



Intro to Data Visualization

SECURESET ACADEMY

IN PREPARATION PLEASE BROWSE TO:

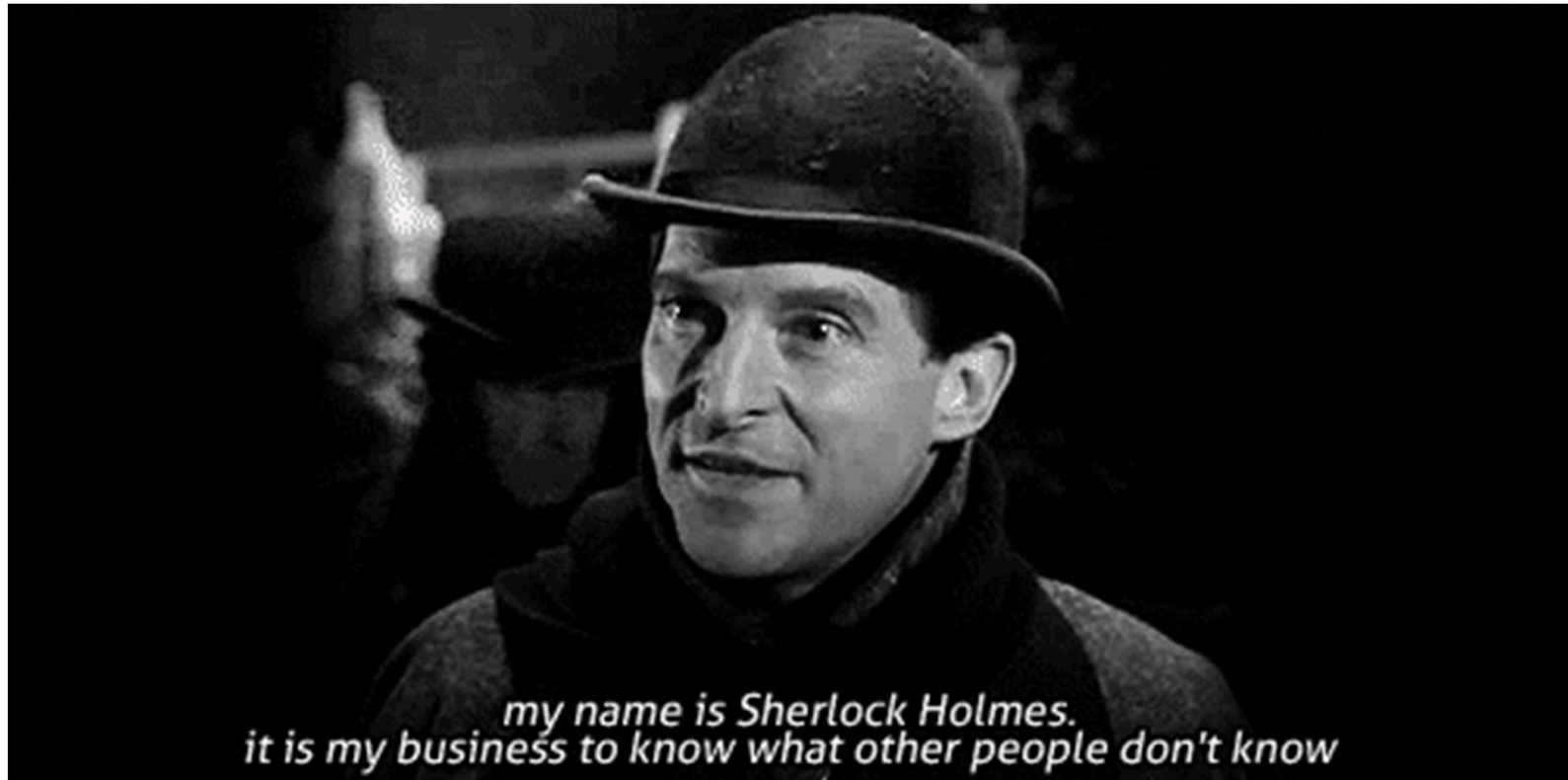
[HTTPS://GITHUB.COM/AJAY63/DATAVIZ101](https://github.com/AJAY63/DATAVIZ101)

SECURESET ACADEMY

IN PREPARATION PLEASE BROWSE TO:

