

Project # 2: Splunk

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 ▼

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. Every day in the companies that we work for, we create data even when you think you are not. The email you send, the slack message, and even something as simple as plugging in a mouse into a usb port, all create data that Splunk takes in and pushes it to different indexes. Splunk allows you to set up reports that can automate alerts for things that could be harmful to the company or the system. It can also help a company make better informed decisions about sales production and where to invest your money within the company.

To demonstrate, I created a search in Splunk that looks at the fields of Price (price) and Product (productId) in the web index. By doing so we can see what products are making this fictional company money and what is not.

One thing that I was not able to do in the demo version that I would have liked to do more of is to narrow that search by marginal increase, or which product makes us the most money every time we sell it. This can then be used in conjunction with marketing. How many ads were targeted for this specific product? Should we be focusing on something that seems to get us more bang for our buck?

Project # 2: Splunk

Kadie Johnston

(Result) See Below.

The screenshot shows the Splunk Search 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"])
```

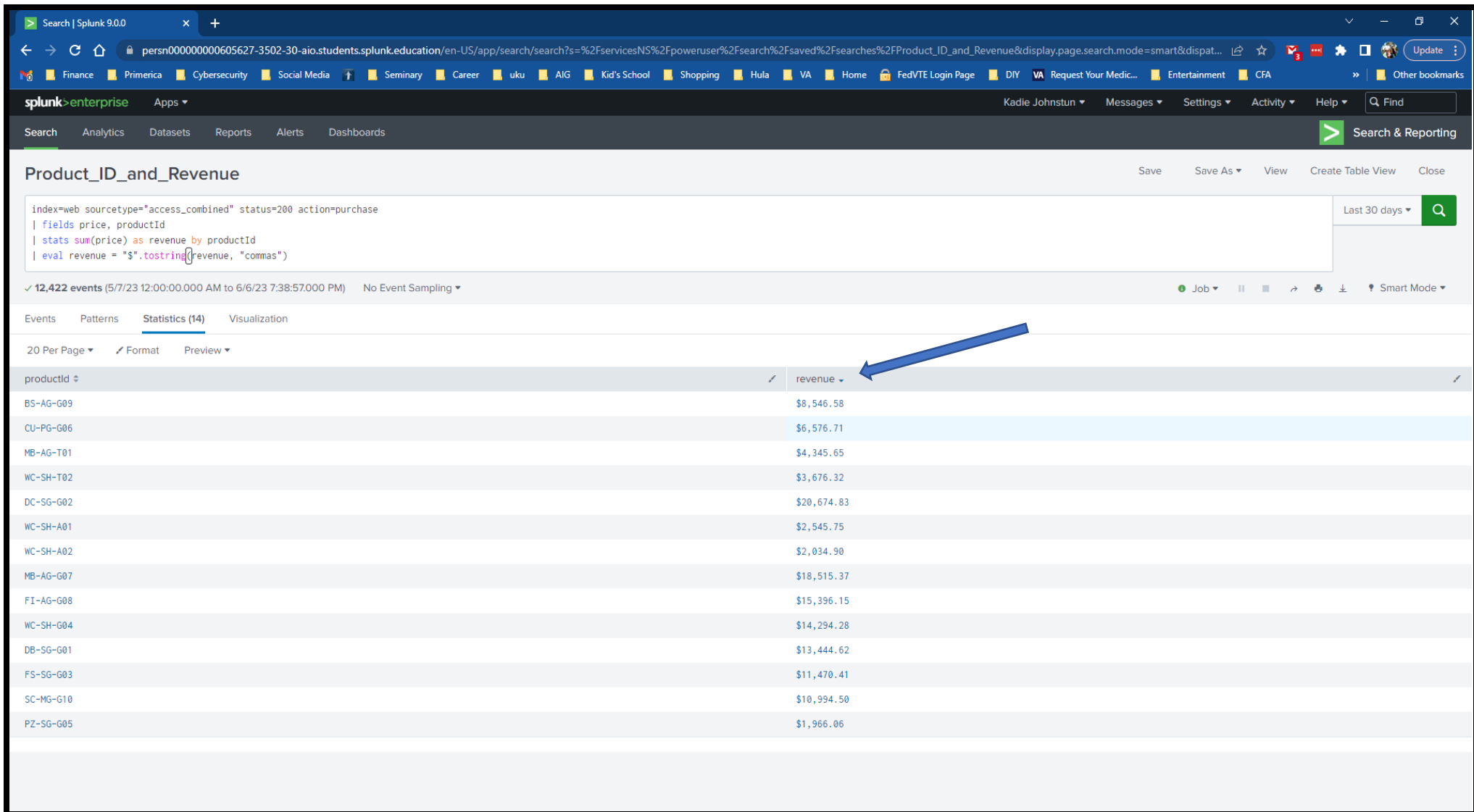
The search results are displayed in a table with 20 items per page. The table has two columns: **productId** and **revenue**. The results show the revenue for various product IDs.

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: Splunk

Kadie Johnstun



The screenshot shows the Splunk web 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 are displayed in a table with 14 events. The table has two columns: 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: Splunk

Kadie Johnstun

The screenshot shows the Splunk web 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 rows of data. Two blue arrows are present: one pointing to the 'rename productId as "Product Number"' line in the search bar, and another pointing 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: Splunk

Kadie Johnstun

The screenshot shows the Splunk Search interface. The search bar contains the following 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")
```

The search results are displayed in a table with 2 columns: productId and revenue. The table shows 14 rows of data, sorted by revenue in descending order. The interface includes a top navigation bar with links to Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The search results are shown in a table view with a 'Statistics (14)' tab selected. The table has a 'productid' column and a 'revenue' column. The revenue values are formatted with commas as thousands separators.

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

Working with Internal Threat Operations (ITO) I am expected to look at alerts through Splunk and determine if the alert is something that should be investigated further or not. If it is something that we believe should be looked into further, then we conduct an investigation. I personally over the last 9 months have ben able to clear over

Project # 2: Splunk

Kadie Johnstun

70,000 alerts, head the implementation of an alert workflow, spear head investigations, and many other things that I wish I could talk more in depth.

The key here is: Don't do anything that you know you shouldn't. It is being logged and processed by your employer. If you wouldn't want it on the front page of your favorite website, don't do it.