Introduction to Big Data

ECAP456

Dr. Rajni Bhalla

Associate Professor

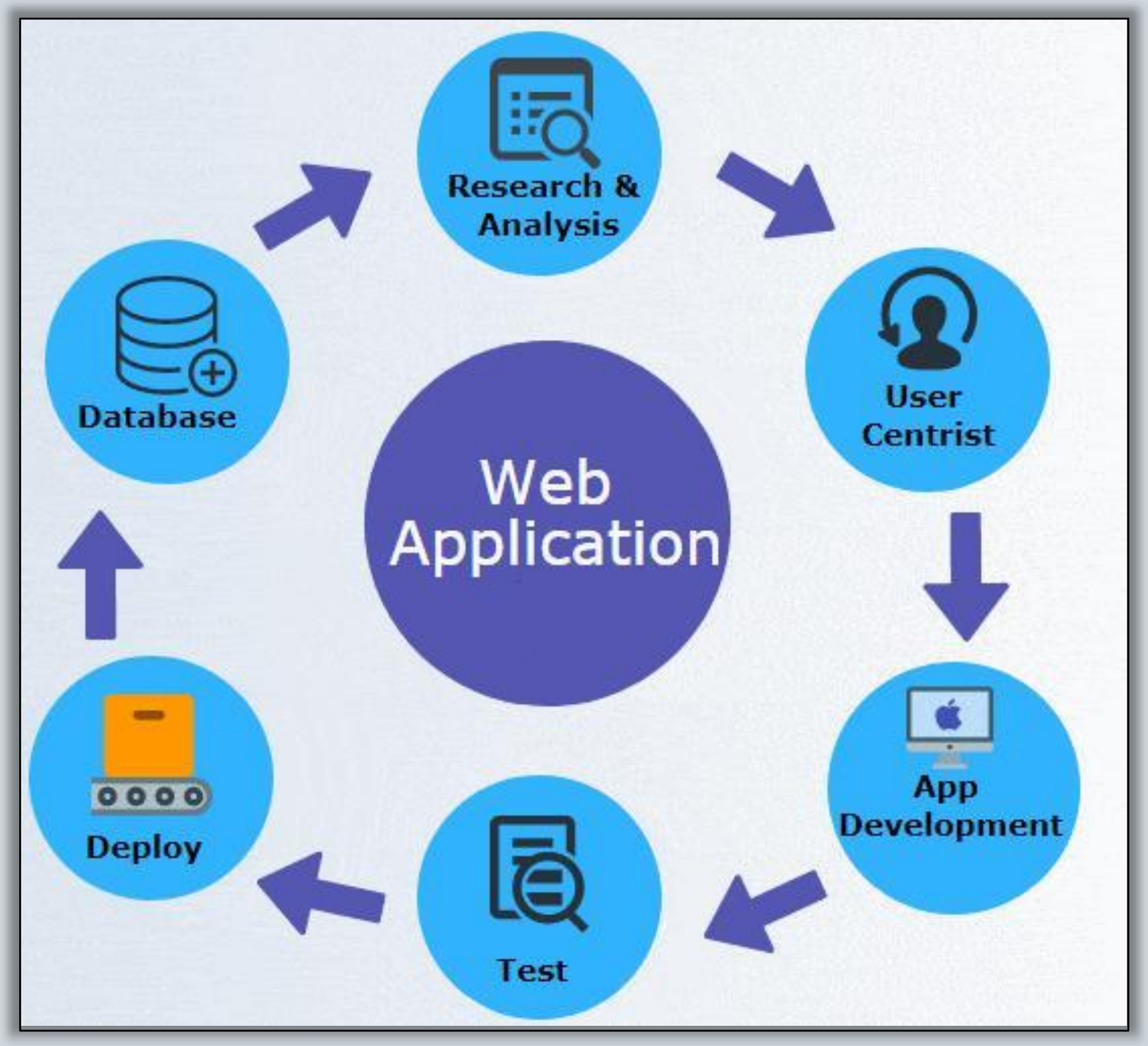
Learning Outcomes

After this lecture, you will be able to

- explore concepts of SPLUNK,
- learn features of Splunk,
- understand Interfaces and data ingestion.