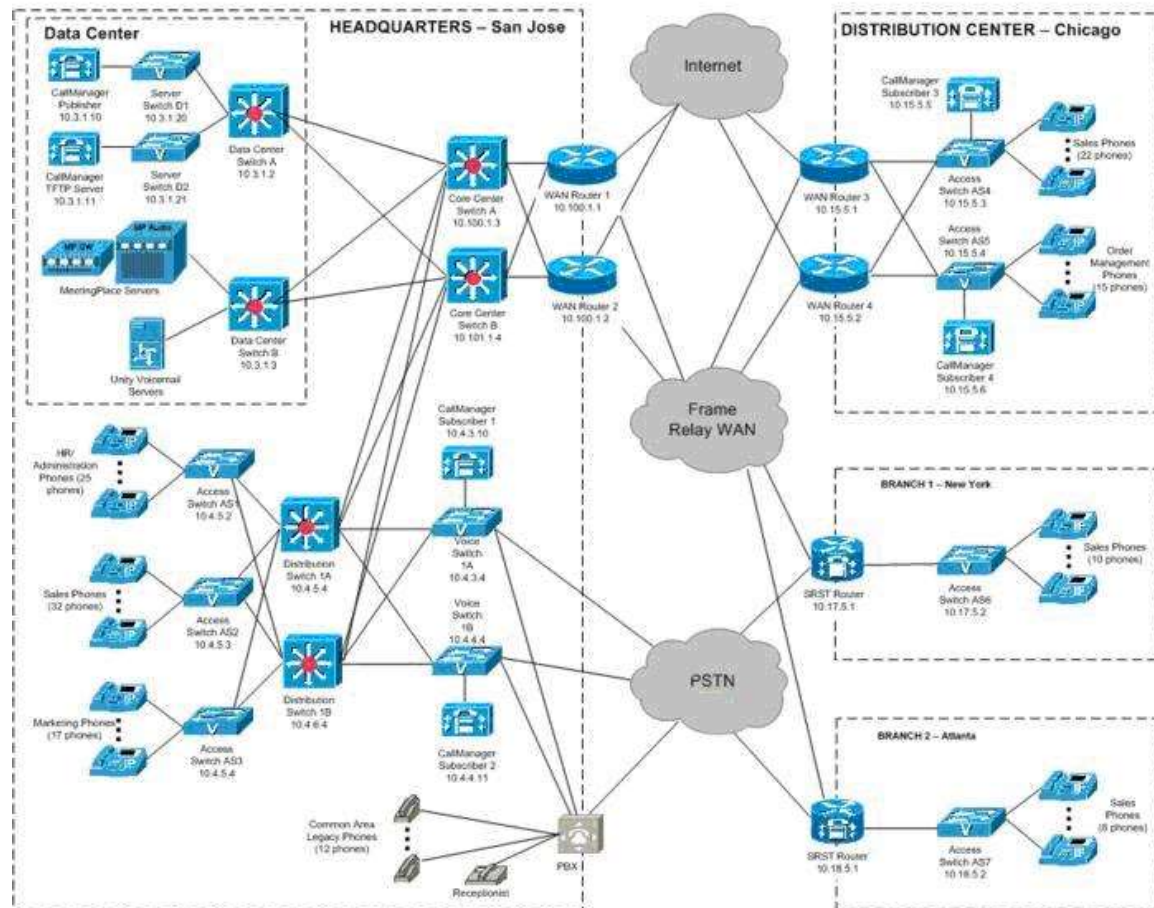
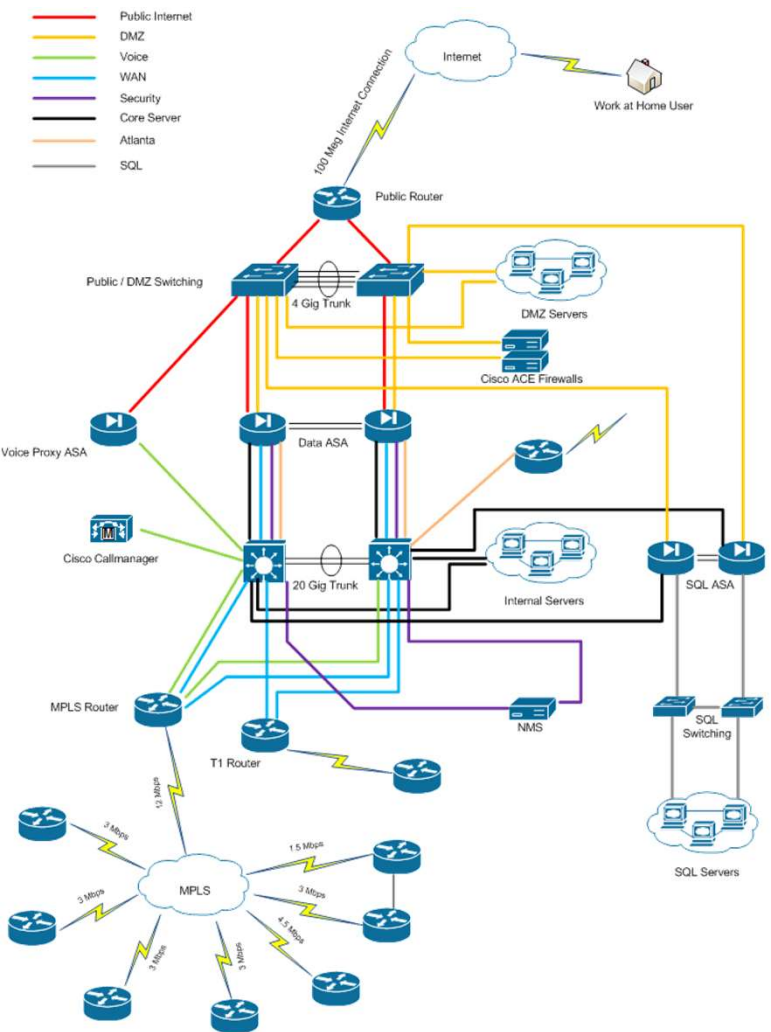
[HTTPS://GITHUB.COM/AJAY63/DATAVIZ101](https://github.com/AJAY63/DATAVIZ101)

