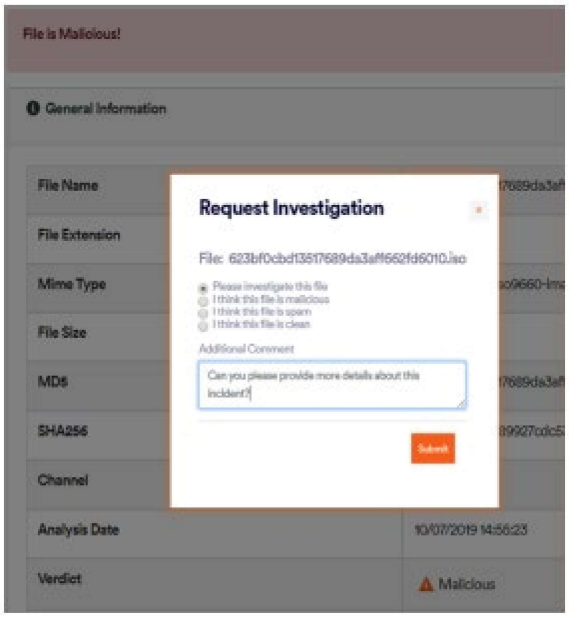
Además de la plataforma, y como parte integral de ella, Perception Point también ofrece un conjunto de servicios que completan su oferta. Estos servicios incluyen, resumidamente: (i) Respuesta a incidentes - un equipo de expertos en seguridad cibernética monitorea y administra constantemente la plataforma para los clientes, actuando como su equipo SOC extendido; (ii) Informes del usuario final y remediación posterior a la entrega; (iii) La herramienta de operaciones X-Ray – Viewer y SOC; (iv) Informes, y; (v) Implementación automática y actualizaciones que aprovechan la tecnología nativa de la nube de la empresa. Además, la oferta incluye soporte 24x7x365.

El equipo de Respuesta a Incidentes actúa como el multiplicador de fuerza del SOC del cliente. Combinando capacidades de aprendizaje automático, procesos automatizados y una estrecha interacción entre sus analistas cibernéticos y el equipo del cliente, Perception Point se asegura de que se analice cada incidente. Este servicio incluye (i) Monitoreo, análisis y reporte de todos los incidentes marcados por el sistema; (ii) Alertas rápidas y análisis de intentos maliciosos; y (iii) Manejo de FP, remediación y liberación según sea necesario.

Además, el equipo de IR permite a los equipos de SOC abrir un ticket de solicitud de investigación para cualquier otro archivo o URL del que deseen obtener un análisis completo. Esto incluye la opción de investigar un incidente, la oportunidad de cambiar el veredicto y la opción de informar FP.

Un detalle más elaborado sobre los servicios antes mencionados se puede encontrar a continuación.

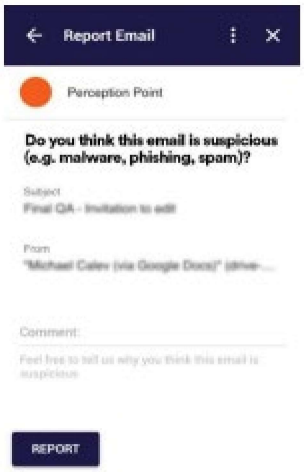
2.1. Respuesta a incidentes:



Un equipo de ciberanalistas e ingenieros cibernéticos que actúa como fuerza multiplicadora de su SOC. Combinando capacidades de AI, procesos automatizados y una estrecha interacción entre sus analistas cibernéticos y su equipo, Perception Point se asegura de que se analice cada incidente. Este servicio incluye: (i) Monitoreo, análisis y reporte de todos los incidentes identificados por el sistema; (ii) Alertas rápidas y análisis de intentos maliciosos; y (iii) Manejo de FP, remediación y liberación según sea necesario.

Además, el equipo de IR permite a los equipos de SOC abrir un ticket de solicitud de investigación para cualquier otro archivo o URL del que deseen obtener un análisis completo. Esto incluye la opción de investigar un incidente, la oportunidad de cambiar el veredicto y la opción de reportar FP. Ver más detalles a continuación.

2.2. Informes del usuario final y corrección posterior a la entrega:



Permitir a los usuarios finales consultar con expertos en seguridad de forma directa e instantánea antes de realizar una acción imprudente.

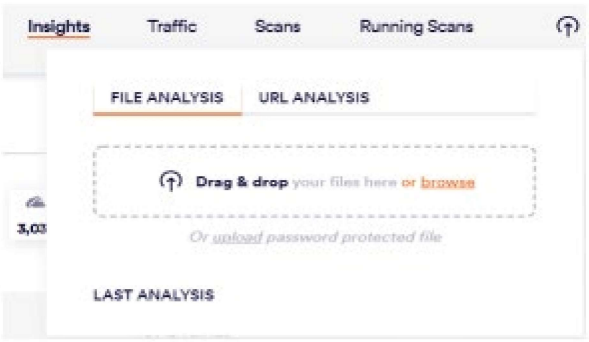
El usuario puede informar correos electrónicos sospechosos directamente desde Office 365 utilizando el complemento de Perception Point. La solicitud va tanto al equipo SOC del cliente como al equipo de respuesta a incidentes de Perception Point.

Además, los correos electrónicos se pueden eliminar de la bandeja de entrada del usuario directamente desde X-Ray, lo que ofrece una reparación completa posterior a la entrega (a través de la aplicación instalada).

