

Question 3: Dashboards

Why are dashboards so important for log analysis?

Answer: real-time visibility in a dashboard. It reduces troubleshooting and resolving time by offering instant results. It is a best-suited tool for root cause analysis. Creating Dashboards contain panels that display data visualizations such as charts, tables, event lists, and maps. Each dashboard panel uses a base search to provide results for the visualizations, or uses searches referenced from reports. When you run a search, you can save it as a report, set an alert and add it to a dashboard.

1. Restate the Problem
2. Provide a Concrete Example Scenario:

Being a SOC manager, I will be getting notifications about performance issues that the public-facing website experiences; and will need to build visualizations that my SOC team can use to determine the severity of the attack. These visualizations will help my SOC team quickly and accurately respond to attacks. I designed a single value radial gauge to assist with monitoring attacks against the website. (designed a search to view the `http_method=POST | stats count as total`) : events for the All Time range

Then I had my SOC team design an alert to trigger when the count reaches the red range. We needed to create a visualization that displays the exact URL path being targeted by attacks. Adding to our query, `(source="radialgauge.csv" host="radialgauge" sourcetype="csv" http_method=POST | top limit=10 uri_path)` and place in a PIE Chart for easy visualization.

I then ask the SOC team to expand our visualizations to provide more geographic information about the attacks; so that our Security team can use this information to create firewall rules that restrict traffic from certain geographic locations. We then designed a geographic map helping visualize where the attacks are ordinating from. Adding to the query `(source="radialgauge.csv" host="radialgauge" sourcetype="csv" http_method=POST | iplocation src_ip | geostats count by uri_path)` to monitor by Source IP and to display a colorful display of the World with all the users colorful highlighted for easy to identify and understand the situation. .

After building the radial gauge, pie chart and geographic map we needed to view all of these data visualizations in a single location by creating a Dashboard and adding in a fourth visualization that contains a statistical report representing the data from the pie chart and placing it next to the pie chart.

The colorful array of graphs, tables, charts, and maps needed to be more interactive so the SOC team could quickly research attacks. The SOC team enhanced the dashboard by adding drilldowns and interactivity features. Also adding time-based input on all panels. And a drill down in the geographic map that links to new searches. Wow!! My SOC team is amazing “TEAM”

Web Data Index Main Index Security Index

- In Project 2, which logging and monitoring systems were in place?

-

- Answer: Monitoring syslog generated by the network can help you keep up to date with activities in your network. Without a centralized logging system, ensuring security becomes impossible. Eventlogs analyzer collects, filters, and organizes syslog messages generated by devices such as routers, switches, firewalls, and Unix/Linux servers on your network. Syslog monitoring A. syslog listener, B. Database-Eventlogs analyzer, C. Log parser

- Which kinds of data did these systems collect?-

Answer: sourcetype = categorize the type of data being indexed. Summary of host, source, and sourcetype. The kinds for data for the

Host= host name, IP address or fully qualified domain name for the machine from which the event originated.

Source= is the 1. file or directory path 2. Network Port. 3. Script from which the event originated.

Sourcetypes= classification of your data examples: cisco_firewall, sales_entries.

- Answer: logs are aggregating data from different parts of the IT environment: operating system, firewalls, servers, switches, routers, etc. When it comes to storage, security systems such as firewalls and intrusion detection systems are the most demanding in terms of data volume they produce