Data Visualization Introduction



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved





©2017 SecureSet Academy, Inc. | All Rights Reserved

MTTD - MTTR



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

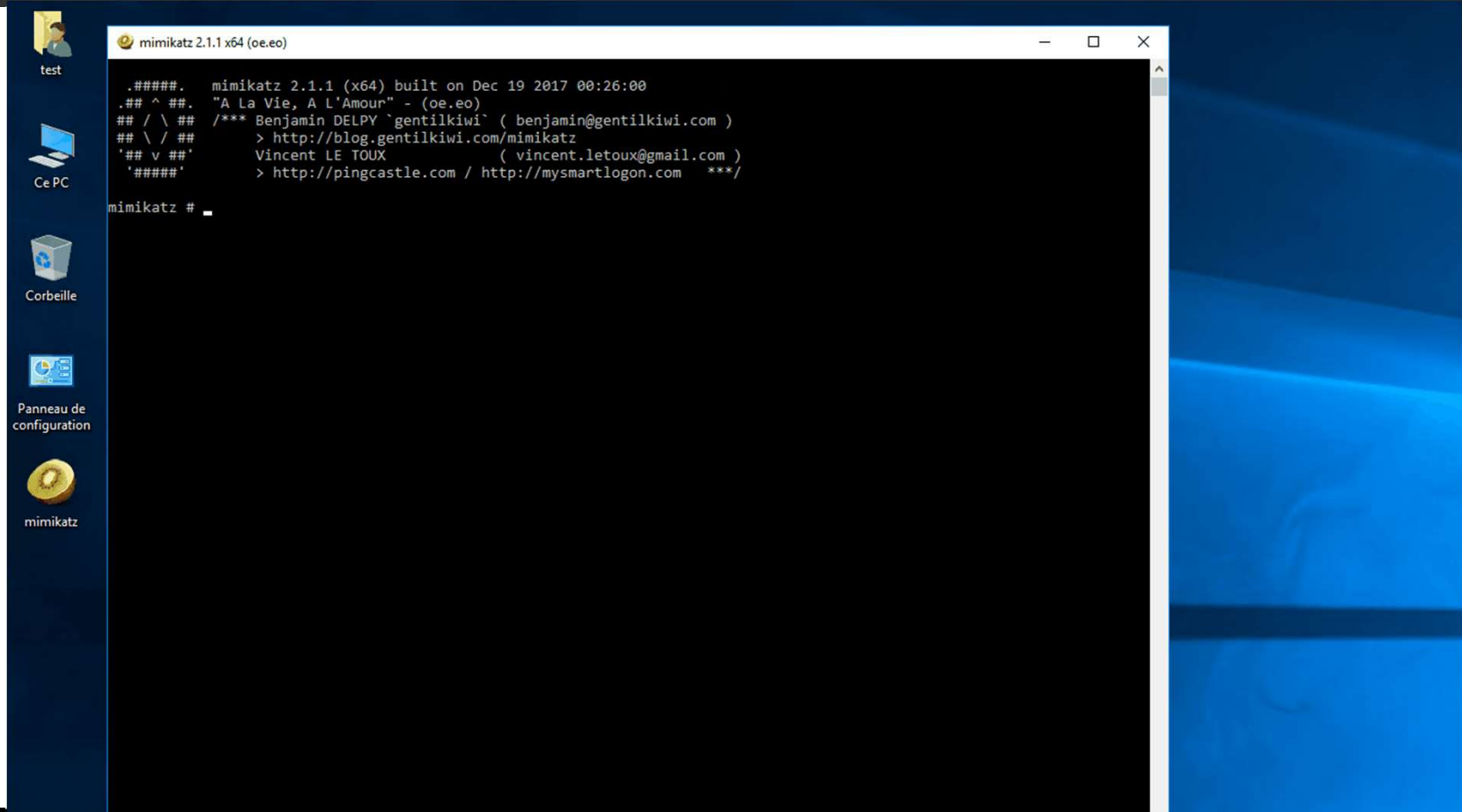
Dwell Time and Metrics



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Ain't nobody got time for that...



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Zero Days



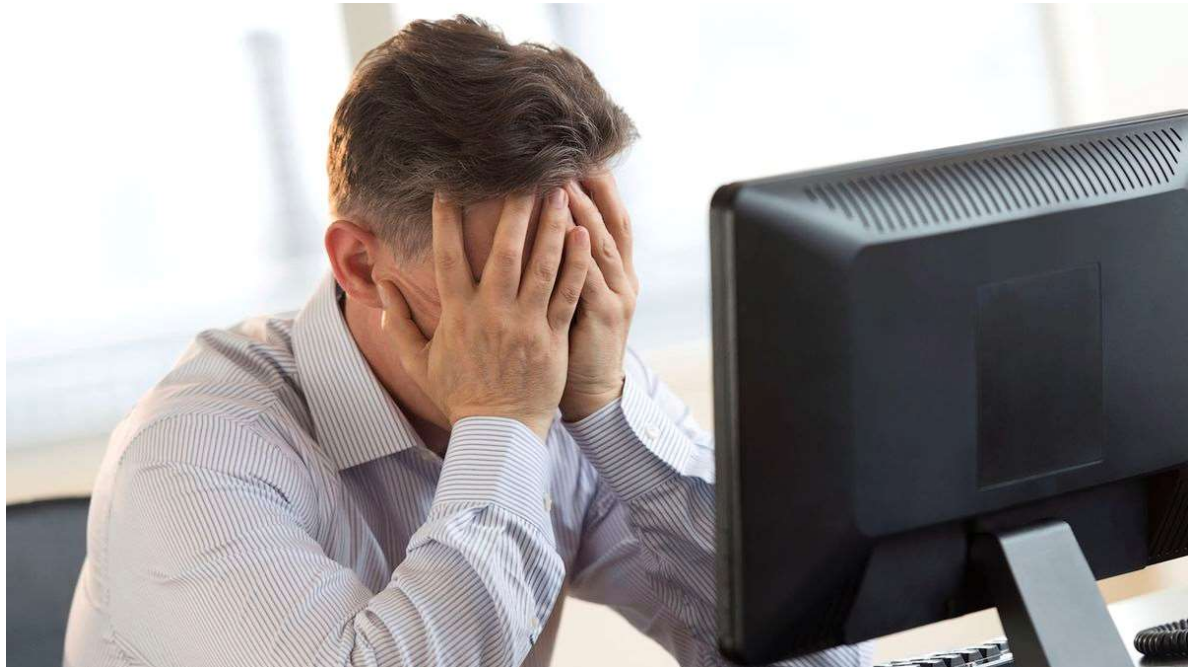
SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Conventional Approaches Aren't Working

Insanity: doing the same thing over and over again and expecting different results.

