Splunk Administrator

Function type:	Freelance	**Location:**	Brussels
Duration:		**Reference:**	202007899

Description:

Splunk what???
Yes indeed, we are looking for a Splunk Administrator who will take the day-to-day accountability for the Splunk platform (v7) made of two forwarders, 10 clustered indexers, 2 x 3 clustered search heads, with the same setup duplicated in the lab and UAT.

You know what this is about??? Ok, you earned already one point, please continue

You will work together with the other Splunk resources within our company to maintain this system (in production and in the lab) and make it evolve according to users requirements: implement specific filtering, dashboards, integrate new data sources or adapt processing for existing ones (e.g. due to software upgrades in the network).

For the internal developer community we have The Elastic Stack (ELK) in place. Knowledge or willingness to learn to maintain and extend this environment is a strong asset.

Your responsibilities:
As Splunk Administrator, you will be responsible for:
• Deploy newer versions of the various components when appropriate: for bug fixes, to get relevant new features, etc.
• Recommend changes to the architecture when appropriate and implement them once approved.
• Maintain a clear documentation of the whole platform: components, versions, data flows, data sources, etc.
• Interact directly with the users (network operations personnel): capture new requirements and defects into Jira tickets, prioritize these, implement, test, deploy fixes and new features.
• Administer the developer ELK instance

Hello, you're still with us??? Perfect, now if you understood the above, maybe check out the skills we need. 1 and 1 is 2 so there might be a fit!

Requirements:

Your skills:
You have a proven experience of at least 2 years as a Splunk Administrator.
This experience covers a.o. following technical skills:

• Expert level knowledge of the Splunk suite with ability to define the best suited architecture for our needs, install, configure, develop, monitor and troubleshoot the whole platform. More specifically:
• Architecture administration and design (plus: Splunk Certified Architect certification)
• General Splunk administration (plus: Splunk Certified Admin certification)
• Searching, reporting and management of data and knowledge objects (plus: Splunk Certified Power User certification)

• Creation and modification of custom apps
• Optionally: Splunk Enterprise Security
• Programming/scripting experience in Python
• Some level of telecoms and networking skills is a plus since it helps to understand the contents of the data
• Comfortable working in a Linux environment

Your profile:
• You have a proven experience of at least 2 years as a Splunk Administrator
• You have great ability to understand the business requirements and converting them into solution designs.
• You’re quality oriented
• You’re open minded team player, ready to adapt to the changing needs
• You have great communication skills
• You’re committed to deliver, pragmatic and solution oriented.
• Experience in a Wholesale environment is a plus
• Languages: English (very good in reading, writing, speaking) is a must. French or Dutch is a plus

Voila, you don't need to know more! If you have read the above, understand what we are talking about, have the right skills, are looking for a new project, don't hesitate and apply.