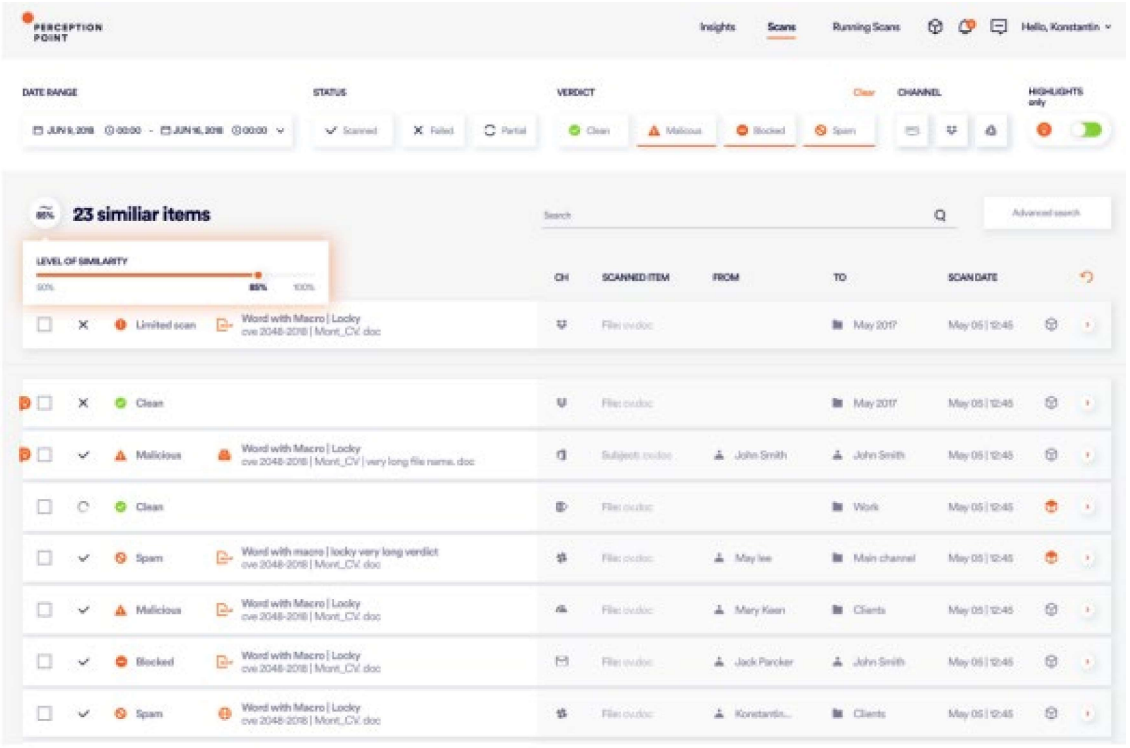
2.3. El visor de rayos X y la herramienta de operaciones SOC

El *dashboard* personalizado ayuda a los expertos en seguridad y TI a ver y comprender cada incidente de la manera más detallada. El X-Ray incluye las siguientes capacidades principales:

- Insights: permite ver el software más en detalle, las URL y las clasificaciones de archivos, los usuarios más atacados, y más. Así se comprenden las rutas de ataque completas, y por qué el contenido se marca como malicioso o limpio.
- Realización de análisis forense: determinamos el alcance y la escala de un intento de ataque. Identificamos las amenazas actuales y priorizamos los esfuerzos de respuesta.
- Analyzer: permite a los usuarios cargar cualquier pieza de contenido sospechoso, desde cualquier software, y obtener un análisis inmediato. Literalmente arrastrar y soltar.
- Administración de políticas y reglas: widgets simples y fáciles de usar para implementar, administrar y actualizar nuevas políticas y reglas, todo en un solo lugar.
- Remediación: permite a los administradores del cliente modificar también cualquier veredicto de análisis y eliminar correos electrónicos de la bandeja de entrada del usuario si es necesario.



The analyzer



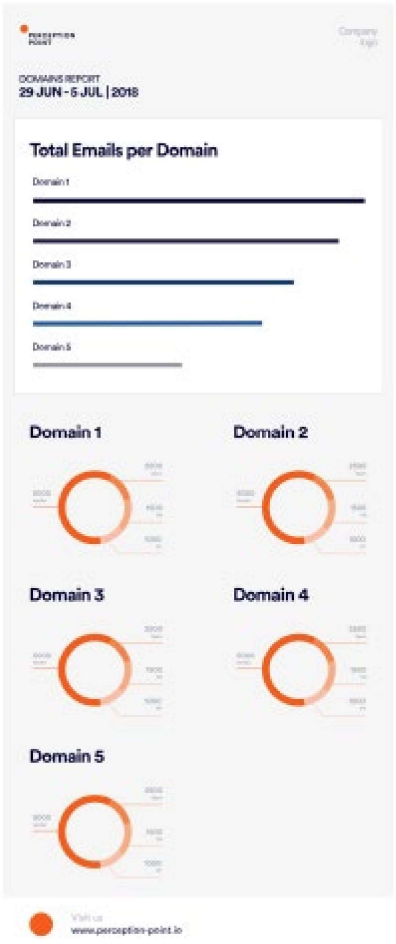
The X-Ray Scans Interface

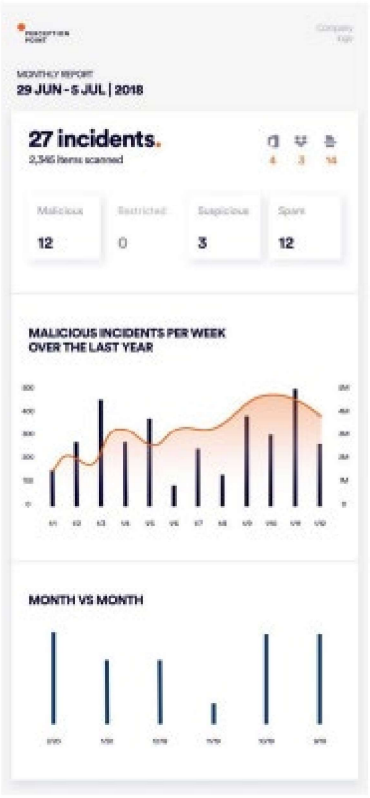
2.4. Reportando a la Gerencia:

Una interfaz única permite a cualquier tipo de usuario (CISO, administrador de TI, administrador de correo electrónico, analista de seguridad) controlar el nivel de profundidad de la interacción con el sistema de Perception Point. Las sólidas capacidades de filtrado y búsqueda permiten exportar cualquier dato solicitado, lo que le permite analizarlo en su aplicación preferida.