~Albert Einstein



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

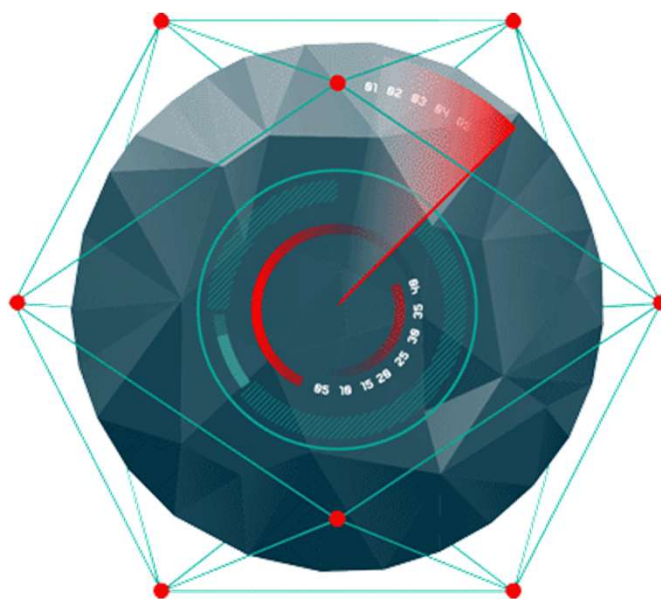
Benefits of Hunting



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Automation



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Preparation and Priorities

Preparation

- Info IT Assets
- Info IT Networks
- Network Maps
- What is Normal
- Deploying Sensors

Priorities

- Initial Assets to HUNT on
- Guidance from MGT on Priority of Assets
- Cyber Risk Assessment

