MEYAJ-TI

Servicios

Servicio de detección de intrusos perimetrales

Servicio de Inspección de tráfico de red que pasa a través de los dispositivos como firewalls, Gateway etc., con el fin de identificar y prevenir intrusiones, proporcionan la detección a través de varios métodos - por ejemplo, firmas , detección de anomalías de protocolo , el monitoreo del comportamiento o heurística. Cuando se despliegan en línea, también puede usar varias técnicas para bloquear los ataques que se identifican con alta confianza.

Servicio de protección perimetral Anti-DDoS

Este servicio protege y bloquea ataques de denegación de servicios, evitando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red identificando la sobrecarga de los recursos de infraestructura.

Servicio Web Application Firewall

Dispositivo que puede ser hardware o software que analiza el tráfico web (entre el servidor web e internet) protege de diversos ataques como SQL Injection, Cross Site Scripting, etc. Protege ataques dirigidos al servidor web que los IDS/IPS no pueden. No enruta el tráfico ni lo NATea, sino que se hacen 2 peticiones diferentes, una desde el cliente hasta el WAF y otra desde el WAF hasta el servidor web final.

Appliances de servicio para filtrado de correo electrónico

Un filtro de Email se encarga de bloquear aquellos correos que pueden tener contenido infectado u ofensivo, a través de ciertos algoritmos el filtro detecta información en el correo entrante que puede llegar a ser o no deseado, por ejemplo, los correos que contienen frases sugestivas, de oferta, o promociones pueden ser bloqueados y dirigidos por medio de un filtro al correo no deseado o detenidos.

Servicios de protección centralizada UTM

Conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Resguarda la infraestructura de red y evitar la entrada y salida de tráfico malicioso por medio de configuración de políticas restrictivas y políticas permisivas, listados de control de acceso, se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet.

Servicio de protección perimetral/interna

Conjunto de dispositivos configurados para permitir, limitar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.Resguarda la infraestructura de red y evitar la entrada y salida de tráfico malicioso por medio de configuración de políticas restrictivas, listados de control de acceso, se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet.

Servicio de protección de acceso a la Red

Conjunto de dispositivos configurados para permitir, limitar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Resguarda la infraestructura de red y evitar la entrada y salida de tráfico malicioso por medio de configuración de reglas, listados de control de acceso, se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas o restringidas de la misma red.

Servicio de detección de patrones de trafico de red a través de con capacidad de lectura de 1Gb de trafico y 1TB de capacidad de almacenamiento

Solución que permite tener visibilidad 360° sobre toda la red y lo que sucede dentro de esta, con la capacidad de hasta de reproducir cualquier sesión. Realizar las tareas de correlación de eventos, Network Security Monitoring, Big Data Management & Analytics con una sola tecnología.

Realiza las tareas de correlación de eventos, Network Security Monitoring, Big Data Management & Analytics con una sola tecnología, todo esto basado en la centralización de bitácoras de diferentes tipos de dispositivos, Red, Sistemas Operativos, Bases de Datos, cualquier sistema que generé y envié logs al sistema pueden ser analizados.

Servicio de Centralización y Correlación de bitácoras de los Sistemas Críticos con la capacidad de 3000 EPS y 1 TB de almacenamiento

Pruebas de penetración internas y externas para la revisión y mejora del nivel de la seguridad de la información del cliente, estas pruebas permitirán conocer las vulnerabilidades técnicas a los que se encuentra expuesta la empresa, y poder así establecer
medidas adecuadas para mitigarlas o reducirlas a un nivel aceptable con base en las mejores prácticas, estándares y metodologías de seguridad de la información orientadas al negocio y a su operación.

Servicio de prueba de penetración de 1 a 5 objetivos críticos;
White Box y Black Box.

Análisis de Código

El análisis de código contempla un esquema para conocer los niveles de seguridad de las aplicaciones del negocio, entre las características del análisis de código se encuentra:

- Detección de vulnerabilidades de programación

- Mejorar la seguridad del sistema de recomendaciones

-Mejora la eficiencia del código en aspectos de reducción de BUG y patrones anómalos.

El objetivo primordial es controlar qué contenido que se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web. El filtrado WEB determina qué contenido estará disponible en una máquina o red particular. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable

Appliance de servicio de Filtrado de Web con la capacidad de protección de 10,000 a 16,000 usuarios

El objetivo de este servicio es proteger , detectar y/o eliminar virus informáticos a través de herramientas especializadas, este puede contemplar áreas usuarias o sistemas críticos de la empresa (Data Center y Correo electrónico).

