Análisis de datos con splunk>

Bienvenidos al curso **Análisis de datos con Splunk.** Encontrarás esta guía en el temario del curso para que puedas consultarla en cualquier momento.

N.º Horas: 30 Fecha Inicio:X Fecha Fin: X

Objetivos del curso

Splunk es un software que permite indexar y consultar datos generados en cualquier tipo de máquina o sistema de forma masiva y escalable. Sus capacidades de búsqueda, monitorización y análisis de datos en tiempo real a través de una interfaz web o de forma programática a través de APIs, lo convierten en una de las soluciones de Big Data más avanzadas y globalmente utilizadas en empresas punteras en todo el mundo.

Originalmente Splunk comenzó su andadura enfocándose en área de la seguridad informática, pero rápidamente sus casos de uso se extendieron a la gestión de las operaciones IT, el análisis de patrones de consumo, el IoT o el DevOps entre otros.

En lo que se refiere a sus funcionalidades, Splunk permite sacar el máximo partido de los datos que indexa mediante la creación de búsquedas distribuidas de alto rendimiento, la generación de dashboards y reportes 100% personalizables, el enriquecimiento de datos a través de fuentes externas o la generación automatizada de alertas. Todos estos ingredientes han convertido a Splunk en una herramienta imprescindible y muy valorada en la mayoría de los perfiles de profesionales IT que el mercado demanda.

Objetivos

- Configurar un entorno de Splunk en Windows y Linux
- Comprender las distintas versiones y arquitecturas de Splunk
- Comprender los conceptos básicos de SPL (Search Processing Language)
- Crear reportes, dashboards y alertas con Splunk
- Profundiza los conocimientos adquiridos realizando tareas prácticas

Requisitos

- Conocimientos básicos sobre Linux y Windows son útiles pero no imprescindibles
- Experiencia previa con la línea de comandos de Linux sería útil pero no imprescindible
- Personas con que tengan interés en el mundo del análisis de datos y el Big Data
- Personas que deseen aprender los conceptos básicos de Splunk con fines personales o profesionales
- Personas que deseen certificarse en Splunk y quieran dominar los conceptos básicos antes de empezar a preparar dichas certificaciones

Plataforma de formación

Cada alumno ha recibido un email con los datos de acceso a la plataforma. Además de a este curso todos los alumnos matriculados con TrainingIT tienen acceso al curso **"Conociendo la plataforma TrainingIT"**. Este curso está conformado por una serie de videos cortos donde se explican las principales **funcionalidades de la plataforma.**

Resumen de contenidos

El curso está dividido en **4 módulos** temáticos. Puedes consultar el temario al final de esta guía.

En cada módulo puede encontrar diferentes elementos:

-Apuntes de la lección

-Videos teórico-prácticos

-Código de la lección

- Test

- Otros recursos

Además, el curso cuenta con un **ejercicio práctico voluntario** que se debe desarrollar durante el curso y que el profesor corregirá y evaluará al finalizar el curso.

Profesor

Alejandro Gómez. Cuenta con más de 9 años de experiencia en el campo de la ciberseguridad y el análisis de datos. A lo largo de su carrera ha trabajado proyectos de distinta índole incluyendo la implantación de sistemas SIEM para la correlación y análisis de datos de ciberseguridad, el hacking ético, la revisión de seguridad en entornos de control industrial, la implementación de medidas de seguridad en entornos cloud y el desarrollo de soluciones de seguridad basadas en infraestructura como código.

Actualmente trabaja como Senior Security Engineer en la compañía farmacéutica Roche Farma. Complementa su actividad profesional con la docencia, a través de su participación en diversas formaciones, y es autor de varios cursos e-learning relacionados con el mundo IT.
En el plano personal, es un apasionado de la música, el deporte y los viajes, aprovechando cualquier oportunidad para hacer una escapada y conocer nuevos lugares y culturas.

Enrique Pascual y **Beatriz Pino**, actuarán como gestores del curso en todo lo relacionado con la plataforma de formación. Te puedes poner en contacto vía mensaje a través de la plataforma, o directamente en **epascual@trainingit.es** o **bpino@trainingit.es**.

A todos ellos los puedes encontrar en la sección **"Participantes"** del curso con sus respectivos roles.

Calendario del curso

El curso comienza el **X** y la fecha de finalización será el **X**, último día en que se podrá entregar la práctica final.

A partir de esa fecha los profesores dejarán de participar en los foros del curso.