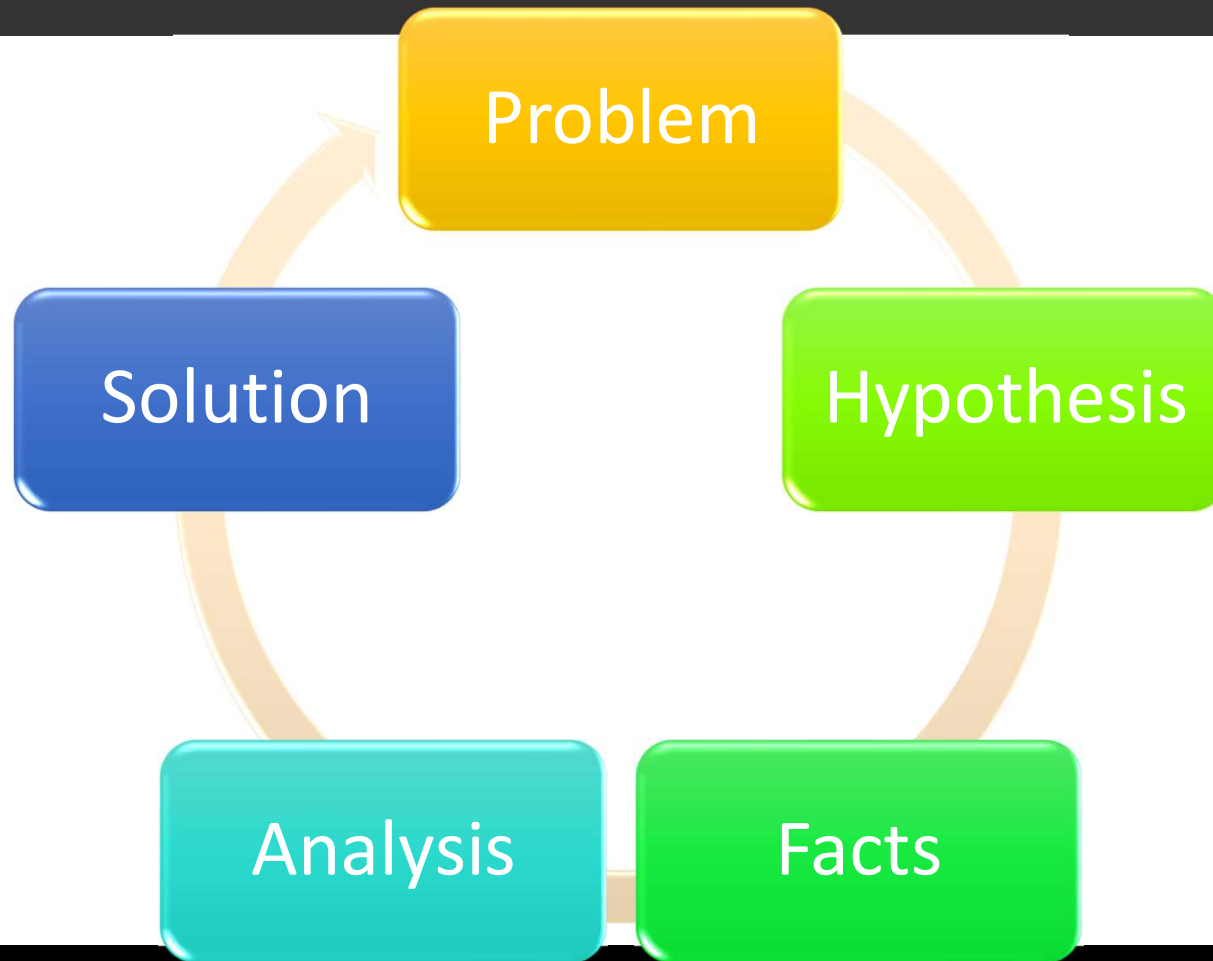
THINK



[SECURESETACADEMY.COM](https://www.securesetacademy.com)

©2017 SecureSet Academy, Inc. | All Rights Reserved

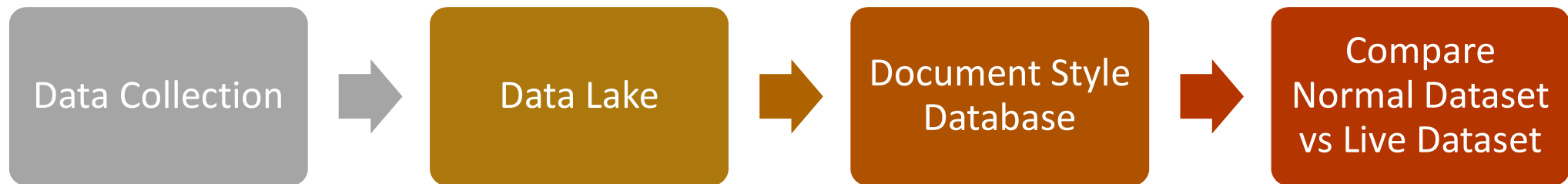
Analysis



SECURESETACADEMY.COM

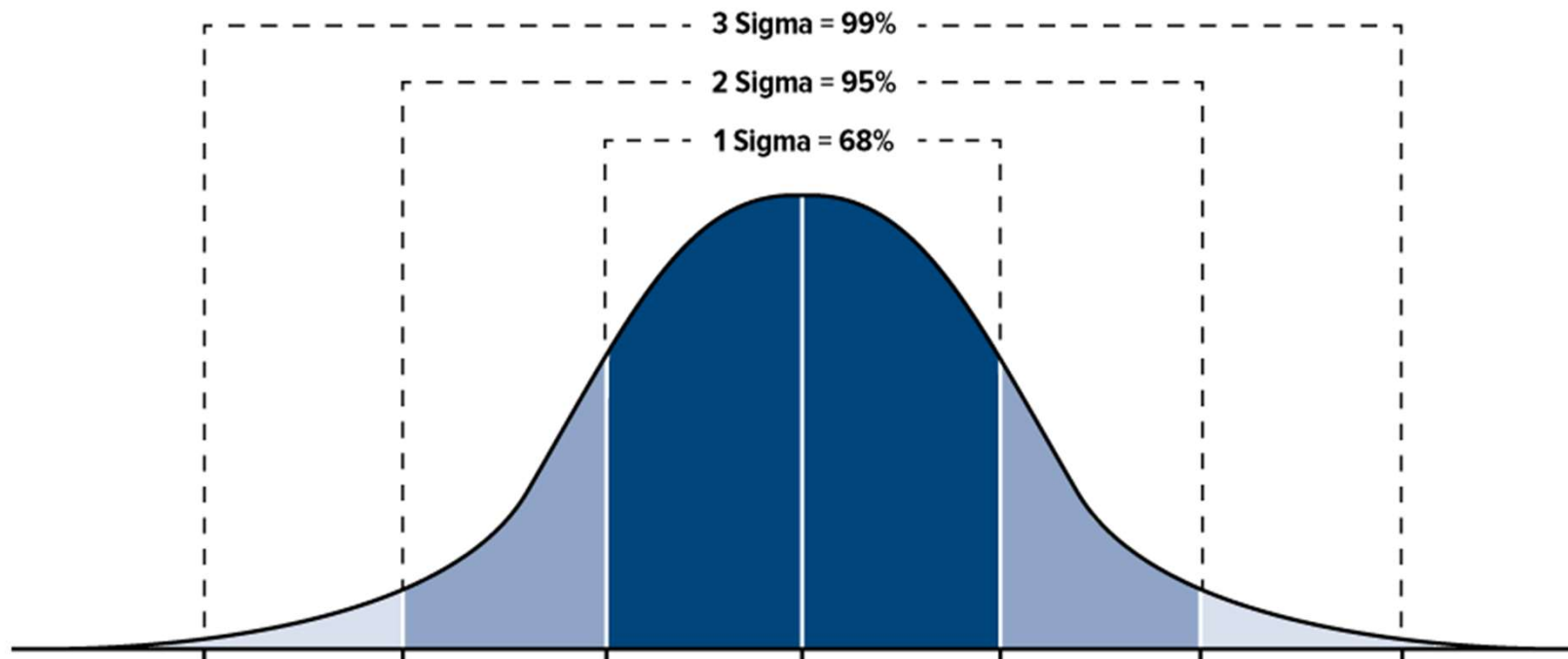
©2017 SecureSet Academy, Inc. | All Rights Reserved

