Splunk: Reports, Statistics, Dashboards and Visualizations

Cybersecurity

SIEMS, Day 3

Class Objectives

By the end of class today, you will be able to:

- Use Splunk’s documentation to implement new search commands.
- Generate and use reports from Intrusion Prevention System logs.
- Perform statistical analysis based on event information.
- Use visualization to compare and aggregate event field data.

Day 2 Recap

Last class, we used Splunk to investigate if brute force attacks were occurring at a website.

We looked at the **volume of activity** at the site and developed a **baseline** and **threshold**.

- A **baseline** differentiates between a real attack and normal daily activity.
- A **threshold** is the volume of activity at which an alert is triggered.

Day 2 Recap

Last class, we used Splunk to investigate if brute force attacks were occurring at a website.

We looked at the **volume of activity** at the site and developed a **baseline** and **threshold**.

- A **baseline** differentiates between a real attack and normal daily activity.
- A **threshold** is the volume of activity at which an alert is triggered.

In the first exercise of the day, you will investigate the **target** of the suspicious activity by looking at the relationship between **locked accounts** and **account and domain names.**

Security teams use Splunk's **`contingency`** command to create a **contingency table** to show the relationship between fields in an event.

- These tables help determine root causes, analyze patterns for advanced threat detection, and discover threat actors.

Activity: Contingency Command Warm-Up

In this activity, you will investigate locked accounts using the `contingency` command.

Activities/1_warmup

Suggested Time:
20 Minutes

Contingency Warm-Up Review

Write an SPL command that will search for locked accounts.

Contingency Warm-Up Review

Write an SPL command that will search for locked accounts.

Answers may vary:

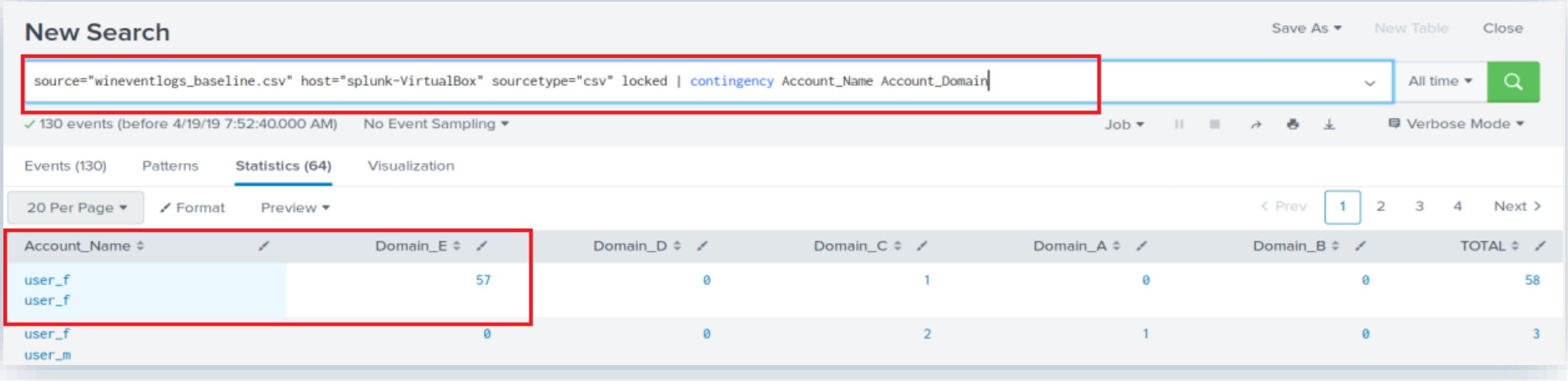
```
source="wineventlogs_baseline.csv" locked
```

Contingency Warm-Up Review

Contingency tables can be used to detect abnormal activity.