Si no lo terminas a tiempo, seguirás teniendo acceso a la plataforma con todo el material disponible. Pero no tendrás a los profesores a tu disposición, aunque sí a otros alumnos que puedan estar en tu misma situación.

Para facilitar el seguimiento del mismo se establece un calendario de temas que semanalmente será anunciado en la plataforma. No obstante, a ser un curso online cada alumno puede seguir el ritmo que mejor se adapte a sus necesidades.

Mediante el foro de avisos se os informará todas las semanas de la programación del curso. En el calendario de la plataforma tendréis marcadas todas las fechas importantes del curso.

Consejos para aprovechar tu curso

1. **Lee toda la documentación relacionada con el curso**
   Antes de comenzar, dedica tiempo a revisar toda la información proporcionada: guías, temarios, requisitos técnicos, y objetivos del curso. Esto te dará una visión clara de lo que se espera de ti y cómo organizarte.

2. **Utiliza un segundo monitor**
   Si es posible, configura un segundo monitor. Esto te permitirá seguir las clases en uno mientras practicas o tomas apuntes en el otro, optimizando tu experiencia de aprendizaje.

3. **Revisa los temas y sus elementos antes de empezar**
   Antes de ver las clases, explora los materiales asociados a cada tema: videos, lecturas, ejercicios, o recursos adicionales. Esto te ayudará a identificar conceptos clave y planificar tu aprendizaje.

4. **Haz un primer visionado de los videos**
   Visualiza los videos del curso de manera inicial, prestando atención al contenido global. No te preocupes por detenerte en cada detalle; el objetivo es obtener una comprensión general del tema.

5. **Realiza un segundo visionado siguiendo los pasos del profesor**
   En el segundo visionado, pausa el video según sea necesario y sigue los pasos del instructor. Reproduce las explicaciones en tu entorno, asegurándote de comprender y aplicar los conceptos explicados.

6. **Practica lo aprendido con otros casos y busca información adicional**
   No te límites a los ejercicios del curso. Aplica los conocimientos adquiridos en casos prácticos nuevos. Además, complementa tu aprendizaje investigando en internet, explorando foros, blogs, y tutoriales relacionados con los temas del curso.

7. **Participa activamente en el foro del curso**

   El foro del curso es una herramienta fundamental para resolver dudas, compartir experiencias y aprender en comunidad. Úsalo para plantear preguntas claras y específicas sobre los temas del curso, mencionando el módulo o ejercicio en cuestión para facilitar la respuesta del profesor. Antes de preguntar, revisa si alguien ya ha planteado una duda similar, y si tienes conocimientos o experiencias útiles, comparte tus propias respuestas para contribuir al aprendizaje de tus compañeros. Además, aprovecha el feedback del profesor, que estará disponible para aclarar conceptos y guiarte en tu progreso, enriqueciendo aún más la experiencia formativa.

Tutorías

El **"Foro de Dudas y Consultas"** es el centro de las tutorías del curso. Todas tus dudas relacionadas con el temario debes plantearlas en el foro ya que también ayudarán a otros compañeros, y otros compañeros podrán ayudarte a ti.

Al tratarse de un foro no existe un horario de tutorías. Se responderá en un plazo de 24 horas laborables. ***Utilizad siempre el foro***.

Enrique Pascual y **Beatriz Pino**, actuarán como gestores del curso en todo lo relacionado con la plataforma de formación. Te puedes poner en contacto vía mensaje a través de la plataforma, o directamente en **epascual@trainingit.es** o **bpino@trainingit.es**.

Práctica final voluntaria y examen teórico

El curso cuenta con un **ejercicio práctico final voluntario** que será corregido por el profesor.

Durante el curso se realizarán varias **pruebas de conocimientos obligatorias** mediante un examen de autoevaluación con preguntas tipo test.

Evaluaciones

En el curso habrá dos áreas de evaluación cada una con una influencia en la nota final del curso:

- ***Práctica final: 40%***
- ***Examen teórico: 60%***

Las calificaciones se podrán visualizar en el apartado **"Calificaciones"** del curso.

Certificado

El curso ofrece dos tipos de certificados:

- **Certificado de asistencia**: para aquellos alumnos que realicen el curso, pero no entreguen el ejercicio práctico voluntario.
- **Diploma acreditativo:** con evaluación positiva en las actividades realizadas en el curso para aquellos alumnos que realicen el ejercicio práctico y cuya calificación final de curso (Test+ Práctica) sea superior a 6.

