KPLABS Course

Splunk 2021 - Beginner to Architect

Domain 10

ISSUED BY
Zeal

REPRESENTATIVE
instructors@kplabs.in

Domain 10 - Advanced Splunk Concepts

Module 1: Using Btool for Troubleshooting

1.1 Need of btool

The Splunk Enterprise configuration file system supports many overlapping configuration files in many different locations.

This flexibility can make it hard to figure out exactly which configuration value Splunk Enterprise is using.

1.2 Overview of btool

btool is a command-line tool that can help us troubleshoot configuration file issues or see what values are being used by your Splunk Enterprise installation.

btool shows you the merged settings in the .conf files

.

Module 2: Overview of Data Models

2.1 Basic Problem Overview

You have data that contains certain critical business indicators.

The data structure is multi-layered and complicated.

The users who want to see business indicators are less technical.

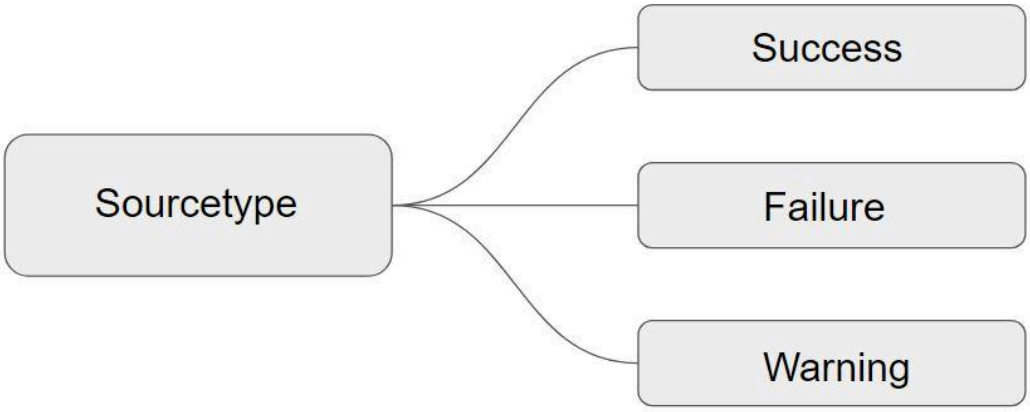
You don’t want to be a point of contact for everything they want out of data.

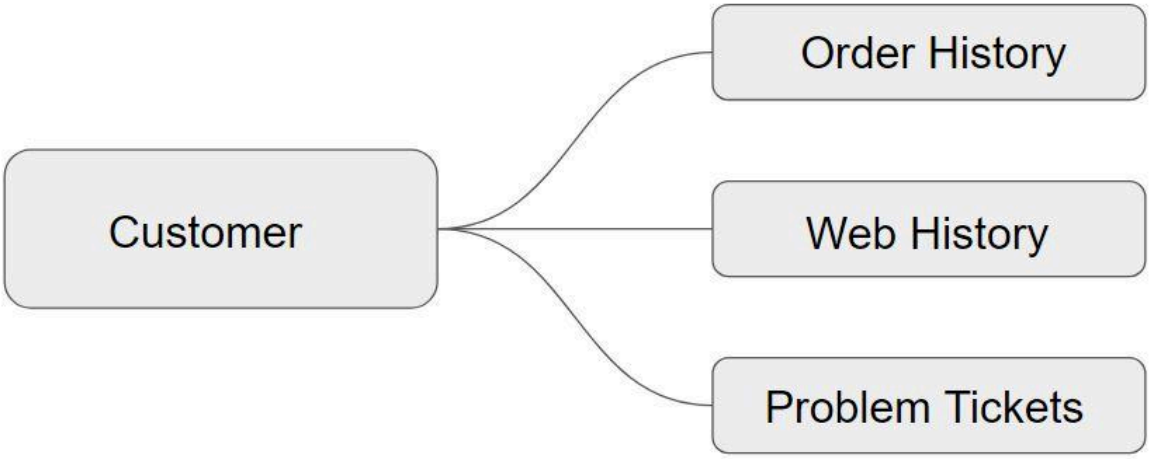
2.2 Searches can be long and complex

```
sourcetype=aws:cloudtrail eventName=RunInstances errorCode=success | bucket span=10m _time | stats count AS instances_launched by _time userName | eventstats avg(instances_launched) as total_launched_avg, stdev(instances_launched) as total_launched_stdev | eval threshold_value = 4 | eval isOutlier=if(instances_launched > total_launched_avg+(total_launched_stdev * threshold_value), 1, 0) | search isOutlier=1 AND _time >= relative_time(now(), "-10m@m") | eval num_standard_deviations_away = round(abs(instances_launched - total_launched_avg) / total_launched_stdev, 2) | table _time, userName, instances_launched, num_standard_deviations_away, total_launched_avg, total_launched_stdev
```

