SYMANTEC ENDPOINT PROTECTION 14

PROPUESTA DE CAPACITACION

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) Exclusiva: Solo para el personal de la empresa que contrate la capacitación. Podrá realizarse on-site en oficinas del cliente o como opción en oficinas de NextVision.
2) Abierta: Para clientes de NextVision y por cupos. A realizarse en oficinas de NV.

Duración y tiempos de capacitación: 24 horas repartidas 3 días hábiles dentro del horario de 09 a 18 hs.

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.

Capacitación 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) **Solución de Producto Symantec Endpoint Protection**
   a. Tecnologías involucradas en Symantec
   b. Capas de protección en el endpoint

b. Servicios asociados a Symantec
c. Componentes de Symantec
d. Políticas y conceptos asociados de Symantec

2) Instalación de Symantec

a. Identificar los requerimientos de Sistema
b. Preparación de Servidores para la instalación
c. Instalación y configuración de SEP Manager
d. Descripción de la compatibilidad de versión y migración de SEPM

3) Configuración del entorno de SEPM

a. Inicio y navegación de SEPM
b. Descripción de tipos de políticas y componentes
c. Consola de Autenticación
d. Licenciamiento del entorno de SEPM

4) Instalación de Clientes

a. Requerimientos de clientes y métodos de instalación
b. Preparación para la instalación de clientes según sistemas operativos
c. Características y configuraciones de los paquetes de instalación
d. Instalación de clientes administrados
e. Configuración del detector de clientes no-administrados
f. Actualización de clientes Symantec

5) Administración de clientes y políticas.

a. Descripción de la comunicación entre clientes y SEPM
b. Administración de clientes
c. Configuración de Grupos
d. Configuración de localizaciones
e. Integración con Active Directory
f. Modos de configuración cliente
g. Configuración de dominios
h. Configuraciones generales de clientes

6) Configuración de Actualizaciones de Contenido.

a. Introducción al servicio de LiveUpdate
b. Configuración de LiveUpdate para SEPM
c. Configuración de políticas de contenidos y LiveUpdate
d. Configuración de GUPs
e. Actualización manual de definiciones de virus

7) Diseño de entorno de Symantec

a. Consideraciones de arquitecturas y dimensionamiento
b. Diseño de la arquitectura
c. Determinación de la relación clientes-SEPM
d. Métodos de distribución de contenidos
e. Dimensionamiento de la base de datos y SEPM

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

a. Definición y Configuración Intrusion prevention
b. Definición y Configuración Generic Exploit Mitigation
c. Configuración de políticas de Virus and Spyware Ptotection
    a. Emulador, técnica de anti-evasión para detectar Malware oculto
d. Configuración de políticas de Preventing ransomware attacks con Download Insgight
e. Configuración de políticas de SONAR (prevención de ataques "zero-day")
f. Administración de tecnología Tamper Protection
g. Configuración de Intelligent Threat Cloud Service
h. Mejores prácticas para remoción y protección de Ransomware
    a. Advanced Machine Learning (AML) detección de malware basado en atributos

9) Administración de 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

10) Introducción a la protección de amenazas de red, de aplicaciones y control de dispositivos.

a. Fundamentos de protección contra amenazas de red
b. Consideraciones de firewall
c. Prevención de intrusiones
d. Protección de acceso a aplicaciones

11) Manejo de políticas de Firewall

a. Introducción a las políticas de Firewall
b. Definición de reglas de componentes
c. Modificación de reglas de Firewall
d. Configuración de reglas predefinidas
e. Configuraciones integradas con Windows

12) Manejo de políticas de prevención de intrusiones

a. Como trabaja el IPS

b. Acerca de las firmas IPS
c. Configuración de prevención de intrusiones
d. Manejo de firmas personalizadas
e. Configuración de notificaciones en clientes
f. Utilización de Generic Exploit Mitigation

13) Manejo de 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

14) 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"

15) Configuración de Replicación, Failover y Balanceo de Carga

a. Conceptos básicos de Sitios y replicación
b. Como trabaja la replicación
c. Escenarios de replicación de SEPM
d. Configuración de la replicación
e. Conceptos de Failover y balanceo de carga

16) Administración del Servidor y la Base de Datos

a. Manejo de los Servidores SEPM
b. Mantenimiento de la seguridad de los servidores
c. Comunicación entre servidores
d. Manejo de los Administradores
e. Manejo de la Base de Datos
f. Técnicas de Recuperación de Desastres

17) Monitoreo y Reportes avanzados.

a. Monitoreo de páginas y sitio principal
b. Análisis y manejo de logs
c. Configuración y visualización de notificaciones
d. Creación y revisión de reportes

18) Administración de licencias

a. Como licenciar SEPM
b. Como cargar nuevas licencias
c. Administración del portal de licencias Symantec

19) Administración de entornos virtuales

a. Mejores prácticas para administración de entornos virtuales
b. Auto-protección en entornos virtuales
c. Análisis programados
d. Configuración de grupos
e. Identificación de equipos virtuales

Limitaciones:

- La capacitación será realizada de forma on-site en oficinas del cliente o en oficinas de NextVision, según los requerimientos.
- La capacitación se realizará en días laborales de lunes a viernes de 9 a 18 Hs horario de Argentina exceptuando días feriados nacionales.

Requerimientos:

- En los casos donde la capacitación se realice en las oficinas del cliente el mismo deberá contar con una sala de capacitación y un proyector con entrada HDMI.
- Las asistentes deberán contar con un Notebook compatible a los requerimientos mínimos de producto.