splunk>

Lab Exercise 3 – Commands for Visualizations

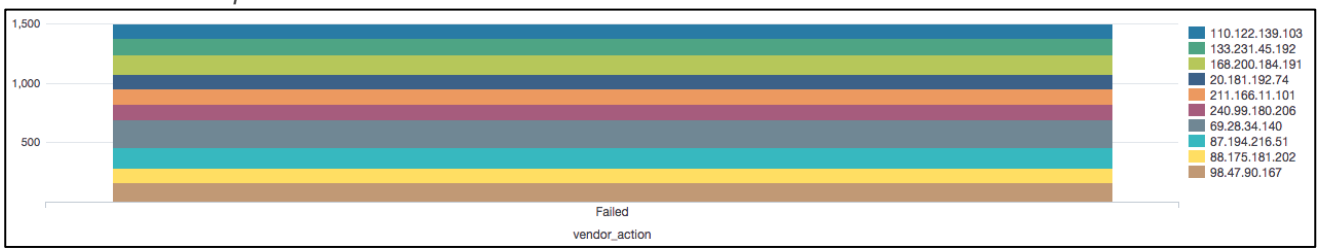
Description

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

Steps

Task 1: Report the failures 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 failed during the **last 24 hours**.

   index=security sourcetype=linux_secure vendor_action=failed

Results Example:

i	Time	Event
>	2/2/18 3:15:52.000 PM	Fri Feb 02 2018 23:15:52 www2 sshd[3208]: Failed password for invalid user mysql from 194.215.205.19 port 2328 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
>	2/2/18 3:15:52.000 PM	Fri Feb 02 2018 23:15:52 mailsv1 sshd[3510]: Failed password for djohnson from 178.164.93.83 port 4056 ssh2 host = mailsv1 source = /opt/log/mailsv1/secure.log sourcetype = linux_secure
>	2/2/18 3:15:52.000 PM	Fri Feb 02 2018 23:15:52 www3 sshd[4329]: Failed password for mail from 183.60.133.18 port 2260 ssh2 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure

2. Using the `chart` command, display a count for each action [`vendor_action`] the users performed by IP [`src_ip`].

   Hint: Use `over … by`

   index=security sourcetype=linux_secure vendor_action=failed
   | chart count over vendor_action by src_ip

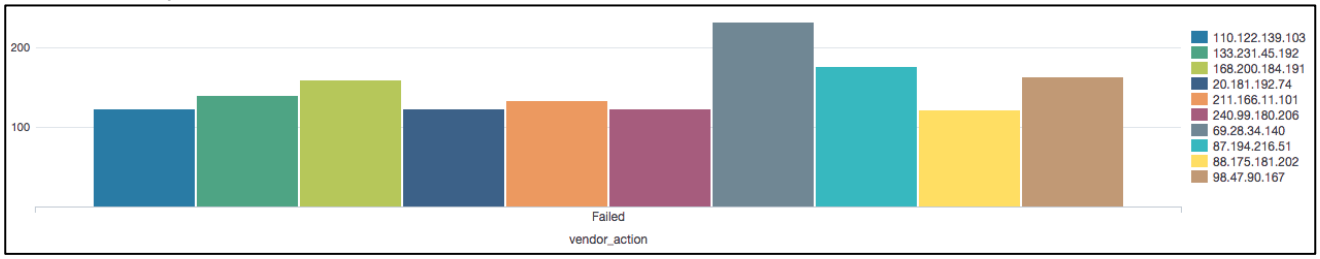
Results Example:

vendor_action	110.122.139.103	133.231.45.192	168.200.184.191	20.181.192.74	211.166.11.101	240.99.180.206	69.28.34.140	87.194.216.51	88.175.181.202	98.47.90.167	OTHER
Failed	124	140	160	123	134	124	233	176	122	164	8299

3. Click on the **Visualization** tab and make sure **Column Chart**  is selected.
4. As you can see, there is an OTHER column at the end of the results. Set the `useother` option to `f`, to remove this column.