Perception Point ofrece varios tipos de informes:

1. Informes de IR: informes de incidentes ad-hoc sobre incidentes únicos, resúmenes diarios para clientes VIP e informes semanales/mensuales sobre tendencias de ataques.
2. Informes de conserjería a pedido: exportar cualquier conjunto de datos de los cientos de puntos de datos recopilados automáticamente por el sistema a su discreción.
3. Informes de conserjería programados: informes semanales, mensuales y trimestrales, que incluyen resúmenes agregados de todas las actividades y tendencias basadas en datos de la vida real.





2.5. Implementación automática y actualizaciones:

La plataforma nativa de la nube garantiza la máxima disponibilidad y eficiencia. En consecuencia, la solución de Perception Point incluye:

- Actualizaciones de detección en curso.
- Acceso directo a expertos cibernéticos.
- Publicaciones de investigación.

- Experiencia de usuario mejorada.

2.6. Soporte 24/7:

El equipo técnico de éxito del cliente de Perception Point es responsable de la operación del servicio, las solicitudes de funciones y la comunicación continua con respecto a las hojas de ruta y los nuevos desarrollos.

3. Cumplimiento de seguridad y estándares de gobierno

Como empresa de ciberseguridad, Perception Point considera que el cumplimiento y la privacidad son pilares fundamentales, lo que garantiza que sus clientes corran un riesgo mínimo. En consecuencia, la empresa cumple con SOC-2 y HIPAA y toma todas las medidas necesarias para garantizar la confidencialidad, integridad o disponibilidad del servicio de correo electrónico de sus clientes. Esto también incluye el cifrado y la protección de los datos. El proceso SOC-2 de la empresa está completamente auditado por una firma de contabilidad y cumplimiento Big-4.

Además, Perception Point cumple con todos los estándares del RGPD y todas las leyes aplicables en materia de protección de datos personales.

4. Funcionalidades clave, por amenazas

4.1. Adjuntos/ataques basados en archivos

Perception Point sobresale en la prevención de cualquier tipo de ataque basado en archivos. El equipo de investigación de Perception Point divide esta amenaza en dos vectores:

- Malware cotidiano: malware básico en curso que generalmente se conoce o no es parte de un ataque APT
- Malware avanzado: ataques basados en archivos que utilizan técnicas avanzadas y el uso de técnicas de explotación.

Para prevenir estos ataques, Perception Point utiliza motores estáticos y dinámicos:

- Recursive Unpacker (la capa anti-evasión): como se describió anteriormente, extrae todos los archivos transferidos, descubriendo y frustrando así las técnicas de evasión. Esto incluye archivos dentro de archivos, enlaces a archivos, archivos

comprimidos, archivos protegidos con contraseña y más. Esta es la primera capa en el proceso, asegurando que todos los archivos estén siendo escaneados.

- Inteligencia de amenazas: las mejores fuentes de inteligencia de su clase junto con motores desarrollados internamente escanean todo el contenido para identificar cualquier malware "conocido".
- Motores antivirus: combina los mejores motores antivirus basados en firmas de su clase para identificar ataques maliciosos con los motores de análisis de firmas de Perception Point para malware altamente complejo.
- HAP: la IP central de Perception Point es HAP (plataforma asistida por hardware) y diferencia a la empresa de todas las demás. El HAP de Perception Point ejecuta archivos de forma dinámica dentro de una máquina virtual. Mientras se procesa el archivo, nuestro sistema le indica a la CPU que encienda Intel PT y comienza a rastrear la aplicación para crear un "rastreo" completo que representa todo el flujo de ejecución del artefacto potencialmente malicioso. Este rastreo rápido, junto con los cambios en la memoria virtual durante la ejecución, son digeridos por los múltiples algoritmos HAP de Perception Point, que pueden detectar de forma determinista cualquier intento de ejecutar código malicioso en solo unos segundos (consulte la explicación técnica abajo).

Puntos fuertes en la detección de malware

Perception Point tiene la oferta más exclusiva en la prevención de malware de cualquier tipo, como ransomware, criptoware, troyanos y más. La plataforma de múltiples capas ofrece muchas ventajas distintas en comparación con otras soluciones, que incluyen:

- Tasas de detección: Perception Point ha desarrollado docenas de algoritmos integrados en varias capas antimalware para garantizar las mejores tasas de detección del mercado. Esto incluye la capa antievasión, AV, inteligencia de amenazas y el motor dinámico de próxima generación, el HAP, que juntos detectan con éxito más intentos de ataques.
- Falsos positivos: el HAP es un motor determinista que le permite evitar los falsos positivos que probablemente ocurran con el sandboxing regular. Además, el equipo de Respuesta a Incidentes se asegura de que la plataforma mejore constantemente y esté perfectamente ajustada a las necesidades específicas del cliente.
- Velocidad: las plataformas de Perception Point analizan todos y cada uno de los contenidos de forma estática y dinámica en 30 segundos, y una media de 10 segundos para todos los archivos limpios. Esta velocidad no tiene precedentes en comparación con otros motores que escanean contenido en minutos: comienzan en 5 minutos y pueden tardar hasta 20 minutos por archivo.
- Escala: la solución se implementa completamente en la nube y, junto con su velocidad, permite que Perception Point escanee el 100 % de los archivos adjuntos de forma dinámica. No se aplican conjeturas ni estadísticas. Perception Point lo escanea todo para garantizar la máxima detección.

