Temario

Trend Micro Apex One SaaS

Insurgentes Sur 1524, Piso 4 / Col Crédito Constructor
Del. Benito Juárez / 03940 México D.F. / T. 5524 8908
www.novasistemas.com.mx

Contenido del curso

1. Introducción

1.1. Acerca de Apex One
Características, módulos, componentes, esquema de comunicación

1.2. La consola web
Requerimientos

1.3. Agente de Apex One
Estructura de menús, árbol de agentes y dominios, navegación en general

1.4. Dashboard
Widgets más comunes

2. Trend Micro Smart Protection

2.1. Acerca de Trend Micro Smart Protection Network
Conceptos

3. Agente de Apex One

3.1. Instalación de agentes
Consideraciones de instalación, despliegue y comunicación

3.2. Post-Instalacion
Revisión en agregar/quitar programas, servicios, actualización y prueba EICAR

3.3. Migración de agentes a un nuevo servidor
Como mover agentes a otro servidor

3.4. Desinstalación de agentes
Proceso de desinstalación de agente

4. Actualización

4.1. Componentes de Apex One
Antivirus, Anti-spyware, Damage Cleanup, Behavior Monitoring, Suspicious Connections, Browser Exploit, Web Reputation

4.2. Actualizaciones del servidor de Apex One
Como actualizar el servidor, actualización manual y automática

4.3. Actualizaciones de agente
Fuentes de actualización y Agent update

5. Escaneos de detección riesgos de seguridad

5.1. Tipos de riesgos de seguridad
Virus & Malware: jokes, packers, ransomware, rootkit, test virus, trojan, boot sector, File infector, Java malicious code, macro, scripts gusanos, virus de red.

Spyware & Grayware: Adware. Dialers, Hacking tool, RAT, Password cracking

5.2. Métodos de escaneo

Smart Scan & Conventional Scan. Configuración común en todos los tipos de escaneo: real time, manual, scheduled. Exclusiones

5.3. Privileges and other settings

Opciones de configuración

5.4. Global Scan Settings

Opciones de configuración

5.5. Notificaciones sobre riesgos de seguridad

Para servidor:Email, SNMP, Windows Event

Para cliente: Violaciones de seguridad

5.6. Logs

Revisión de logs: Virus, Spyware, Suspicious File.

6. Protección ante amenazas no conocidas

6.1. Predictive Machine Learning

Concepto y tipos de detección. Configuración

6.2. Suspicious Connection Service

Concepto y listas. Configuración

6.3. Sample Submission

Configuración

6.4. Logs de amenazas no conocidas

Revisón de logs

7. Behavior Monitoring

7.1. Behavior Monitoring

Concepto y configuración

Revisión de logs

8. Device Control

Conceptos, permisos para dispositivos de almacenamiento y configuración

Revisión de logs

9. Web Reputation

9.1. Amenazas web & servicio alertas de command & control

Conceptos y características. Configuración

Revisión de logs WRS y C&C

10. Administración del servidor de Apex One

10.1. Licenciamiento

10.2. Administración basada en roles

10.3. Lista de objetos sospechosos

10.4. Administración de logs y notificaciones

10.5. Configuración agente - servidor

10.6. Administración de cuarentena

11. Administración de agentes Apex One Agent

11.1. Endpoint Location

11.2. Configuración de proxy

11.3. Información sobre agentes

11.4. Importación y exportación de configuración

11.5. Cumplimiento de seguridad

12. Recursos para la resolución de problemas

12.1. Case Diagnostic Tool

12.2. Performance Tunning tool

13. Data Loss Prevention

13.1. Políticas de DLP

Configuración reglas, plantillas, canales, acciones, excepciones e identificadores de datos (Expresiones, atributos de archivos, lista de palabras claves).

13.2. Logs de DLP

Revisión de logs