

---

## Lab Exercise 2 – Using Transforming Commands for Visualizations

### Description

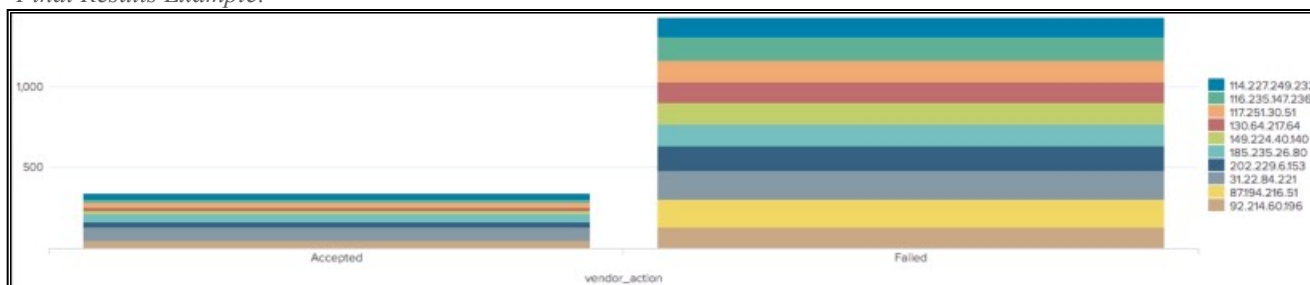
In this lab exercise, you use the `chart` and `timechart` commands.

### Steps

**Task 1: Report the top ten completed events on the web server during the last 24 hours and add it to a new security dashboard as a column chart.**

---

*Final Results Example:*



1. Search the web server [`sourcetype=linux_secure`] for events where the [`vendor_action`] is not equal to “session opened” during the **last 24 hours**.

*Results Example:*

| i | Time                      | Event   |
|---|---------------------------|---|
| > | 7/24/19<br>8:04:59.000 PM | Wed Jul 24 2019 20:04:59 www0 sshd[37002]: Failed password for user myuan from 133.166.61.223 port 5826 ssh2<br>host = www1   source = /opt/log/www1/secure.log   sourcetype = linux_secure |
| > | 7/24/19<br>8:04:56.000 PM | Wed Jul 24 2019 20:04:56 www0 sshd[94890]: Failed password for user myuan from 133.166.61.223 port 5826 ssh2<br>host = www1   source = /opt/log/www1/secure.log   sourcetype = linux_secure |
| > | 7/24/19<br>8:04:53.000 PM | Wed Jul 24 2019 20:04:53 www0 sshd[91204]: Failed password for user myuan from 133.166.61.223 port 5826 ssh2<br>host = www1   source = /opt/log/www1/secure.log   sourcetype = linux_secure |

2. Using the `chart` command, display a count for each of these actions by IP [`src_ip`].

**Hint:** Use `over ... by`

*Results Example:*

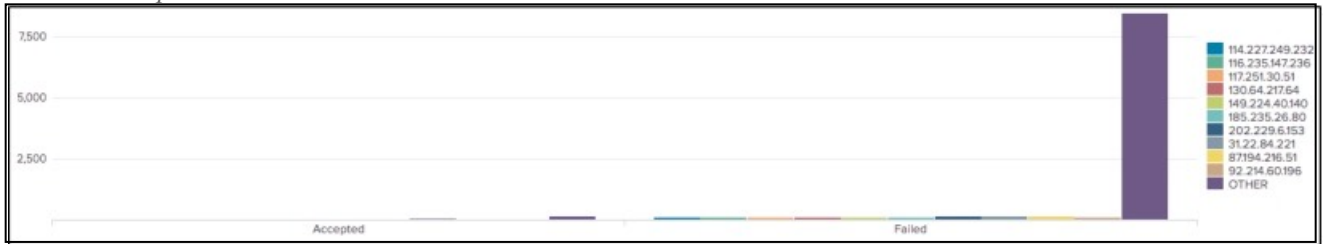
| vendor_action | 114.227.249.232 | 116.235.147.236 | 117.251.30.51 | 130.64.217.64 | 149.224.40.140 | 185.235.26.80 | 202.229.6.153 | 31.22.84.221 | 87194.216.51 | 92.214.60.196 | OTHER |
|---------------|-----------------|-----------------|---------------|---------------|----------------|---------------|---------------|--------------|--------------|---------------|-------|
| Accepted      | 33              | 21              | 30            | 21            | 23             | 48            | 29            | 80           | 0            | 52            | 188   |
| Failed        | 121             | 146             | 131           | 128           | 134            | 131           | 151           | 175          | 176          | 132           | 8478  |