Feature	PERCEPTION POINT	Sandboxing
Threat coverage		
Level of analysis	CPU	Application
Speed	<30 **seconds**	5-20 **minutes**
Accuracy	Deterministic	Statistic (behavioral)
File functionality post-scan		
URL Scanning		
APT module capacity		
Detection of zero-days & obfuscated N-days		
Coverage of next-gen exploitation techniques (e.g. COOP)		

Tecnologías antivirus y de análisis estático

Las tecnologías de análisis estático de Perception Point incluyen lo siguiente:

- Inteligencia sobre amenazas: detecta e identifica el malware básico actual y generalizado, las URL maliciosas y las campañas de ataque. Perception Point administra una base de datos de inteligencia de amenazas que recopila múltiples listas de direcciones URL maliciosas y hashes de archivos de terceros, además de una base de datos interna que recopila información de clientes protegidos, prospectos y de la naturaleza. La base de datos se actualiza cada minuto, agregando millones de URLs y archivos diariamente. Además, nuestro equipo de Respuesta a incidentes incluye manualmente las URL y los archivos en la lista negra de forma regular, después de un análisis exhaustivo.
- AV: detecta la ejecución de código malicioso en archivos mediante firmas conocidas y otros métodos de análisis estático. La capa combina los mejores motores antivirus basados en firmas de su clase (por ejemplo, ESET y Avira) para identificar ataques maliciosos con una herramienta interna, el "Disector", que identifica firmas altamente complejas. Los AV de Perception Point están proporcionando mejores resultados debido a:
    - Mejores capacidades de desembalaje.
    - Admite formatos de archivo esotéricos.
    - El sistema de configuración avanzada ajusta automáticamente la sensibilidad de todos los motores.
- Anti evasión: descubre ataques que utilizan técnicas de evasión, incluida la incrustación de contenido malicioso en archivos y direcciones URL. Los motores anti-evasión patentados y los algoritmos de soporte descomprimen y descubren URLs y archivos maliciosos ocultos dentro de otros objetos.

El motor busca recursivamente archivos y URLs, los extrae y los escanea por separado en varios motores. Los ejemplos seleccionados incluyen el seguimiento de URLs dentro de archivos, la extracción de documentos y objetos incrustados dentro de documentos (por ejemplo, Word dentro de Excel), la extracción de archivos entregados a través de plataformas de almacenamiento en la nube, incluida la búsqueda de carpetas, la apertura de archivos comprimidos en casi cualquier formato, la extracción de archivos .msg y .eml, y más.

En total, Perception Point utiliza docenas de algoritmos para el análisis estático, 6 fuentes diferentes de inteligencia de amenazas y 4 antivirus, todo en una plataforma.

4.1.1. Sandbox/tecnología de escaneo dinámico de Perception Point

Perception Point revolucionó el escaneo dinámico e inventó una tecnología única (patentado), que redefine el concepto de sandboxing. El motor dinámico, llamado HAP™ (abreviatura de Plataforma asistida por hardware) aprovecha Intel Processor Trace (Intel PT) para escanear cada pieza de contenido para identificar la intención maliciosa, en el nivel de explotación (y no en el nivel de malware como los sandboxes utilizados por otros vendedores).

Profundice sobre el HAP:

Cualquier ataque avanzado siempre comienza en el nivel de la CPU, por lo que el acceso a los datos del nivel de la CPU es fundamental. Mediante el uso de Intel Processor Trace (PT), Perception Point obtiene acceso a los datos relevantes, lo que le permite evitar ataques en su origen.

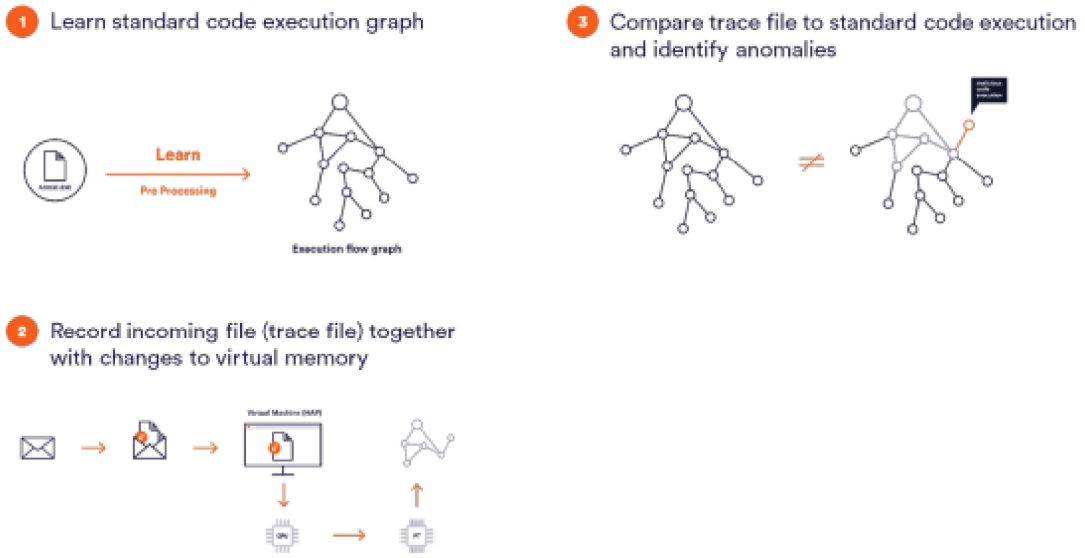
Intel PT (una función que ha estado disponible desde Skylake) se diseñó originalmente para monitorear el rendimiento y la depuración. Puede rastrear las aplicaciones y proporcionar acceso a todo el flujo de ejecución de estas aplicaciones. Perception Point aprovecha estos datos con fines de ciberseguridad: dado que se genera directamente desde la fuente, la información derivada de Intel PT revela cualquier intento de utilizar la ejecución de código de forma malintencionada.