Identifying and preparing Normal



What is NORMAL

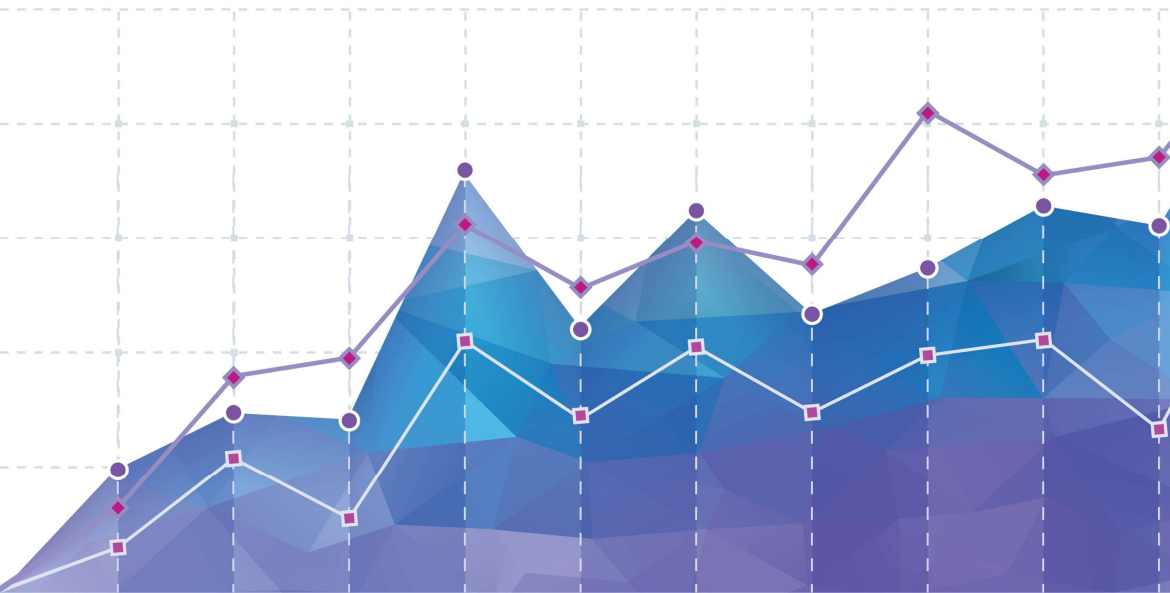
Standard Deviation (Sigma) Measures Degree of Variance from Average



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

What is NORMAL



Data Visualization

Data visualization is the presentation of data in a pictorial or graphical format. It enables decision makers to see analytics presented visually, so they can grasp difficult concepts or identify new patterns. With interactive visualization, you can take the concept a step further by using technology to drill down into charts and graphs for more detail, interactively changing what data you see and how it's processed.

https://www.sas.com/en_us/insights/big-data/data-visualization.html

What is NORMAL

Data Visualization

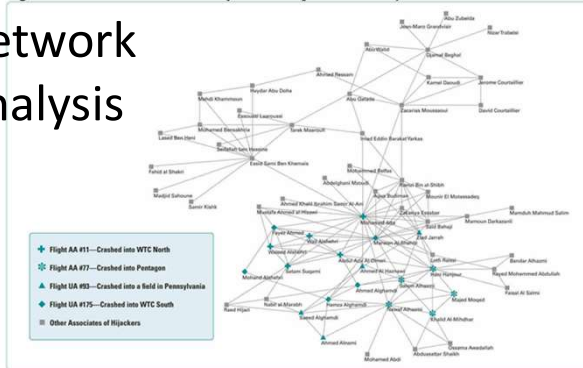
It makes complex data more accessible, understandable and usable. Users may have particular analytical tasks, such as making comparisons or understanding [causality](#), and the design principle of the graphic (i.e., showing comparisons or showing causality) follows the task. Tables are generally used where users will look up a specific measurement, while charts of various types are used to show patterns or relationships in the data for one or more variables.



Weighted Ranking Matrix

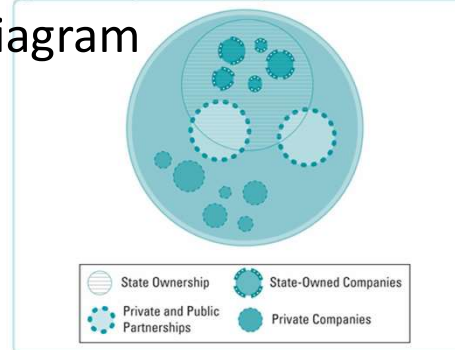
Items							
Criteria	Weight	A	B	C	D	E	F
1	3	3 x 7 = 21	3 x 8 = 24	3 x 8 = 24	3 x 5 = 15	3 x 6 = 18	3 x 7 = 21
2	3	3 x 5 = 15	3 x 8 = 24	3 x 9 = 27	3 x 7 = 21	3 x 4 = 12	3 x 5 = 15
3	2	2 x 8 = 16	2 x 9 = 18	2 x 3 = 6	2 x 2 = 4	2 x 3 = 6	2 x 7 = 14
4	1	1 x 6 = 6	1 x 3 = 3	1 x 8 = 8	1 x 6 = 6	1 x 9 = 9	1 x 7 = 7
5	1	1 x 7 = 7	1 x 9 = 9	1 x 7 = 7	1 x 8 = 8	1 x 6 = 6	1 x 8 = 8
Totals	10	65	78	72	54	51	65
%	100	16.9%	20.3%	18.7%	14%	13.2%	16.9%

