Week 3 Splunk Questions

Key knowledge/skills: common attributes selection & Splunk SPL commands

Exercise 1. Add network data “tcp_stream_2500.csv” in Splunk, and name the index as “tcp_stream_2500”.

Q1. Select the common attributes/fields, they should be able to describe the events in terms of Who, What, When and Where (hint: “app” field is useful in the absence of “protocol”).

Q2. List all the IP addresses that run HTTP over non-standard port (hint: dest_port != 80), with the event counts.

Q3. What’s the Skype server IP address?

Assignment Project Exam Help

Exercise 2. Add endpoint data “symantec_ep_trafffic_file.csv” in Splunk, and name the index as “symantec_ep_trafffic_file”.

https://tutorcs.com

Q1. Select the common attributes/fields, they should be able to describe the events in terms of Who, What, When and Where.

WeChat: cstutorcs

Q2. List all the blocked traffic detailing src_ip, dest_ip, Network_Protocol, and user information.