Introduction

Introduction



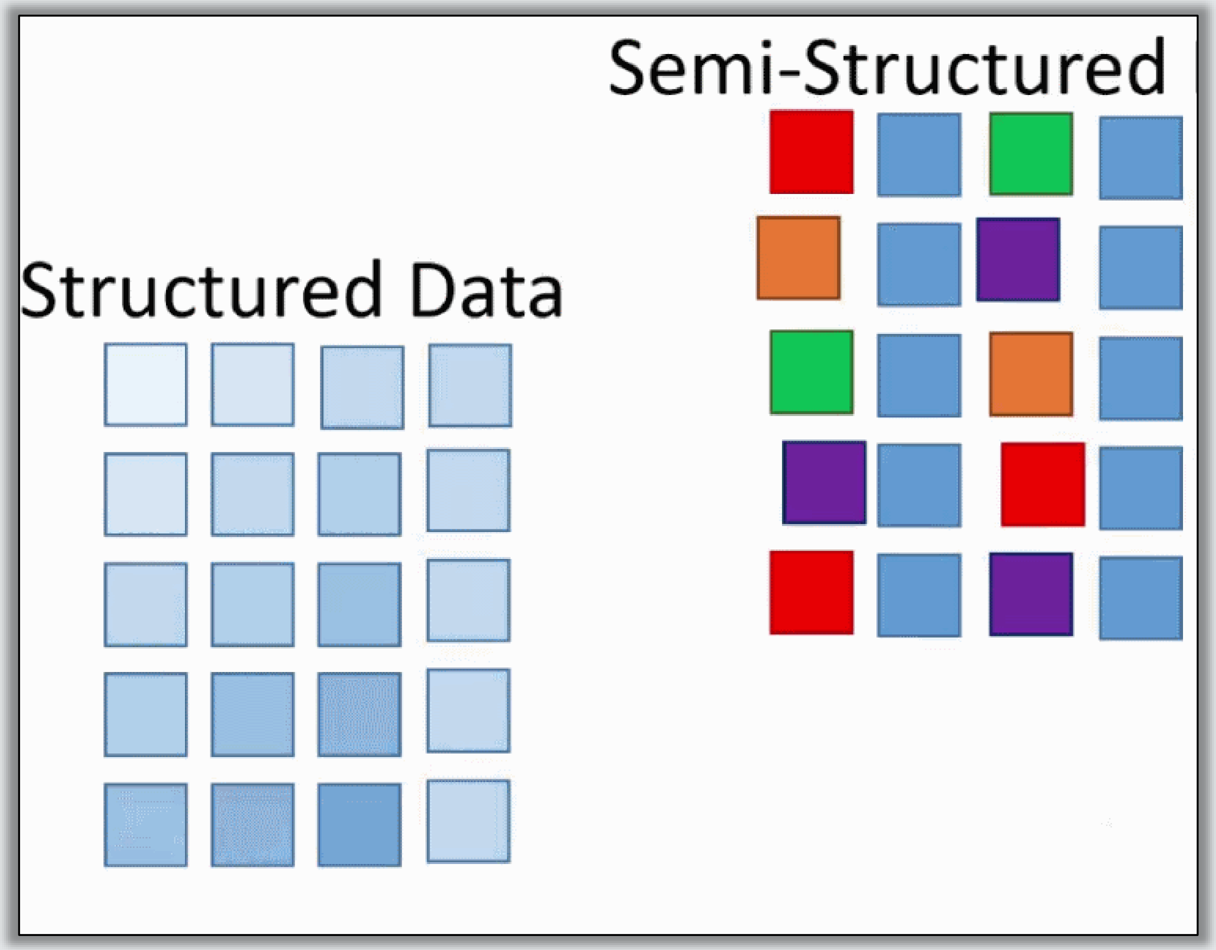
Introduction

Sensors

Introduction

Data

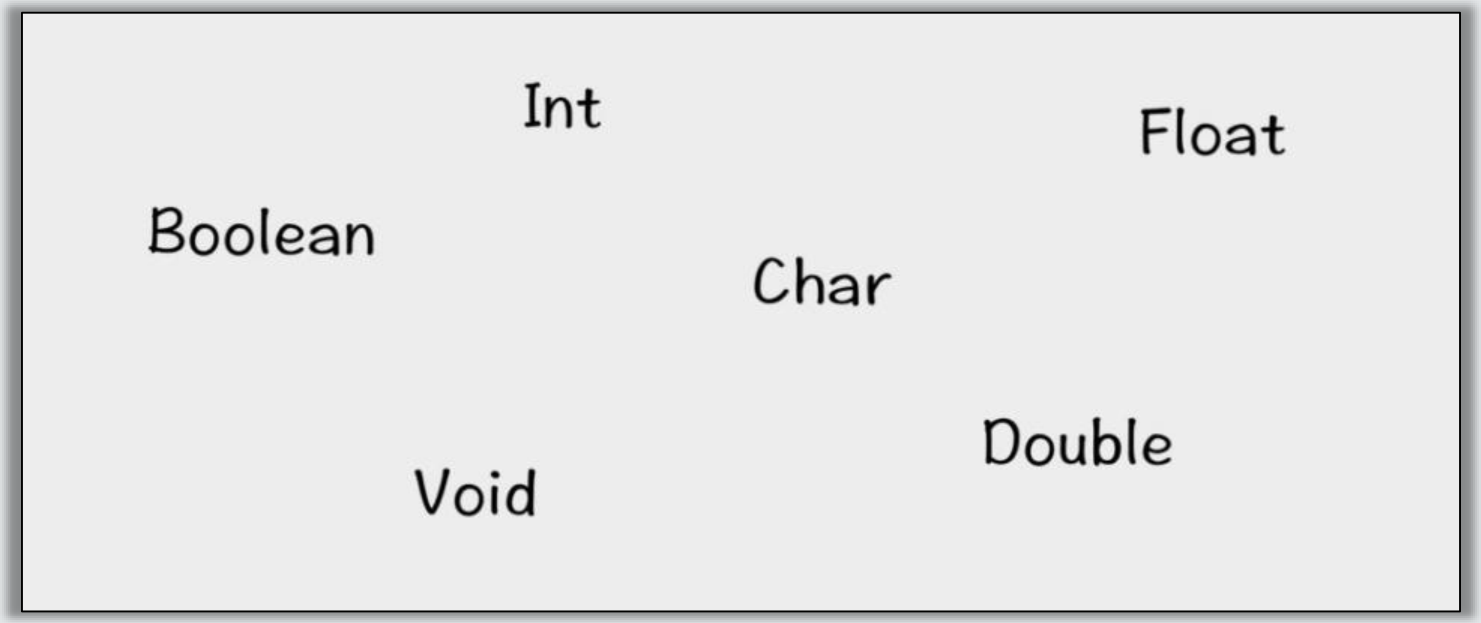
IT Infrastructure



Semi-Structured

Structured Data

Introduction

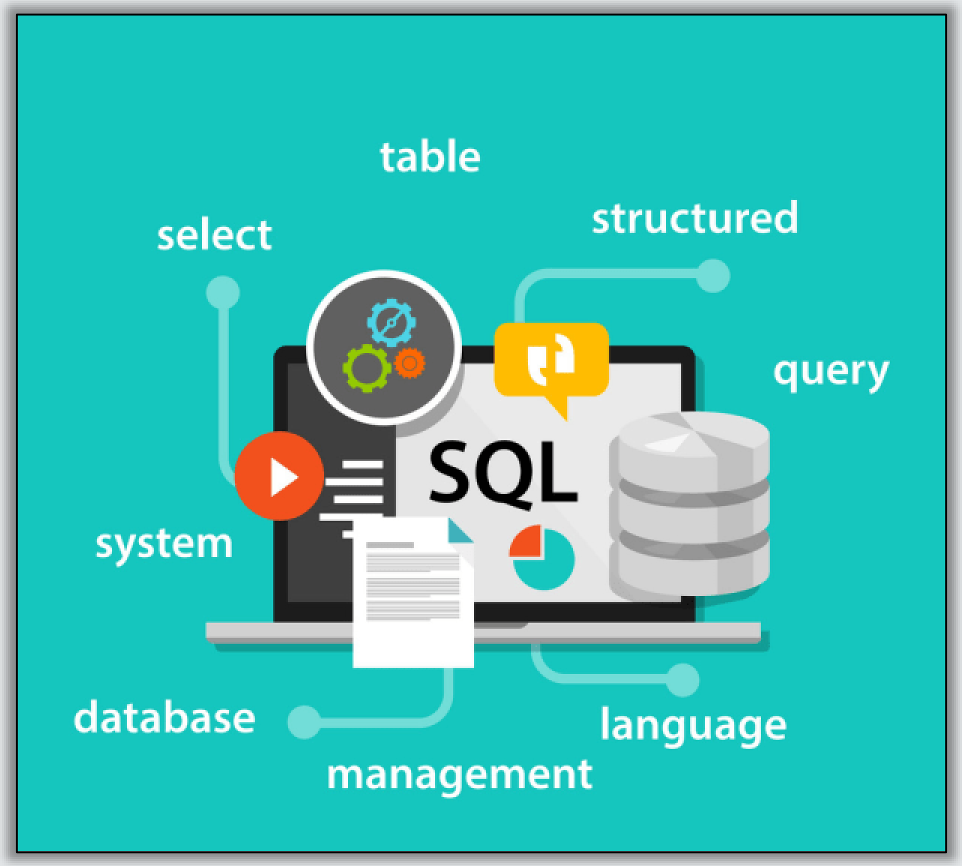


Built-in feature to recognize data types

Introduction

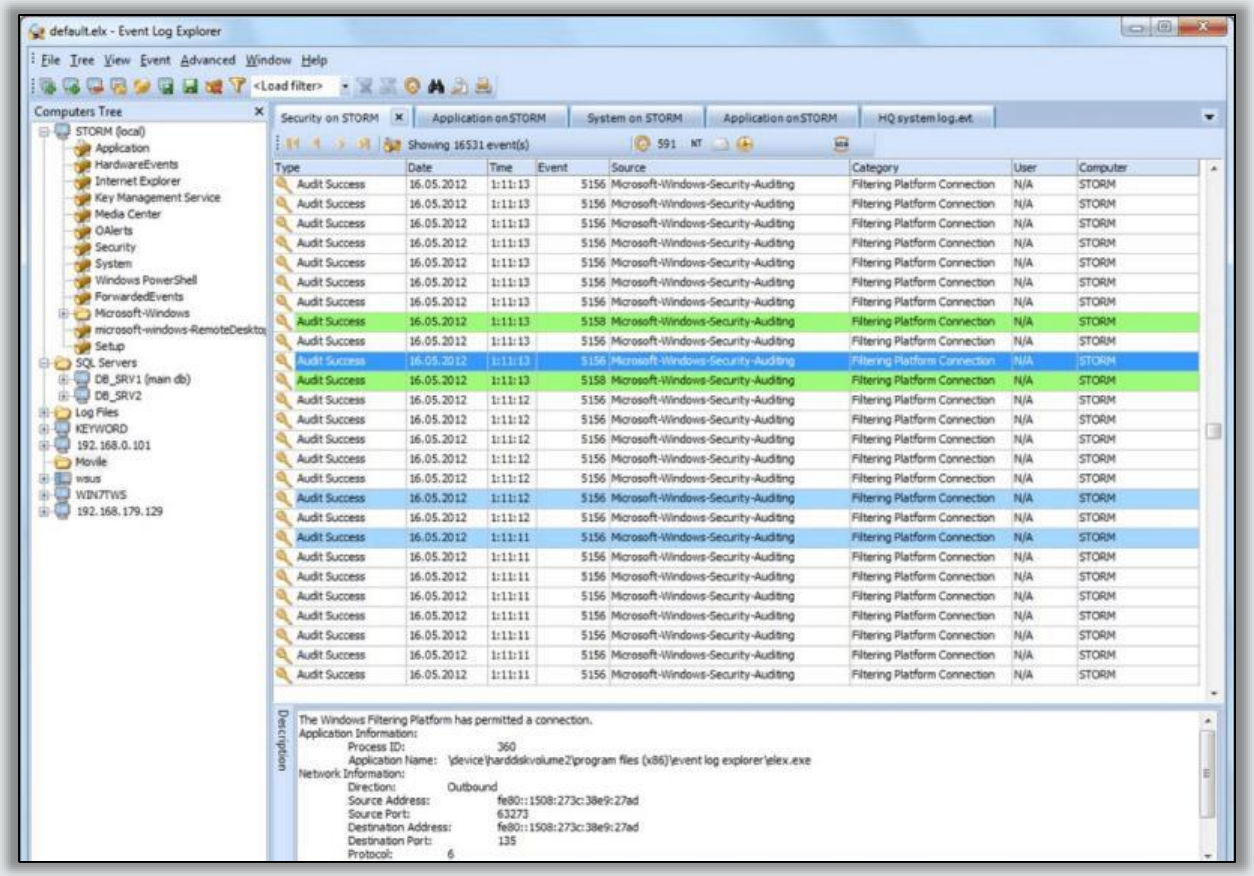
Data Visualization

Prerequisites



Structured Query Language

Prerequisites

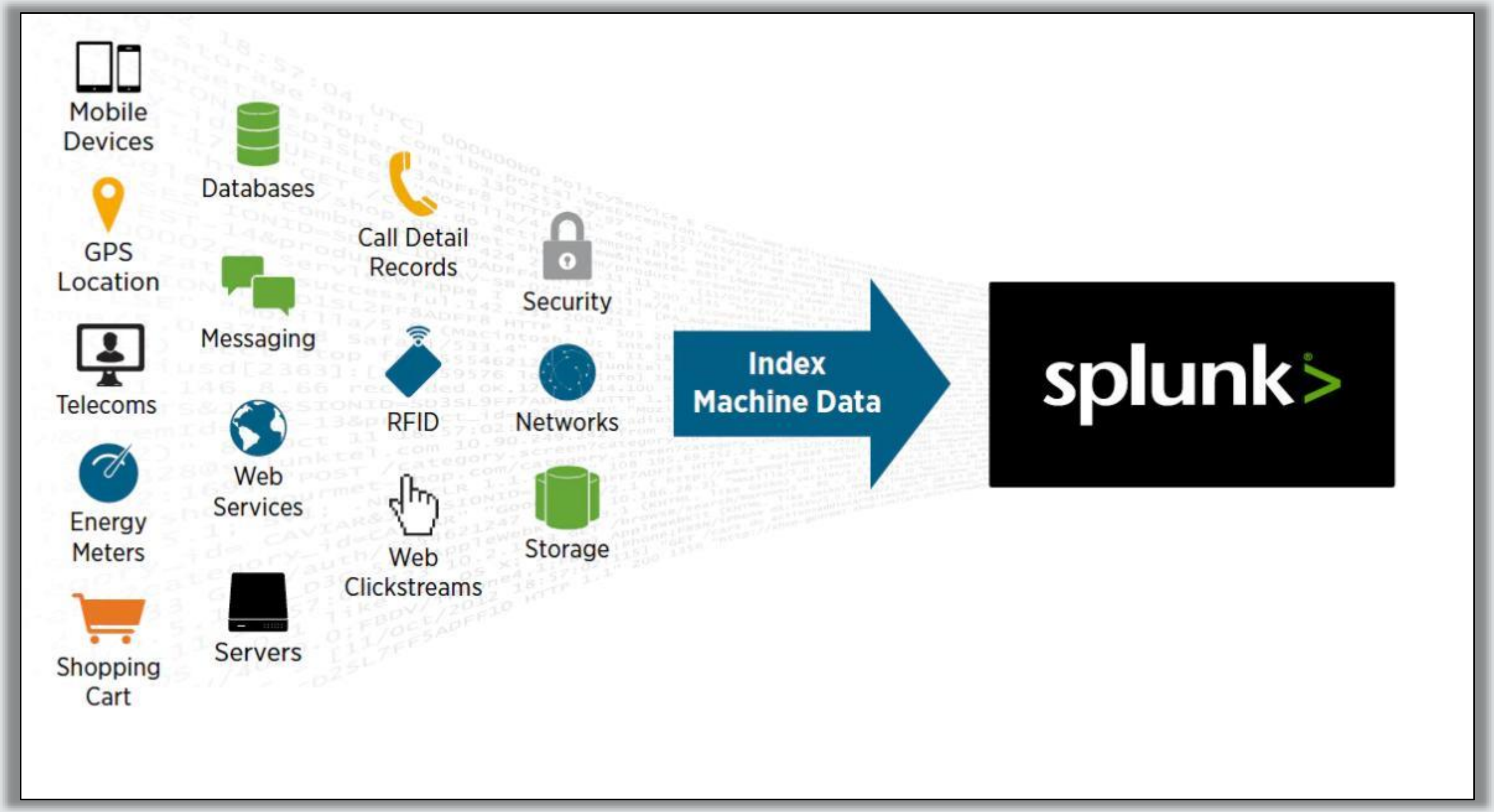


Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5158	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:13	5158	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:12	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM
Audit Success	16.05.2012	1:11:11	5156	Microsoft-Windows-Security-Auditing	Filtering Platform Connection	N/A	STORM

```
The Windows Filtering Platform has permitted a connection.
Application Information:
        Process ID:             360
        Application Name:   \device\harddiskvolume2\program files (x86)\event log explorer\elex.exe
Network Information:
        Direction:          Outbound
        Source Address:             fe80::1508:273c:38e9:27ad
        Source Port:                63273
        Destination Address:        fe80::1508:273c:38e9:27ad
        Destination Port:           135
        Protocol:           6
```

Log

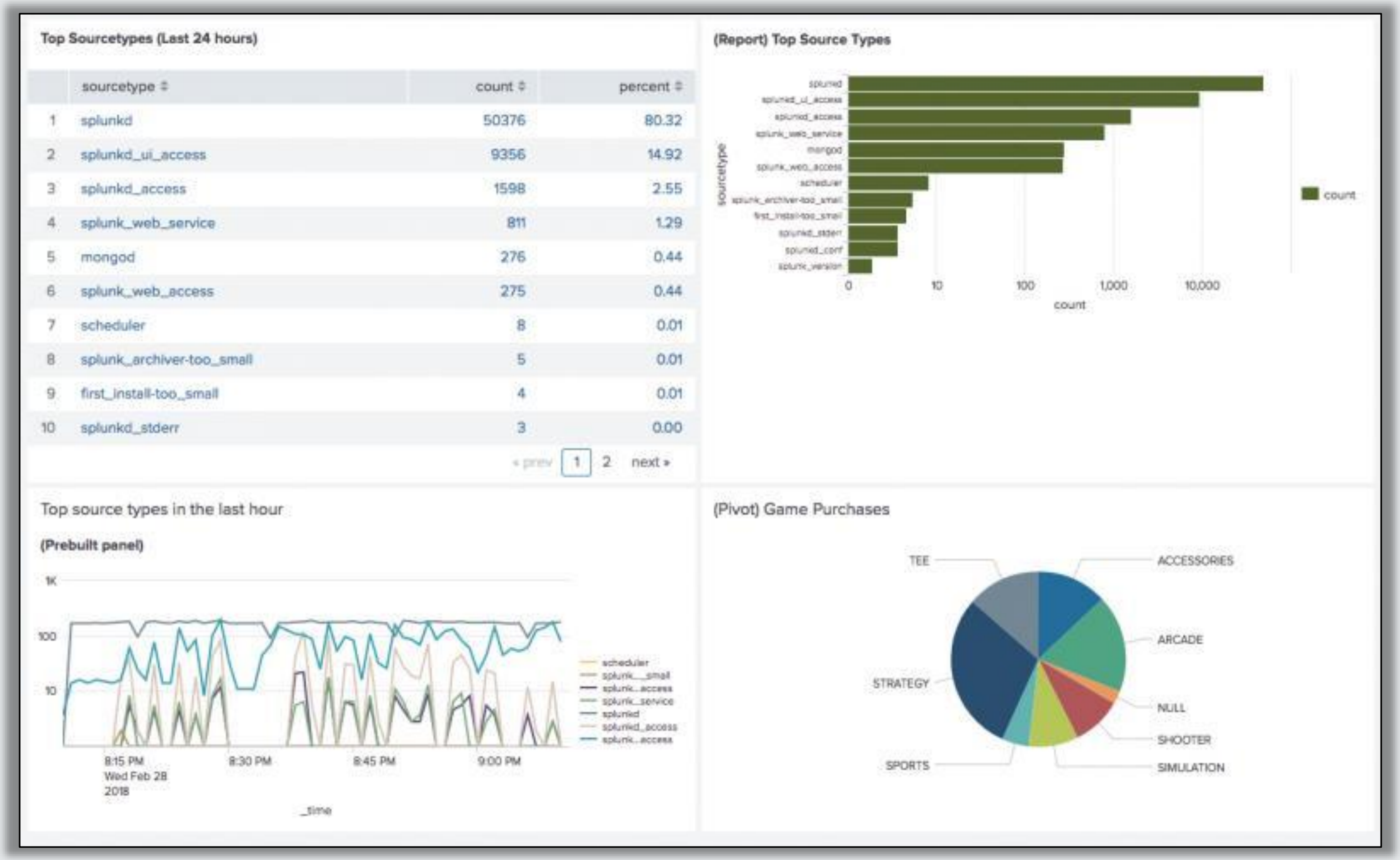
Prerequisites



Prerequisites

Splunk can read this unstructured, semi-structured or rarely structured data

Prerequisites



Top Sourcetypes (Last 24 hours)

	sourcetype ⇕	count ⇕	percent ⇕
1	splunkd	50376	80.32
2	splunkd_ui_access	9356	14.92
3	splunkd_access	1598	2.55
4	splunk_web_service	811	1.29
5	mongod	276	0.44
6	splunk_web_access	275	0.44
7	scheduler	8	0.01
8	splunk_archiver-too_small	5	0.01
9	first_install-too_small	4	0.01
10	splunkd_stderr	3	0.00

