cyber & data

"From bits to information"

Splunk Data Analysis

Outline

- Analysing data with SPL.
- Filtering with **where**.
- Sorting.

cyber & data

"From bits to information"

Sorting

Inputlookup

```
| inputlookup broadband.csv
```

All time

✓ 54 results (before 06/09/2020 21:52:55.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (54)** Visualization

20 Per Page Format Preview

Prev 1 2 3 Next

Above 10Mbps	Above 15Mbps	Above 4Mbps	Average peak	Average speed	Country	GDP per capita
3.10	0.50	39.00	26.9	4.2	Argentina	13589
18.00	7.40	72.00	41.9	7.8	Australia	50962
33.00	17.00	90.00	44	11.4	Austria	43724
52.00	26.00	91.00	59.3	12.8	Belgium	40107
0.20	0.10	2.80	13.9	1.8	Bolivia	2886
2.20	0.60	32.00	29	3.6	Brazil	8670

Show

Inputlookup … head

```
| inputlookup internet_traffic.csv
| head 10
```

Last 24 hours

✓ 10 results (06/09/2020 07:00:00.000 to 07/09/2020 07:48:59.000) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

_time	bits_transferred
2005-06-07 14:00:00	3562279127
2005-06-07 14:05:00	3710215571
2005-06-07 14:10:00	3877469703
2005-06-07 14:15:00	3876354871
2005-06-07 14:20:00	4582542581
2005-06-07 14:25:00	5016336869
2005-06-07 14:30:00	5202513642
2005-06-07 14:35:00	5410604985
2005-06-07 14:40:00	5408071320

Show

Inputlookup … tail

```
| inputlookup internet_traffic.csv
| tail 10
| reverse
```

Last 24 hours

✓ 10 results (06/09/2020 07:00:00.000 to 07/09/2020 07:54:46.000) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

_time	bits_transferred
2005-07-28 20:10:00	7067542380
2005-07-28 20:15:00	6723781884
2005-07-28 20:20:00	6716706535
2005-07-28 20:25:00	6878028186
2005-07-28 20:30:00	6725282942
2005-07-28 20:35:00	6694253099
2005-07-28 20:40:00	6795832158
2005-07-28 20:45:00	6729727208

Show

Where …

```
| inputlookup broadband.csv where ("Average speed">6)
```

All time

✓ 35 results (before 06/09/2020 21:54:14.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (35)** Visualization

20 Per Page Format Preview

Prev 1 2 Next

Above 10Mbps	Above 15Mbps	Above 4Mbps	Average peak	Average speed	Country	GDP per capita
18.00	7.40	72.00	41.9	7.8	Australia	50962
33.00	17.00	90.00	44	11.4	Austria	43724
52.00	26.00	91.00	59.3	12.8	Belgium	40107
43.00	21.00	87.00	52.4	11.9	Canada	43332
46.00	27.00	86.00	50.9	14.5	Czech Republic	17257
51.00	29.00	94.00	50.1	14	Denmark	52114

Show

&cyber data

Sorting

```
| inputlookup broadband.csv where ("Average speed">6) | sort "Average speed"
```

All time

✓ 35 results (before 06/09/2020 21:55:31.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (35)** Visualization

20 Per Page Format Preview

Prev 1 2 Next

Above 10Mbps	Above 15Mbps	Above 4Mbps	Average peak	Average speed	Country	GDP per capita
7.60	2.90	77.00	38.5	6.2	Turkey	9437
9.20	3.40	71.00	30.1	6.5	Italy	29867
10.00	2.30	85.00	45.8	6.8	United Arab Emirates	36060
0.90	0.40	17.00	31	7.45	Indonesia	3362
18.00	7.40	72.00	41.9	7.8	Australia	50962
21.00	8.70	74.00	38.9	8.2	France	37675

Show

Sorting

```
| inputlookup broadband.csv where ("Average speed">6) | sort "Average speed" | reverse
```

All time

✓ 35 results (before 06/09/2020 21:56:45.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (35)** Visualization

20 Per Page Format Preview

Prev 1 2 Next

Above 10Mbps	Above 15Mbps	Above 4Mbps	Average peak	Average speed	Country	GDP per capita
68.00	45.00	96.00	86.6	20.5	South Korea	27195
55.00	38.00	92.00	69	17.4	Sweden	49866
54.00	37.00	88.00	55.9	16.4	Norway	74822
61.00	36.00	93.00	62.6	16.2	Switzerland	80675
59.00	36.00	92.00	101.1	15.8	Hong Kong	42390
60.00	34.00	95.00	63.5	15.6	Netherlands	43603
54.00	32.00	90.00	78.4	15	Japan	32486

Show

&data

Logical operations …

```
| inputlookup broadband.csv where ("Average speed">6 AND "GDP per capita"<10000) | sort "Average speed" | reverse
```

All time

✓ 5 results (before 07/09/2020 08:01:37.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (5)** Visualization

20 Per Page Format Preview

Above 10Mbps	Above 15Mbps	Above 4Mbps	Average peak	Average speed	Country	GDP per capita
57.00	27.00	94.00	72.9	13.1	Romania	8906
38.00	15.00	87.00	57.9	10.2	Russia	9055
18.00	5.80	93.00	58.3	8.2	Thailand	5742
0.90	0.40	17.00	31	7.45	Indonesia	3362
7.60	2.90	77.00	38.5	6.2	Turkey	9437

Show

&cyber data

cyber & data

"From bits to information"

Splunk Data Analysis