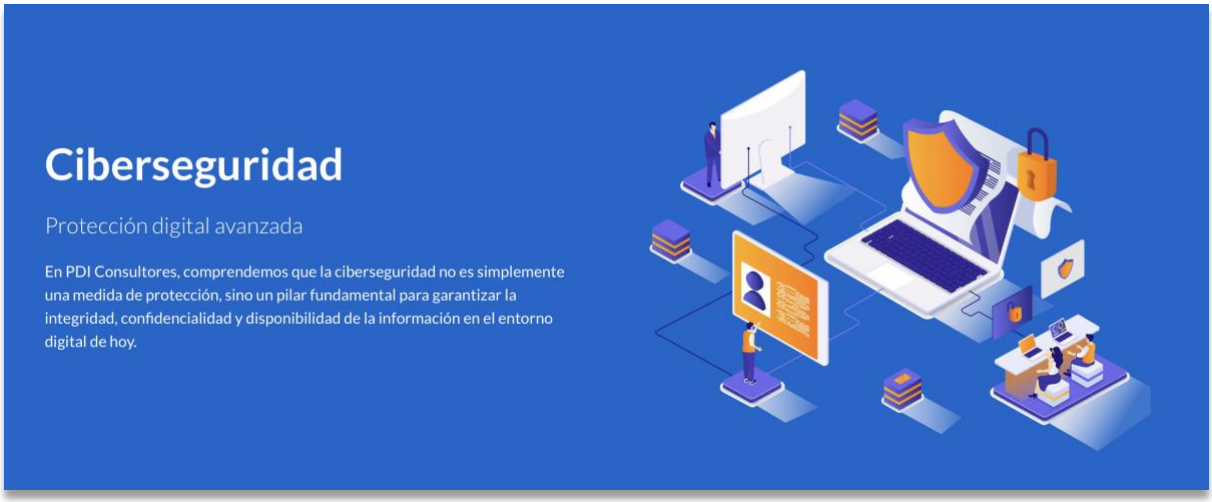
Descripción de la plataforma CORO y propuesta de servicios gestionados



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

TABLA DE CONTENIDO

Documento elaborado por, Producción Diseño e Informática, SL - CIF: B81569741
Castillo de Fuensaldaña, 4, oficina 134, 28232 - Las Rozas de Madrid, Madrid - España
Teléfono +34 913783644 - info@pdi.es - www.pdi.es

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

SERVICIO DE SEGURIDAD “All in One”

Un servicio basado en la Plataforma CORO.net que protegerá el 100% de la infraestructura, sea cual sea su tamaño.

La Ciberseguridad, como la conocemos hasta ahora, siempre ha significado comprar múltiples herramientas segmentadas de múltiples proveedores, capacitarnos en cada una y tratar con múltiples interfaces y agentes EndPoint.

- Todos los módulos se integran en un panel fácil de usar, en el que puede ver rápidamente e incluso responder a estados, eventos y registros.

- La situación del dispositivo, NGAV, EDR, VPN, firewall y control de datos están todos en un único agente de EndPoint fácil de administrar, lo que elimina los conflictos entre agentes de diferentes aplicaciones.

- Los módulos se informan entre sí a través de un motor de datos compartido, lo que elimina la necesidad de integración y mejora la posición de seguridad.

Protección de seguridad integral gracias a la IA

Construimos nuestra tecnología con la protección crítica e integral que las empresas de hoy necesitan. Contamos con un potente motor, impulsado por inteligencia artificial (IA) en su núcleo, para identificar y remediar automáticamente las amenazas y vulnerabilidades cibernéticas más conocidas. En todos los Endpoints, usuarios, datos y aplicaciones en la nube.

Un motor tan inteligente que aprende continuamente de los muchos errores involuntarios que cometen las personas mientras avanzan en su búsqueda diaria de excelencia e

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

innovación, los ataques intencionales de empleados dispuestos a hacer daño o los piratas informáticos inteligentes que encuentran en las empresas en crecimiento y en los usuarios residenciales una presa fácil.

Facilidad de uso

Coro se propuso encontrar y reparar los numerosos agujeros de seguridad que enfrentan los usuarios y empresas de hoy en día, sin que expertos en ciberseguridad tengan que preocuparse, investigar o solucionarlos ellos mismos.

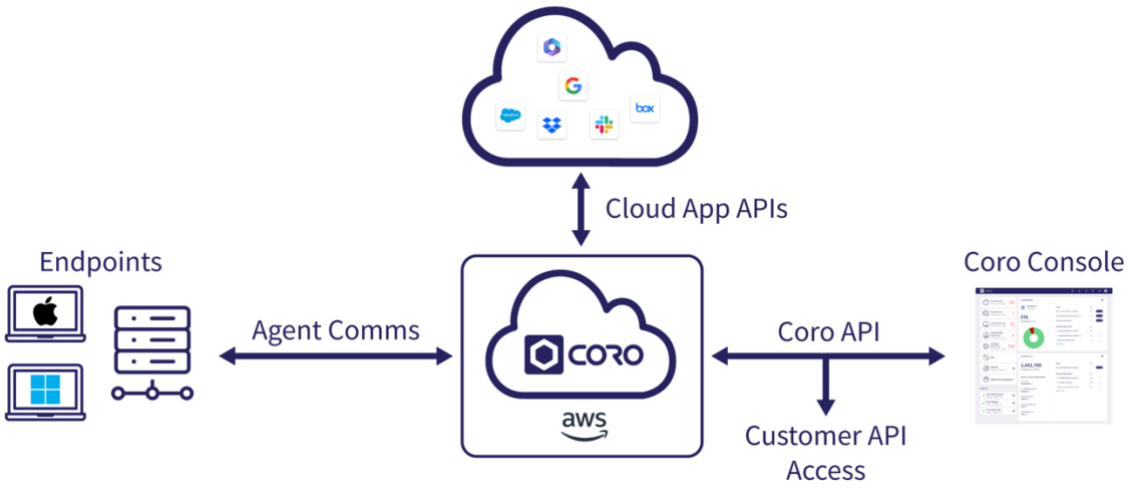
Coro automatiza la reparación y pone fin a las interminables alertas falsas, las llamadas de pánico a las 2 am o las horas perdidas rastreando archivos comprometidos, sistemas infectados o dispositivos terminales. Para aquellos problemas que aún requieren intervención humana, nos propusimos hacerlo muy fácil: la mayoría de los problemas críticos en la plataforma Coro se pueden resolver con un clic.

Coro elimina la complejidad de la seguridad.

Cómo funciona CORO

La plataforma CORO se compone de cuatro componentes.

- El servicio CORO: un SaaS basado en la nube que gestiona el procesamiento de datos en todos los módulos y gestiona la comunicación con dispositivos terminales y aplicaciones en la nube.
- CORO Console: una interfaz web que funciona como un panel de vidrio único.
- CORO Agent: un agente único que se ejecuta en MacOS y Windows y proporciona capacidades de EPP, EDR, SASE y gobierno de datos.
- La API de CORO: facilita la integración de SIEM y socios.



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

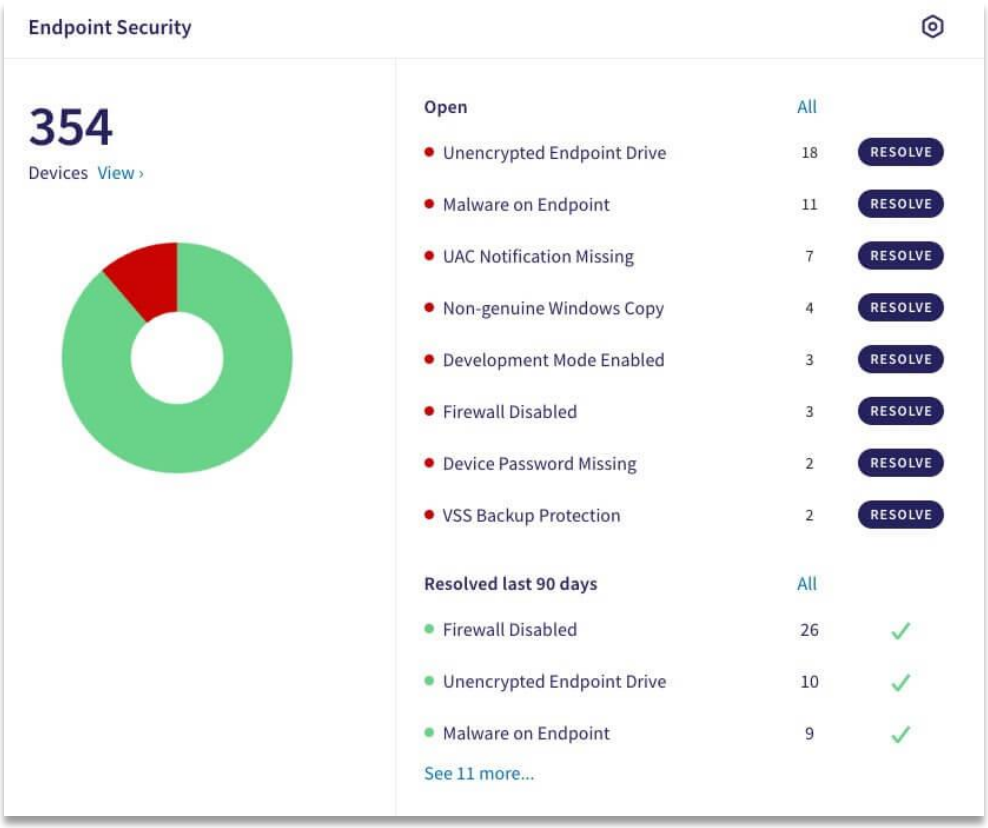
1. Módulos para proteger dispositivos (endpoints)

I. EndPoint Security

Políticas en el dispositivo
Aplique políticas de Seguridad del dispositivo a usuarios o grupos y determine la acción correctiva para las vulnerabilidades.