3. Click on the **Visualization** tab and make sure **Column Chart**

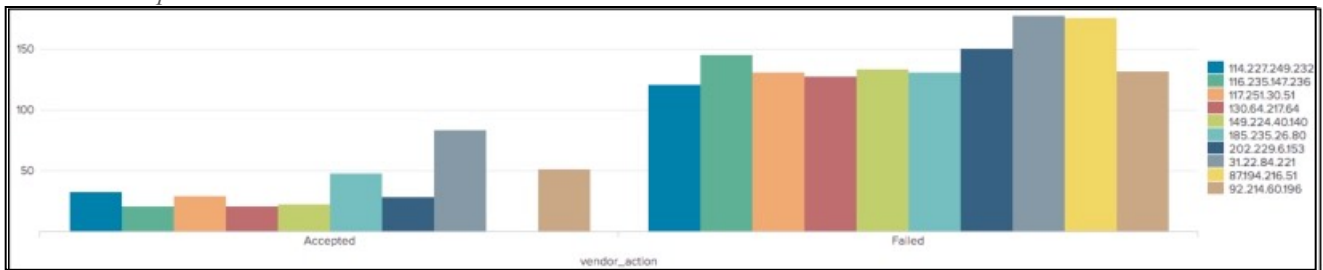
is selected.

*Results Example:*



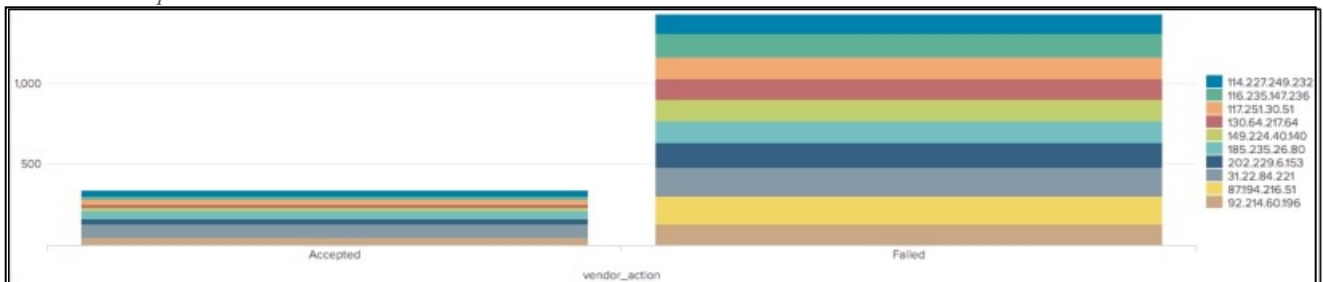
4. As you can see, there is an OTHER column at the end of the Failed results that overwhelms all the other data on the chart, making the other data difficult to see. Set the `useother` option to `f` in order to remove this column.

*Results Example:*



5. Click **Format**; in the General section, set the Stack Mode to **Stacked**.

*Results Example:*



6. Click **Save As** and choose **Report**.

7. Name your report **L2S1** and click **Save**.

8. On the Your Report Has Been Created screen, click **Add to Dashboard**.

9. Save the dashboard with these values:

Dashboard: *New*

- Dashboard Title: *IT Ops*
- Panel Title: *Accepted vs. Failed Web Events*
- Panel Powered By: *Report*

10. Click **Save** and view your dashboard.

11. Mouse over your column chart and click one of the bars. Notice that, by default, the drilldown feature is not activated.

