Cibersoluciones para teletrabajo

OneseQ by alhambra

Tu organización puede estar desprotegida

Tras la declaración del Estado de Alarma en España por la pandemia del COVID-19, las áreas de IT de las compañías han buscando soluciones de trabajo remoto con el objetivo de proteger a sus empleados y garantizar la continuidad de sus negocios.

Sin embargo, las vulnerabilidades generadas por la “inexperiencia” sobre el teletrabajo seguro y el aumento de los ciberataques, hacen que la situación sea poco alentadora para las compañías.

Esto las coloca en una situación de sobreexposición hacia los ciberatacantes.

¿Cómo podemos protegernos ante estas vulnerabilidades?

En esta guía te ofrecemos un conjunto de soluciones que pueden ajustarse a vuestras necesidades de seguridad.

¿Cómo evitamos las vulnerabilidades?

> Securización de entornos
> Securización de aplicaciones web
> Securización del acceso del usuario
> Securización del Desktop
> Control de servicios Cloud
> Securización de Navegación Internet
> Securización de correo
> Monitorización y detección
> Test de vulnerabilidades de sistemas
> CISO as a Service
> Concienciación de usuarios

A continuación te detallamos estas soluciones y sus beneficios.

Securización de entornos

FWaaS

Firewall as a Service ofrece un modelo de gestión unificada de las amenazas, que abarca una gama completa de funciones de red y seguridad: cortafuegos, VPN, control de aplicaciones, antivirus, anti-spam, protección contra intrusos, control de aplicaciones, filtrado de contenidos web, supervisión de clientes, gestión de vulnerabilidades e incluso aceleración WAN.

Analyze_aaS

Se trata de un servicio basado en la solución de Fortinet Analyzer que aporta una mayor visión de los logs de los sistemas perimetrales de dicho fabricante.

Beneficios

- Protección a medida
- Pago por uso
- Alta disponibilidad de nuestro servicio
- Flexibilidad de un servicio en la nube
- Adaptable a cualquier compañía

¿Por dónde empezamos?

- Contratación y despliegue de contexto
- Configuración y parametrización en remoto
- Soporte de nuestro SOC

Securización de aplicaciones web

WAFaaS

Web Application Firewall as a Service te proporciona todas las herramientas necesarias para neutralizar fugas de datos y ataques contra infraestructuras informáticas.

Además, te facilita el cumplimiento de las normas internas y sectoriales que regulan la protección de datos. Todo ello gracias a:

- Servicio de reputación de direcciones IP
- Módulo de análisis de vulnerabilidades
- Perfilado automático y en tiempo real de las aplicaciones
- Alto rendimiento

Beneficios

- Protección a medida
- Pago por uso
- Alta disponibilidad de nuestro servicio
- Registros e informes
- Flexibilidad de un servicio en la nube

¿Por dónde empezamos?

- Contratación y despliegue de contexto.
- Configuración y parametrización en remoto y
- Soporte de nuestro SOC

Securización del acceso del usuario

VPN (FWaaS –VDOM)

Desde OneseQ ponemos a tu disposición el servicio de seguridad túneles VPN para habilitar accesos remotos seguros. Embebido también en el servicio FWaaS.

OTP (MFA)

Implantación de servicio de doble autenticación con OTP (One Time Password) multifactor, que te permitirá controlar tu identidad y que así, no pueda ser suplantada por una autenticación débil de usuario y contraseña.

Beneficios

- Pago por uso
- Alta disponibilidad

¿Por dónde empezamos?

- Contratación y despliegue de contexto.
- Configuración y parametrización en remoto y
- Soporte de nuestro SOC

Securización del Desktop

AV + EDR (o Servicio CCEndPoint - SOC EP)

Implantación y despliegue de seguridad Antivirus y opcionalmente EDR (Endpoint Detection and Response), que permite controlar los procesos sospechosos del endpoint para una elevación de incidente temprana.

Adicionalmente, podemos dar ese servicio no solo como despliegue de implantación, sino como servicio gestionado por nuestro SOC (CCEndPoint - Control Countinous EndPoint de OneseQ).

Cifrado de Desktop

Ciframos el disco duro de tu equipo destacado, con el objetivo de cubrir cualquier pérdida o acceso no permitido al mismo. Confiere la capacidad de confidencialidad necesaria en el puesto de trabajo.

Beneficios

- Desplegable en remoto
- Pago por uso
- Alta disponibilidad de nuestro servicio

¿Por dónde empezamos?

- Te proveemos de los servicios técnicos especializados para el despliegue, así como de los acuerdos con los mejores fabricantes para dichas tecnologías (Sophos y Panda).
- Adicionalmente nuestro SOC podrá ofrecer el servicio de Control Continuado de EP para monitorizar y elevar la alerta de modo temprano.

Control de servicios Cloud

CASB (NetSkope)

Servicio que nos ofrece la capacidad de controlar al usuario en el acceso y trabajo en el cloud, por ejemplo en Office 365, Azure, etc.

De manera que ganamos capacidad de control para evitar exfiltraciones de datos y riesgos de negocio con acceso fraudulento a los recursos cloud de nuestra compañía.

Beneficios

- Control de accesos y permisos a documentos
- Extensión del perímetro de permisos
- Control del contenido y accesos a plataformas Cloud

¿Por dónde empezamos?

Te proveemos de los servicios técnicos especializados para el despliegue, así como de los acuerdos con los mejores fabricantes para dichas tecnologías (NetSkope).

Securización de Navegación Internet

Navegación Segura (Cisco Umbrella)

Servicio de Cisco que te permite la navegación segura estés donde estés.