Antivirus de próxima generación
La protección avanzada contra amenazas (ATP) analiza tanto los archivos estáticos como los procesos en ejecución en busca de anomalías.

Listas de permitidos/bloqueados
Cree listas de archivos, carpetas y procesos para permitir o bloquear en sus Endpoint protegidos.



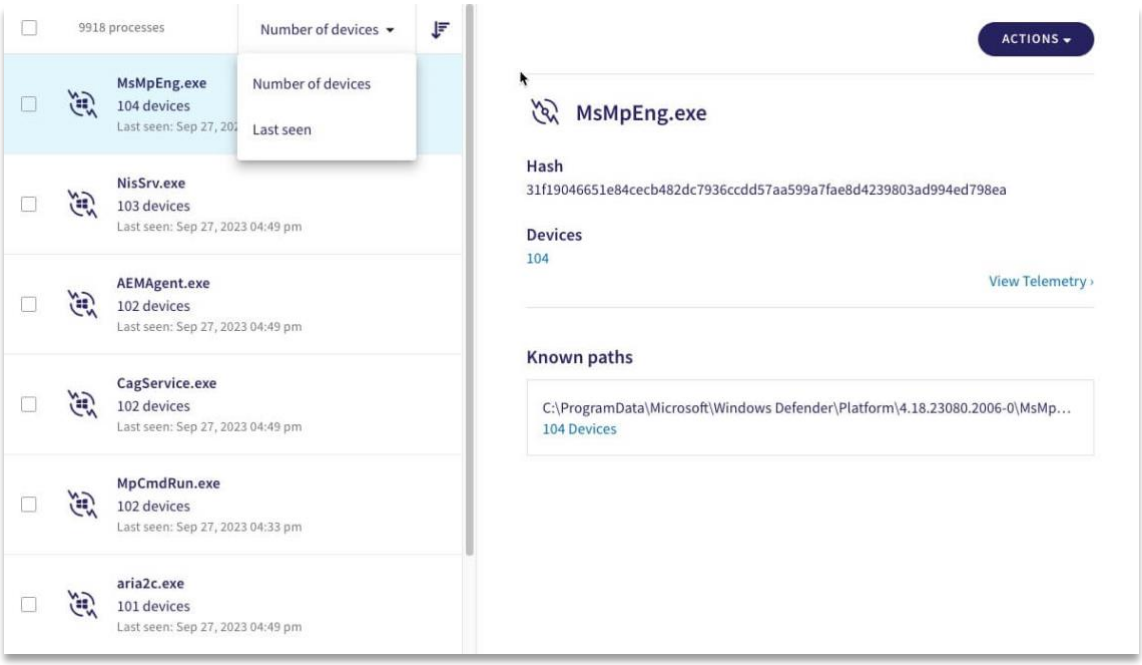
Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

II. EndPoint Detection and Response

El módulo de detección y respuesta de endpoints (EDR) amplía su capacidad para manejar incidentes a medida que ocurren, remediarlos rápidamente para evitar daños mayores provenientes de fuentes de amenazas conocidas y desconocidas y realizar análisis posteriores a las infracciones.

Supervisa continuamente los dispositivos terminales y presenta estos hallazgos en pestañas claras y fáciles de administrar desde el panel de Coro. Filtre los datos según sea necesario y reciba orientación sobre remediación y acciones de respuesta inmediata.

- Detección de software malicioso mejorada
- Aislamiento proactivo de dispositivos infectados
- Corrección automática en todos los puntos finales



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

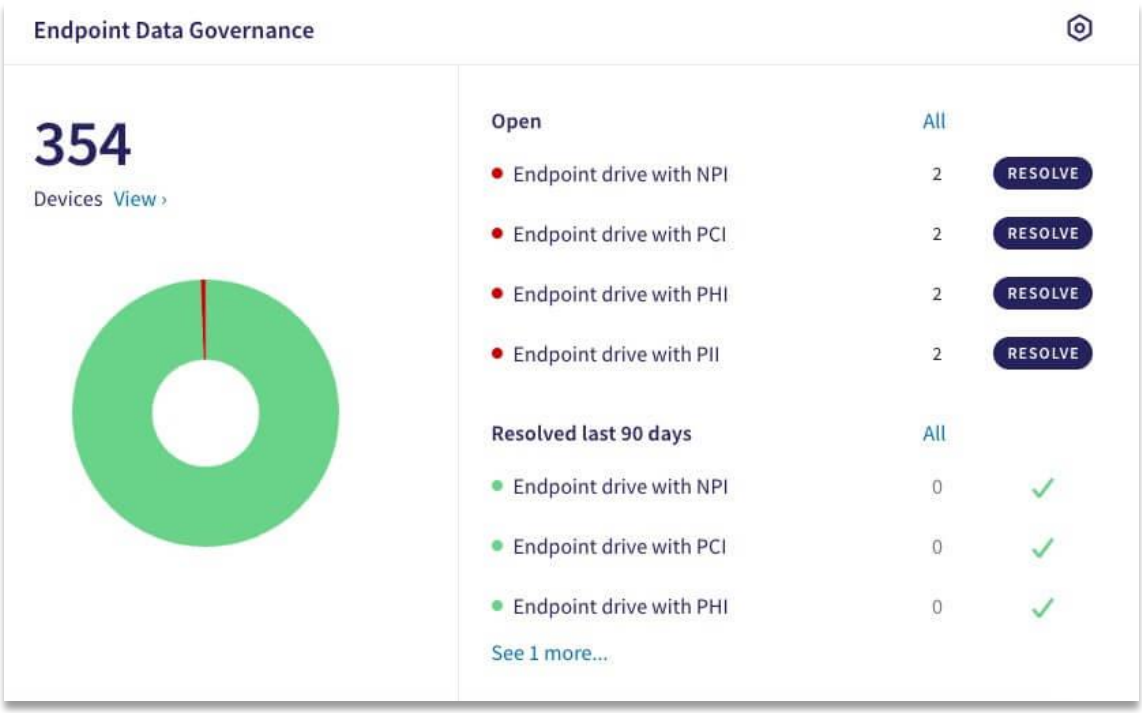
III. EndPoint Data Governance

Proteger los datos confidenciales del acceso, uso, divulgación, modificación o destrucción no autorizados.

El módulo Endpoint Data Governance protege los datos confidenciales contra el acceso, uso, divulgación, modificación o destrucción no autorizados en todos los terminales.

Para ayudar a garantizar el cumplimiento de estos estándares regulatorios, Coro le permite escanear terminales de forma remota en busca de:

- PII (información de identificación personal)
- PHI (información de salud protegida)
- PCI (información de la tarjeta de pago)
- NPI (información no pública)