HAP™ de Perception Point ejecuta dinámica y rápidamente archivos y direcciones URL dentro de una máquina virtual. Mientras se procesa el archivo/URL, nuestro sistema le indica a la CPU que encienda Intel PT y comienza a rastrear la aplicación para crear un "rastreo" completo que representa todo el flujo de ejecución del artefacto potencialmente malicioso. Este rastro, junto con los cambios en la memoria virtual durante la ejecución, son digeridos por los diferentes algoritmos HAP de Perception Point, que pueden detectar de manera determinista cualquier intento de ejecutar código malicioso.

Como se describió anteriormente, el HAP se compone de 3 algoritmos principales, todos designados para brindar protección completa contra cualquier explotación de día cero (es decir, sin conocimiento previo y el ataque), ataques de día N y cualquier tipo de intento de ejecución maliciosa. código, incluido JavaScript dentro de archivos PDF o un VBScript dentro de un documento de Word. Los algoritmos son:

- CFG: detecta vulnerabilidades de corrupción de memoria. Perception Point desarrolló gráficos de flujo de control para cada aplicación que identifican las desviaciones del flujo de ejecución durante el tiempo de ejecución
- FFG: detecta técnicas de explotación avanzadas, como explotaciones escritas para eludir algoritmos CFI comunes. Los gráficos de flujo de control conscientes de la semántica patentados desarrollados para cada aplicación identifican las desviaciones del flujo de ejecución durante el tiempo de ejecución.
- Dropper: detecta errores lógicos en aplicaciones y scripts maliciosos (p. ej., macros) en documentos de Office. El motor heurístico único escanea el flujo de ejecución en busca de rutas de código prohibidas.

Una explicación gráfica del proceso HAP se puede encontrar en la siguiente página:



Actualmente, Perception Point escanea dinámicamente los siguientes tipos de archivo:

7z	com	dot	html_firefox	lzop	msg	pdf	prg	sct	uue	xfdf	Z
ace	compress	dothtml	html_ie	mad	msh	pdfx	printerexport	shar	vb	xhtml	zip
ade	cpio	dotm	html_ie_latest	maf	msh1	pdx	ps	shb	vbe	xla	zoo
adf	cpl	dotx	inf	mag	msh1xml	pif	ps1	shn	vbp	xlam	zpaq
adp	CramFS	dqy	ins	mam	msh2	pl	ps1xml	shs	vbs	xlb	
alzip	crt	eml	iqy	maq	msh2xml	plg	ps2	sldm	vhd	xlk	
ape	csh	exe	iso	mar	mshxml	pot	ps2xml	sldx	vsmacros	xll	
app	csv	fdf	isp	mars	msi	pothtml	psc1	slk	vsw	xlm	
ar	daa	flac	its	mas	msp	potm	psc2	SquashFS	vxd	xls	
arc	deb	fxp	jar	mat	msrcincident	potx	psd1	sys	wbk	xlsb	
arj	der	gadget	jnlp	mau	mst	ppa	psdm1	tar	webpnp	xlshtml	
asp	diagcab	grp	js	mav	msu	ppam	pst	tar.gz	website	xlsm	
bas	dll	gz	jse	maw	nsh	pps	pwz	tbz2	wiz	xlsx	
bat	dmg	gzip	kfp	mcf	odc	ppsm	r07	tgz	ws	xlt	
bzip2	DMG	hlp	ksh	mda	odf	ppsx	rar	theme	wsc	xltam	
cab	dms	hpj	lib	mdb	odp	ppt	reg	thmx	wsf	xlthtml	
cer	doc	hta	lnk	mde	ods	ppthtml	rpm	tmp	wsh	xltm	
chm	dochtml	htm	lrzip	mdt	odt	pptm	rtf	tnef	XAR	xltx	
chm	docm	html	lzh	mdw	ops	pptx	rzip	tnef	xbap	xlw	
cmd	docx	html_chrome	lzip	mdz	osd	pptxml	scf	url	xdp	xnk	
cnt	docxml	html_edge	lzma	msc	pcd	prf	scr	urlspack	xfd	xz	

Sistemas operativos:

- Windows: Perception Point brinda protección completa para el entorno de Windows y protege todas las aplicaciones relacionadas con Windows.
- macOS: Perception Point es la única empresa en el mercado que ofrece una solución dinámica para la prevención de ataques dirigidos a computadoras Apple que aprovechan las técnicas de explotación.

Velocidad de la tecnología Sandbox:

El escaneo dinámico de Perception Point a través del HAP ("el asesino de la caja de arena", como a veces se lo denomina internamente) es ultrarrápido, lo que permite un escaneo completo de todo el tráfico en 30 segundos y un promedio de solo 10 segundos. Esta es una gran diferencia en comparación con las soluciones basadas en sandbox y proporciona el siguiente valor agregado:

Modo de implementación: con la velocidad y la escala de Perception Point, el cliente puede desplegar la solución en modo prevención y no en modo de detección (!). Hoy en día, si una organización está buscando escanear su contenido dinámicamente, por ejemplo, usando un sandbox o navegando activamente en un sitio web, tendrá que comprometerse con uno de los siguientes: escanear solo una parte del contenido (por ejemplo, usar estadísticas para adivinar qué escanear y qué no) o permitir la entrada de contenido y escanearlo en paralelo/después de la entrega ("modo de detección"). Esto es especialmente cierto para las grandes organizaciones donde los volúmenes de datos son extremadamente altos. Perception Point resuelve este problema. Aprovechando su tecnología única y su infraestructura en la nube, Perception Point escanea todo el tráfico con un retraso mínimo.

