TEMARIO DEL CURSO

Splunk Enterprise 9.0 Data Administration

21 horas

El curso forma al alumno en la administración de datos en entornos Splunk Enterprise.

A QUIÉN VA DIRIGIDO

- Administradores de Splunk responsables de la ingesta de datos en los indexadores
- Profesionales que han completado el curso Splunk Enterprise System Administration

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.
Ingesta de datos en Splunk

- Descripción general de Splunk y el modelo distribuido
- Tipos de inputs de datos y configuración de metadatos
- Configuración inicial de inputs con Splunk Web
- Prueba de índices con input staging

MÓDULO 02.
Archivos de configuración y apps

- Archivos de configuración y directorios de Splunk
- Precedencia en tiempo de índice y tiempo de búsqueda
- Validación y actualización de archivos de configuración
- Apps de Splunk e instalación de apps

MÓDULO 03.
Configuración de forwarders

- Configuración de Universal Forwarders
- Configuración de Heavy Forwarders

MÓDULO 04.
Personalización de forwarders

- Configuración de forwarders intermedios
- Opciones adicionales de forwarders

MÓDULO 05.
Gestión de forwarders

- Splunk Deployment Server: descripción y uso
- Gestión de forwarders con deployment apps
- Configuración de deployment clients y grupos de clients
- Supervisión de actividades de gestión de forwarders

MÓDULO 06. **Inputs de monitorización**	• Creación de inputs de monitorización de archivos y directorios • Configuración opcional de inputs de monitor • Despliegue de inputs de monitor remotos
MÓDULO 07. **Inputs de red**	• Creación de inputs de red TCP y UDP • Opciones de configuración para inputs de red
MÓDULO 08. **9. Inputs scriptados y agentless**	• Creación de inputs scriptados básicos • Configuración del HTTP Event Collector (HEC) agentless • Splunk App for Stream
MÓDULO 09. **Inputs de sistema operativo**	• Inputs específicos de Linux • Inputs específicos de Windows
MÓDULO 10. **12. Ajuste fino e inputs y fase de parsing**	• Procesamiento predeterminado durante la fase de input y parsing • Configuración del salto de línea de eventos • Gestión de timestamps y zonas horarias • Data Preview para validación de eventos
MÓDULO 11. **14. Manipulación y enrutamiento de datos**	• Métodos de transformación Splunk • Creación de reglas con Ingest Actions • Enmascaramiento de datos con Ingest Actions, SEDCMD y TRANSFORMS • Filtrado y enrutamiento de datos con Ingest Actions y TRANSFORMS
MÓDULO 12. **Soporte de knowledge objects**	• Extracciones de campo en tiempo de búsqueda e índice • Gestión de knowledge objects huérfanos