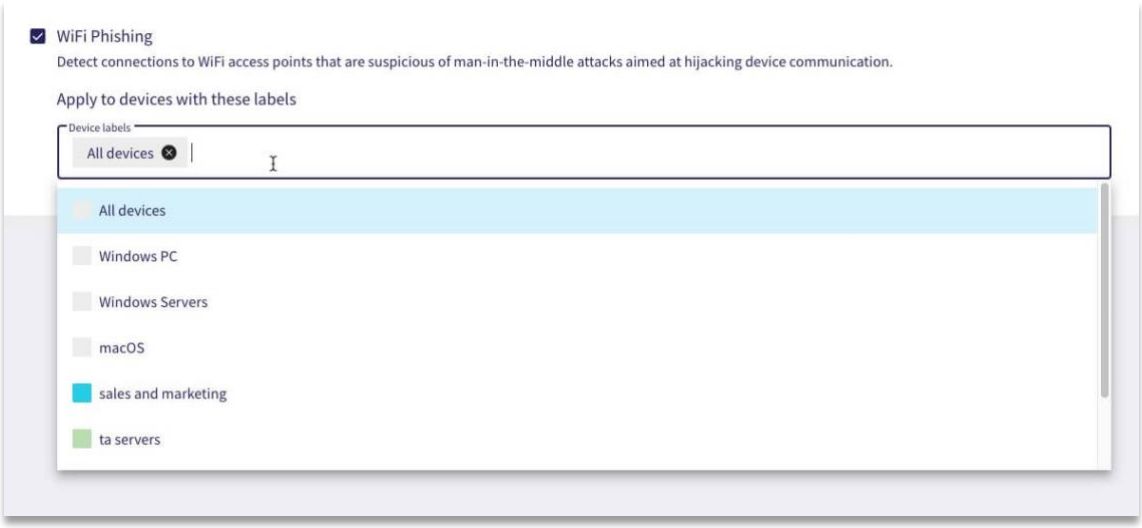


Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

IV. Wifi Phishing

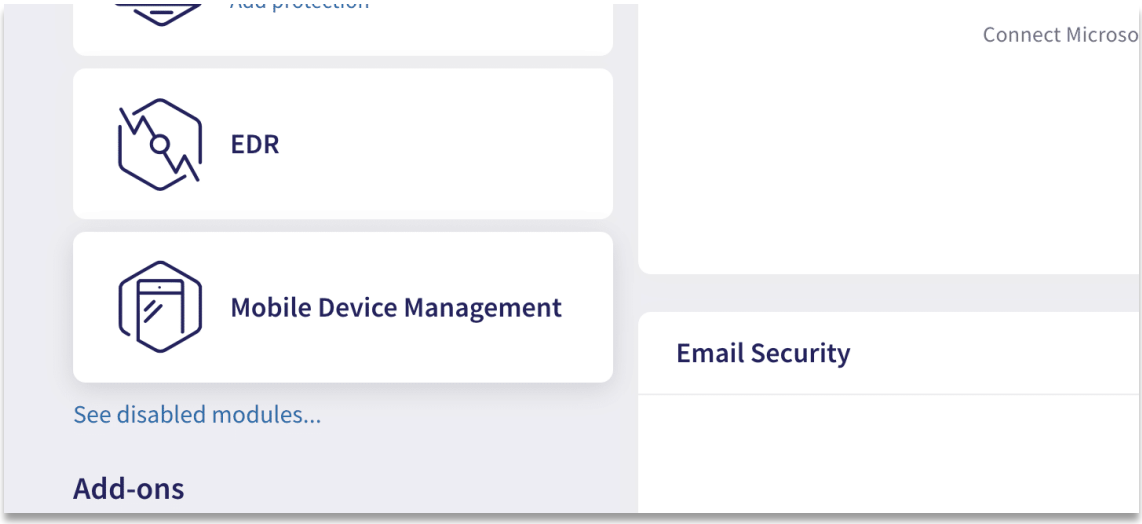
El complemento WiFi Phishing protege los EndPoints fuera de la LAN impidiendo conexiones a puntos de acceso WiFi sospechosos. Funciona detectando conexiones a puntos de acceso WiFi que son sospechosas de ataques “man in the middle” destinados a secuestrar la comunicación del dispositivo.

Los administradores pueden aplicar protección WiFi Phishing a todos los dispositivos protegidos en un espacio de trabajo, o solo a grupos específicos de dispositivos. Este complemento es una solución especialmente eficaz para empleados remotos o que viajan.



V. Mobile Device Management

La administración de dispositivos móviles (MDM) le permite administrar los dispositivos móviles iOS y Android utilizados por los usuarios finales de su organización.



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

2. Módulos para proteger correo electrónico y usuarios

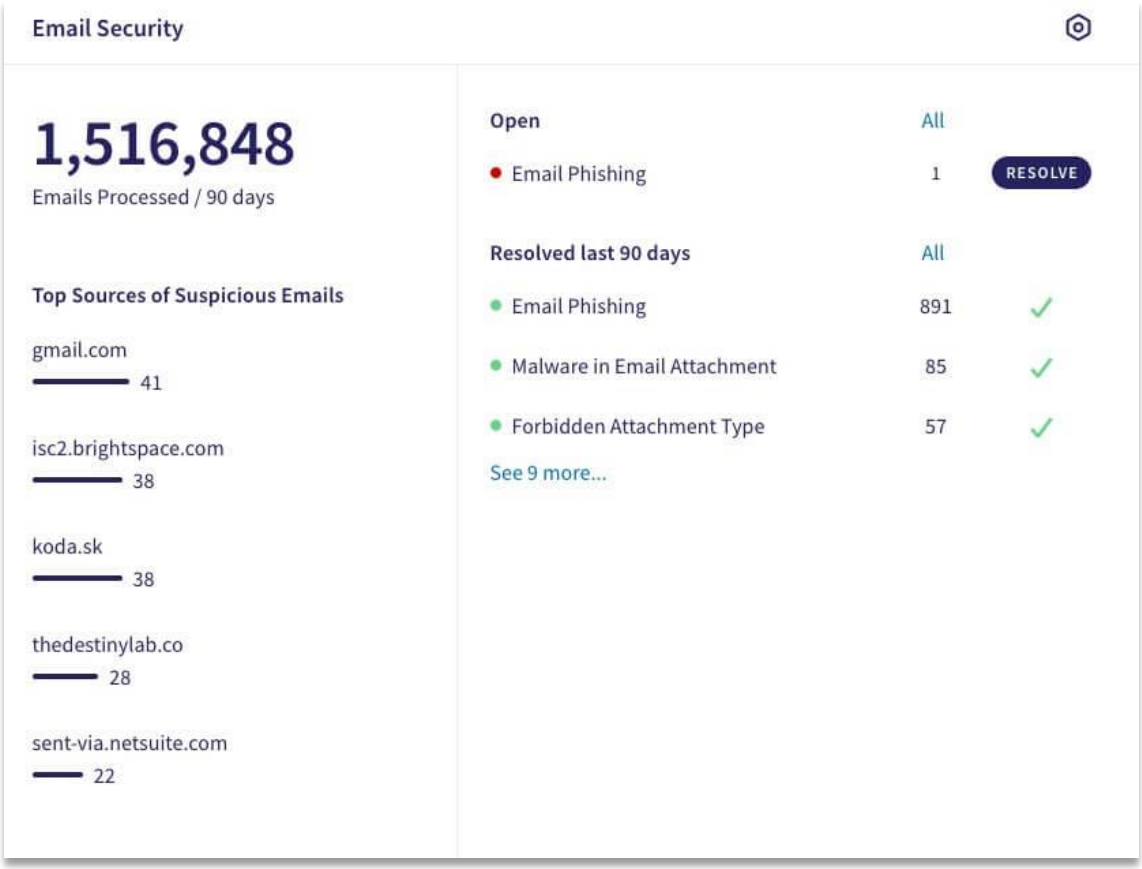
I. Email Security

Email Security es el módulo de correo electrónico principal de Coro. Incluye las siguientes capacidades:

Escaneo de malware
Identifique y ponga en cuarentena correos electrónicos con posibles archivos adjuntos de malware o ransomware.

Protección contra phishing por correo electrónico
Evite las amenazas de suplantación de dominio, suplantación de identidad y otros intentos de phishing engañosos.

Listas de permitidos/bloqueados
Cree y mantenga una lista de remitentes individuales o dominios de envío para permitir o bloquear desde las bandejas de entrada de su empresa.



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

II. User Data Governance

El módulo User Data Governance ayuda a los administradores a establecer una estrategia para el manejo correcto y seguro de los activos de datos por parte de usuarios autorizados, manteniendo al mismo tiempo el cumplimiento de estrictos estándares regulatorios.

Analiza los correos electrónicos en busca de divulgación no autorizada de datos confidenciales y comerciales, incluidos

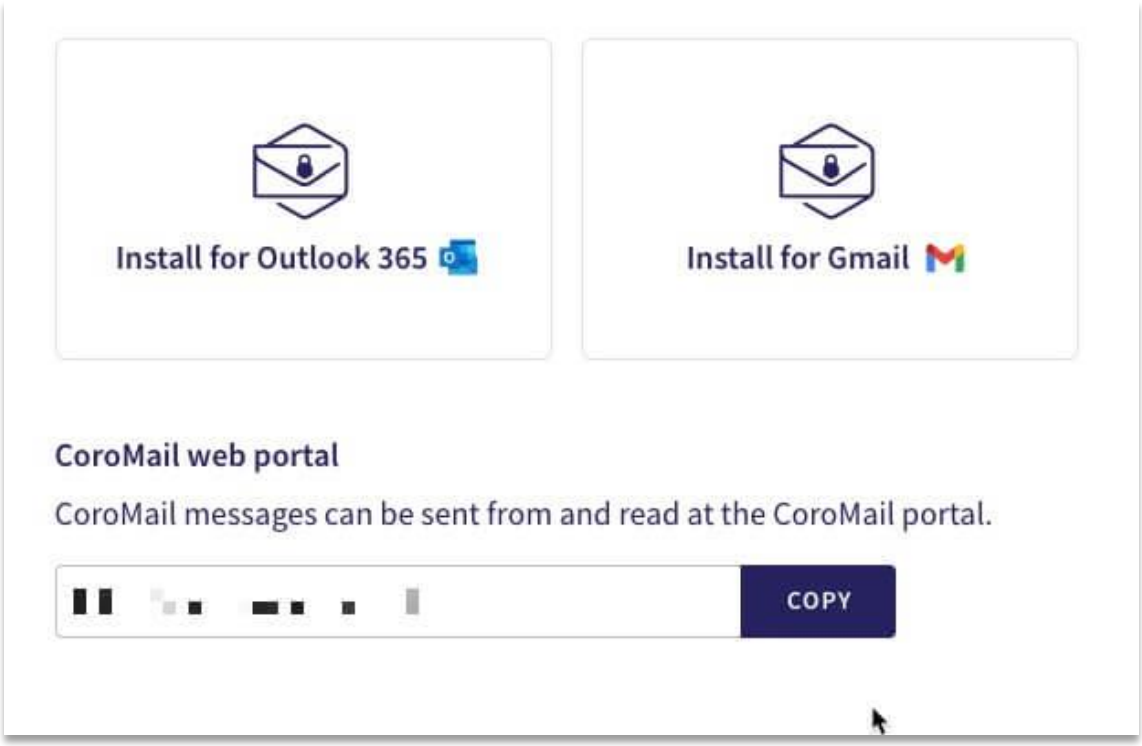
- PII (información de identificación personal)
- PHI (información de salud protegida)
- PCI (información de la tarjeta de pago)
- NPI (información no pública)
- Contraseñas
- Código fuente
- Certificados
- Palabras clave personalizadas

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

III. Secure Messages

El complemento Mensajes seguros le permite cifrar los correos electrónicos salientes, permitiendo que solo los destinatarios previstos accedan a ellos y los lean utilizando una clave privada.