- Experiencia del usuario: además del retraso mínimo en la entrega del correo electrónico, Perception Point no manipula el archivo, es decir, no lo cambia ni lo altera, manteniendo su usabilidad máxima.
- Escala: Perception Point escanea el 100 % del tráfico de forma dinámica, lo que mejora la detección y las tasas de falsos positivos.

4.2. Ataques provenientes de enlaces

La solución de Perception Point combina una innumerable cantidad de algoritmos en cuatro capas para evitar ataques basados en URL:

- Recursive Unpacker: este exclusivo motor anti evasión es responsable de descubrir los ataques basados en URL más ocultos. Explora recursivamente las URL, las extrae y las escanea por separado con nuestros diversos motores. Los casos de uso seleccionados incluyen el seguimiento de URL dentro de URL y archivos, la extracción de archivos entregados a través de plataformas de almacenamiento en la nube, incluida la búsqueda en carpetas, la extracción de enlaces en invitaciones de calendario, la extracción de enlaces dentro de imágenes y códigos QR, y más.
- Anti-phishing: algoritmos que pueden detectar y prevenir intentos de phishing basados en el reconocimiento de imágenes. Esto incluye el análisis de páginas de inicio de sesión falsas y la detección del uso de marcas falsas. Perception Point también tiene un algoritmo OCR que analiza el texto malicioso y las URL dentro de las imágenes (consulte los detalles a continuación).
- Reputación de URL: incorpora motores de reputación de URL de datos que supervisan el tráfico global en busca de ataques. La tecnología de Perception Point también analiza el vector de reputación de varios parámetros del remitente y el destinatario.
- Inteligencia de amenazas: detecta e identifica campañas de ataques y URL maliciosas muy difundidas. La base de datos de inteligencia de amenazas recopila

múltiples listas de direcciones URL maliciosas de terceros, además de nuestra base de datos interna que recopila información de clientes protegidos, de prospectos... La base de datos se actualiza cada minuto, agregando millones de URL únicas diariamente.

Es importante tener en cuenta que al usar la función Seguir URL, todas las URL se extraen y se siguen/escanean desde varios lugares, como el asunto, el cuerpo, dentro de los archivos, los códigos de control de calidad y las imágenes. Además, las capacidades de reescritura de URL están disponibles.

Manejo de enlaces anidados/incrustados

Todos los enlaces incrustados son descubiertos por Recursive Unpacker. Este motor sigue las URL anidadas y extrae cada URL que se encuentra en el correo electrónico o el archivo. Estas URL (o cualquier otro artefacto) son escaneadas por nuestros motores estáticos y dinámicos. La URL relevante se representa completamente en varios navegadores para que el sistema ejecute sus algoritmos anti-phishing y busque vulnerabilidades.

Los escenarios adicionales de ataques relacionados con URL cubiertos por nuestra plataforma incluyen:

- La propia URL tal como se presenta en el correo electrónico.
- El texto que aparece en el correo electrónico que describe la URL.
- Cualquier redirección desde la URL original a la URL de destino final.
- El título de la página web del destino final de la URL.
- El contenido de la página web final (con una opción para bloquear elementos HTML específicos).
- La captura de pantalla de la página web final.

Opciones de escaneo de URLs

Perception Point ofrece dos opciones para el análisis de URL.

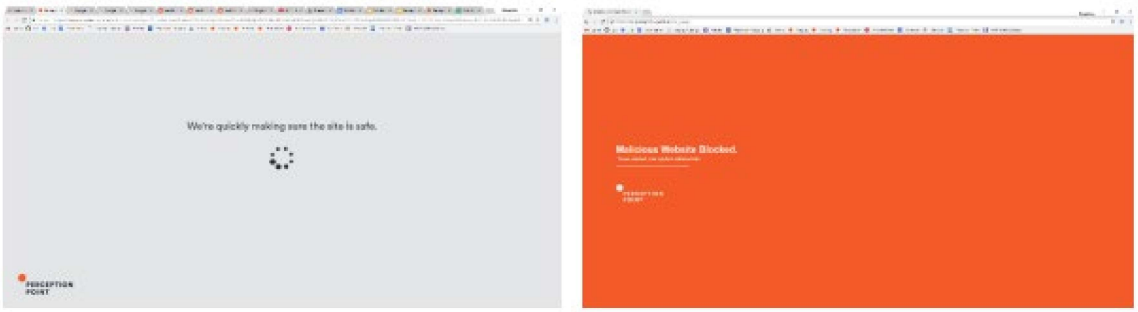
1. *Reescritura de URL:*

Esta capacidad permite que Perception Point reciba una alerta cuando el usuario hace clic en cualquier enlace dentro del correo electrónico. El cliente puede decidir si prefiere implementar esta capacidad con dos opciones ofrecidas:

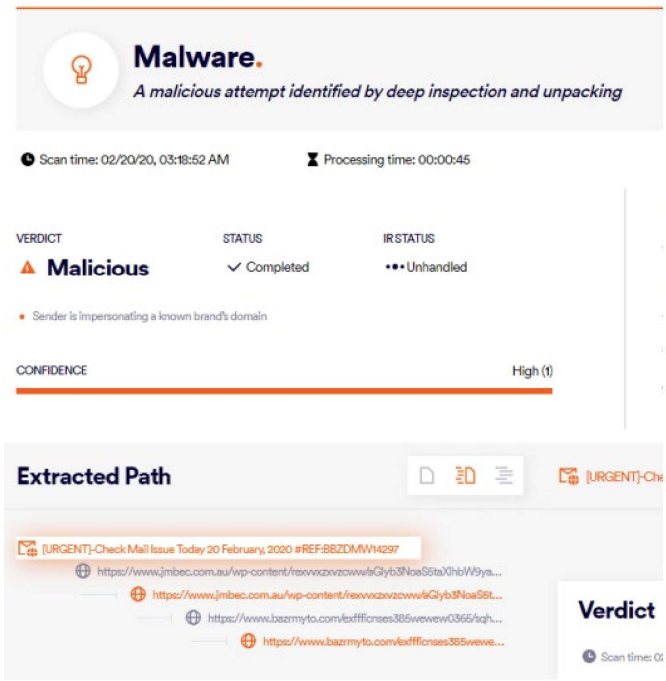
- Modo sin bloqueo: el escaneo se realiza casi en tiempo real una vez que el usuario hace clic en él, pero el usuario aún puede acceder a la página web.
- Modo de bloqueo: después de hacer clic, la plataforma "retiene" al usuario durante unos segundos antes de redirigirlo a la URL original. Durante ese tiempo, Perception Point ejecuta los motores de análisis profundo y los algoritmos de reconocimiento de imágenes en la página original para proporcionar un veredicto claro sobre la URL en la que se hizo clic.

2. *Siga la URL:*

Búsqueda de vulnerabilidades. A continuación, se muestra un ejemplo visto desde X-Ray donde se puede entender cómo el sistema siguió todas las URL (consulte la sección "Ruta extraída").



Los objetos naranjas son las cargas útiles maliciosas:



Es importante tener en cuenta que la gran mayoría de los clientes de Perception Point prefieren utilizar la opción Seguir URL, ya que impide que el correo electrónico llegue al usuario final en primer lugar.

Detección y reparación de phishing enviado por correo

Perception Point ha combinado varias capas de prevención anti-phishing, incluidos motores patentados desarrollados específicamente para burlar cualquier intento de phishing avanzado y mantenerse al día con las técnicas más recientes:

- Reconocimiento de imágenes: un motor patentado que identifica la suplantación de identidad de marca y los ataques de phishing al aprovechar la visión artificial con capacidades de IA. El motor validó que todas las URL son realmente legítimas. El motor es completamente dinámico e identifica intentos de suplantar activos de ambas marcas conocidas (por ejemplo, Microsoft, WeTransfer) y de los activos de los clientes.
- Gráfico de la cadena de suministro: uso de capacidades de IA/ML para monitorear constantemente y proporcionar comentarios sobre la reputación y la puntuación de riesgo de cualquier metadato de correo electrónico, incluidos dominios, URL, IP y más.
- Análisis léxico de URL: análisis de la estructura de URL y búsqueda de similitudes con URL maliciosas mediante IA/ML.
- Reputación de URL: además de aprovechar los recursos de terceros, el motor también analiza múltiples parámetros de cada contenido entregado, centrándose en los activos del remitente y el destinatario, para identificar el intento de phishing del empleado.
- Escaneo avanzado de páginas: utiliza ML para identificar la suplantación de identidad y el robo de contraseñas en sitios que se sabe que roban credenciales (por ejemplo, Google Form, incluida cualquier evasión en esta plataforma).
- Escaneo de URL o archivos html para la identificación de kits de phishing.
- Algoritmos de similitud: búsqueda y comparación de indicadores de phishing para ataques similares usando AI/ML

Todos los correos electrónicos y URL considerados maliciosos con ataques de phishing se ponen en cuarentena y no se entregan al usuario. Perception Point también funciona en modo de prevención para este tipo de ataques. A discreción del cliente, también se envía una alerta al equipo SOC.

4.3. Ataques basados en ingeniería social (BEC y ATO)

Perception Point ha desarrollado algoritmos únicos con el objetivo específico de prevenir cualquier tipo de técnica de suplantación de identidad, incluido el fraude de CEO, el fraude de abogados, las facturas falsas y más. La tecnología anti-BEC inspecciona todos los datos y metadatos relevantes para identificar cualquier desviación de las operaciones estándar y detectar cualquier intento de ingeniería social, cubriendo la suplantación de identidad, dominio similar y engaño de nombre para mostrar.

Entre los diversos algoritmos en esta capa se encuentran:

- Comprobaciones de SPF y DKIM.
- Comprobación SPF interna patentada que identifica la IP de origen (incluso en los casos en que Perception Point no está en el MX).
- Suplantación de nombres para mostrar: identificación de direcciones de correo electrónico privadas y creación de listas VIP para detectar la suplantación de nombres para mostrar.

- Suplantación de identidad de dominio (la “Suplantación de identidad perfecta”): una reputación de IP patentada combinada con información SPF/DKIM.
- Ataques de apariencia de dominio: prevención de intentos de usar un nombre de marca mediante cambios menores en el dominio.
- Una amplia base de datos de marcas para detectar la suplantación de identidad de marcas conocidas.
- Análisis de texto, incluidas expresiones regulares y aprendizaje automático para identificar texto sospechoso.
- Puntuación de remitentes, dominios y otros vectores para identificar remitentes sospechosos.
- Análisis de lenguaje para detectar correos electrónicos fraudulentos comunes, sextorsión, estafas de bitcoin, etc.