12. Click the **Edit** button.



13. Click the More actions icon on the top right of the panel.

14. Click **Edit Drilldown**.

15. In the Drilldown Editor, choose **Link to search** from the **On click** dropdown menu.

16. Click **Apply**.

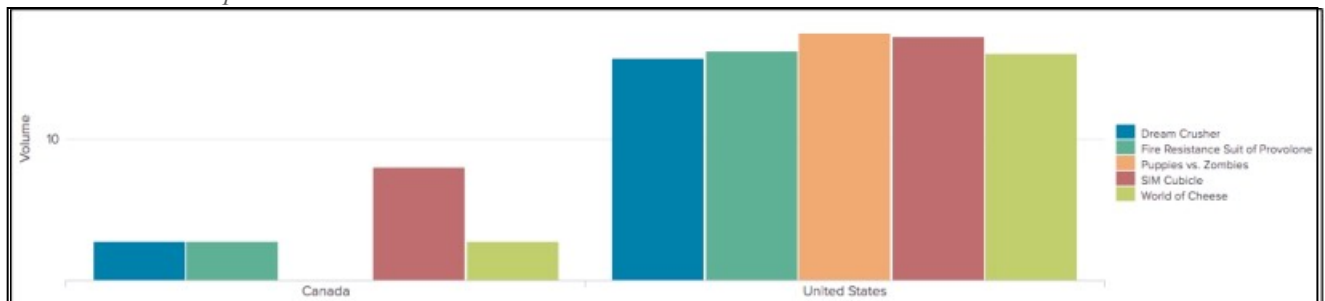
17. Click **Save** to save the dashboard.

18. Mouse over your column chart and click one of the bars. Notice that the drilldown feature is now activated.

19. Use your browser's Back button to return to your dashboard. (This is the easiest way to return to the dashboard from a drilldown.)

## Task 2: Chart by country the five best selling products for the vendors in North America during the last 7 days.

*Final Results Example:*



— VendorID:

- 1000-2999 USA
- 3000-3999 Canada
- 4000-4999 Caribbean, Central & South America
- 5000-6999 Europe and the Middle East
- 7000-8999 Asia and Pacific Region
- 9000-9900 Africa
- 9901-9999 Outliers, such as the South Pole

20. Search for retail store events [vendor\_sales] from North America (United States and Canada) during the last 7 days.

Results Example:

| i | Time                     | Event  |
|---|--------------------------|--|
| > | 2/5/18<br>9:19:28.000 AM | [05/Feb/2018:17:19:28] VendorID=1106 Code=F AcctID=xxxxxxxxxx1352<br>host = vendorUS1   source = /opt/log/vendorUS1/vendor_sales.log   sourcetype = vendor_sales |
| > | 2/5/18<br>9:19:08.000 AM | [05/Feb/2018:17:19:08] VendorID=3106 Code=H AcctID=xxxxxxxxxx0271<br>host = vendorUS1   source = /opt/log/vendorUS1/vendor_sales.log   sourcetype = vendor_sales |
| > | 2/5/18<br>9:17:12.000 AM | [05/Feb/2018:17:17:12] VendorID=1149 Code=N AcctID=xxxxxxxxxx9840<br>host = vendorUS1   source = /opt/log/vendorUS1/vendor_sales.log   sourcetype = vendor_sales |

21. Using the `chart` command, count the events over VendorCountry.

Results Example:

| VendorCountry | count |
|---------------|-------|
| Canada        | 303   |
| United States | 4839  |

22. To see the count of each product sold in each country, add a `by` clause to further split the data by `product_name`.