Funciona perfectamente con Microsoft O365 y Google Workspaces, lo que permite a los usuarios enviar mensajes seguros directamente desde su web y aplicaciones nativas de Outlook 365 y Gmail.



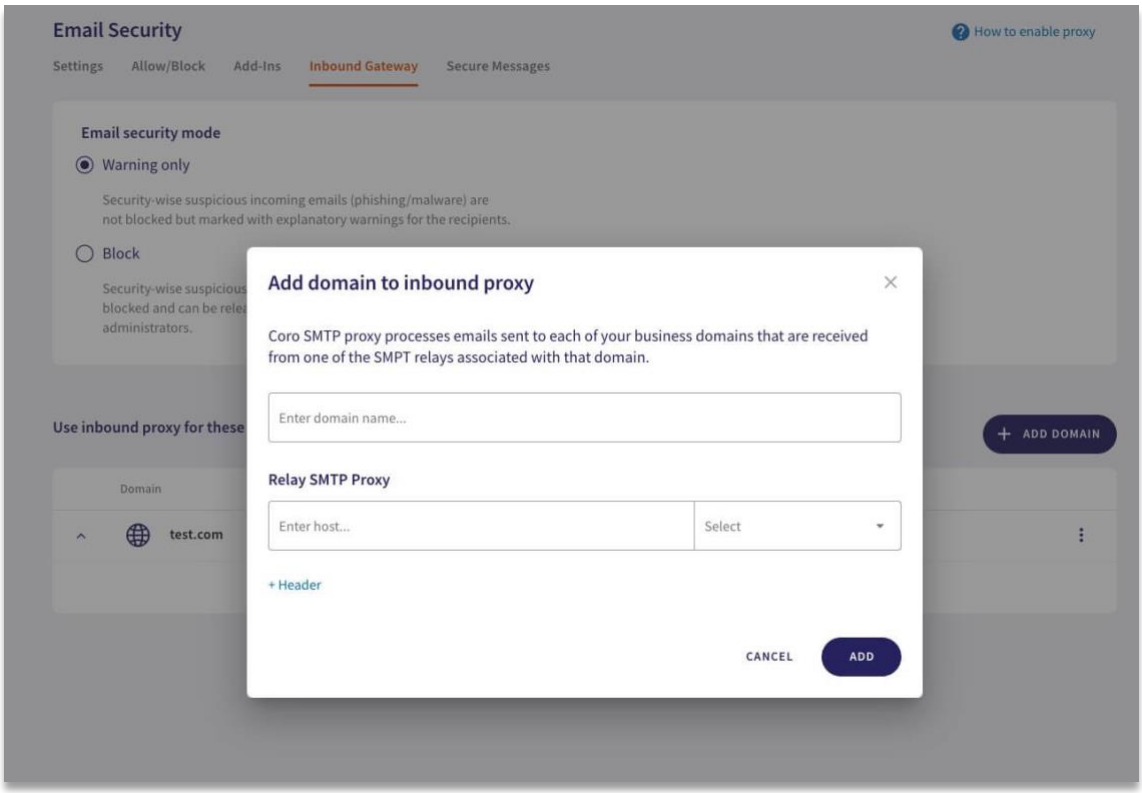
Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

IV. Inbound Gateway

El complemento Inbound Gateway es un proxy que proporciona detección y protección en tiempo real para los correos electrónicos entrantes. Le permite interceptar correos electrónicos entrantes e inspeccionarlos, permitiendo que solo lleguen a los destinatarios correos electrónicos confiables o libres de amenazas.

Puede elegir entre las siguientes opciones para correos electrónicos sospechosos:

- Solo advertencia: los correos electrónicos no se bloquean, pero están marcados con advertencias explicativas para los destinatarios.
- Bloquear: los correos electrónicos se bloquean y solo los administradores del espacio de trabajo pueden liberarlos de la cuarentena.



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

3. Módulos para protección de redes y entornos Cloud

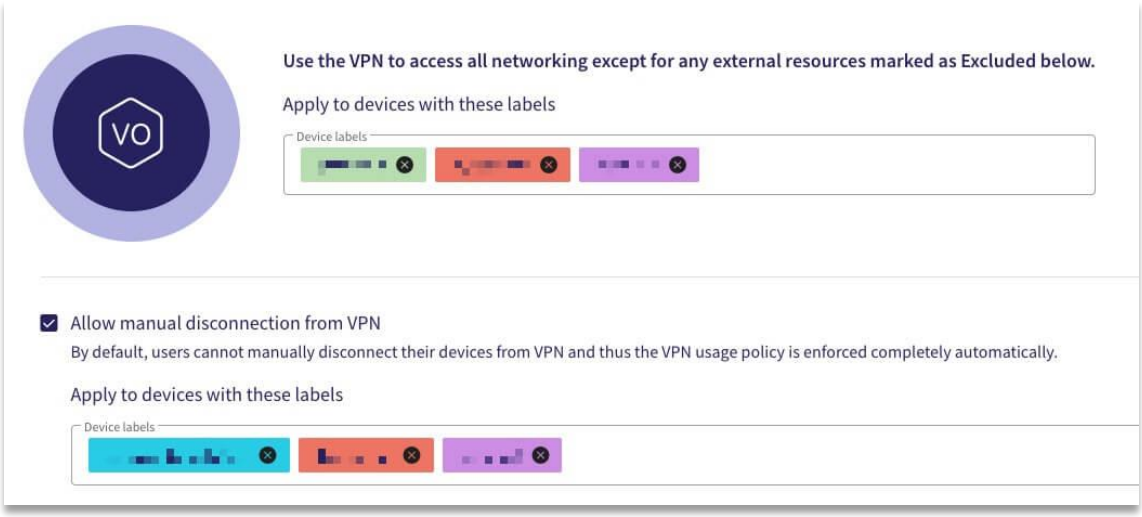
I. Network Security

Network Security es uno de los módulos principales de SASE en Coro. Las capacidades de este módulo incluyen:

Clúster de oficinas remotas
Proteja su red corporativa contra ataques de secuestro, intrusión, adware, malware y phishing.

VPN en la nube
Cifre todos los datos de la red para usuarios remotos sin afectar el rendimiento ni aumentar la sobrecarga de administración.

Cortafuegos en la nube
Enrute todo el tráfico a través de un firewall virtual en la nube, eliminando el malware antes de que pueda atacar sus dispositivos.



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

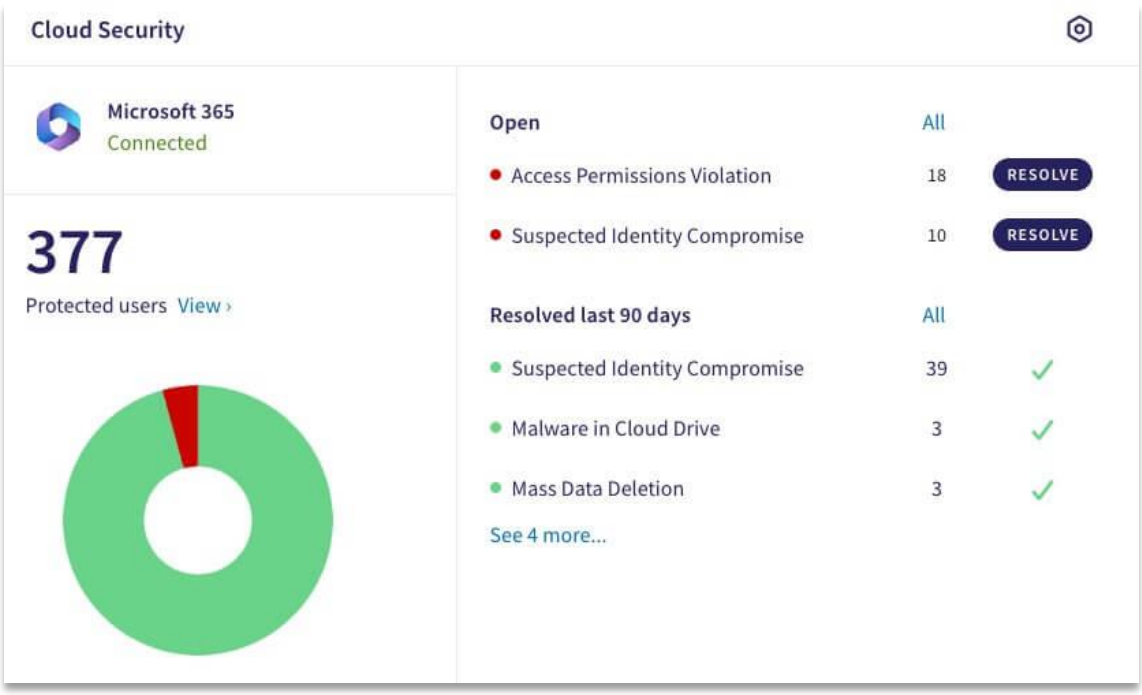
II. Cloud Security

Cloud Security es uno de los módulos principales de SASE en Coro.

