

Project # 2

Kadie Johnstun

Product_Sales

```
index=web sourcetype=access_combined action=purchase status=200  
| fields price, productId  
| stats sum(price) as revenue by productId  
| eval revenue = "$".toString(revenue,"commas")
```

✓ 12,268 events (5/7/23 12:00:00.000 AM to 6/6/23 3:40:49.000 PM) No Event Sampling ▼

(Situation) Splunk is used to take so much data and use it to narrow down your search based on the criteria you want to use to make informed decisions.

(Task) I created a search in Splunk that looks at the fields of Price (price) and Product (productId) in the web index.

(Action) This allows us to look at the different products by the revenue it produces.

(Result) See Below.

Project # 2

Kadie Johnstun

The screenshot shows the Splunk 9.0.0 interface. The search bar at the top contains the following query:

```
index=web sourcetype="access_combined" status=200 action=purchase
| fields price, productId
| stats sum(price) as revenue by productId
| eval revenue = "$".tostring(revenue, "commas")
```

The search results are displayed in a table with 20 items per page. The table has two columns: productId and revenue. The results show the revenue for various product IDs, sorted in descending order.

productId	revenue
BS-AG-G09	\$8,546.58
CU-PG-G06	\$6,576.71
DB-SG-G01	\$13,444.62
DC-SG-G02	\$20,674.83
FI-AG-G08	\$15,396.15
FS-SG-G03	\$11,470.41
MB-AG-G07	\$18,515.37
MB-AG-T01	\$4,345.65
PZ-SG-G05	\$1,966.06
SC-MG-G10	\$10,994.50
WC-SH-A01	\$2,545.75
WC-SH-A02	\$2,034.90
WC-SH-G04	\$14,294.28
WC-SH-T02	\$3,676.32

First, we see that the search has produced 20 items per page and how much revenue is being made by the item.

Project # 2

Kadie Johnstun

The screenshot shows the Splunk 9.0.0 interface. The search bar contains the following query:

```
index=web sourcetype="access_combined" status=200 action=purchase
| fields price, productId
| stats sum(price) as revenue by productId
| eval revenue = "$".toString(revenue, "commas")
```

The search results show 12,422 events. The table below displays the results, with columns for productID and revenue. A blue arrow points to the 'revenue' column header.

productID	revenue
BS-AG-G09	\$8,546.58
CU-PG-G06	\$6,576.71
MB-AG-T01	\$4,345.65
WC-SH-T02	\$3,676.32
DC-SG-G02	\$20,674.83
WC-SH-A01	\$2,545.75
WC-SH-A02	\$2,034.90
MB-AG-G07	\$18,515.37
FI-AG-G08	\$15,396.15
WC-SH-G04	\$14,294.28
DB-SG-G01	\$13,444.62
FS-SG-G03	\$11,470.41
SC-MG-G10	\$10,994.50
PZ-SG-G05	\$1,966.06

We can now filter by revenue or product ID.

Project # 2

Kadie Johnstun

The screenshot shows the Splunk 9.0.0 interface. The search bar contains the following query:

```
index=web sourcetype="access_combined" status=200 action=purchase
| fields price, productId
| stats sum(price) as revenue by productId
| eval revenue = "$".tostring(revenue, "commas")
| rename productId as "Product Number"
```

The search results are displayed in a table with the following columns: Product Number and revenue. The table shows 14 results, with the first row highlighted in blue. A blue arrow points to the 'rename' command in the search bar, and another blue arrow points to the 'Product Number' column header in the table.

Product Number	revenue
BS-AG-G09	\$8,546.58
CU-PG-G06	\$6,576.71
MB-AG-T01	\$4,345.65
WC-SH-T02	\$3,676.32
DC-SG-G02	\$20,674.83
WC-SH-A01	\$2,545.75
WC-SH-A02	\$2,038.89
MB-AG-G07	\$18,515.37
FI-AG-G08	\$15,396.15
WC-SH-G04	\$14,294.28
DB-SG-G01	\$13,444.62
FS-SG-G03	\$11,470.41
SC-MG-G10	\$10,994.50
PZ-SG-G05	\$1,966.06

The final thing that we have done is change the table name from productid to Product Number.

Project # 2

Kadie Johnstun

Splunk Enterprise interface showing search results for Product_Sales.

Search Query:

```
index=web sourcetype=access_combined action=purchase status=200
| fields price, productId
| stats sum(price) as revenue by productId
| eval revenue = "$".tostring(revenue, "commas")
```

Results: 12,268 events (5/7/23 12:00:00.000 AM to 6/6/23 3:40:49.000 PM) No Event Sampling

Statistics (14)

productId	revenue
BS-AG-G09	\$7,646.94
CU-PG-G06	\$6,736.63
DB-SG-G01	\$14,244.30
DC-SG-G02	\$20,754.81
FI-AG-G08	\$14,476.38
FS-SG-G03	\$10,820.67
MB-AG-G07	\$17,555.61
MB-AG-T01	\$4,875.12
PZ-SG-G05	\$1,921.15
SC-MG-G10	\$10,534.73
WC-SH-A01	\$2,324.12
WC-SH-A02	\$1,967.07
WC-SH-G04	\$14,394.24
WC-SH-T02	\$3,966.03