- Which kinds of data did these systems not collect?-

- Answer: Archived

-

1. Explain the Solution Requirements

- What did you use Kibana for on Day 2?
 - Answer: Geographic Map visualization can monitor where users access their application from to help determine the source of security issues. (geostats and iplocations to help display Contextualizing data (displays the number of logins per minute into a web application. Gauge visualization contextualizes the number of severity of the login count.)
 - Answer: Kiban's visualizations can display single values, such as total count of attacks, and multiple values, such as a chart of attacks correlated by attack type
 - Answer: Creating simple bar and column charts to complex horizon charts and punch cards.
 - Answer: Multiple Value visualization list out the users being attacked and the number of attacks experienced by each user.
 - Answer: Monitoring a website will display all the following at the same time: Successful logins on the website. Unsuccessful logins on the website. A geographic map illustrating where the activity is coming from and Pie chart to display the specific pages of the website that are being accessed.
 - Answer: I used Kabana's easy to load, view and edit feature to gather all the data from all the sources of attacks and set alarms, reports, and escalate alerts via email, text, phone, or all the above to the entire SOC team for immediate response.
-
- What kinds of data did you look for during your analysis?
 - Answer: 1.Successful logins on the website. 2. Unsuccessful logins on the website. 3. A geographic map illustrating where the activity is coming from and 4. Pie chart to display the specific pages of the website that are being accessed. Brute Force Attacks, Supply Chain Attacks with various PROCESSES and MODES you go thru to build your product ie software from a Cyber supply Chain infiltrate their network once the attacker was able to alter the code in the software development companies' Code Attaching Malicious code every time the company does and system update the injection is made to all the users.
-
- Which tools did you use to analyze the data -- search, queries, dashboards, etc.?
 -

- Answer: Radial gauge to visualize the data for all the POST requests during the 2 hour period of the attack. (``source="radialgauge.csv" `http_method=POST `stats count as total`) and then ran a query with the top URI paths (`uri_path`).
-
- Answer: Pie chart was saved as a visualization as a report titled "Pie Chart-Top URI_PATH"
- (`source="radialgauge.csv" host="radialgauge" sourcetype="csv" http_method=POST | top limit=10 uri_path`)
-
- Answer: Bar chart was saved to visualize the and titled Bar Graph to show all the successful logins for the top 10 users
- (`"an account was successfully logged on | top limit=10 user`)
-
- Answer: Geographical map to visualize the iplocation, geostats , and identify `http=POST | iplocation src_ip | geostats count by uri_path`
- (`source="radialgauge.csv" host="radialgauge" sourcetype="csv" http_method=POST | iplocation src_ip | geostats count by uri_path`)
-
- Answer: Designed a baseline and threshold for hourly level of failed windows activity.

`(source="windos_server_logs.csv" status=failure)`

Answer: Created an alert to trigger when the threshold has been reached.

`(source="windows_server_logs.csv" signature="an account was successfully logged on")`

Answer: Determine a baseline and threshold for hourly count of the signature: A user account was deleted.

`(source="windows_server_logs.csv" signature="A user account was deleted")`

Answer: Created an alert to trigger when the threshold has been reached

`(source="windows_server_logs.csv signature_id=4726)` and email to `SOC@VSI-company.com`)

Answer: Set alert another to trigger an email to `SOC@VSI-company.com` which displays the different

'signature' field values over time. And a line chart that displays the different 'user' field values over time.

(source=source="windows_server_logs.csv" host="windows_server" sourcetype="csv" | timechart span=1d

count by signature) chart (source="windows_server_logs.csv" host="windows_server" sourcetype="csv"

|timechart span=1hr count by signature 3. A bar, column, or pie chart that illustrates the count of different

signatures. source="windows_server_logs.csv" | timechart span=1h count by user)

Answer: A bar, column, or pie chart that illustrates the count of different users. I used a pie chart.

(source="windows_server_logs.csv" | top limit=10 user)

Answer: Created an alert to trigger when the threshold has been reached and email to SOC@VSI-

company.com.

(source="apache_logs.txt" | iplocation clientip Country!="United States")

- Relative to the other tools,
-
- Question: how much did you use dashboards?
-
- Answer: The dash boards made it possible to visualize all the data that was needed in the queries and shower all the data in colorful graphs, maps and stats all in each dashboard.
-
- Question: and why?
-
- Answer: This allows for the SOC to monitor and set alerts and triggers allowing for mitigation of attachments to quickly be escalated thru email , text, and phone calls.

1. Explain the Solution Details

- Which dashboards did you use?
 - Answer: Geolocation map, Radial Dial, Bar Graph, and Statistical Dashboard.
- Give at least three specific examples, including: {the best uses for comparison, composition, or relationship analysis when there are only a few variables and data points.} {Use tables when you need to compare or look up individual values.}
 - The name of the charts
 -
 - Answer: 1. The Gauge is data visualization of materialized charts. The scale represents the metric, the pointer represents the dimension, and the pointer angle represents the value. It can visually represent the progress or actual situation of an indicator. Suitable for comparison between intervals. One example is The Radial Chart is used to compare multiple quantized variables, such as seeing which variables have similar values, or if there are extreme values. They also help to observe which variables in the data set have higher or lower values. Radar charts are suitable for demonstrating job performance.