Puntos fuertes de Perception Point en el dominio de la ingeniería social

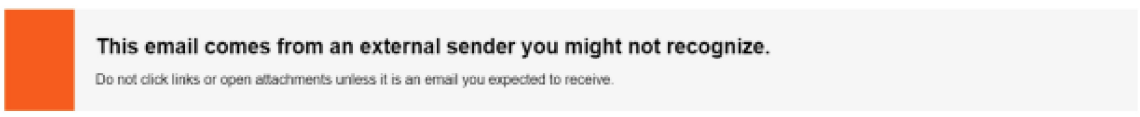
Perception Point tiene múltiples fortalezas en el dominio BEC:

- Prevención completa de amenazas de todos los ataques basados en suplantación de identidad en una única plataforma holística, que proporciona la mejor detección del mercado contra estas amenazas.
- Capacidad para aplicar rápidamente múltiples métodos de detección y utilizar varios mecanismos de detección en paralelo.
- Capacidad para identificar intentos de BEC únicos de forma personalizada que están dirigidos específicamente a clientes protegidos.
- Servicios completos de IR que aprenden y se adaptan en función de las necesidades del cliente. El equipo de IR se compromete a ajustar y mejorar todos los mecanismos de detección de forma continua.
- Las implementaciones y actualizaciones automáticas de la solución en función de los ataques interceptados en el sistema garantizan que el nivel de detección se mantenga en lo más alto todo el tiempo.
- Capacidad para descubrir cualquier intento de evasión, incluido el desempaquetado de ataques ocultos, la solución incluye una capacidad de desempaquetado recursivo.

Banners condicionales

Perception Point ha diseñado varios mensajes y pancartas para notificar a los usuarios sobre diferentes signos en el correo electrónico. Nuestros banners más utilizados son para correos electrónicos externos que se reciben de un nuevo remitente, correos electrónicos que indicaron SPF fallido y banners relacionados con la suplantación de nombre.

Ejemplo de tal banner se puede encontrar a continuación:



5. Nuestros servicios de IR: detalles y beneficios

Como se describió anteriormente, Perception Point proporciona servicios profesionales de respuesta a incidentes como parte integral de la solución. El equipo revisa cada escaneo que la solución marca como malicioso, verifica la precisión del veredicto y ajusta constantemente el sistema para minimizar los falsos positivos y maximizar la protección. Si el equipo encuentra falsos positivos, enviará estos correos electrónicos a los usuarios finales y eliminará esta carga del equipo SOC de la organización, proporcionándole una experiencia superior al usuario final.

Además, el equipo identifica constantemente nuevas tendencias de ataque y mejora la protección de Perception Point para bloquear estos ataques. En los casos inusuales en que un correo electrónico malicioso pase por los motores, el equipo de IR tiene la capacidad de crear una protección dinámica en segundos y bloquear futuros ataques.

Con el tiempo, el equipo de IR crea automatización para ataques que se bloquean con alta confianza y se enfoca solo en correos electrónicos con mayores posibilidades de un falso positivo para que puedan ser entregados al usuario final lo antes posible.

Corrección de correo malicioso/sospechoso de los buzones de correo de los usuarios

El objetivo de Perception Point es proporcionar la solución de prevención más eficaz del mercado, lo que significa la mejor tasa de detección y la tasa de falsos positivos más baja. Sin embargo, ninguna solución puede garantizar una protección del 100 %. En consecuencia, la solución tiene la capacidad de identificar y remediar correos electrónicos maliciosos (o sospechosos) después de la entrega. Como se describió anteriormente, el informe de dicho evento puede provenir del usuario final, los administradores de los clientes o los servicios de IR de Perception Point.

Una vez notificado, el sistema de Perception Point comprueba el informe y el evento. En caso de que el evento haya sido realmente un ataque malicioso, se puede extraer y eliminar de la bandeja de entrada del usuario final con un solo clic desde el panel de control de Perception Point, el X-Ray.

Gestión de Políticas y Reglas

La plataforma de Perception Point está diseñada con un mecanismo de “Decisiones” que permite crear una “Decisión” (política) sobre cualquier evidencia que recopile el sistema. Esta capacidad robusta permite la máxima flexibilidad y abre la oportunidad de actuar libremente en cualquier tipo de correo electrónico que requiera atención.

El equipo de Perception Point IR mantiene el mecanismo de Decisiones de forma continua y puede ayudar con cualquier personalización y política.

Medición de falsos/verdaderos positivos y negativos

Perception Point utiliza las siguientes medidas para probar y garantizar que su solución ofrece los mejores y más efectivos resultados de detección en el mercado de la seguridad del correo electrónico:

- Verdaderos positivos: cualquier correo electrónico malicioso que haya sido validado automática o manualmente por el servicio IR. Todo se informa en tiempo real en el tablero de Perception Point X-Ray y en informes semanales y mensuales.
- Falsos positivos: el objetivo del equipo de Perception Point IR es llegar a cero falsos positivos. Para ello, el equipo revisa todos los eventos del sistema para asegurarse de que el veredicto sea correcto. Si la plataforma falla, el analista liberará el correo al usuario final y hará las modificaciones necesarias para que no vuelva a suceder. Los falsos positivos se informan en tiempo real en el panel de rayos X.
- Falsos negativos: informados en tiempo real en el panel de rayos X. La página de información incluye una tasa de protección en tiempo real y cada vez que hay un falso negativo afectará el porcentaje de protección.

Los equipos de I+D, IR y Producto de Perception Point se miden continuamente en las tres medidas y forman parte de los KPI de la empresa.

Como se vio en la prueba de SE Labs y en los innumerables POC y pruebas, Perception Point proporciona la detección más efectiva del mercado.

Perception Point: Prevention-as-a-Service company intercepting any content-based attack across all collaboration channels including email, cloud storage, CRM apps, and messaging platforms.

Contact Us: www.perception-point.io