The `locked` search uses a pipe with the `contingency` command to gather the search results.

```
source="wineventlogs_baseline.csv" host= "splunk-VirtualBox"
sourcetype="csv" locked | contingency Account_Name Account_Domain
```



Account_Name	Domain_E	Domain_D	Domain_C	Domain_A	Domain_B	TOTAL
user_f user_f	57	0	1	0	0	58
user_f user_m	0	0	2	1	0	3

Contingency Warm-Up Review

Where was the attacker trying to gain access?

Contingency Warm-Up Review

Where was the attacker trying to gain access?

`User_f` and `Domain_E`, which showed 57 locked events.

Contingency Warm-Up Review

Additional Challenge: Using the access_30DAY.log file, give another example of where a contingency table can be used such as **User agent and status** analysis.

New Search

Save As ▾ New Table Close

```
source="access_30DAY.log" sourcetype="access_combined_wcookie" | contingency useragent status
```

All time ▾

71,274 of 71,274 events matched No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (71,274) Patterns **Statistics (27)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 Next >

useragent	200	503	406	400	500	408	404	505	403	TOTAL
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)	10688	218	172	180	184	210	182	128	46	12008
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	5060	134	88	94	98	84	78	74	36	5746
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)	4936	116	82	84	90	56	86	48	26	5524
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)	4376	86	102	66	76	78	54	64	26	4928
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)	4186	78	70	66	78	72	50	50	34	4684

Generating Reports in Splunk

Generating Reports in Splunk

Reports are created when you **save a search**.

- Each report contains the events, field and statistical data that was generated from running the SPL search command.

Reports can be run anytime and they **fetch fresh search results** each time they run.

Reports can be **scheduled** to run at any interval .

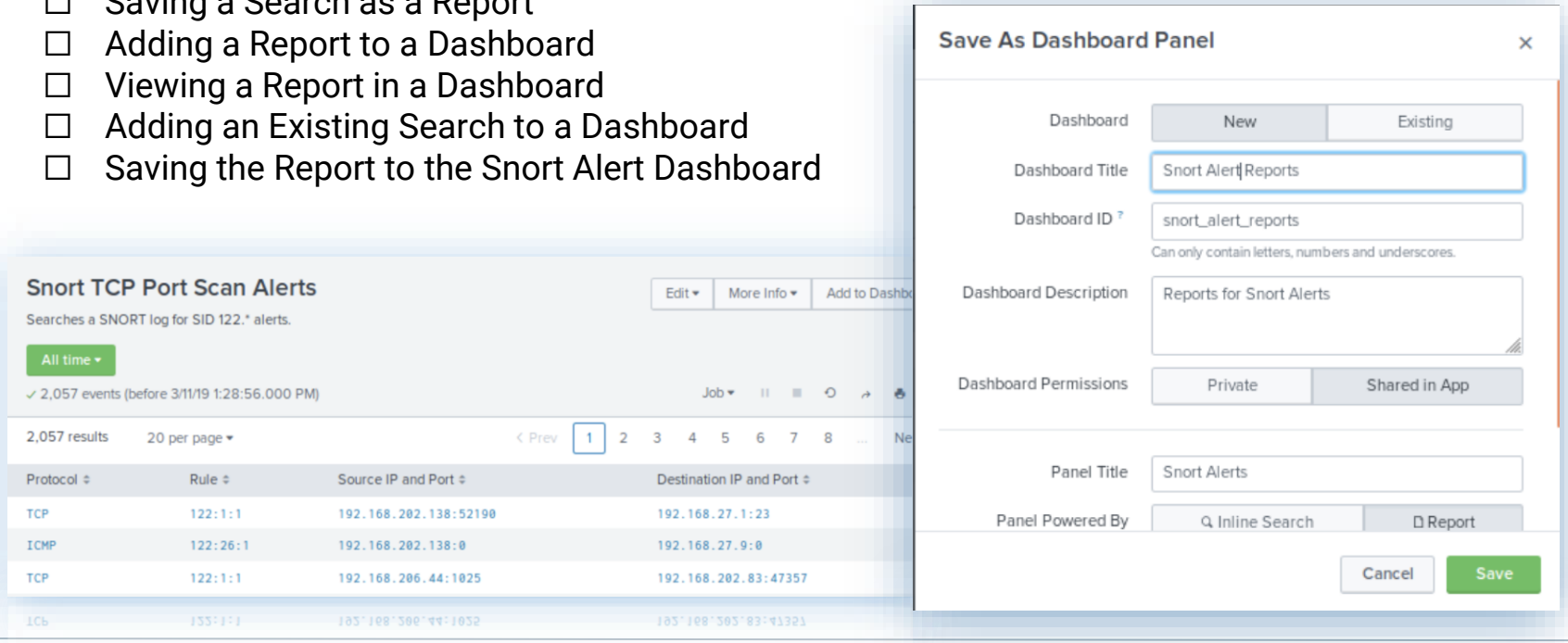
Reports show **statistics** and **visualizations**. They can also be used in **dashboards**.