Administracion de consola de antivirus

Appliance para el Servicio de inspección de trafico (Anti malware)

Servicio de Inspección del tráfico que pasa a través de los dispositivos como firewalls, Gateway etc., con el fin de identificar y prevenir código malicioso embebido en programas, archivos o documentos que viajen a través de la red o los equipos de computo. Cuando se despliegan en línea, también puede usar varias técnicas para bloquear archivos, programas o documentos infectados.

Appliance de servicio de MDM

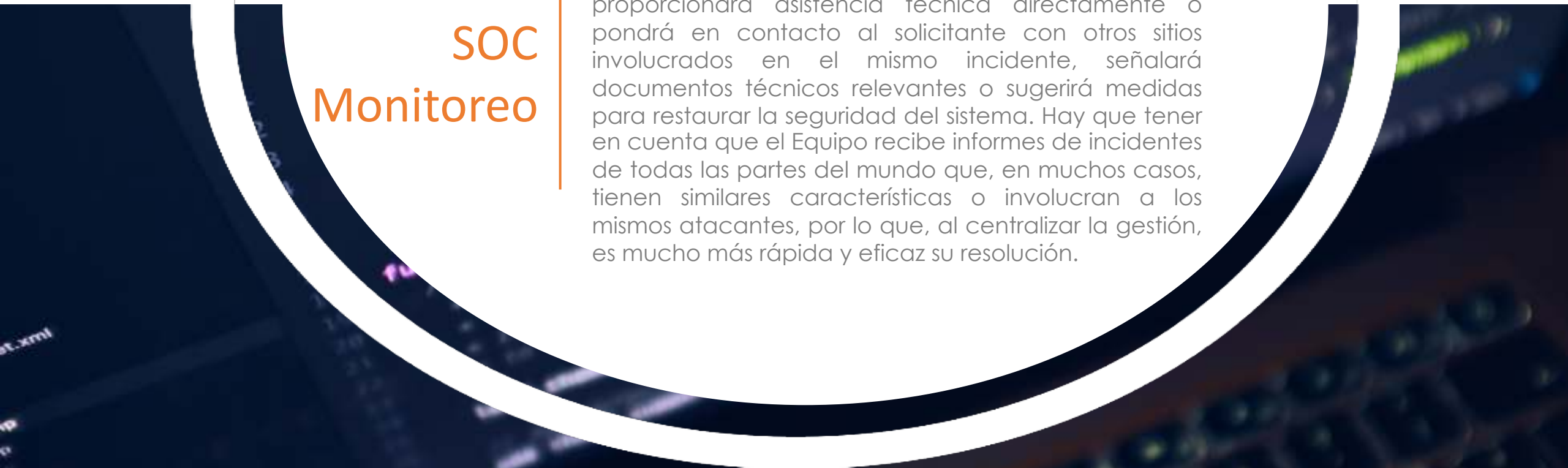
Servicio de Inspección de los dispositivos móviles que utilizan los servicios administrados del instituto, con el fin de identificar y prevenir fuga de información, archivos o documentos que viajen a través de la red o los equipos de computo. Cuando se despliegan en línea, también puede usar varias técnicas para bloquear archivos, programas o documentos infectados, inventario de aplicación y servicios de repositorio centralizado.

SOC Administración

Servicio de Administración de herramientas de seguridad; proporcionará asistencia técnica directamente o pondrá en contacto al solicitante con otros sitios involucrados en el mismo incidente, señalará documentos técnicos relevantes o sugerirá medidas y llevará acabo la contención para restaurar la seguridad del sistema.

SOC Monitoreo

Servicio de monitoreo de herramientas de seguridad; proporcionará asistencia técnica directamente o pondrá en contacto al solicitante con otros sitios involucrados en el mismo incidente, señalará documentos técnicos relevantes o sugerirá medidas para restaurar la seguridad del sistema. Hay que tener en cuenta que el Equipo recibe informes de incidentes de todas las partes del mundo que, en muchos casos, tienen similares características o involucran a los mismos atacantes, por lo que, al centralizar la gestión, es mucho más rápida y eficaz su resolución.



Business Partes

Sophos Authorized Partner

Licencias OnLine

Business Partner IBM

DDRMéxico Always up


MEYAJ-TI
Servicios
contacto@meyaj-ti.com | Buzón General
www.meyaj-ti.com
/meyaj-ti
/meyaj-ti
@Meyaj_TI