(Report) Top Source Types

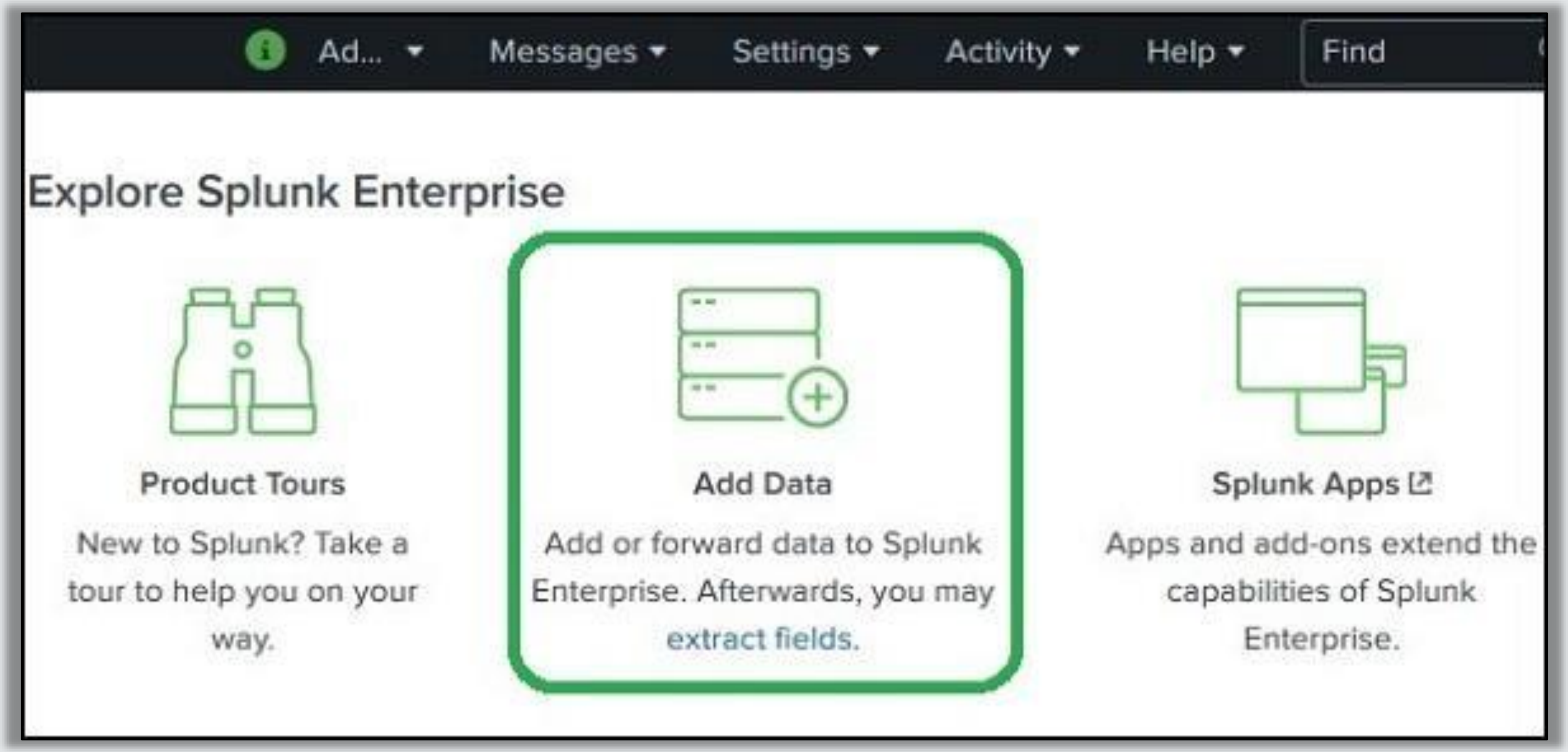
Top source types in the last hour

(Prebuilt panel)

(Pivot) Game Purchases

search, tag, create reports and dashboards on these data.

Prerequisites



Explore Splunk Enterprise

Product Tours

New to Splunk? Take a tour to help you on your way.

