Question 1

In Search Processing Language (SPL), which special character is a wildcard that can be used to substitute with any other character? 1 / 1 point

=

|

*

!=

Correct

In Search Processing Language (SPL), the * character is a wildcard which is a special character that can be substituted with any other character.

Question 2

Which of the following steps are part of the security information and event management (SIEM) process? Select three answers. 1 / 1 point

Normalize data so it is ready to read and analyze

Correct

The SIEM process involves the following steps: collect and process data, normalize data, and index data. Normalizing data formats it in a consistent way that only includes relevant information.

Monitor activity and alerts related to intrusions

Index data to improve search performance

Correct

The SIEM process involves the following steps: collect and process data, normalize data, and index data. Indexing data improves search performance by creating a searchable index of data.

Collect and process data

Correct

The SIEM process involves the following steps: collect and process data, normalize data, and index data. SIEM tools collect and process data that is generated by devices and systems from all over an environment.

Question 3

Fill in the blank: Chronicle uses ______ to search through unstructured logs. 1 / 1 point

metadata

unified data model

entity search

raw log search

Correct

Chronicle uses raw log search to search through unstructured logs.

Question 4

Which of the following is Splunk's query language? 1 / 1 point

SPL

UDM

IDS

SQL

Correct

Splunk uses its own query language known as Search Processing Language (SPL).