Figure 4.10a Social Network Analysis: The September 11 Hijackers



Network Analysis

Figure 4.9c Venn Diagram of Zambrian Corporations



Venn Diagram

Timeline

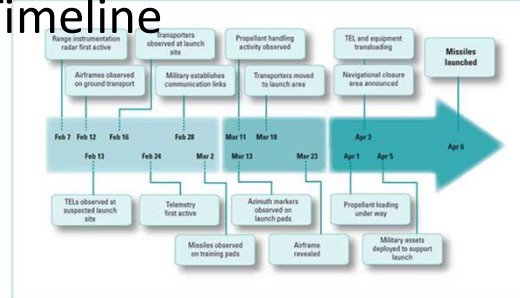
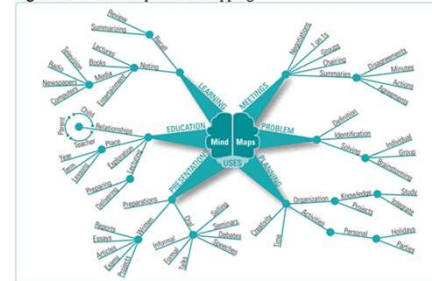
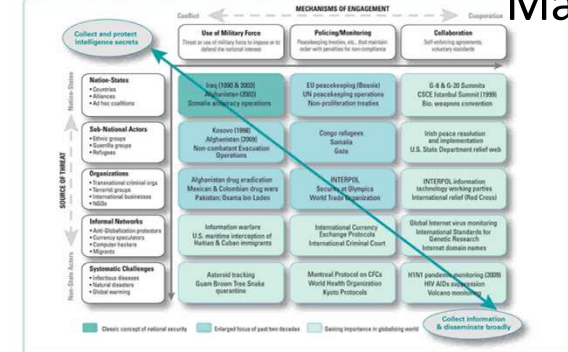


Figure 4.11b Mind Map of Mind Mapping



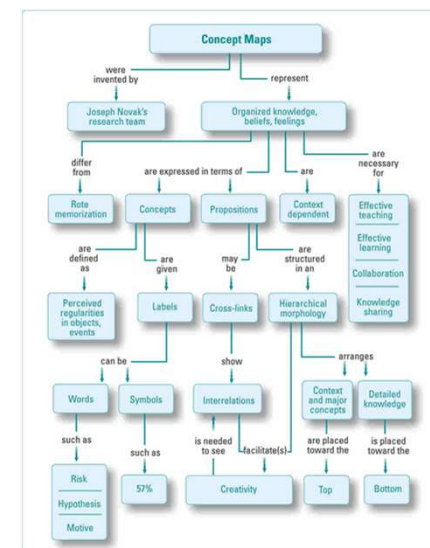
Mind Map

Figure 4.8 Rethinking the Concept of National Security: A New Ecology



Matrices

Concept Map



What is NORMAL



Lets do some Data Visualization 101 Exercises

LABS

1. DIFF with words
2. DIFF with data

What is DIFF?

DIFF



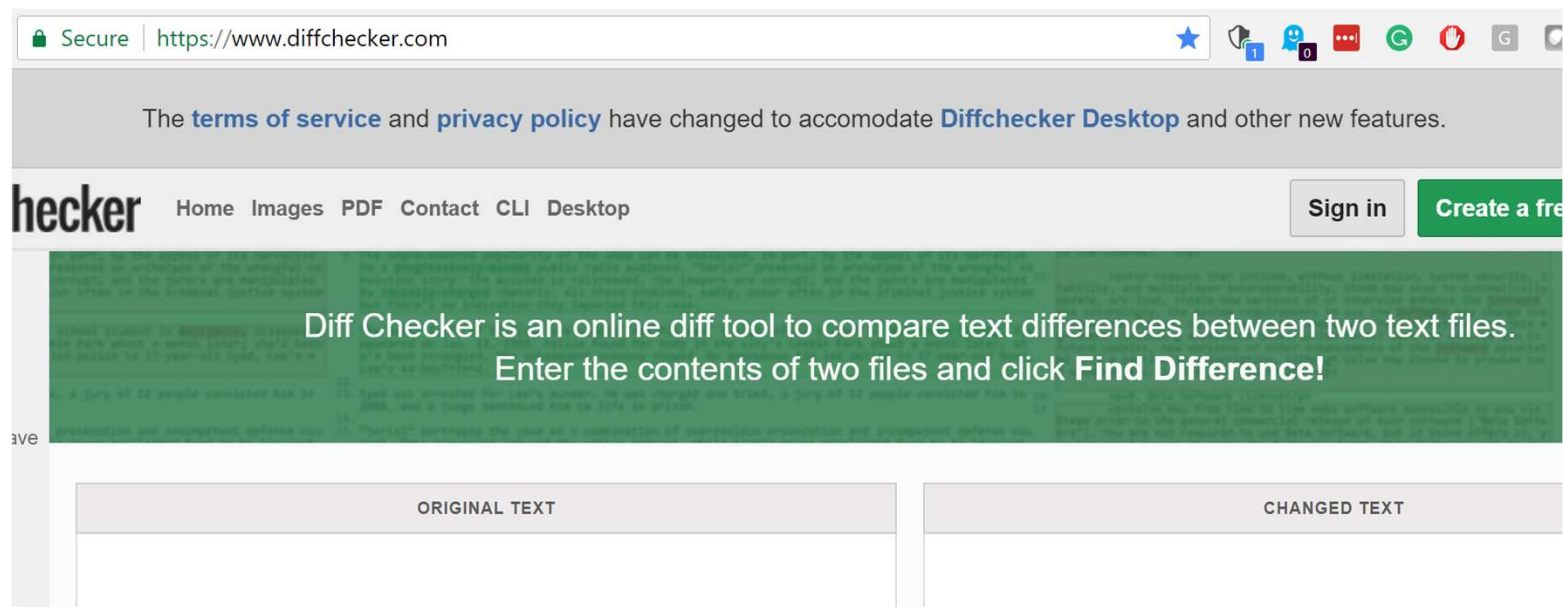
https://en.wikipedia.org/wiki/Diff_utility