Reports can be run as **historical searches** during a security incident investigation.

Reports and Dashboards Demo

Now that you're more familiar with searching in Splunk, the next step is creating reports and dashboards from search results.

- ☐ Saving a Search as a Report
- ☐ Adding a Report to a Dashboard
- ☐ Viewing a Report in a Dashboard
- ☐ Adding an Existing Search to a Dashboard
- ☐ Saving the Report to the Snort Alert Dashboard



Introduction to the Next Activity:

In the next activity, you will pair up and create a statistical report to analyze events from Intrusion Prevention System(IPS) logs from the Fortinet Security System.

Fortinet provides network, firewall, application and endpoint/device security solutions that can be integrated with Splunk Enterprise.

What is the difference between an **IDS** and an **IPS**?

Introduction to the Next Activity:

In the next activity, you will pair up and create a statistical report to analyze events from Intrusion Prevention System(IPS) logs from the Fortinet Security System.

Fortinet provides network, firewall, application and endpoint/device security solutions that can be integrated with Splunk Enterprise.

What is the difference between an **IDS** and an **IPS**?

- IDS simply monitors where as an IPS can prevent a packet from delivery.

Introduction to the Next Activity:

In the next activity, you will pair up and create a statistical report to analyze events from Intrusion Prevention System(IPS) logs from the Fortinet Security System.

Fortinet provides network, firewall, application and endpoint/device security solutions that can be integrated with Splunk Enterprise.

What is the difference between an **IDS** and an **IPS**?

- IDS simply monitors where as an IPS can prevent a packet from delivery.

This activity contains a new command called **`stats`**, which generates a report that displays summary statistics. Searches return the sum, count, or average of event field data.

Activity: Generating a Statistical Report from Firewall Attack Logs

In this activity, you will create a statistical report to analyze events from Intrusion Prevention System logs.

Activities/2_Reports_and_Stats

Suggested Time:
20 Minutes

Activity Review

There was **a lot** of information in the attack log for each event. Splunk quickly indexed and extracted the metadata field data.

`stats by count <field>, <field>, <field>...`

- `stats` is the Splunk command.
- `count` provides the number of events.
- `field` is a field in the event

This is another SPL command that takes the input from a previous command via a pipe.

- The command also takes arguments such as sum or average.
- Example: `| stats by count “scr_ip”, “dst_ip”`

Activity Review Part 1: Creating the Search

What fields contain the **year(s)** for the attack?

Which fields contain the **month(s)** for the attack?

What is the **attack name?**

Using the NIST National Vulnerability Database, what does the attack **do**?

Activity Review Part 1: Creating the Search

What fields contain the **year(s)** for the attack?

`date_year`

Which fields contain the **month(s)** for the attack?

What is the **attack name?**

Using the NIST National Vulnerability Database, what does the attack **do**?

Activity Review Part 1: Creating the Search

What fields contain the **year(s)** for the attack?

`date_year`

Which fields contain the **month(s)** for the attack?