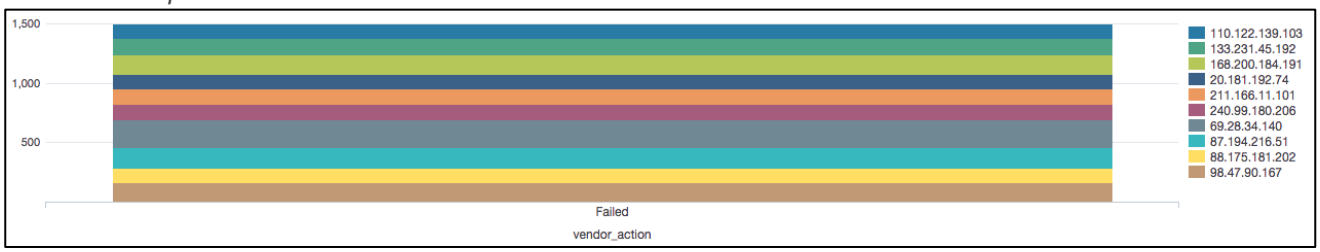
```
index=security sourcetype=linux_secure vendor_action=failed
| chart count over vendor_action by src_ip useother=f
```

Results Example:



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

Results Example:

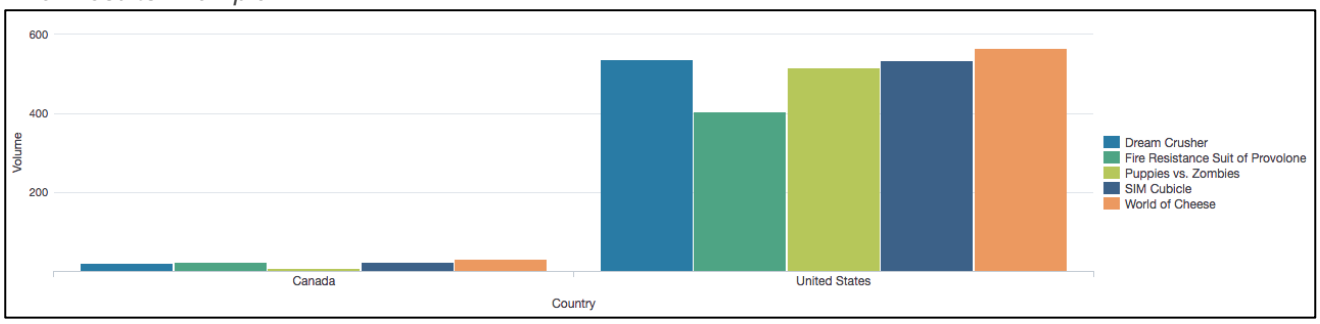


6. Click **Save As** and choose **Report**.
7. Name your report **L2S1** and click **Save**.
8. On the Your Report Has Been Created screen, click **Add to Dashboard**.
9. Save the dashboard with these values:
   - Dashboard: *New*
   - Dashboard Title: *IT Ops*
   - Panel Title**:** Potential Security Breaches
   - 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 far right of the screen.
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.

Task 2: Chart by country the five best selling products for our 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**.

    index=sales sourcetype=vendor_sales VendorID<4000

Results Example:

i	Time	Event
>	2/5/18 9:19:28.000 AM	[05/Feb/2018:17:19:28] VendorID=1106 Code=F AcctID=xxxxxxxxxxx1352 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales
>	2/5/18 9:19:08.000 AM	[05/Feb/2018:17:19:08] VendorID=3106 Code=H AcctID=xxxxxxxxxxx0271 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales
>	2/5/18 9:17:12.000 AM	[05/Feb/2018:17:17:12] VendorID=1149 Code=N AcctID=xxxxxxxxxxx9840 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales

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

```
index=sales sourcetype=vendor_sales VendorID<4000
| chart count 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`.

```
index=sales sourcetype=vendor_sales VendorID<4000
| chart count over VendorCountry by product_name
```

Results Example:

VendorCountry	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Manganiello Bros. Tee	OTHER	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of 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).