Answer: 2. Bubble chart A bubble chart is a multivariate chart that is a variant of scatter plot. Except for the values of the variables represented by the X and Y axes, the area of each bubble represents the third value.

Answer: 3. Pie Chart visualized the top 10 URI_PATH being targeted by attacks by the POST request. {Bar chart required a SQL query: (source="radialgauge.csv" http_method=POST | top limit=10 uri_path)} Pie chart was helpful in breaking up all the % in a colorful Column and bar charts. Data for charts and line and area charts. The pie charts are used in fields to represent the proportion of different classifications, and to compare various classifications by the arc. The pie chart is not suitable for multiple series of data, because as the series increases, each slice becomes smaller and finally the size distinction is not obvious. Also pie charts can also be made into a multi-layer pie chart, showing the proportions of different categorical data, while also reflecting the hierarchical relationship.

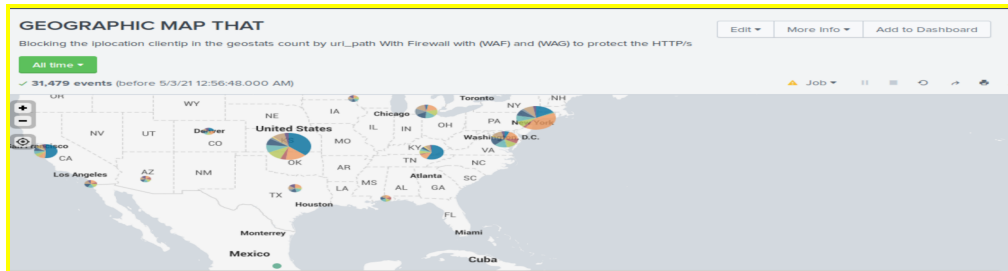
Answer: 4 {Column charts use vertical columns to show numerical comparisons between categories} The column chart takes advantage of the height of the column to reflect the differences.

Answer: 5 {Line chart is used to show the change of data over a continuous time interval or time span. It reflects things as they change time or ordered categories}

Answer: 6 {The area chart is formed on the basis of the line chart. It fills the area between the polyline and the axis in the line chart with color. The fill color can better highlight the trend information.}

- The type of data on the plot axes (e.g., # of Requests vs Time) The stats, chart and timechart commands are great commands to know **(stats)**
 - **Answer: The status field forms the X-axis and the host values form the data series. The range of count values form the Y-axis [list of commands below]**
 -
 - **(| timechart count BY status)**
 - **(| stats count BY status, host, action)**
 - **(| chart count BY status, host)**
 - **(| chart count OVER status BY host)**
 - **Answer: Statistics displays requests based on time into a web application.**
-
- **What kind of activity it indicates**
 - **Answer: The Radial Dashboard generated a single value radial visualization using a timechart to generate a single value and trend indicator. are used to compare multiple quantized variables, such as seeing which variables have similar values, or if there are extreme values. They also help to observe which variables in the data set have higher or lower values. The dial includes a red section that indicates when the level is too high, yellow section shows increased averages, and the green section is normal use. We received 1,200 POST requests during a 2 hour period of the attack. So we designed a radial gauge with the following criteria {Count of total POST request}. source="radialgauge.csv" http_method=POST | stats count as total}**
-
- **Recall the first "interesting" dashboard you examined. What stood out?**
 - **Answer: The Radial Dashboard was amazing with the ability to set the green, yellow and red settings and seeing the dial it the number of attacks. Also setting it to Alert everyone in the SOC in many different ways. Email, text, phone call, and escalate to higher levels if no response. We were tasked with designing a single value radial gauge to assist with monitoring attacks in the radialgauge.csv file. Using the http_method=POST stats count as total. We were notified that they received approximately 1,200 POST requests during a 2 hour period of the attack.**
-
- **Which dashboard did it lead you to next?**