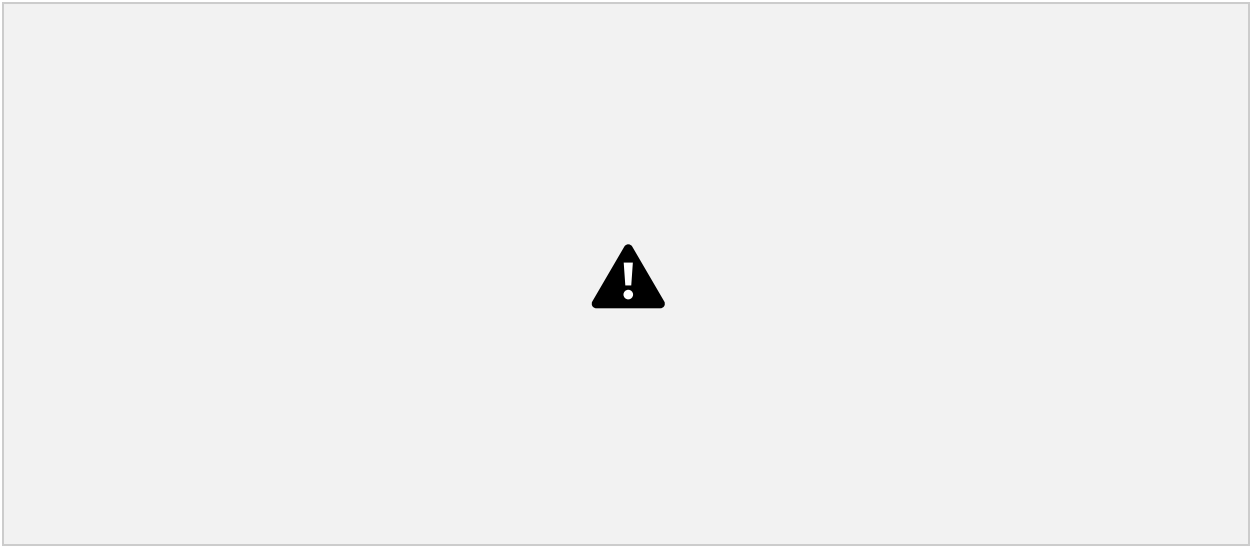
2.3 Basics of Data Model

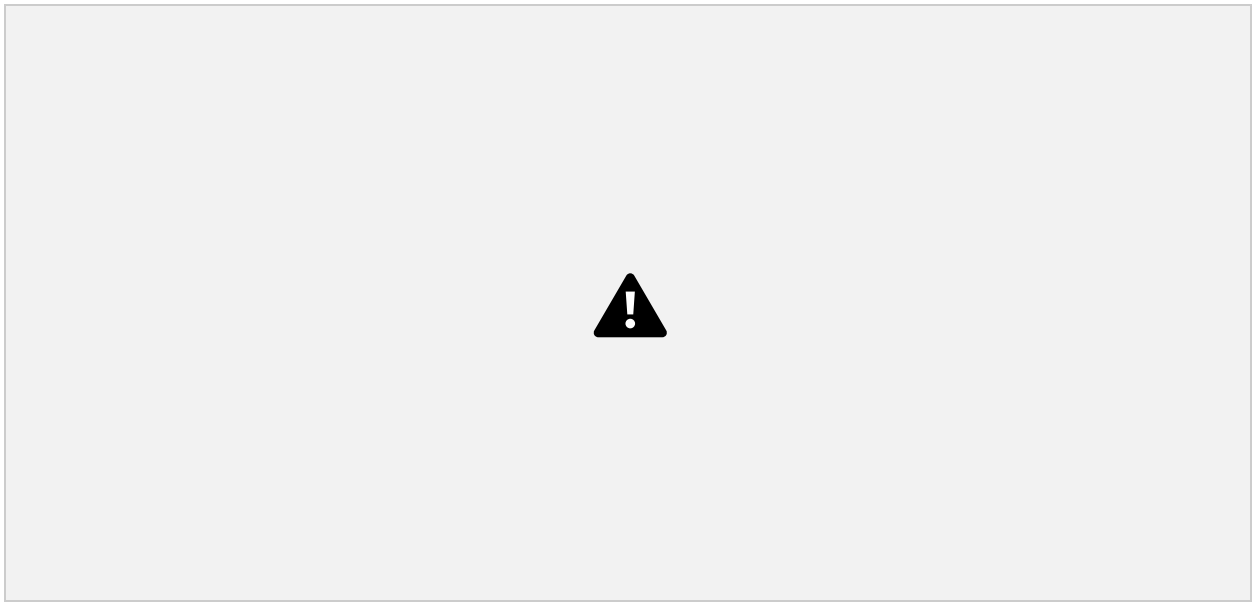
Data Model allows us to provide a meaningful representation of underlying raw data.

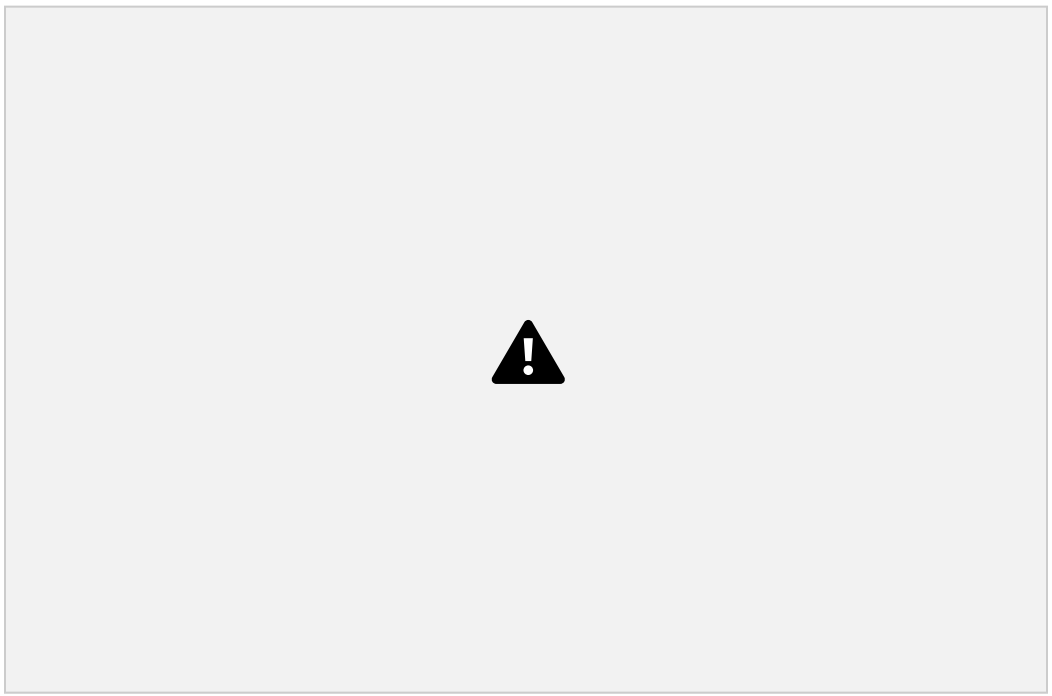




The following diagram shows details about the Vulnerability data model







.Module 3: Splunk Support Programs

Splunk offers a variety of support plans for customers.

These are primarily divided into the following categories:

- Community
- Base
- Standard
- Premium

Join Our Discord Community

We invite you to join our Discord community, where you can interact with our support team for any course-based technical queries and connect with other students who are doing the same course.

Joining URL:

http://kplabs.in/chat