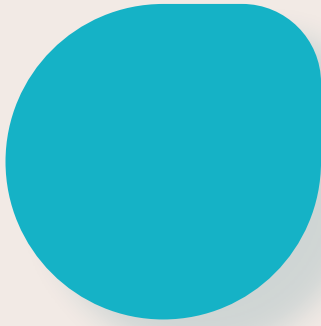


SERVICIOS GESTIONADOS



SEGURIDAD



Alcance

Servicio de Seguridad Gestionada del CPD a nivel de:

- Máquinas virtuales
- Servidores
- Networking
- Firewalls.



La seguridad, como forma de protección de usuarios, redes y sistemas de información frente a posibles ataques, es una de las prioridades de Tigloo, que pone especialmente el foco en dar una respuesta proporcional y asequible a las amenazas que afrontan sus clientes.

Evolución del servicio

Durante el tiempo en el que se prestan los distintos servicios descritos, se realiza un seguimiento de datos e información para identificar posibles actividades de mejora del servicio, así como un soporte continuo al cliente.

Nuestra aproximación a la hora de abordar los proyectos es mixta, es decir, nos apoyamos en soluciones tecnológicas y organizativas que aseguren la confidencialidad en todo el ciclo de vida de la información.

Nuestro objetivo final es formar parte de una nueva generación de empresas más fuertes en cuanto a ciberseguridad, protección y defensa, así como la difusión y sensibilización a medida del uso seguro de los sistemas de información.

Monitorización

La actividad básica de monitorización de los elementos consiste en:

- Identificar los activos y elementos que componen el sistema de disponibilidad de la infraestructura (Checklist).
- Monitorización de alertas de seguridad y vulnerabilidades de activos.
- Gestión de eventos y análisis de positivos / falsos positivos.
- Creación, categorización y enrutado de tickets.
- Descubrimiento semanal de elementos de la red.
- Análisis automático mensual de vulnerabilidades de la red.
- Identificar las acciones a ejecutar en el caso de activación de alertas . (Incidencias, problemas, destinatarios y automatismos)

Operación

En el nivel de operación, nuestra labor no acaba con la notificación de la alerta sino que además nos encargamos de:

- Reparación de posibles problemas que pueda tener servidor OSSIM y/o sensores adicionales que pueda tener configurados.
- Mantenimiento de los sensores que puedan tener algún problema.
- Reconfiguración de los dispositivos con las configuraciones previas
- Asesoramiento en la optimización del uso de los dispositivos existentes.
- Investigación, seguimiento y resolución de las incidencias de seguridad identificadas por el sistema si estas afectan a sistemas gestionados por nuestros servicios. Si no se notificara al cliente dando propuestas de solución.

Administración

En el nivel de administración además de todas las actividades anteriores, incluimos las siguientes actividades:

- Revisión del estado de la bbdd de OSSIM.
- Mensualmente purgado de logs, alertas y tickets de OSSIM
- Valoración informe mensual de vulnerabilidades e incidentes detectados con propuesta de acciones de mejora.
- Backup de configuración de activos.

Ejecución de cambios estándar:

- Instalación de Agentes OSSIM (servidores Windows-Linux)
- Gestión de usuarios accesos consolas de administración.
- Elaboración de políticas de restricción de falsos positivos cuando sean muy recurrentes.
- Alta de plugin en el sistema para incluir equipos que no sean servidores pero que sean críticos, siempre y cuando estén soportados por otro servicio gestionado.



tigloo
A DCS GROUP COMPANY

www.tigloo.es