- **Answer: The Geographic map in multicolor with the ability to zoom in to visually see the exact City with the users out puts % using the iplocation src_ip | geostats count (source="radialgaug.csv" host="radialgaug" sourcetype="csv" http_method=POST | iplocation src_ip | geostats count by uri_path)**



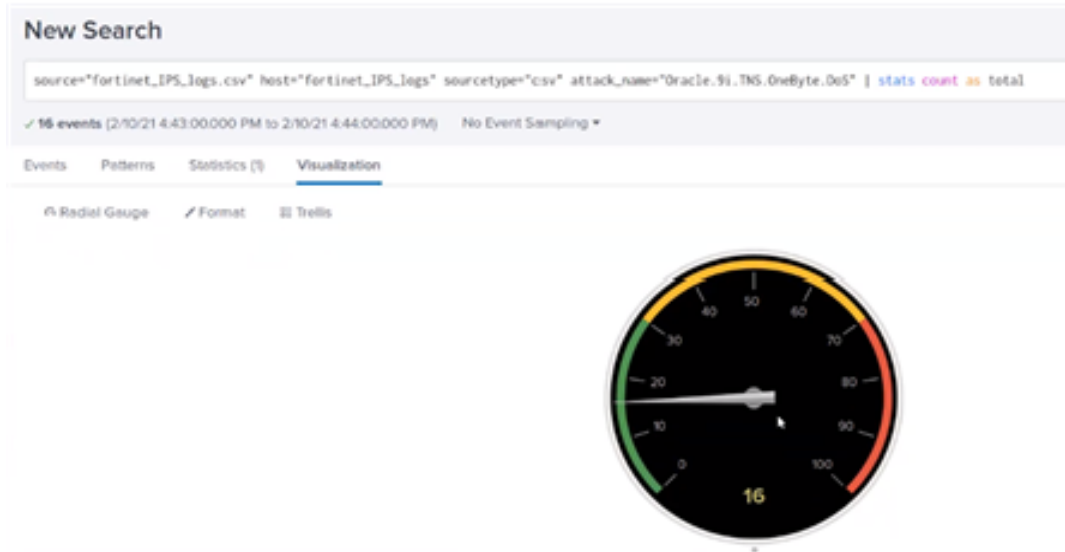
1. Identify **Advantages/Disadvantages** of the Solution

- **Suppose you couldn't use dashboards. Which tools would you use instead?**

(no problem, with the search and creating reports, and developing baselines and setting Alerts thru a link that protects the integrity and avoid tipping off the attacker)

Answer: **Search and create reports , develop baselines and setting alerts were very valuable tools with powerful ability to generate, detect, and alert in email, text, phone.**

Advantage of the dashboard was all the different visualizations with the normal , average and danger Green, Yellow and Red allows for easier detection across multiple screens. All the different data either in the same time span or each dashboard with different times.