Con él, puede detener actividades administrativas anormales, violaciones de acceso, compromiso de identificación, malware y cambios masivos de datos en las siguientes aplicaciones en la nube: Microsoft Office 365, Google Workspace, Slack, Dropbox, Box y Salesforce.

El módulo Cloud Security le protege contra

- Actividad administrativa anormal
- Malware en la unidad de la nube
- Sospecha de compromiso de identidad
- Violación de permisos de acceso
- Sospechosos ataques de bots
- Descarga masiva
- Eliminación masiva



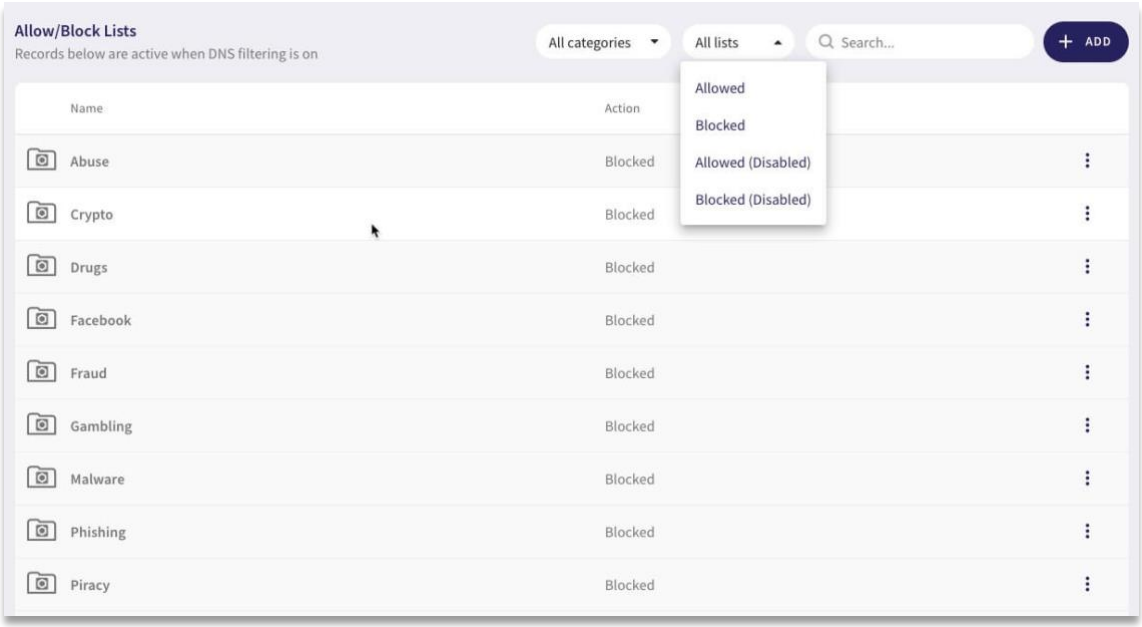
Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

III. Secure Web Gateway

El complemento Secure Web Gateway (SWG) le permite aplicar filtrado DNS para restringir el tráfico de red. El filtrado DNS puede proteger su empresa contra malware, virus y otras amenazas potenciales. Secure Web Gateway incluye las siguientes capacidades:

Filtrado DNS
Bloquee el acceso a recursos externos no deseados desde su oficina virtual.

Listas de permitidos/bloqueados
Restrinja el acceso a URL específicas, grupos de URL o categorías de contenido.



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

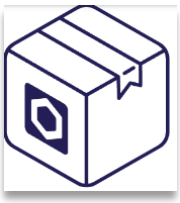
IV. Zero Trust Network Access

El módulo Zero Trust Network Access (ZTNA) le permite aplicar protocolos de seguridad estrictos para trabajadores remotos sin obstaculizar la productividad del usuario final.

Para proteger y proteger el trabajo remoto, puede verificar cada usuario, dispositivo y flujo de red antes de otorgar acceso a los recursos corporativos.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

4. **BUNDLES**

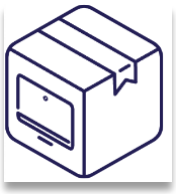


Coro Essentials

Cobertura esencial para terminales, correo electrónico y aplicaciones en la nube, automatizando la resolución de la mayoría de los incidentes de seguridad.

Módulos incluidos

- Endpoint Security (protección del dispositivo, antivirus de próxima generación, listas de permitidos/bloqueados)
- Detección y respuesta de terminales (EDR)
- Seguridad del correo electrónico (escaneo de malware, protección contra phishing, listas de permitidos/bloqueados)
- Seguridad en la nube (O365, GSuite, Dropbox, Box, Slack, Salesforce)

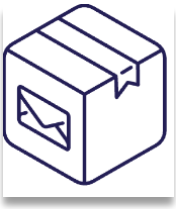


Endpoint Protec.

Registre toda la actividad de los terminales, analice anomalías de datos y automatice la resolución de la mayoría de los incidentes de seguridad.

Módulos incluidos

- Endpoint Security (protección del dispositivo, antivirus de próxima generación, listas de permitidos/bloqueados)
- Gobernanza de datos de terminales
- Detección y respuesta de terminales (EDR)
- Phishing por Wifi

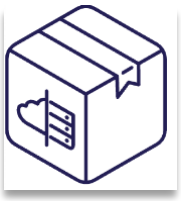


Email Protection

Analice los correos electrónicos en busca de amenazas y corríjalos automáticamente, reduciendo el tiempo necesario para administrar la seguridad del correo electrónico.

Módulos incluidos

- Seguridad del correo electrónico (escaneo de malware, protección contra phishing, listas de permitidos/bloqueados)
- Gobernanza de datos de usuario
- Mensajes seguros
- Inbound Email Gateway



SASE

Agregue protección de grado militar a los dispositivos de la empresa dondequiera que estén a través de una red en la nube impenetrable.

Módulos incluidos

- Seguridad de red (clúster de oficina remota, VPN en la nube, firewall en la nube)
- Seguridad en la nube (O365, GSuite, Dropbox, Box, Slack, Salesforce)
- Puerta de enlace web segura
- Acceso a la red de confianza cero (ZTNA)

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

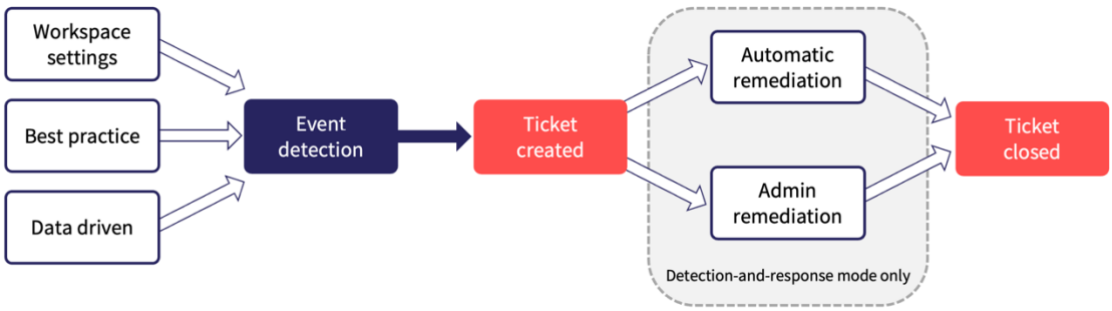
5. SERVICIO DE DETECCIÓN Y RESPUESTA

Nuestro SOC está dedicado al 100% a detectar, remediar y proteger todos los posibles incidentes que se registran en CORO.

Nuestros analistas monitorizan sus endpoints, correo electrónico, aplicaciones en la nube y entorno de red para investigar y resolver amenazas potenciales. Trabajamos en cada instancia de Coro para cubrir todas las alertas que no son resueltas por el software, respondiendo con rapidez y precisión a las amenazas y protegiendo su red y su infraestructura crítica en la nube. Estamos comprometidos a brindarle el mejor servicio y responder de manera integral y oportuna a todos y cada uno de los problemas que puedan surgir.

PROTECCIÓN	**DETECCIÓN**	**RESPUESTA**

Tiempos de respuesta frente a incidentes (SLA). **Modalidad 8x5**
Coro emplea decisiones adaptativas basadas en datos o inteligencia artificial (IA) para la detección, alerta y remediación. Por ejemplo, clasificación de texto para la detección de phishing por correo electrónico o análisis de anomalías para identificar accesos sospechosos a cuentas de aplicaciones en la nube.



Coro utiliza cada uno de los principios anteriores para detectar comportamientos sospechosos. El evento podría ser una única detección sospechosa o una serie de detecciones que desencadenen la creación de un ticket.