Results Example:

| VendorCountry | Dream<br>Crusher | Final<br>Sequel | Fire<br>Resistance Suit of<br>Provolone | Holy<br>Blade of<br>Gouda | Manganiello<br>Bros. | Manganiello<br>Bros. Tee | OTHER | Puppies<br>vs. Zombies | SIM<br>Cubicle | World<br>of Cheese | World of<br>Cheese Tee |
|---------------|------------------|-----------------|---|---------------------------|----------------------|--------------------------|-------|------------------------|----------------|--------------------|------------------------|
| Canada        | 22               | 17              | 24                                      | 17                        | 36                   | 9                        | 101   | 7                      | 24             | 31                 | 15                     |
| United States | 538              | 297             | 404                                     | 308                       | 306                  | 311                      | 747   | 517                    | 536            | 565                | 314                    |

23. Use the `limit` option to include only the 5 best-selling products.

**NOTE:** Splunk automatically calculates the top products by totaling each column and taking the top  $n$  results ( $n$  being the number you specify in your limit).

Results Example:

| VendorCountry | Dream Crusher | Holy Blade of Gouda | Puppies vs. Zombies | SIM Cubicle | World of Cheese | OTHER |
|---------------|---------------|---------------------|---------------------|-------------|-----------------|-------|
| Canada        | 1             | 3                   | 0                   | 2           | 3               | 27    |
| United States | 68            | 51                  | 67                  | 71          | 68              | 304   |

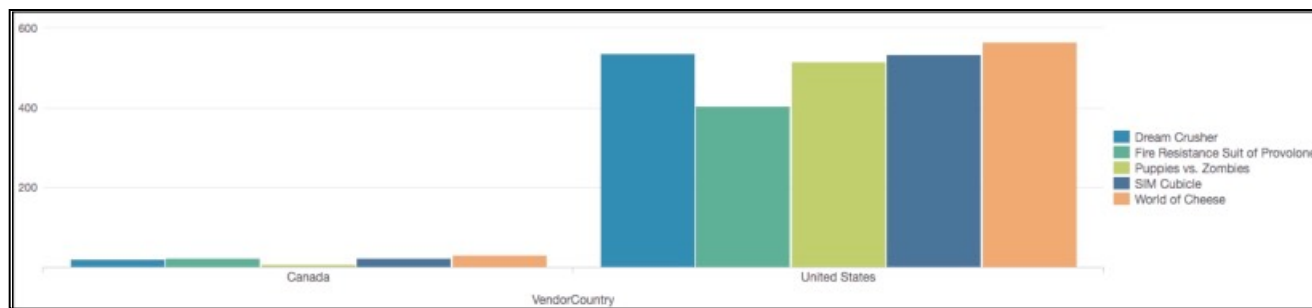
24. Remove the **OTHER** column from your table.

Results Example:

| VendorCountry | Dream Crusher | Fire Resistance Suit of Provolone | Puppies vs. Zombies | SIM Cubicle | World of Cheese |
|---------------|---------------|-----------------------------------|---------------------|-------------|-----------------|
| Canada        | 22            | 24                                | 7                   | 24          | 31              |
| United States | 538           | 404                               | 517                 | 536         | 565             |

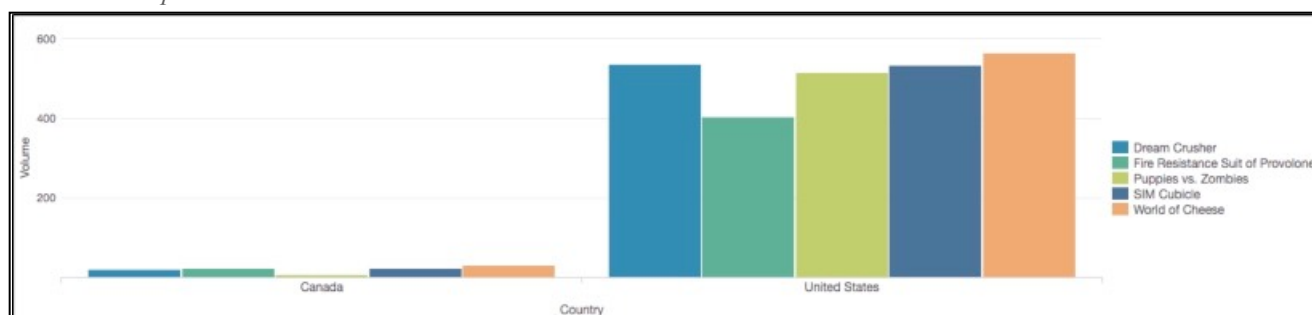
25. Switch to the **Visualization** tab and, if a column chart was not automatically shown, set the chart type to **Column Chart**.