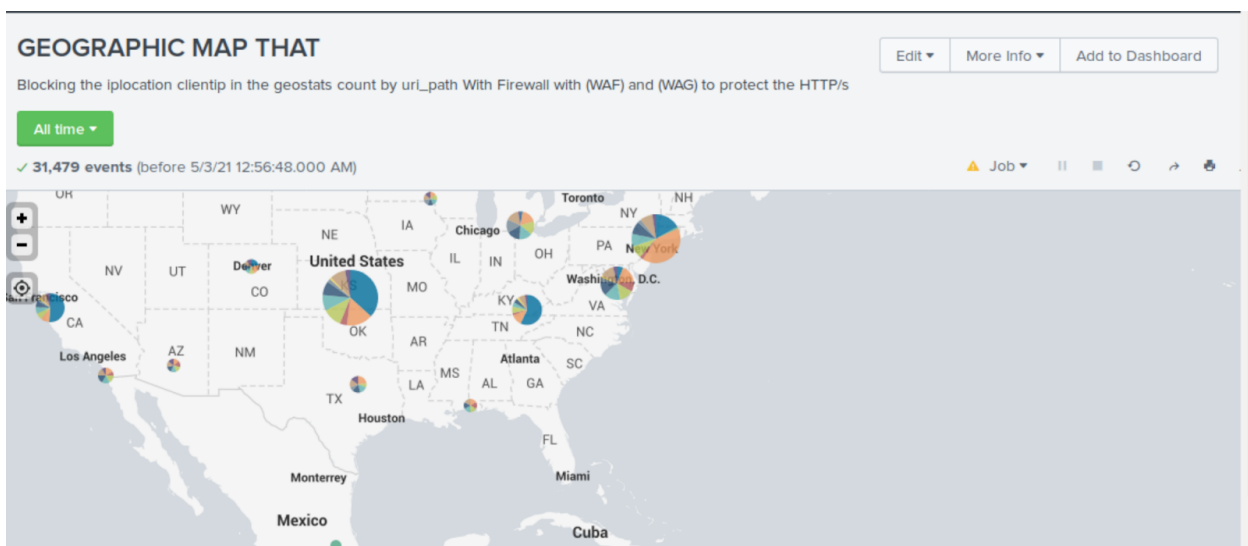


Disadvantages of presenting information without the Dashboard decreases the visualization of all the data being gathered.

- Which dashboards were most useful?

Answer: 1. The Radial Dashboard was very helpful in setting Alerts to go off before the attack and set up different perimeters based on time and numbers of events.

Answer: 2. Yes The Geographic map was helpful in identifying users_ip and geographic location on a colorful map. The Pie Dashboard was helpful in breaking up all the % in a colorful well laid out easy to read dashboard.



- Describe at least one dashboard you wish you had, but which does not exist.

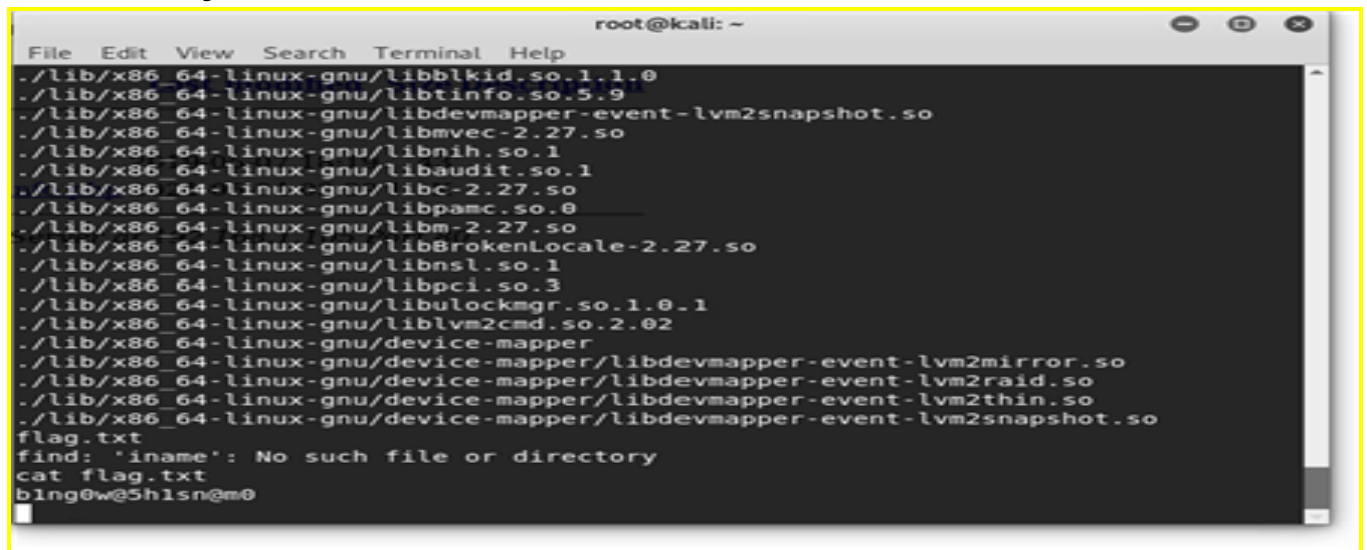
1. Answer: **"DASHBOARD WITH VIDEO OF THE ATTACKER"**

I would like a dashboard that will set: 1.alerts, 2.monitors,3. iplocation src_ip 4. http_method=POST stats count as total, 5. geostats count by uri_path with audible alerts with different sounds for Yellow and Red settings, 6 Dashboard with video of attack sending the attack.