Toda la navegación Internet del usuario se realiza filtrada por la plataforma y la Threat Intelligence de Cisco, lo que aportará un gran control de IOC (Indicadores de compromiso) sobre los destinos de navegación y así poder realizar de manera más segura las conexiones a los sites legítimos.

Lo que te evita multitud de fraudes de páginas ilegítimas que te podrían infectar.

Beneficios

- Servicio prestado en la nube de Cisco
- Disponibilidad e Inteligencia de ataques

¿Por dónde empezamos?

Gracias a nuestro acuerdo de partnership, nosotros te facilitamos la contratación del servicio de Cisco y te ofrecemos el despliegue del servicio desde nuestro SOC.

Securización de Correo - AntiSPAM

FortiMAIL y Mail Security Sophos

Servicios en la nube con tecnología Fortinet y Sophos que filtran y eliminan el correo ilegítimo y fraudulento.

Constituyen una capa más de seguridad sobre uno de los vectores más usados para la entrada de ciberdelincuentes: el correo electrónico.

Beneficios

- Disponibilidad
- Ancho de banda ilimitado

¿Por dónde empezamos?

Gracias a nuestros acuerdos de partnership con Fortinet y Sophos, nosotros te facilitamos la contratación de los servicios y te ofrecemos sus despliegues desde nuestro SOC.

Monitorización y detección

Servicio SOC - Alerta Temprana

Para detectar un ciberataque a tiempo es necesario contar con: la monitorización de los sistemas, la información exterior de patrones de ataques, feeds de inteligencia, IOC, etc. Y, después, relacionar toda la información para que nos permita contextualizar y detectar un ataque en alerta temprana.

NOC - Remediación y forénsico

Una vez levantada la alerta, nuestros especialistas asisten en su remediación, así como en la realización de un audit forense que capacite la recuperación lo mas rápido posible. Además, si se necesita (y es posible) se evidencia el origen del ataque "pericialmente".

Beneficios

- Capacidad de actuación rápida
- Evidencia de la vigilancia de activos (necesaria para ciertas normas)

¿Por dónde empezamos?

Despliegue desde nuestro SOC de las sondas de correlación y la integración en nuestros sistemas SIEM para dotar de inteligencia de amenazas al contexto de tu compañía.

Test de vulnerabilidades de sistemas

VAK – Qualys

Plataforma de testing de vulnerabilidades de sistemas, tanto internos como externos. Servicio que puede ser gestionado o no (podremos liberar el contexto para que puedas operarlo directamente) por nuestros analistas del SOC.

PenTest

Servicios profesionales de Ethical Hacking, realizados por los analistas de nuestro Red Team, con el que descubrimos las brechas de los servicios con las mismas técnicas usadas por los ciberdelincuentes.

Beneficios

- Generar una consciencia del riesgo real que sufren nuestros sistemas y nuestra compañía.

¿Por dónde empezamos?

Servicio proporcionado por herramientas de primer nivel (Qualys), en conjunción con el soporte técnico especializado de nuestros integrantes del SOC y del Red Team.

CISO as a Service (vCISO)

Virtual Ciso

Ponemos a tu disposición el conocimiento de un "gestor de seguridad" en la figura de vCISO.

El trabajo de asesoramiento, cumplimiento de normativa y legislación, generación de procedimientos internos, evaluación de proveedores de seguridad, etc. recae en este perfil que en modo onsite y offsite puede proveer a tu pyme de las capacidades de gestión y conocimiento que actualmente tienen las compañías enterprise en sus CISOs.

De esta manera, no tienes que dedicar un recurso de personal específico para la gestión de la seguridad, y así puede descargar esa tarea en especialistas formados para ello en modo servicio.

Además, no todas las compañías necesitan un CISO 8h al día. Con este servicio generamos economías de escala.

Beneficios

- Protección a medida
- Pago por uso
- Personal altamente cualificado

¿Por dónde empezamos?

Contratación y puesta en marcha de planes de seguridad.

Concienciación de usuarios

Test Phishing

Consiste en la simulación de cientos de ataques de phishing realistas y desafiantes con tan solo unos clics.

Nuestros analistas monitorizan millones de mensajes de correo electrónico, direcciones web, archivos y otros datos que llegan a diario en busca de las amenazas más recientes.

Este flujo de información constante garantiza que la formación de los usuarios comprendan tácticas de phishing actuales con plantillas de simulación de ataques, socialmente pertinentes, y abarque varios escenarios desde principiante a experto.

Sesiones Concienciación

Sesiones online de concienciación para dar a conocer las técnicas más habituales de los ataques, así como saber identificarlas. Todo ello mediante información, ejemplos prácticos y preguntas debate tipo test.

Durante la formación se describen las brechas y ataques más comunes en los entornos de trabajo llevándolo desde el entorno físico al entorno lógico, así como se abarcan los conceptos básicos de la seguridad IT.

Concienciación de usuarios

Beneficios

- Mejora de la comprensión de los escenarios de ataques de los eslabones más débiles
- Sesiones ágiles con participación activa de los asistentes
- A medida según tus infraestructuras (con casos aplicables)
- Sesiones online vía WebEx

¿Por dónde empezamos?

- Contratación y realización del test de Phishing por parte de nuestros analistas del SOC de modo remoto
- Contratación del servicio y comienzo de la formación

¿Hablamos?

¿Necesitas asesoramiento para saber qué soluciones de seguridad son las que necesita tu organización en este momento?

¿Quieres ampliar información de alguna solución o servicio concreto?

Contacta con nosotros ahora a través del siguiente formulario
o llámanos al 91 787 23 00

Estaremos encantados de ayudarte a
identificar, proteger, detectar, responder, recuperar y concienciar.

www.oneseq.es