In [computing](#), the **diff utility** is a [data comparison](#) tool that calculates and displays the differences between two files. Unlike [edit distance](#) notions used for other purposes, diff is line-oriented rather than character-oriented, but it is like [Levenshtein distance](#) in that it tries to determine the smallest set of deletions and insertions to create one file from the other. The diff command displays the changes made in a standard format, such that both humans and machines can understand the changes and apply them: given one file and the changes, the other file can be created.

Typically, diff is used to show the changes between two versions of the same file. Modern implementations also support [binary files](#).^[1] The output is called a "diff", or a [patch](#), since the output can be applied with the [Unix](#) program [patch](#). The output of similar file comparison utilities are also called a "diff"; like the use of the word "[grep](#)" for describing the act of searching, the word *diff* became a generic term for calculating data difference and the results thereof.^[2]

ONLINE WORD DIFF TOOLS

<https://www.diffchecker.com/>



The screenshot shows the Diff Checker website in a web browser. The address bar displays "Secure | https://www.diffchecker.com". A notification banner at the top states: "The [terms of service](#) and [privacy policy](#) have changed to accomodate [Diffchecker Desktop](#) and other new features." The navigation bar includes the "diffchecker" logo, links for "Home", "Images", "PDF", "Contact", "CLI", and "Desktop", along with "Sign in" and "Create a free account" buttons. The main content area has a green background with white text: "Diff Checker is an online diff tool to compare text differences between two text files. Enter the contents of two files and click **Find Difference!**". Below this, there are two large text input fields labeled "ORIGINAL TEXT" and "CHANGED TEXT".

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

What is different from NORMAL

Diffchecker [Home](#) [Images](#) [PDF](#) [Contact](#) [CLI](#) [Desktop](#) [Sign in](#) [Create a free account](#)

RECENT DIFFS

ved diff

ved diff

Clear diffs

nt diffs are deleted on refresh

DIFFS

ust [log in](#) to save diffs

nd this means war; if you still try to defend the innocents and horrors perpetrated by that Antichrist- I really believe he is Antichrist- I will have nothing more to do with you and you are no longer my friend, no longer my 'faithful slave,' as you call yourself! But how do you do? I see I have frightened you- sit down and tell me all the news."

3.

4. It was in July, 1805, and the speaker was the well-known Anna Pavlovna Scherer, maid of honor and favorite of the Empress Marya Fedorovna. With these words she greeted Prince Vasili Kuragin, a man of high rank and importance, who was the first to arrive at her reception. Anna Pavlovna had had a cough for some days. She was, as she said, suffering from la grippe; grippe being then a new word in St. Petersburg, used only by the elite.

5.

nd this means war; if you still try to defend the innocents and horrors perpetrated by that Antichrist- I really believe he is Antichrist- I will have nothing more to do with you and you are no longer my friend, no longer my 'faithful slave,' as you call yourself! But how do you do? I see I have frightened you- sit down and tell me all the news."

3.

4. It was in July, 2018, and the speaker was the well-known Anna Pavlovna Scherer, maid of honor and favorite of the Empress Marya Fedorovna. With these words she greeted Prince Vasili Kuragin, a man of high rank and importance, who was the first to arrive at her reception. Anna Pavlovna had had a cough for some days. She was, as she said, suffering from la grippe; grippe being then a new word in St. Petersburg, used only by the elite.

5.

ONLINE IMAGE DIFF TOOLS

Let's go to <https://online-image-comparison.com/> where we will be using this free online tool to determine deviations from the original or the Delta. (The variation of a variable of function)



Symbol for Delta

TEXT

Compare the Leopard 1 image with the Leopard 2 image. You will see that the website highlights the delta or deviation from the original in red.



Difference in Visualizations

Let's compare a pair of line graph images. Compare DownSlope1 with DownSlope2. Nothing red, that is because they are the same.

Let's compare DownSlope1 with DownSlope3.

WOAH, check out the **RED**!



Difference in Visualizations

Here are numerous frequency charts of network activity. Compare days 2-6 with **Day 1 (The norm)**. Which days vary from the norm?



Data Analysis 1.png



Data Analysis 2.png



Data Analysis 3.png



Data Analysis 4.png

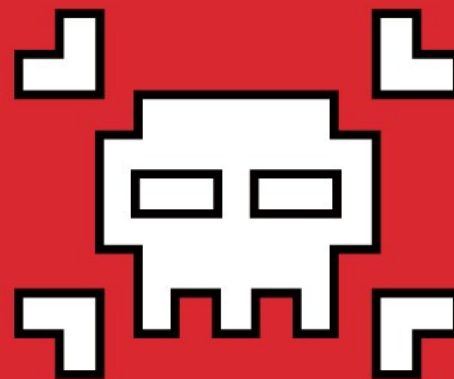


Data Analysis 5.png



Data Analysis 6.png

HUNT Analyst



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