Add Data

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps

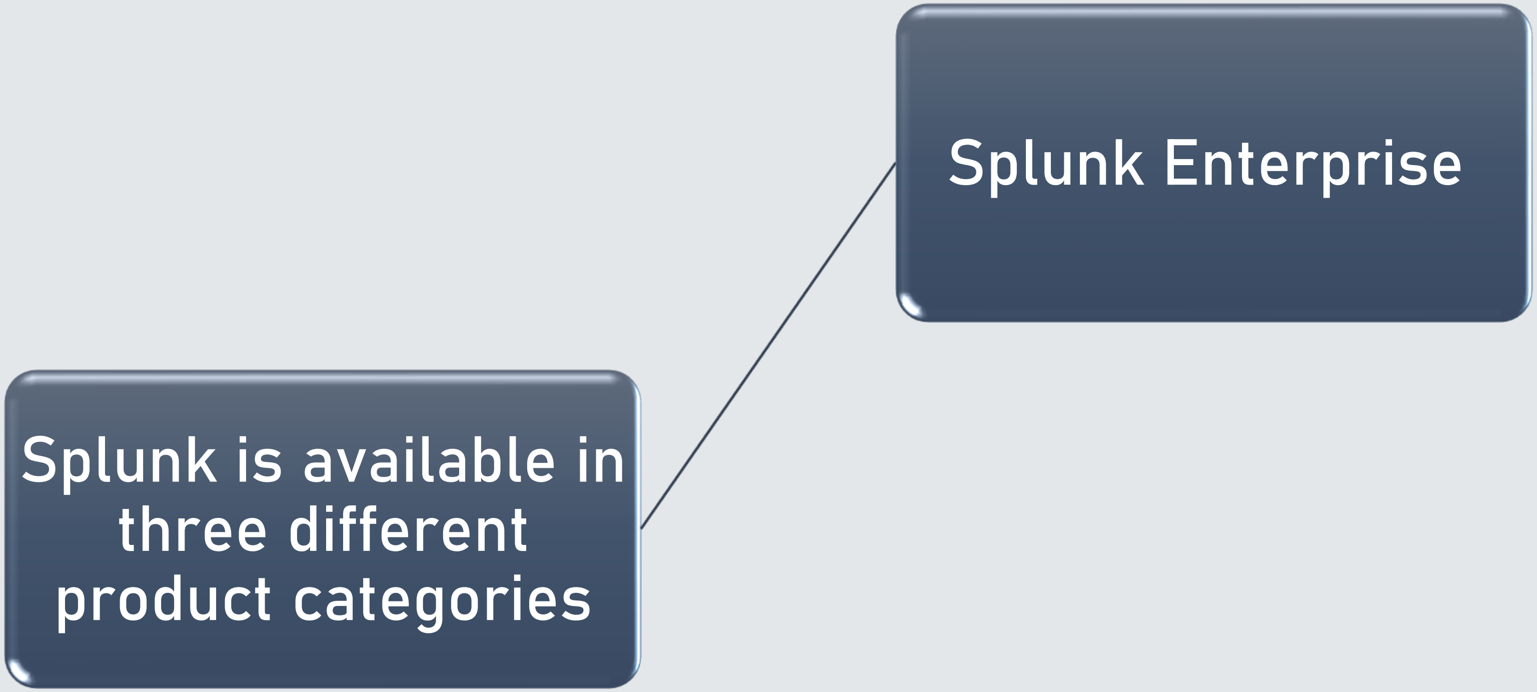
Apps and add-ons extend the capabilities of Splunk Enterprise.

General analytical tool for unstructured machine data and various forms of big data.