`date_month`

What is the **attack name?**

Using the NIST National Vulnerability Database, what does the attack **do**?

Activity Review Part 1: Creating the Search

What fields contain the **year(s)** for the attack?

`date_year`

Which fields contain the **month(s)** for the attack?

`date_month`

What is the **attack name?**

`Oracle.9i,TNS.OneByte.Dos`

Using the NIST National Vulnerability Database, what does the attack **do**?

Activity Review Part 1: Creating the Search

What fields contain the **years** for the attack?

`date_year`

Which fields contain the **months** for the attack?

`date_month`

What is the **attack name?**

`Oracle.9i,TNS.OneByte.Dos`

Using the NIST National Vulnerability Database, what does the attack **do**?

"The Transparent Network Substrate (TNS) Listener in Oracle 9i 9.0.1.1 allows remote attackers to cause a denial of service (CPU consumption) via a single malformed TCP packet to port 1521."

Activity Review Part 1: Creating the Search

Create an SPL search command that searches the firewall IPS event logs using the attack name and returns:

- The count of attacks by `year` and `month`
- Then sorts the counts in descending order
- Executes the search using `All Time`.

Activity Review Part 1: Creating the Search

Create an SPL search command that searches the firewall IPS event logs using the attack name and returns:

- The count of attacks by `year` and `month`
- Then sorts the counts in descending order
- Executes the search using `All Time`.

Add the SPL stats and sort command:

```
|stats count by date_year, date_month | sort - count
```

```
fortinet_logs.csv attack_name=Oracle.9i.TNS.OneByte.DoS | stats count by date_year, date_month | sort - count
```

Activity Review

2. Creating the Statistical Report

Save the search as a Report with the titler `OPS115: Firewall IPS Report`

3. Find and Display the Report in the Reports list

Activity Review

2. Creating the Statistical Report.

Save the search as a Report with the title = `OPS115: Firewall IPS Report`

Click on Save As > Report. Give it a title of OPS115:Firewall IPS Report

3. Find and Display the Report in the Reports list.

Activity Review

2. Creating the Statistical Report.

Save the search as a Report with the title = `OPS115: Firewall IPS Report`

Click on Save As > Report. Give it a title of OPS115:Firewall IPS Report

3. Find and Display the Report in the Reports list.

Select the Report tab located in the App bar.

Click the Report Title (`OPS115: Firewall IPS Report`) and Open in Search

Activity Review: Extra Challenge and Report Results

4. How would you obtain the total number of attacks for each month of each year in the attack log?

5. What month(s) and year(s) had the most attacks?

Activity Review: Extra Challenge and Report Results

4. How would you obtain the total number of attacks for each month of each year in the attack log?

Change the sort to **`sort - date_month`**

```
source="foritnet_logs.csv" attack_name="Oracle.9i.TNS.OneByte.DoS" | stats
count by date_year, date_month | sort - date_month
```

5. What month(s) and year(s) had the most attacks?

Activity Review: Extra Challenge and Report Results

4. How would you obtain the total number of attacks for each month of each year in the attack log?

Change the sort to **`sort - date_month`**

```
source="foritnet_logs.csv" attack_name="Oracle.9i.TNS.OneByte.DoS" | stats
count by date_year, date_month | sort - date_month
```