```
index=sales sourcetype=vendor_sales VendorID<4000
| chart count over VendorCountry by product_name limit=5
```

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.

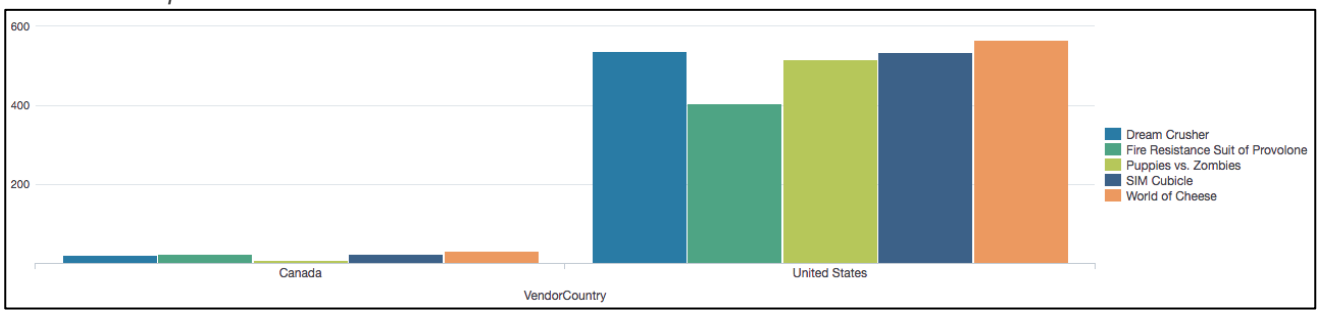
```
index=sales sourcetype=vendor_sales VendorID<4000
| chart count over VendorCountry by product_name limit=5 useother=f
```

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

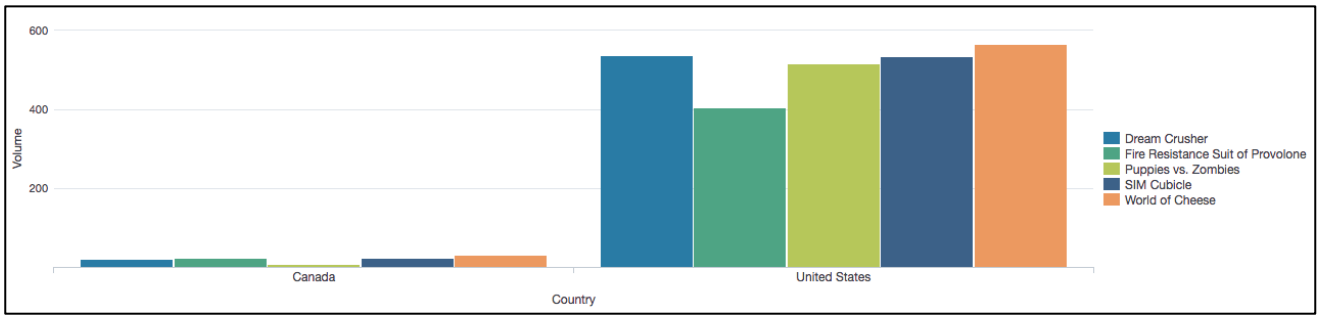
25. Switch to the **Visualization** tab and, if a column chart was not automatically shown, set the chart type to **Column Chart**.

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

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

28. Search for web appliance events [`cisco_wsa_squid`] during the **last 24 hours**.

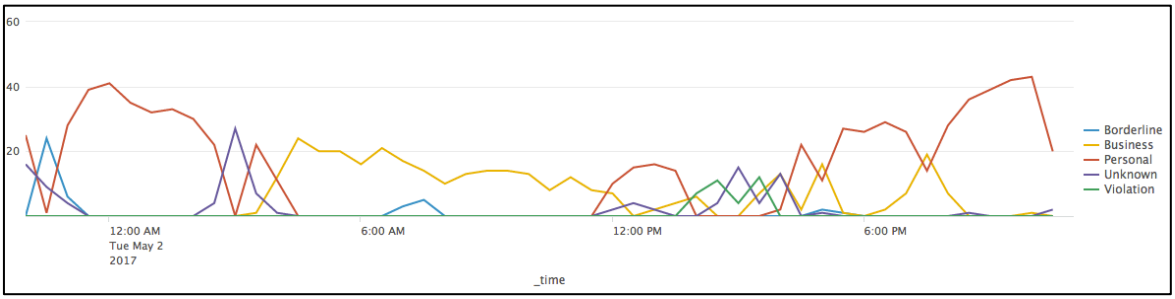
```
index=network sourcetype=cisco_wsa_squid
```

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