Results Example:

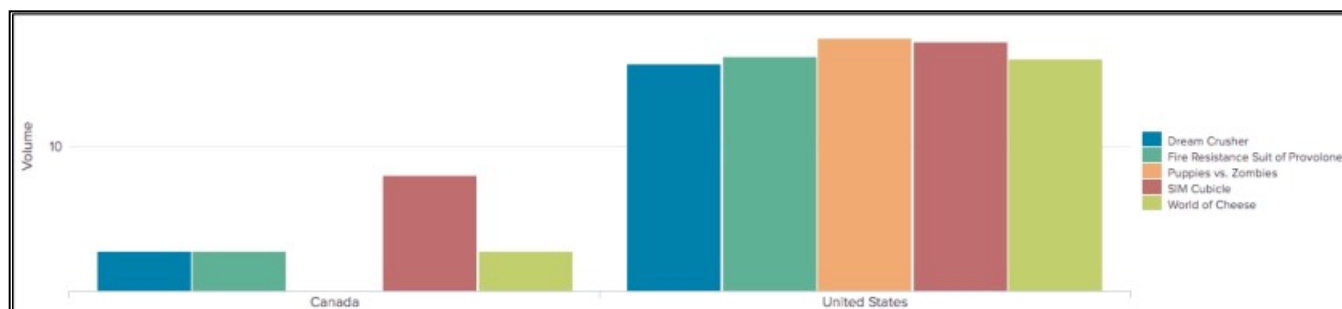


26. Use the **Format** options to define custom labels of **Country** and **Volume** for the X and Y axes, respectively.

*Results Example:*



27. Use the **Format** option to change the scale of the Y axis from linear to logarithmic (Log).



28. Save your search as report, **L2S2**.

### Task 3: Display Internet usage in a timechart during the last 24 hours.

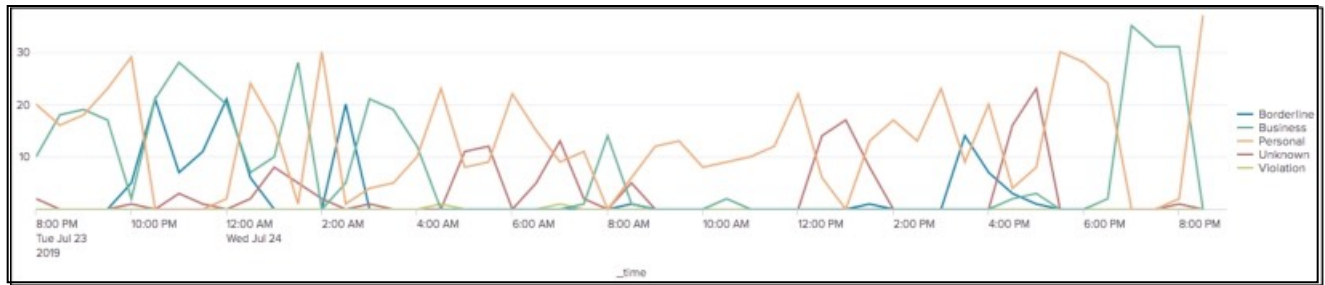
29. Click **Search** to clear the previously set **Format** options.

30. Search for web appliance events [cisco\_wsa\_squid] during the **last 24 hours**.

31. Use the `timechart` command to count the events by usage.

32. Change the visualization to **Line Chart**.

*Results Example:*



33. Save the search as report, **L2S3**.
34. Add this report to your *IT Ops* dashboard in a panel named: **Internet Usage - Last 24 Hours**. Do **not** click the button to view the dashboard; instead, close the Your Dashboard Panel Has Been Created window by clicking the x in the upper right corner. (If you accidentally do click **View Dashboard**, click your browser's Back button to get back to the L2S3 report.)
35. Click on **Trellis**.
36. Click the **Use Trellis Layout** checkbox.
37. For Scale, click **Independent**.