Product Categories

Splunk is available in three different product categories

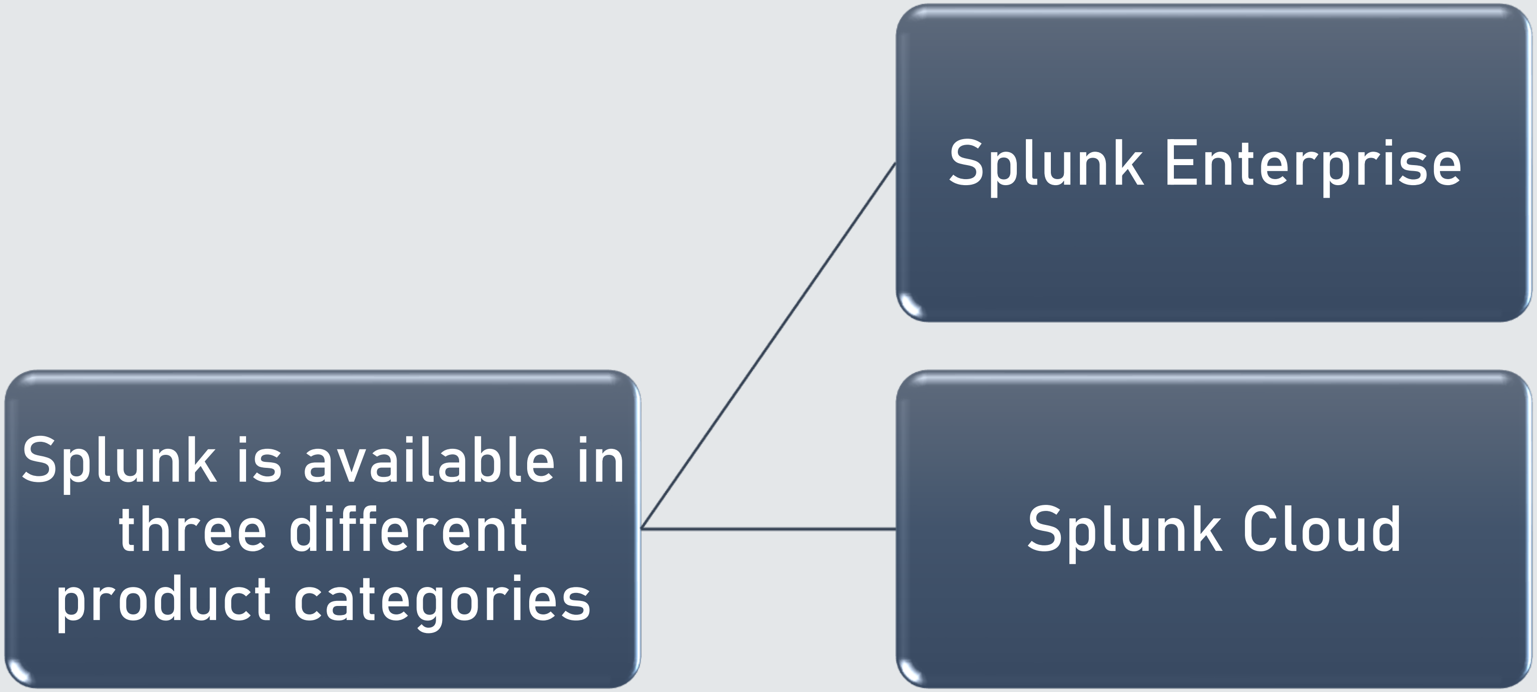
Product Categories



Splunk is available in three different product categories

Splunk Enterprise

Product Categories

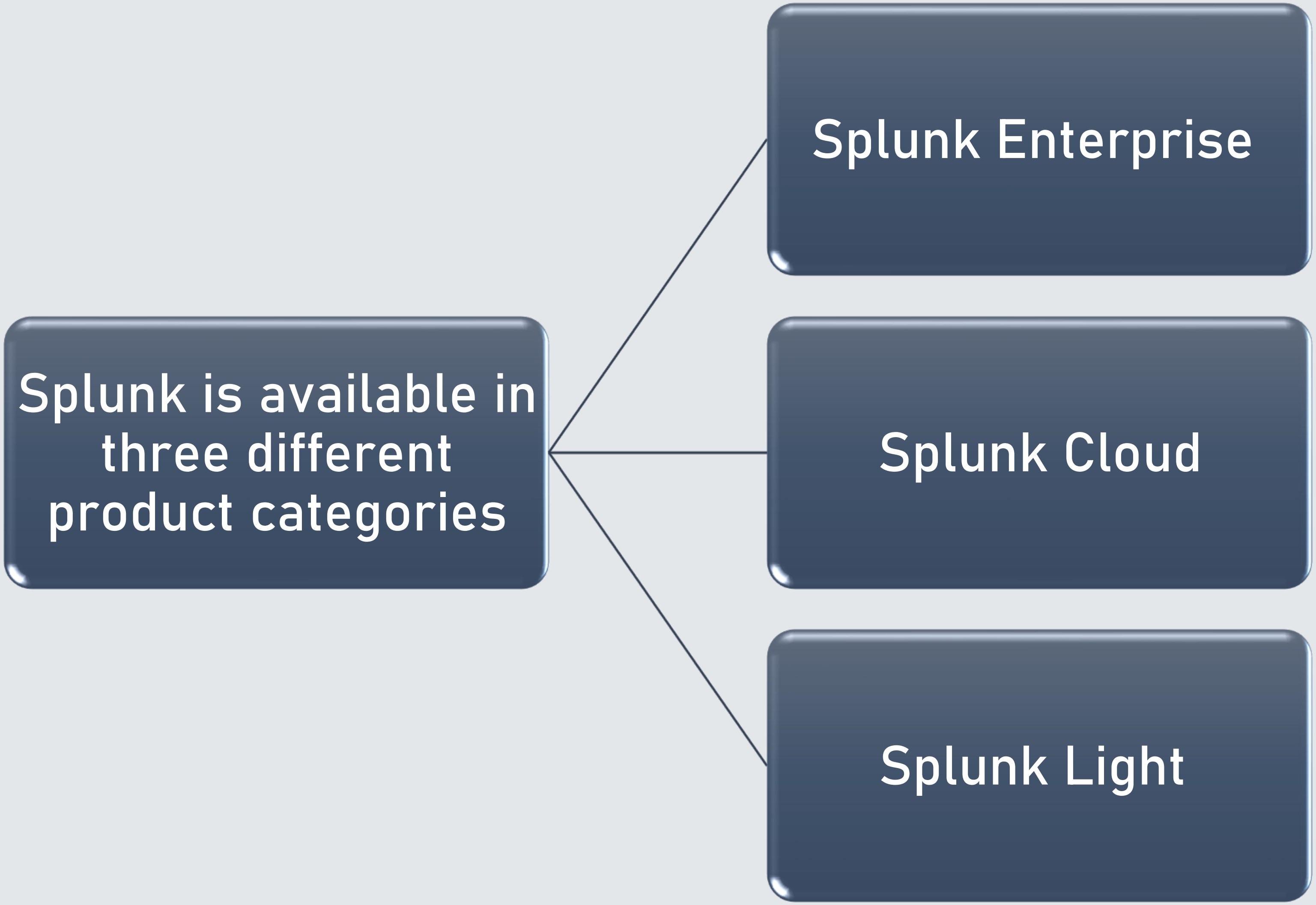


Splunk is available in three different product categories

Splunk Enterprise

Splunk Cloud

Product Categories



Splunk is available in three different product categories

Splunk Enterprise

Splunk Cloud

Splunk Light

Splunk Features

Data Ingestion

Data Indexing

Data Searching

Using Alerts

Dashboards

Data Model

Splunk Interface

That’s all for now…