Los certificados se entregarán una vez finalice el plazo del curso y se revisen que se cumplen todas las condiciones.

Bonificación

Para la evaluación y seguimiento del alumnado, la plataforma de Teleformación provee dos tipos de mecanismos distintos:

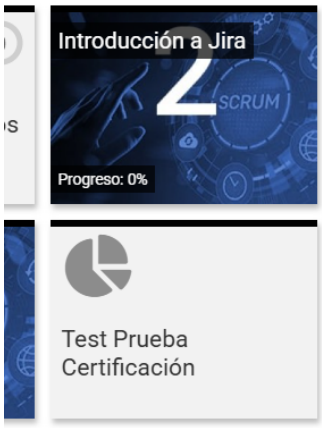
Sistemas de control internos del Aula Virtual. La plataforma registra la actividad del alumno dentro de la plataforma, obteniendo datos como:

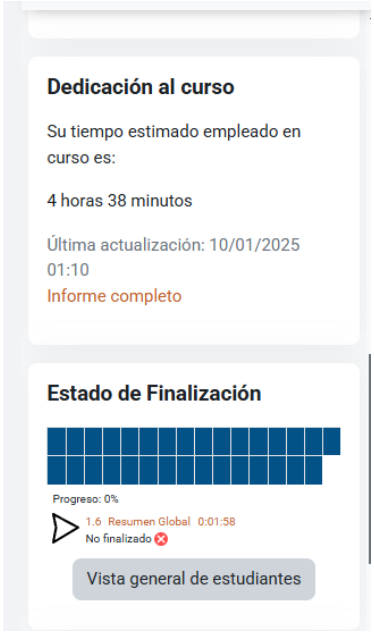
- ***Acceso del alumno a los distintos módulos del curso***
- ***Días de acceso y clics realizados dentro del curso***
- ***Tiempo total empleado en el curso***
- ***Seguimiento de las lecciones visualizadas***
- ***Seguimiento de los recursos utilizados***
- ***Evaluación obtenida en cuestionarios de autoevaluación***

Los alumnos que vayan a bonificar el curso a través de sus empresas deberán cumplir lo siguiente:

- Completar al menos el **75% de las actividades** del curso.
- Completar al menos el **75% de las pruebas** obligatorias del curso (test)
- Los **tiempos de conexión** a la plataforma deben ser iguales o superiores al **75%** del tiempo de estudio estimado del curso (el tiempo estimado de estudio se indica en la cabecera de esta guía y en la cabecera del propio curso).

Los alumnos pueden observar su progreso en el curso dentro de la plataforma en los bloques "**Dedicación al curso"** y **"Estado de Finalización"** que aparece en los menús laterales de la derecha de la pantalla.





- Desplegar menú lateral.

Acerca de TrainingIT

TrainingIT es una iniciativa para ofrecer formación especializada IT de alta calidad y bonificable por Fundae.

Descubre nuestros cursos online creados por especialistas en sus materias en www.trainingit.es.

Queremos formar a los mejores profesionales para que no se diga que en España no hay talento.

Te agradecemos que hayas confiado en TrainingIT para tu formación. Esperamos que este curso sea de tu agrado y que te ayude en tu carrera profesional.

Un saludo,

Enrique Pascual

epascual@trainingit.com

Gestor de Curso

Temario

1. Introducción, componentes e instalación

1.1 ¿Qué es Splunk?

1.2 Componentes básicos de Splunk

1.3 Versiones y arquitecturas

1.4 Instalando Splunk en Windows

1.5 Instalando Splunk en Linux

1.6 Introduciendo datos en splunk

2. Búsquedas y lenguaje SPL

2.1 Búsquedas básicas

2.2 Utilizando campos en las búsquedas

2.3 Mejores prácticas para optimizar las búsquedas en Splunk

2.4 Lenguaje de búsqueda de Splunk

3. Comandos y funciones más comunes de SPL

3.1 Comandos fields y table

3.2 Comandos rename y dedup

3.3 Comandos sort, top y rare

3.4 Comando stats y funciones count y dc

3.5 Función sum y avg

3.6 Funciones list y value

4. Reportes, dashboards y alertas

4.1 Reportes y visualizaciones

4.2 Dashboards

4.3 Pivotes y sets de datos

4.4 Creando y utilizando Lookups

4.5 Alertas