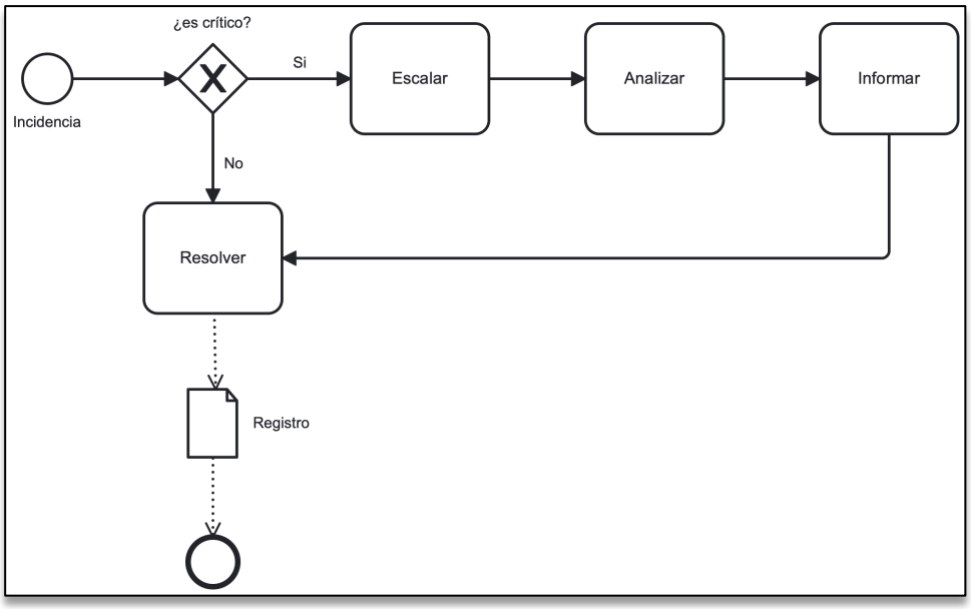
Cuando se requiere revisión y corrección manual, el ticket permanece abierto en la Consola para revisión del administrador. Los usuarios administradores pueden acceder a una lista categorizada de tickets abiertos que requieren revisión y corrección manual. Si un ticket

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

permanece sin resolver después de un período de tiempo, Coro lo cierra automáticamente y registra el evento en el Registro de actividad.
Un ticket proporciona detalles para comprender la causa, los hallazgos, la duración y el contexto de un evento. Es posible que los usuarios administradores deban tomar medidas sobre el ticket a través del Registro de tickets, según el tipo y el estado del ticket. Una vez seleccionados los tickets para la corrección del administrador, Coro ofrece una opción para cerrar el ticket y considerarlo solucionado.

MTR Tiempo medio para reaccionar	**MTE Tiempo medio de ejecución**	**Tiempo medio de respuesta**
Nos comprometemos a reaccionar ante cualquier problema de seguridad crítico en un plazo de 30 minutos y en un plazo de 60 minutos para problemas no críticos.	Ejecutaremos las acciones acordadas en un plazo de 30 minutos para problemas críticos y de 60 minutos para problemas no críticos.	Nos comprometemos a responder a todas sus consultas en un plazo mínimo de 4 horas para problemas críticos y 24 horas para problemas no críticos.

Proceso de respuesta



Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

A. Tipos de tickets: Seguridad en la Nube

Coro genera tickets para aplicaciones en la nube cuando identifica los siguientes incidentes de seguridad:

Actividad administrativa anormal
Coro identificó actividad para una cuenta de administrador de una aplicación en la nube desde una dirección IP inesperada. Los Tickets se clasifican como “sugeridos para revisión” y se cierran automáticamente después del período de revisión de cuatro semanas.

Violación de permisos de acceso
Coro observó un inicio de sesión exitoso que violaba los permisos de acceso a la aplicación en la nube, configurados para un grupo de usuarios al que pertenece un usuario, según el país de origen o la dirección IP del usuario. Los tickets permanecen abiertos para que un usuario administrador los revise y se cierran automáticamente después de un período de tiempo.

Malware en la unidad de la nube
Coro identificó malware potencial en una unidad de nube monitoreada en una de sus aplicaciones conectadas. Los archivos detectados como maliciosos se mueven automáticamente a una carpeta de cuarentena y no es necesario realizar ninguna otra acción. Sin embargo, los usuarios administradores tienen la opción de revisar el ticket y elegir aprobar o eliminar permanentemente el archivo. Los boletos se sugieren para revisión con un tiempo de revisión de dos semanas.

Eliminación masiva de datos
Coro observó un evento de eliminación de datos anormalmente grande de la cuenta de la aplicación en la nube de un usuario protegido. Estos tickets se cierran automáticamente.

Descarga masiva de datos
Coro observó un evento de descarga de datos anormalmente grande desde la cuenta de la aplicación en la nube de un usuario protegido. Estos tickets se cierran automáticamente.

Ataques de bot sospechosos
Coro identificó una cuenta de usuario protegida como objetivo de un presunto intento de inicio de sesión de un bot desde una fuente externa. Estos tickets se cierran automáticamente.

Sospecha de compromiso de identidad
Coro crea un modelo de comportamiento normativo para cuentas de usuario y genera un ticket si detecta actividad anómala o comportamiento de inicio de sesión. Los boletos se clasifican como sugeridos para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

B. Tipos de tickets: detección y respuesta para endpoints (EDR)

Coro EDR detecta y crea tickets basados en reglas de detección de procesos maliciosos.

Componentes del ticket EDR
Los tickets EDR contienen los siguientes componentes:

- Descripción: La regla de detección de tickets EDR.
- Proceso: el nombre del archivo ejecutable del proceso que desencadenó la creación del ticket.
- Hash: el identificador único del proceso.
- Dispositivos afectados: muestra los dispositivos afectados relacionados con el ticket.
- Hallazgos: Más detalles relacionados con el proceso que desencadenó la creación del ticket:
    - Línea de comando: el comando completo utilizado para iniciar el proceso.
    - Ruta: la ruta del directorio del archivo de imagen del proceso malicioso.

Reglas de detección de EDR
Coro EDR identifica procesos maliciosos basándose en reglas de detección y crea tickets para los eventos detectados.

Comando y control
Comando y control se refiere a un tipo de amenaza cibernética en la que un atacante toma el control de un dispositivo comprometido para robar datos, difundir malware o crear una botnet. El atacante utiliza un servidor de comando y control para enviar comandos a los dispositivos comprometidos y recibir datos robados de ellos.

Coro EDR detecta y crea tickets para las siguientes reglas de comando y control:

- Ataque a herramienta de acceso remoto
- Uso sospechoso de un LOLBin

Acceso a credenciales
Acceso a credenciales se refiere a cualquier intento de robar o utilizar ilegalmente credenciales de inicio de sesión para obtener acceso no autorizado a datos o dispositivos.
Coro EDR detecta y crea tickets para las siguientes reglas de acceso a credenciales:

- Intento de fuerza bruta utilizando un nombre de usuario inexistente
- Intentos repetidos de fuerza bruta utilizando contraseñas incorrectas
- Ataque de pulverización de contraseña que involucra 200 intentos de inicio de sesión
- Ataque de pulverización de contraseña que involucra 100 intentos de inicio de sesión

Evasión de defensa
La evasión de defensa se refiere a técnicas y estrategias que utilizan los atacantes para evitar la detección y eludir los mecanismos de seguridad.
Coro EDR detecta y crea tickets para las siguientes reglas de evasión de defensa:

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

- Omisión maliciosa de UAC
- Uso sospechoso de un LOLBin
- Ejecución de una herramienta renombrada

Descubrimiento
El descubrimiento se refiere a acciones o comportamientos de un atacante destinados a recopilar información sobre los dispositivos, redes o infraestructura en los que se ha infiltrado. Coro EDR detecta y crea tickets para las siguientes reglas de descubrimiento:

- Actividad de descubrimiento del sistema no autorizada

Ejecución
La ejecución se refiere a técnicas y estrategias utilizadas por los atacantes para ejecutar código malicioso en un dispositivo o red de destino.
Coro EDR detecta y crea tickets para las siguientes reglas de ejecución:

- Uso sospechoso de un LOLBin
- Descarga y/o ejecución de archivos maliciosos
- Descarga maliciosa de PowerShell desde una fuente externa
- Uso malicioso de comandos de PowerShell codificados en Base64

Acceso inicial
El acceso inicial se refiere a las técnicas y estrategias utilizadas por los atacantes para ingresar a una red o dispositivo por primera vez.
Coro EDR detecta y crea tickets para las siguientes reglas de acceso inicial:

- Ataque a herramienta de acceso remoto

Persistencia
La persistencia se refiere a técnicas y estrategias utilizadas por los atacantes para mantener el control de un dispositivo o red durante un período prolongado, a menudo de forma sigilosa.
Coro EDR detecta y crea tickets para las siguientes reglas de persistencia:

- Creación/ejecución de tareas programadas maliciosas
- Inicio de sesión en la cuenta fuera del horario laboral habitual
- Modificación de Cuentas de Usuario en Grupos con privilegios elevados

C. Tipos de tickets: Email Security

Coro levanta tickets por correos electrónicos cuando identifica los siguientes incidentes de seguridad:

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Remitente bloqueado
Coro identifica que la dirección de correo electrónico o el dominio del remitente se encuentran actualmente en la lista de bloqueo de contenido sospechoso. El correo electrónico se elimina para todos los destinatarios y Coro cierra automáticamente el ticket.

