MIGRACIÓN A SYMANTEC ENDPOINT PROTECTION 14

Cómo administrar la nueva plataforma de symantec endpoint protection manager

**Objetivo:** Transmitir a los asistentes el conocimiento en el uso de las herramientas tecnológicas para la administración y gestión diaria de la plataforma de seguridad Symantec EndPoint Protection Manager.

**Modalidades:**

1. Presencial en NextVision.
2. Remoto: Se podrá participar en modalidad remota.

 **Beneficios de la capacitación:**

* Brindada por personal certificado de NextVision.
* Los asistentes del curso tendrán el conocimiento necesario para poder administrar la nueva plataforma de Symantec Endpoint Protection Manager.
* Certificado de asistencia a los participantes.

**Capacitation Symantec Endpoint Protection Manager:**

El entrenamiento estará a cargo de personal certificado de NextVision. La capacitación propuesta está basada en el curso: “Symantec Endpoint Protection 14: Installation and Administration Guide”.

**Temario**

**1)      Nueva versión Symantec Endpoint Protection**

a. Nuevas tecnologías involucradas en SEP14

b. Capas de protección en el endpoint

c. Nuevos componentes de SEP 14

d. Políticas y conceptos asociados de Symantec

**2)      Migración de SEP Manager**

a. Requerimientos de Sistema.

b. Preparación de Servidores para la migración

c. Upgrade y configuración de SEP Manager

d. Descripción de la compatibilidad de versión y migración de SEPM

**3)      Migración de Clientes a SEP 14**

a. Requerimientos de clientes y métodos de actualización

b. Preparación para la migración de clientes según sistemas operativos

c. Características y configuraciones de los paquetes de instalación

d. Migración de clientes administrados

**4)      Configuración de Actualizaciones de LiveUpdate**

a. Introducción al servicio de LiveUpdate.

b. Configuración de LiveUpdate  para SEPM

c. Configuración de políticas de contenidos y LiveUpdate

d. Configuración de nuevas opciones de GUPs

**5)      Administración de las políticas de Protección Anti-Malware (incluidas técnicas de mitigación Ransomware)**

1. Definición y Configuración Intrusion prevention
2. Definición y Configuración Generic Exploit Mitigation
3. Configuración de políticas de Virus and Spyware Ptotection

-. Emulador, técnica de anti-evasión para detectar Malware oculto

1. Configuración de políticas de Preventing ransomware attacks con Download Insgight
2. Configuración de políticas de SONAR (prevención de ataques “zero-day”)
3. Administración de tecnología Tamper Protection
4. Configuración de Intelligent Threat Cloud Service
5. Mejores prácticas para remoción y protección de Ransomware

-. Advanced Machine Learning (AML) detección de malware basado en atributos

**6)      Administración de nuevas políticas de excepción**

a. Exclusiones y excepciones

b. Configuración de políticas de excepción

c. Creación de políticas de excepción en análisis

d. Creación de excepciones desde el log de eventos

**7)   Políticas de control de Aplicaciones y Dispositivos**

a. Creación de políticas de control de dispositivos y aplicaciones

b. Definición de control de aplicaciones

c. Modificar reglas de políticas

d. Definición del control de dispositivos

**8)   Personalización de la protección de amenazas de red y control de dispositivos y aplicaciones**

a. Herramientas para la personalización de la protección contra amenazas de red

b. Manejo de políticas de componentes

c. Configuración de “learned applications”

d. Configuración de “system lockdown”

**9)   Nueva interface Monitoreo y Reportes avanzados**

a. Sitio principal y nuevas características

b. Análisis y manejo de logs

c. Configuración y visualización de notificaciones

d. Creación y revisión de reportes

**Limitaciones:**

* La capacitación se realizará en días laborales de lunes a viernes de 9 a 18 Hs horario de Argentina (-03 GMT) exceptuando días feriados nacionales.

**Requerimientos capacitación remota:**

* Las asistentes deberán contar con un Notebook compatible a los requerimientos mínimos de producto.
* El cliente deberá contar para la conexión a la sesión remota, computadoras con disponibilidad de parlantes, micrófono y acceso a la plataforma https://global.gotomeeting.com/

**Duración y tiempos de capacitación:** 8 horas, 1 día hábil dentro del horario laboral de Argentina de 09 a 18 hs.