```
index=network sourcetype=cisco_wsa_squid
| timechart count by usage
```

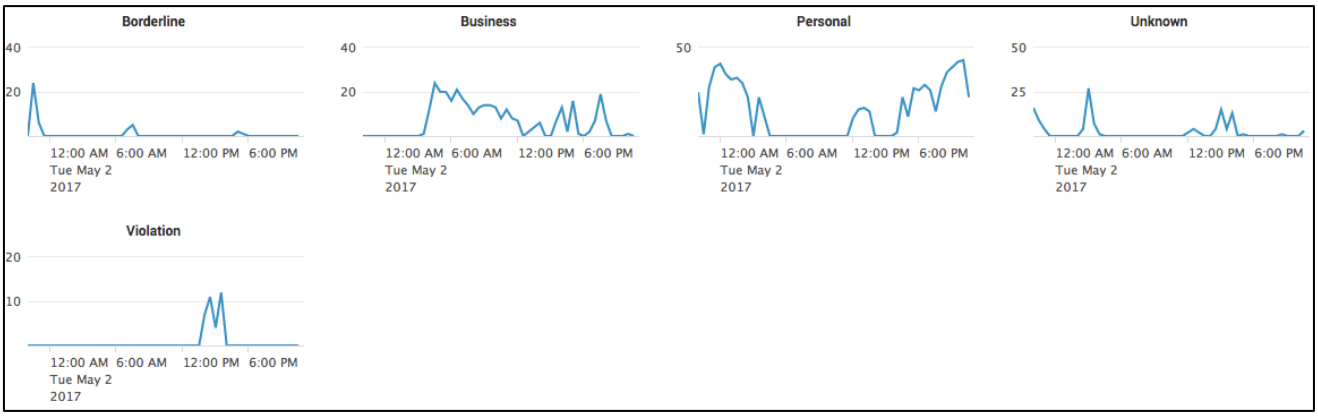
30. Change the visualization to **Line Chart**.

Results Example:



31. Save the search as report, **L2S3**.
32. 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.)
33. Click on **Trellis**.
34. Click the **Use Trellis Layout** checkbox.
35. For Scale, click **Independent**.

Results Example:



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

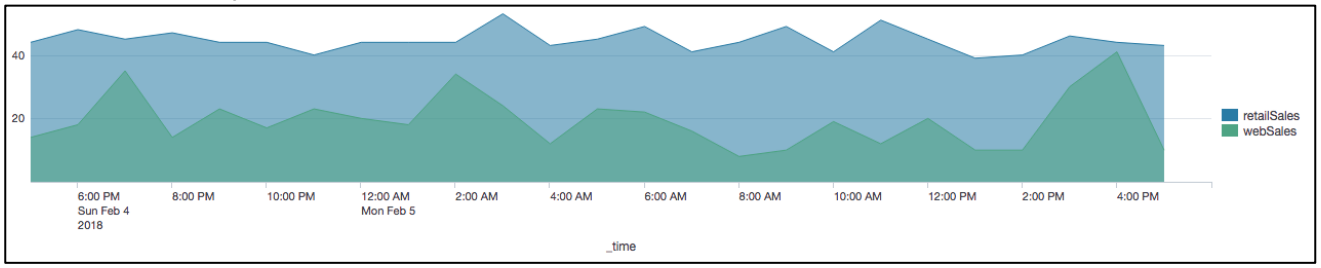
Results Example:

39. Click **Save**.

NOTE:	You may want to turn off Trellis layout and any other visualization formatting options before proceeding. Visualization formatting options persist until turned off or changed.

Task 4: Display and compare online and vendor sales during the last 24 hours.

Final Results Example:



40. 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.)

    (index=web sourcetype=access_combined action=purchase status=200)

41. 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).

    ```
    (index=web sourcetype=access_combined action=purchase status=200) OR (index=sales sourcetype=vendor_sales)
    ```

42. 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.

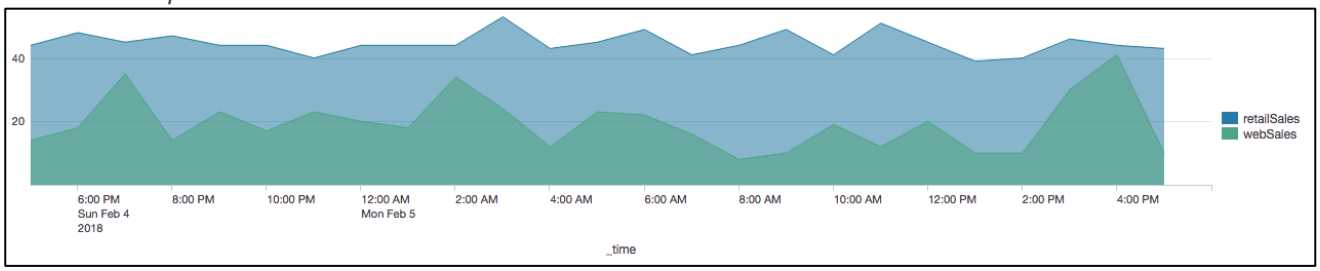
    ```
    (index=web sourcetype=access_combined action=purchase status=200) OR (index=sales sourcetype=vendor_sales)
    | timechart span=1h count by sourcetype
    ```

43. Rename the access_combined column to webSales and the vendor_sales column to retailSales.

    ```
    (index=web sourcetype=access_combined action=purchase status=200) OR (index=sales sourcetype=vendor_sales)
    | timechart span=1h count by sourcetype
    | rename access_combined as webSales, vendor_sales as retailSales
    ```

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

Results Example:



45. Save the search as report, **L2C1**.
46. Optionally, revise the formatting to show `retailSales` as a chart overlay, and save as **L2C2**.