TEMARIO DEL CURSO

Splunk Enterprise 9.0 System Administration

14 horas

El curso forma al alumno en la administración del entorno Splunk Enterprise. El trabajo se organiza en torno al conocimiento del license manager, los indexadores y los search heads, cubriendo la configuración, gestión y supervisión de los componentes principales de la plataforma.

A QUIÉN VA DIRIGIDO

- Administradores de sistemas responsables de gestionar el entorno Splunk Enterprise
- Profesionales de operaciones IT que trabajan con plataformas de análisis de datos

EL CURSO INCLUYE

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

TEMARIO

MÓDULO 01.
Despliegue de Splunk

- Descripción general de Splunk
- Componentes de Splunk Enterprise y tipos de despliegue
- Requisitos previos de instalación
- Pasos de instalación de Splunk
- Uso de comandos CLI de Splunk
- Prácticas recomendadas de seguridad

MÓDULO 02.
Supervisión de Splunk

- Uso del Splunk Health Report
- Habilitación y uso de la Monitoring Console
- Uso de Splunk Diag y Rapid Diag

MÓDULO 03.
Licencias de Splunk

- Tipos de licencias de Splunk
- Descripción de violaciones de licencia
- Instalación de una licencia Splunk
- Configuración del License Manager, License Peers y License Pools
- Gestión de avisos de licencia y supervisión del uso

MÓDULO 04.
Archivos de configuración

- Estructura del directorio de configuración de Splunk
- Proceso de capas de configuración (index time y search time)
- Uso de herramientas como btool para examinar configuraciones

MÓDULO 05.
Aplicaciones

- Descripción de apps y add-ons de Splunk
- Instalación de una app en una instancia Splunk
- Gestión de accesibilidad y permisos de apps

MÓDULO 06.
Creación de índices

- Funcionamiento de los índices de Splunk
- Tipos de buckets de índice
- Creación y trabajo con índices
- Índices de métricas

MÓDULO 07.
Gestión de índices

- Conceptos básicos de gestión de índices
- Recomendaciones de retención y backup de datos
- Mover y eliminar datos de índice
- Uso del fishbucket y restauración de frozen buckets

MÓDULO 08.
Gestión de usuarios

- Roles de usuario en Splunk
- Adición de usuarios con autenticación nativa
- Creación de roles personalizados
- Gestión de usuarios en Splunk

MÓDULO 09.
Configuración de forwarding básico

- Pasos de configuración del forwarder
- Configuración de un Universal Forwarder
- Gestión de agentes

MÓDULO 10.
Configuración de búsqueda distribuida

- Configuración de búsqueda distribuida
- Roles del search head y los search peers
- Uso de la Monitoring Console para supervisar la actividad de búsqueda
- Cuarentena de search peers
- Opciones para múltiples search heads
- Prácticas recomendadas de búsqueda distribuida
- Casos de uso de Federated Search