*Results Example:*



38. Save the search as a report, **L2S4**.
39. Add this report to your IT Ops dashboard in a panel named: **Internet Usage by Category**.
40. Edit your dashboard and arrange your panels so that the dashboard looks like this:

*Results Example:*



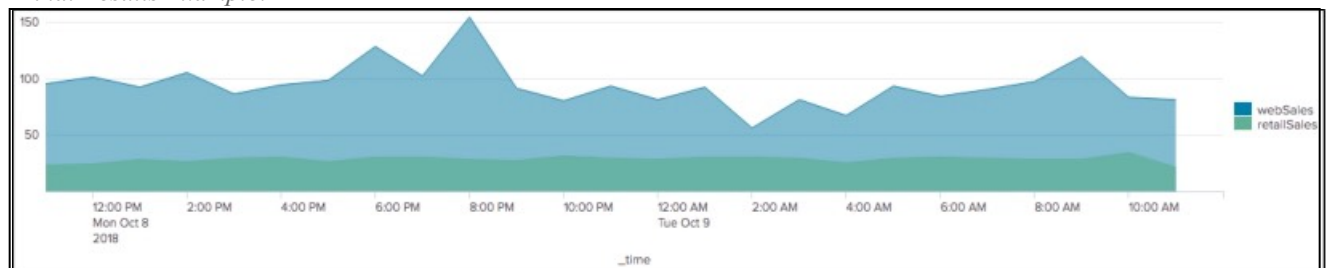
41. Click **Save**.

**NOTE:** Visualization formatting options persist until you turn them off or change them. So, the next time you do a visualization, by default, it will appear as a line chart with the Trellis option, because that's what you chose previously. And if that's not what you want, just change the options—turn off the Trellis option, choose a different type of visualization, etc.

### CHALLENGE Exercise:

Display and compare online and vendor sales during the last 24 hours.

*Final Results Example:*



42. Search for successful online purchase events [`access_combined`] during the **last 24 hours** and enclose the entire search string in parentheses. (As you continue to modify this search string in the upcoming lab steps, the parentheses will be helpful.)

43. Modify the search string to also search for all retail sales [vendor\_sales]. Enclose this new clause in a separate set of parentheses.

**Hint:** Use OR to view events from multiple indexes and sourcetypes (not AND).

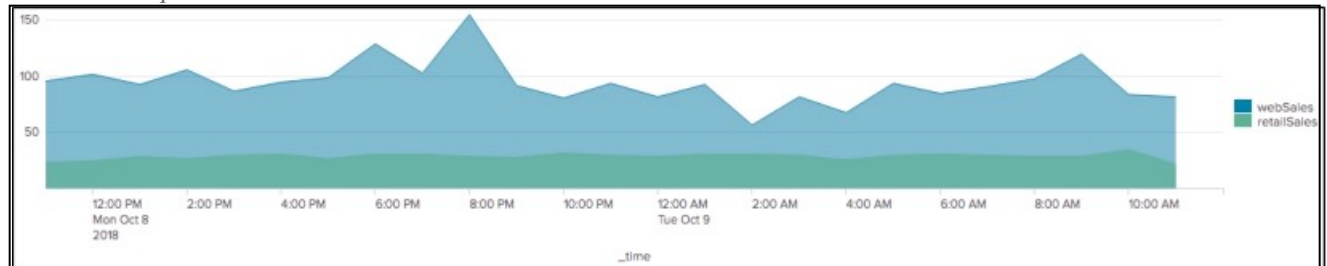
44. Use `timechart` to count the sales events by `sourcetype`. Change the sampling interval to 1 hour.

**Hint:** View the results in the **Statistics** tab to see the time values.

45. Rename the `access_combined` column to `webSales` and the `vendor_sales` column to `retailSales`.

46. Display the results as an **Area Chart**.

*Results Example:*



47. Save the search as report, **L2C1**.

48. Optionally, revise the formatting to show `retailSales` as a chart overlay, and save as **L2C2**.