5. What month(s) and year(s) had the most attacks?

`March 2019`

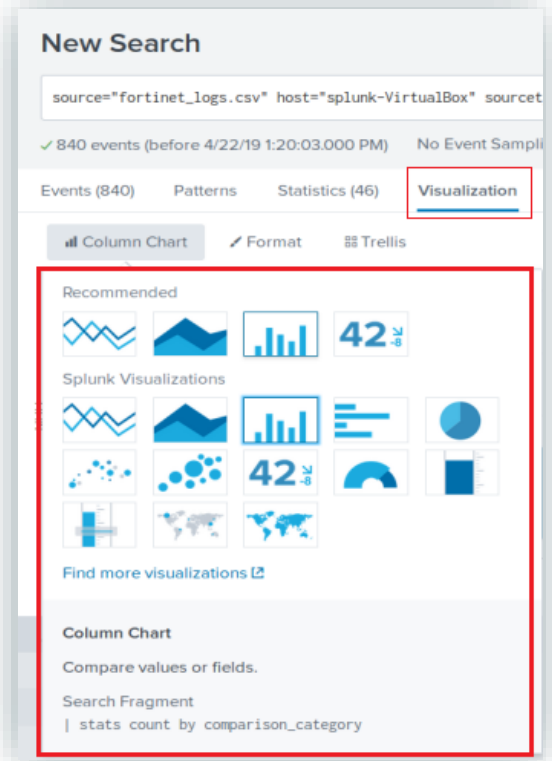
Visualizations

Visualizing Event Data in Splunk

We can create visualization elements such as charts, buttons and maps, and add them to our dashboards.

We have been displaying our data in the Events and Statistics tab, but Splunk provides more useful visual representations, making it easier for Security teams to analyze and interact with data during investigations and day-to-day operations.

These elements are available under the **Visualizations** tab, where you'll find options like: bar, pie and bubble charts, radial and filter gauges, and geographic maps.



Single Data and Multiple Data

Visualization elements are selected based on whether the data being represented it a **single point data** or a **multiple point data.**

- An example of a single data point visualization would be a total count of attacks displayed as a *single number*.

- An example of a multiple data point visualization would be a spreadsheet of counts of attacks, *correlated to attack types*.

Representing Single Data Points

There are times when a single data point needs to be visualized with severity levels.

- For example, if a web application wanted to look at a single data point such as "count of bad logins" over the last hour.
- A visualization could illustrate if that data point is currently at a normal, high or critical level.

This visualization can be accomplished by using a **Radial Gauge Visualization**.

- Radial Gauges are similar to what you see in your Car's Dashboard when looking at your car's RPM.
  - RPM - (Revolutions per minute) is the single data point your car's Dashboard is visualizing.
  - In your RPM display, if your RPMs reach a certain value, it is typically represented in Red indicating you have reached a level that is too high.

Student Activity: Single Data Point Visualization

In this activity, you will create visual elements for your Fortinet Firewall Research using a radial gauge.

Activities/Stu_Visualization-1

Suggested Time:
20 Minutes

Single Data Point Review

Create a Radial Gauge to monitor the the attack_id=10725 over a one hour period

Set the ranges and colors to values you determine would be appropriate

The query will be:

source= “fortinetlogs.csv” attack_id=“10725” | stats count as total

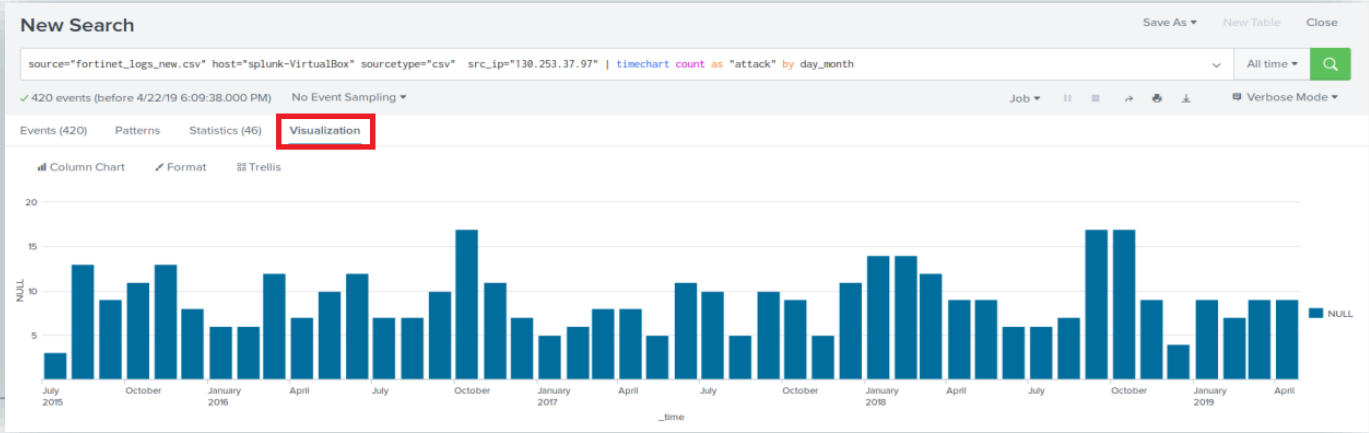
Multiple Data Point Visualization

Visualization Demo: Time Chart

In the next demo, we'll create a **time chart** and a **cluster map** using event data from the Fortinet Firewall Attack Log activity.

- The `timechart` command produces **trends over time** searches.
- We'll create a time chart that displays the monthly activity for all years of the attack.

```
| timechart count as attack by day_month
```



Visualization Demo: Cluster Map

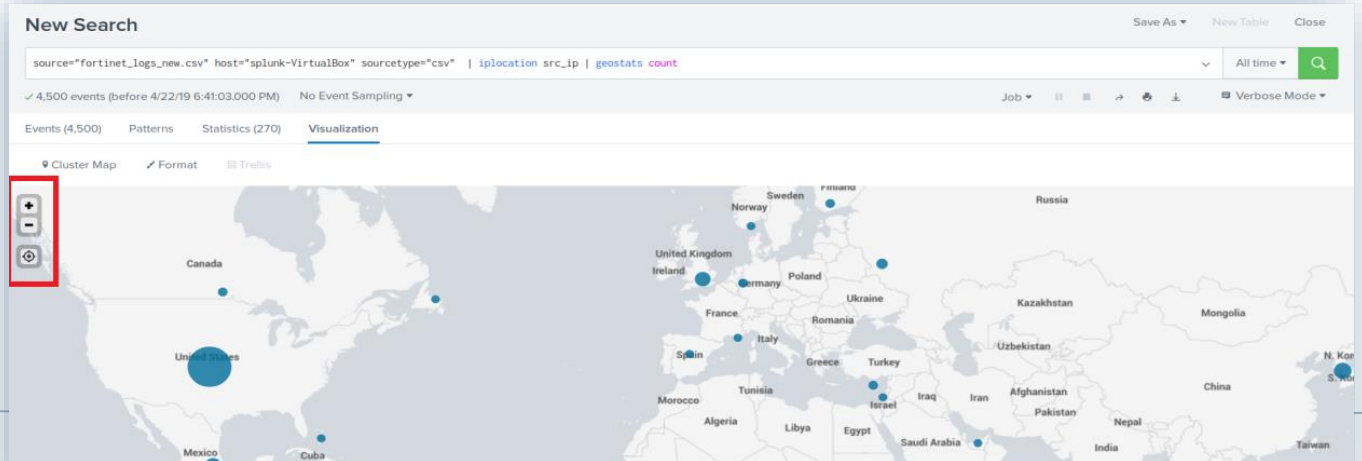
We'll use **`iplocation`** and **`geostats`** command to report on the locations of attack activities.

`Iplocation` command extracts local information from IP addresses.

- `Iplocation` returns *City, Country, latitude, longitude* and *region* in event fields

`Geostats` command takes the IP data and generates statistics which are grouped into geographical data points that can then be rendered on a map.

```
source="_fortinet_logs_new.csv" | iplocation src_ip | geostats count
```



Student Activity: Multiple Data Point Visualization

In this activity, you will create visual elements for your Fortinet Firewall Research using timecharts, attack counts, maps and area charts.

Activities/4_Visual

Suggested Time:
20 Minutes

Visualizations Activity Review

Timechart: Create a **timechart** for the top source IP for the DOS attacks by month.