Suplantación de marca
Coro identificó que el correo electrónico podría contener suplantación de identidad o suplantación de una marca, debido a un ataque homógrafo detectado en un dominio reconocido como una marca popular. El correo electrónico se mueve a la carpeta de cuarentena seleccionada y Coro cierra automáticamente el ticket.

Remitente bloqueado por multitud
Coro identifica que la dirección de correo electrónico o el dominio del remitente está en la lista de bloqueo global. El correo electrónico se elimina para todos los destinatarios y Coro cierra automáticamente el ticket.

Suplantación de dominio
Coro identificó que el correo electrónico podría contener suplantación de identidad o suplantación de un dominio, debido a un ataque homógrafo detectado en un dominio reconocido como de uso frecuente en su espacio de trabajo. El correo electrónico se mueve a la carpeta de cuarentena seleccionada y Coro cierra automáticamente el ticket.

Phishing por correo electrónico
Coro determina que un correo electrónico contiene un intento de phishing, como la suplantación de dominio o cualquier intención de engañar al destinatario para que revele información de identificación sobre sí mismo. Coro cierra automáticamente los correos electrónicos de phishing, incluidos aquellos marcados como seguros a través del complemento Coro.
Nota: Este tipo de ticket ha quedado obsoleto y se incluye solo para tickets previamente generados contra él.

Tipo de archivo adjunto prohibido
El correo electrónico contiene un archivo adjunto de un tipo incluido en la lista de cuarentena de tipos de archivos. Para obtener más detalles, consulte Configuración de seguridad del correo electrónico. El correo electrónico se mueve a la carpeta de cuarentena seleccionada y Coro cierra automáticamente el ticket.

Malware en archivos adjuntos de correo electrónico
Coro escanea los archivos adjuntos de un correo electrónico e identifica malware potencial. Si se detecta malware, el correo electrónico se elimina para todos los destinatarios y Coro cierra automáticamente el ticket.

Falta la autenticación requerida
El correo electrónico no cumplió con los requisitos de autenticación obligatorios. Es decir, se cumplieron las siguientes condiciones:

- El dominio del remitente del correo electrónico está en la lista de bloqueo de autenticación del espacio de trabajo.
- El remitente no pasó las pruebas de autenticación de Coro.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

- El correo electrónico se elimina para todos los destinatarios y Coro cierra automáticamente el ticket.

Reportado por el usuario
El usuario final informó que el correo electrónico era phishing a través del complemento M365 o Gmail Coro, aunque Coro no detectó ningún contenido malicioso. Los tickets permanecen en estado abierto para la revisión del operador y se cierran automáticamente después de un período de dos semanas.

Contenido sospechoso
Se activaron uno o más de los siguientes detectores, lo que llevó a Coro a identificar que el correo electrónico contenía contenido potencialmente sospechoso:

- Enlace malicioso: el correo electrónico contiene un enlace URL malicioso o de phishing conocido o sospechoso.
- Código QR sospechoso: el correo electrónico contiene un código QR codificado con una URL maliciosa o de phishing conocida o sospechada.
- Contenido de correo electrónico sospechoso: el cuerpo del mensaje de correo electrónico contiene contenido que Coro identifica como sospechoso. Es decir, el correo electrónico no pasó una prueba de detección basada en estadísticas que involucraba datos de clientes y de phishing.
- Contenido adjunto sospechoso: el correo electrónico incluye un archivo adjunto que Coro identifica como sospechoso o que incluye un posible intento de phishing.

El correo electrónico se mueve a la carpeta de cuarentena seleccionada y Coro cierra automáticamente el ticket.

Suplantación de usuario
Coro detectó un *Envelope honeypot*: evento de suplantación de usuario, mediante el cual el correo electrónico potencialmente contiene suplantación o suplantación de un usuario. Si bien el nombre del remitente mostrado está asociado con un empleado conocido, la dirección de correo electrónico del remitente no es familiar en este espacio de trabajo. El correo electrónico se mueve a la carpeta de cuarentena seleccionada y Coro cierra automáticamente el ticket.

D. Tipos de tickets: Endpoint Security

Coro genera tickets para dispositivos protegidos cuando identifica las siguientes vulnerabilidades de seguridad:

Integridad de archivos móviles de Apple deshabilitada
Coro detectó que Apple Mobile File Integrity (AMFI) está deshabilitado en el dispositivo. AMFI ayuda a garantizar la integridad y seguridad del código ejecutable y los archivos del sistema en los dispositivos Apple. Cuando AMFI está deshabilitado, las aplicaciones pueden verse comprometidas con código malicioso.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Se pueden aplicar las siguientes acciones de política:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión. El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.
- Aplicar: la corrección automática se realiza, se registra en un ticket y el ticket se cierra automáticamente.

Modo de desarrollo habilitado
Coro detectó que el modo de desarrollo está habilitado en el dispositivo. El modo de desarrollo es una configuración del dispositivo destinada a desarrolladores y usuarios avanzados. Habilitar el modo de desarrollo puede exponer el dispositivo a posibles vulnerabilidades de seguridad.

El modo de desarrollo habilitado es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de sus Dispositivos endpoint (consulte Configuración de postura del dispositivo):

Se pueden aplicar las siguientes acciones de política:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión. El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.
- Aplicar: la corrección automática se realiza, se registra en un ticket y el ticket se cierra automáticamente.

Falta la contraseña del dispositivo
Coro detectó que falta la contraseña en el dispositivo.

La falta de contraseña del dispositivo es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de Dispositivos terminales (consulte Configuración de postura del dispositivo):

Se pueden aplicar las siguientes acciones políticas:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión. El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.

Firewall desactivado
Coro detectó que el firewall del dispositivo está deshabilitado. Un firewall es un mecanismo de seguridad basado en software o hardware que monitorea y controla el tráfico de red en un dispositivo, según reglas de seguridad predefinidas. Firewall deshabilitado se refiere a un estado en el que el firewall de un dispositivo no está activo.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Firewall deshabilitado es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de sus Dispositivos endpoint (consulte Configuración de postura del dispositivo):

Se pueden aplicar las siguientes acciones de política:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión. El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.
- Aplicar: la corrección automática se realiza, se registra en un ticket y el ticket se cierra automáticamente.

Gatekeeper deshabilitado
Coro detectó que Gatekeeper está deshabilitado en el dispositivo. Gatekeeper es una tecnología de seguridad que ayuda a garantizar que solo se ejecute software confiable en el dispositivo.

Se pueden aplicar las siguientes acciones de política:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión. El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.
- Aplicar: la corrección automática se realiza, se registra en un ticket y el ticket se cierra automáticamente.

Proceso infectado
Coro detectó un posible proceso malicioso en el dispositivo. Los procesos detectados como maliciosos se finalizan inmediatamente y no se requiere ninguna acción adicional. Sin embargo, los usuarios administradores tienen la opción de revisar el ticket y elegir aprobar el grupo de procesos. Los tickets se sugieren para revisión, con un tiempo de revisión de dos semanas.

Malware en el endpoint
Coro detectó potencial malware en el dispositivo. Los archivos detectados como maliciosos se mueven automáticamente a una carpeta de cuarentena y no es necesario realizar ninguna otra acción. Sin embargo, los usuarios administradores tienen la opción de revisar el ticket y elegir aprobar los archivos. También pueden configurar el análisis de malware de Coro para ignorar la carpeta original en la que reside el archivo marcado. Los tickets se sugieren para revisión, con un tiempo de revisión de dos semanas.

Protección de integridad del sistema deshabilitada
Coro detectó que la Protección de integridad del sistema (SIP) está deshabilitada en el dispositivo. SIP es una tecnología de seguridad que ayuda a proteger el dispositivo de software malicioso que podría modificar archivos y carpetas protegidos. Restringe la cuenta de usuario root y limita las acciones que el usuario root puede realizar en partes protegidas del sistema operativo.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Se pueden aplicar las siguientes acciones políticas:

Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión. El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente del endpoint de Coro observa que la vulnerabilidad se ha resuelto.

Falta la notificación UAC
Coro detectó que faltaban notificaciones UAC (Control de acceso de usuarios) en el dispositivo.

La notificación de UAC que falta es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de Dispositivos finales (consulte Configuración de postura del dispositivo):

Se pueden aplicar las siguientes acciones:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión.

- Aplicar: la corrección automática se realiza, se registra en un ticket y el ticket se cierra automáticamente.

Endpoint drive sin cifrar
Coro detectó una unidad no cifrada en el dispositivo.

El endpoint drive no cifrado es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de Dispositivos de punto final (consulte Configuración de postura del dispositivo):

Se pueden aplicar las siguientes acciones:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión.

El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.

Protección de copia de seguridad VSS
Cuando la protección de copia de seguridad VSS (Servicio de instantáneas de volumen) está habilitada, Coro aplica instantáneas de copia de seguridad cada cuatro horas y bloquea los procesos que presentan riesgos para la copia de seguridad (consulte la ayuda y documentación de Coro sobre el uso de la protección de copia de seguridad VSS en sus terminales Windows). Los tickets se sugieren para revisión con un tiempo de revisión de dos semanas.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Copia de Windows no original
Coro detectó una copia no original de Windows en el dispositivo.

La copia de Windows no original es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de Dispositivos endpoint (consulte Configuración de postura del dispositivo):

Se pueden aplicar las siguientes acciones políticas:

- Revisión: no se realiza ninguna corrección automática y se genera un ticket y se clasifica como que requiere revisión.

