Publicatiedatum : 15/01/2024

# Opleiding : Splunk, operationele gegevensanalyse

***Praktijkcursus - 3d - 21u00 - Ref. PUK***
***Prijs : 2100 € V.B.***

4,2 / 5

BEST

Splunk is een tool die bedoeld is om ons te helpen relevante informatie te verzamelen en te sorteren: een tool die zou kunnen worden omschreven als een [[event correlator]]. Deze training stelt u in staat om gegevens te configureren, analyseren en rapporten te genereren op basis van uw aangepaste waarschuwingen.

## Pedagogische doelstellingen

**Aan het einde van de training is de deelnemer in staat om:**

- Splunk gebruiken om gegevens te verzamelen, analyseren en erover te rapporteren
- Verrijk operationele gegevens met zoekopdrachten en feeds
- Creëer realtime, gescripte en andere intelligente waarschuwingen
- Geavanceerde JavaScript-afbeeldingen integreren
- De Splunk API gebruiken

## Doelgroep

Systeem- en netwerkbeheerders.

## Voorafgaande vereisten

Basiskennis van netwerken en systemen.

## Opleidingsprogramma

**DEELNEMERS**

Systeem- en netwerkbeheerders.

**VOORAFGAANDE VEREISTEN**

Basiskennis van netwerken en systemen.

**VAARDIGHEDEN VAN DE CURSUSLEIDER**

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

**BEOORDELINGSMODALITEITEN**

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

## 1 Splunk configureren

- Een Splunk.com-account verkrijgen.
- Splunk installeren op Windows.
- Indexeer bestanden en mappen via de webinterface, CLI of configuratiebestanden.
- Verkrijg gegevens via netwerkpoorten, script of modulaire ingangen.
- Implementatie van de Universal Forwarder.

### Praktisch werk

Splunk configureren. Veldextracties, gebeurtenistypes en labels definiëren.

## 2 Datamining

- SPL-query's. Booleaanse operatoren, commando's.
- Zoeken met tijdsloten.

### Praktisch werk

De meest bezochte webpagina's, de meest gebruikte browser, de meest bezochte sites, enz. uit logbestanden halen.

## 3 Dashboards

- Dashboards en operationele intelligentie, die de gegevens naar buiten brengen. Soorten grafieken.

### Praktisch werk

Maak en verbeter een dashboard met grafieken die gekoppeld zijn aan het uitgevoerde onderzoek.

## 4 Nieuwe toepassing

- Installeer een bestaande toepassing van Splunk of een derde partij.
- Dashboards en zoekopdrachten toevoegen aan een applicatie.
- Interactieve dashboards.
- Produceer regelmatig (geplande) dashboards in PDF-indeling.

### Praktisch werk

Een nieuwe Splunk-toepassing maken. Installeer een toepassing en bekijk gebeurtenissen met betrekking tot Cisco-switches.

## 5 Gegevensmodellen

- Gegevensmodellen.
- Maak optimaal gebruik van reguliere expressies.
- Zoekprestaties optimaliseren.
- Gegevens draaien.

### Praktisch werk

Gebruik de pivotopdracht in de modellen om de gegevens weer te geven.

**PEDAGOGISCHE EN TECHNISCHE MIDDELEN**

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

**TOEGANGSMODALITEITEN EN TERMIJNEN**

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

**TOEGANKELIJKHEID VOOR MINDERVALIDEN**

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

### 6 Gegevensverrijking

- Groeperen van gerelateerde gebeurtenissen, begrip transactie.
- Maak gebruik van verschillende gegevensbronnen.
- Relaties tussen velden identificeren.
- Toekomstige waarden voorspellen.
- Ontdek abnormale waarden.

**Praktisch werk**
Praktische toepassing van diepgaand databaseonderzoek.

### 7 Soorten waarschuwingen

- Gecontroleerde omstandigheden.
- Actie ondernomen na een bevestigde waarschuwing.
- Wees proactief met waarschuwingen.

**Praktisch werk**
Voer een script uit wanneer de webserverfout 503 optreedt en schrijf de details van de gebeurtenis naar een bestand.

## Data en plaats

**KLAS OP AFSTAND**
2026 : 25 maa., 1 juni, 16 sep., 2 dec.

**PARIS LA DÉFENSE**
2026 : 1 juni, 16 sep., 2 dec.