Visualizations Activity Review

Timechart: Create a **timechart** for the top source IP for the DOS attacks by month.

```
| src_ip="130.253.37.97" | timechart count as "attack" by day_month
```

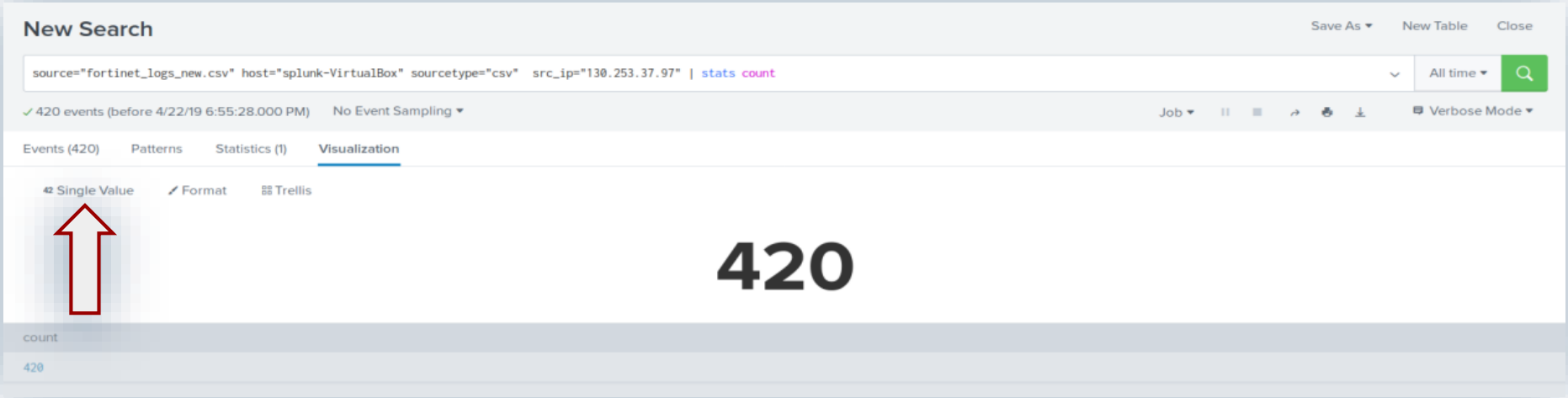
Visualizations Activity Review

Attack Count: Generate the count (420) using the stats command.

Visualizations Activity Review

Attack Count: Generate the count (420) using the stats command.

```
src_ip="130.253.37.97" | stats count
```