El ticket permanece abierto hasta que el usuario administrador lo cierra manualmente o el agente de punto final de Coro observa que la vulnerabilidad se ha resuelto.

Conexión Wi-Fi prohibida
Coro detectó una red Wi-Fi pública bloqueada. Un dispositivo tiene prohibido conectarse a una red Wi-Fi pública bloqueada.

Después de configurar la política e intentar conectarse a una red Wi-Fi pública, el intento de conexión falla y se crea un ticket de conexión Wi-Fi prohibida que se cierra automáticamente y no hay acciones disponibles.

Se agrega un registro al Registro de actividad: "Se ha bloqueado la conexión del dispositivo <nombre del dispositivo> a la red WiFi <nombre de la red Wi-Fi>".

La conexión Wi-Fi prohibida es una vulnerabilidad definida en la pestaña Postura del dispositivo de la configuración de Dispositivos finales (consulte Configuración de postura del dispositivo).

E. Tipos de tickets: User Data Governance

Para obtener más información sobre cómo Coro protege los datos de los usuarios de una organización, consulte Introducción a la gobernanza de datos de usuarios. Para obtener más información sobre qué información constituye estos tipos de datos confidenciales, consulte Tipos de información confidencial regulatoria.

Coro genera tickets relacionados con la gobernanza de datos cuando identifica incidentes de seguridad que involucran los siguientes tipos de datos confidenciales:

NPI (Información no pública), PII (información de identificación personal), PHI (Información de salud protegida), PCI (información de la tarjeta de pago)
Coro detectó que un usuario compartió o envió por correo electrónico información que incluye NPI, PII, PHI o PCI, y el usuario administrador tiene habilitado el monitoreo para esa categoría. El usuario administrador también puede haber configurado políticas de permisos que rigen los derechos de los usuarios para acceder, o acceder y exponer, estos tipos de datos.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Estos tickets pueden requerir la atención de usuarios encargados de la protección de datos (DPO), de acuerdo con regulaciones como GDPR, HIPAA, SOC2 y otras, por lo que se clasifican como sugerido para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Exposición sospechosa del certificado
Coro identificó una cuenta de usuario que estuvo involucrada en un posible evento de exposición de datos con certificados de seguridad monitoreados (archivos con extensión .crt o .pem utilizados para establecer una conexión segura entre un cliente y un servidor). Esto ocurre cuando se habilitó la supervisión de Certificados (consulte Supervisión). Los tickets se clasifican como sugeridos para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Exposición sospechosa de datos críticos
Coro identificó una cuenta de usuario que estuvo involucrada en un posible evento de exposición de datos con datos críticos monitoreados (palabras clave específicas definidas en correos electrónicos y contenido de archivos compartidos). Esto ocurre cuando se habilitó la supervisión de palabras clave específicas (consulte Supervisión). Los tickets se clasifican como sugeridos para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Exposición sospechosa del tipo de archivo
Coro identificó una cuenta de usuario que estuvo involucrada en un posible evento de exposición de datos con tipos de archivos monitoreados (tipos de archivos específicos definidos agregados como archivos adjuntos de correo electrónico y en contenido de unidad compartida). Esto ocurre cuando se habilitó la supervisión de tipos de archivos específicos (consulte Supervisión). Los tickets se clasifican como sugeridos para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Exposición sospechosa de contraseña
Coro identificó una cuenta de usuario que estuvo involucrada en un posible evento de exposición de datos que incluía contraseñas. Esto ocurre cuando se habilitó la supervisión de contraseñas (consulte Supervisión). Los tickets se clasifican como sugeridos para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Exposición sospechosa del código fuente
Coro identificó una cuenta de usuario que estuvo involucrada en un posible evento de exposición de datos que incluía archivos de código fuente monitoreados (archivos con un código conocido o extensión de script como .md, .yaml, .sh). Esto ocurre cuando se habilitó la supervisión del código fuente (consulte Supervisión). Los tickets se clasifican como sugeridos para revisión y se cierran automáticamente después del período de revisión de dos semanas.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

F. Tipos de tickets: Endpoint Data Governance

Coro genera tickets relacionados con la gobernanza de datos de endpoints cuando se identifican incidentes que involucran los siguientes tipos de datos confidenciales y el usuario administrador ha habilitado la configuración de Privacidad de datos confidenciales en Panel de control > Gobernanza de datos de endpoints:

Endpoint drive con NPI
Endpoint drive con PCI
Endpoint drive con PHI
Endpoint drive con PII

Tipos de amenazas

Endpoint Data Governance de Coro proporciona los medios para reducir el riesgo de filtraciones de datos y proteger la información confidencial del acceso no autorizado y el uso indebido. Varias amenazas pueden poner en riesgo los datos de una organización y es importante ser conscientes de ellas y tomar medidas para limitar su impacto:

- Ataques cibernéticos: los ciberdelincuentes pueden utilizar una variedad de métodos para acceder a información confidencial, como piratería de sistemas, estafas de phishing y malware.
- Amenaza interna: los empleados y contratistas pueden acceder o hacer mal uso intencional o no de información confidencial.
- Robo físico: la información confidencial puede ser robada o perdida mediante robo físico o extravío de dispositivos portátiles y teléfonos inteligentes.
- Error humano: un error humano, como enviar accidentalmente información confidencial a la persona equivocada, puede provocar violaciones de datos.

Información de identificación personal (PII)

PII es cualquier información perteneciente a un individuo específico que puede usarse para descubrir la identidad de ese individuo. Estos datos incluyen:

Números de seguro social (SSN)
Nombre completo
Dirección de correo electrónico
Industria de tarjetas de pago (PCI)

Los principales proveedores de tarjetas de crédito hacen cumplir los estándares de seguridad establecidos por el PCI. Estos estándares garantizan que las empresas mantengan un entorno seguro para aceptar, procesar, almacenar o transmitir datos de tarjetas de crédito. El Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC) gestiona y administra estos estándares de seguridad para mejorar la seguridad de las cuentas de pago. Para obtener más información sobre los estándares PCI, visite el sitio web de PCI SSC aquí.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Información de salud protegida (PHI)

La PHI son datos recopilados, almacenados, utilizados o transmitidos durante la prestación de servicios de atención médica. Estos datos incluyen al paciente:

Nombre
Historial médico
Información del seguro médico
Información personal no pública (NPI)

NPI son datos financieros personales recopilados y almacenados por instituciones financieras. NPI es una combinación de PII y otros indicadores. Por ejemplo, los SSN son indicadores de PII, pero en combinación con la información de la tarjeta de crédito, también se clasifican como NPI.

Un ticket NPI cerrado se genera cuando la PII Y otro indicador, por ejemplo, palabras clave financieras (metadatos financieros, contenido, formularios o PCI).
Se genera un ticket NPI abierto si además de PII, también se detecta PCI.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

6. SE LABS REPORT

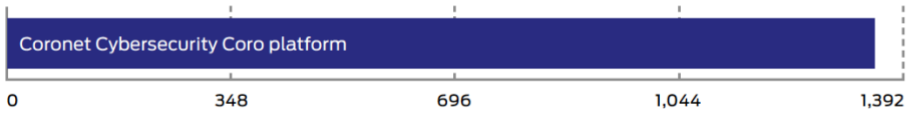
SE Labs probó la plataforma Coronet Cybersecurity Coro contra una variedad de piratería y ataques diseñados para comprometer sistemas y penetrar redes objetivo de la misma manera en que los delincuentes y otros atacantes violan sistemas y redes.
Se utilizaron cadenas completas de ataque, lo que significa que los evaluadores se comportaron como atacantes reales, investigando objetivos, utilizando una variedad de herramientas, técnicas y vectores antes de intentar obtener un nivel inferior y acceso más potente. Finalmente, los evaluadores/atacantes intentaron completar sus misiones, que podrían incluir robar información, dañar sistemas y
conectarse a otros sistemas en la red.

Examinamos sus capacidades para:

- Detectar ataques altamente dirigidos
- Proteger contra las acciones de personas altamente específicas.
- Proporcionar reparación de daños y otros riesgos planteados por las amenazas
- Manejar aplicaciones legítimas y otros objetos

Executive Summary			
Product Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Coronet Cybersecurity Coro platform	94%	100%	97%

Total Accuracy Ratings			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Coronet Cybersecurity Coro platform	1,346	97%	**AAA**



Total Accuracy Ratings combine protection and false positives.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida

Conclusiones

Esta prueba expuso Coronet Cybersecurity Coro a un conjunto diverso de exploits, sin archivos ataques y archivos adjuntos de malware, que comprenden
la más amplia gama de amenazas disponibles actualmente.
Todos estos tipos de ataques han sido presenciados en ataques del mundo real en los últimos años.
Son representativos de una amenaza real y presente a redes empresariales en todo el mundo.

A veces los productos son demasiado agresivos y detectan todo, incluidas las amenazas y los objetos legítimos.
En esta prueba Coro no generó errores, y manejó correctamente todos los archivos legítimos e inofensivos.

La plataforma Coronet Cybersecurity Coro gana una calificación AAA por su gran rendimiento.

Confidencial © 2024 Producción Diseño e Informática, SL - Distribución Prohibida