I would like to share what I call "The Golden Nuggets' ' or in the Medical field they call that: " The **Myelin Sheath**" which enables nerve signals (electrical impulses) to be conducted along the nerve fiber with speed and accuracy up to 800 miles per hour. Wow. That is "The Gold Nugget" explanation when I am referring to the Network, Hardware, software, all run off of electrical impulses and developing new neural pathways. Each "Golden Nugget" connects together and eventually your whole mental Network is reconfigured allowing you the ability to perform Red Team and Blue Team SOC with more clarity, more precision of execution, and a better understanding of how to compartmentalize data, and how to communicate to the Cyber Security professionals and non professional with clarity , precision, and understandability.

The Journey has transformed me and equipped me to pursue and excel in the Cyber Security World.

I will leave you all with this to summarize:

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays a list of system libraries: `./lib/x86_64-linux-gnu/libblkid.so.1.1.0`, `./lib/x86_64-linux-gnu/libtinfo.so.5.9`, `./lib/x86_64-linux-gnu/libdevmapper-event-lvm2snapshot.so`, `./lib/x86_64-linux-gnu/libmvec-2.27.so`, `./lib/x86_64-linux-gnu/libnih.so.1`, `./lib/x86_64-linux-gnu/libaudit.so.1`, `./lib/x86_64-linux-gnu/libc-2.27.so`, `./lib/x86_64-linux-gnu/libpamc.so.0`, `./lib/x86_64-linux-gnu/libm-2.27.so`, `./lib/x86_64-linux-gnu/libBrokenLocale-2.27.so`, `./lib/x86_64-linux-gnu/libnsl.so.1`, `./lib/x86_64-linux-gnu/libpci.so.3`, `./lib/x86_64-linux-gnu/libulockmgr.so.1.0.1`, `./lib/x86_64-linux-gnu/liblvm2cmd.so.2.02`, `./lib/x86_64-linux-gnu/device-mapper`, `./lib/x86_64-linux-gnu/device-mapper/libdevmapper-event-lvm2mirror.so`, `./lib/x86_64-linux-gnu/device-mapper/libdevmapper-event-lvm2raid.so`, `./lib/x86_64-linux-gnu/device-mapper/libdevmapper-event-lvm2thin.so`, `./lib/x86_64-linux-gnu/device-mapper/libdevmapper-event-lvm2snapshot.so`. Below the list, it shows `flag.txt`, `find: 'iname': No such file or directory`, `cat flag.txt`, and the prompt `blng0w@5h1sn@m0`.

AND

blng0-w@5-hls-n@m0

Thank you all for being my “Golden Nuggets” and allow my neuro pathways to develop for my own “Cloud Network” in My mind with the ELK Stack and the flexibility and expandability processing DATA so efficiently with more precision of execution, Clarity and a better understanding of how to compartmentalize data, and how to communicate to the Professional and Non-Professional’s with Confidence of my abilities and skills that I have obtain from each and every staff member, student and Tutor. I Thank you for your time, energy, wisdom, knowledge:

Your “**Golden Nuggets**”

that you shared throughout the BootCamp. “Golden Nugget”

1. It is easier to build a multi-dimensional web cloud environment with Blue_Prints. 2. It is easier to travel when you know where you are going and which ports are open to ifconfig and then run a nmap and look out because I will be

coming round the mountain when I come using the reverse shell and very carefully listen and hopefully go undetected. Hold on, I don't want to leave you hanging. I then put on my Blue jacket and Defend at all cost and all in a "Good Day's" work and make today just a little safer, more protected trying to maintain the **C.I.A** triad and uphold my civil duty as a SSOC to Honor: Protect: Execute: Exploit Vulnerabilities, and mitigate risk and guard against attacks both on land and in the Cloud environment. Thank you for an amazing journey believing in me when some days I had doubt and didn't believe in myself and you all were there for me. Thanks to you all! I have Transformation.. Title: Darrel Mills SSOC

The End.