Then, under the visualization tab, select **Single Value.**

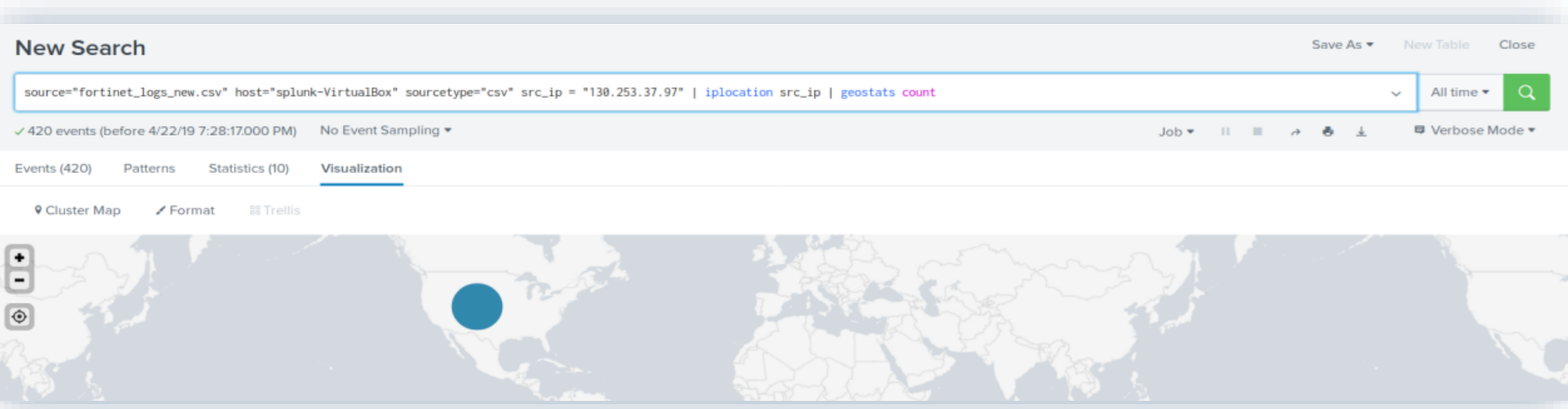
Visualizations Activity Review

Map: Generate a map for only the top IP source.

Visualizations Activity Review

Map: Generate a map for only the top IP source.

```
src_ip="130.253.37.97" | iplocation src_ip | geostats count
```



Visualizations Activity Review

Area Chart: Generate an area chart that displays the **targets** of the attack for the source IP address.

Visualizations Activity Review

Area Chart: Generate an area chart that displays the **targets** for the attack for the source IP address

```
src_ip="130.253.37.97" AND dest_ip=* | timechart count by dest_ip | sort - dest_ip
```

Working with Splunk Dashboards

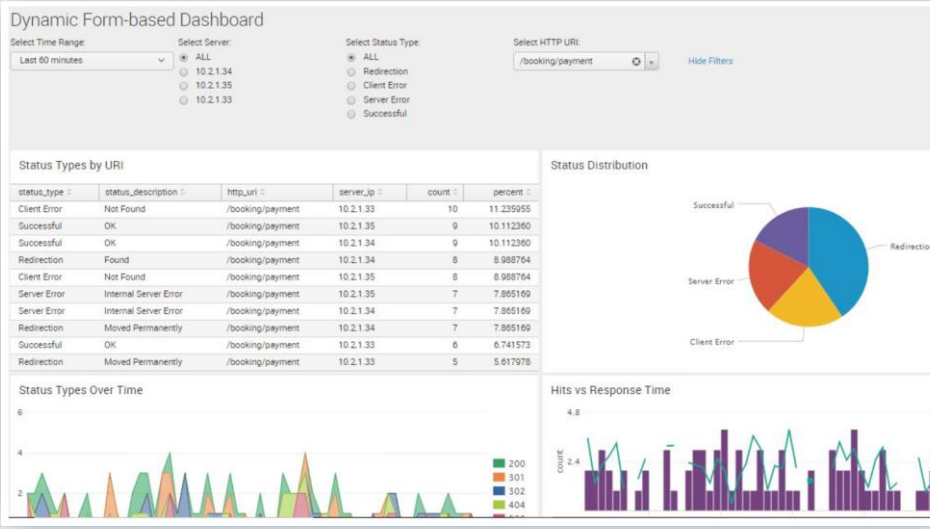
Splunk Dashboards

Dashboards integrate elements in panels to display the most relevant information for different teams and use cases.

Dynamic form-based dashboards allow for modifications using radio, buttons, and check boxes.

Real-time dashboards are displayed on panel screens for constant viewing in network and security operations centers.

Dashboards as scheduled reports can be saved as a PDF file or sent as emails to NOC or SOC teams at scheduled.



Activity: Create a Dashboard for Failed Password Attempts

In this activity, you will create a Linux and Windows Failed Password Dashboard for Monitoring login attempts by an SOC Team.

Activities/Dashboards

Suggested Time:
15 Minutes

Class Objectives

By the end of class today, you will be able to:

- Use Splunk's documentation to implement new search commands.
- Generate and use reports from Intrusion Prevention System logs.
- Perform statistical analysis based on event information.
- Use visualization to compare and aggregate event field data.

Any Questions?