Intro to Data Visualization

SECURESET ACADEMY

IN PREPARATION PLEASE BROWSE TO:

HTTPS://GITHUB.COM/AJAY63/DATAVIZ101

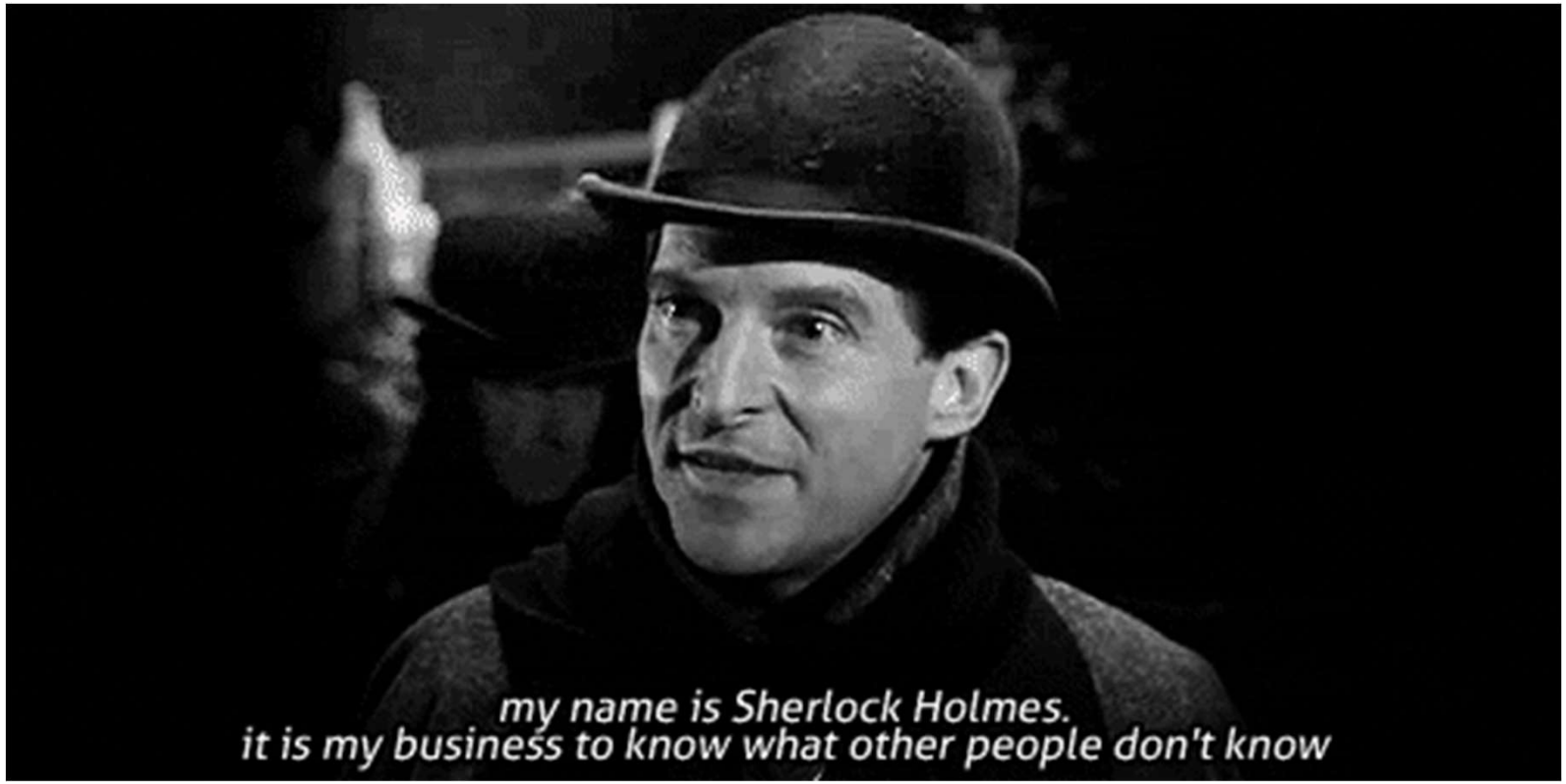
SECURESET ACADEMY

IN PREPARATION PLEASE BROWSE TO:

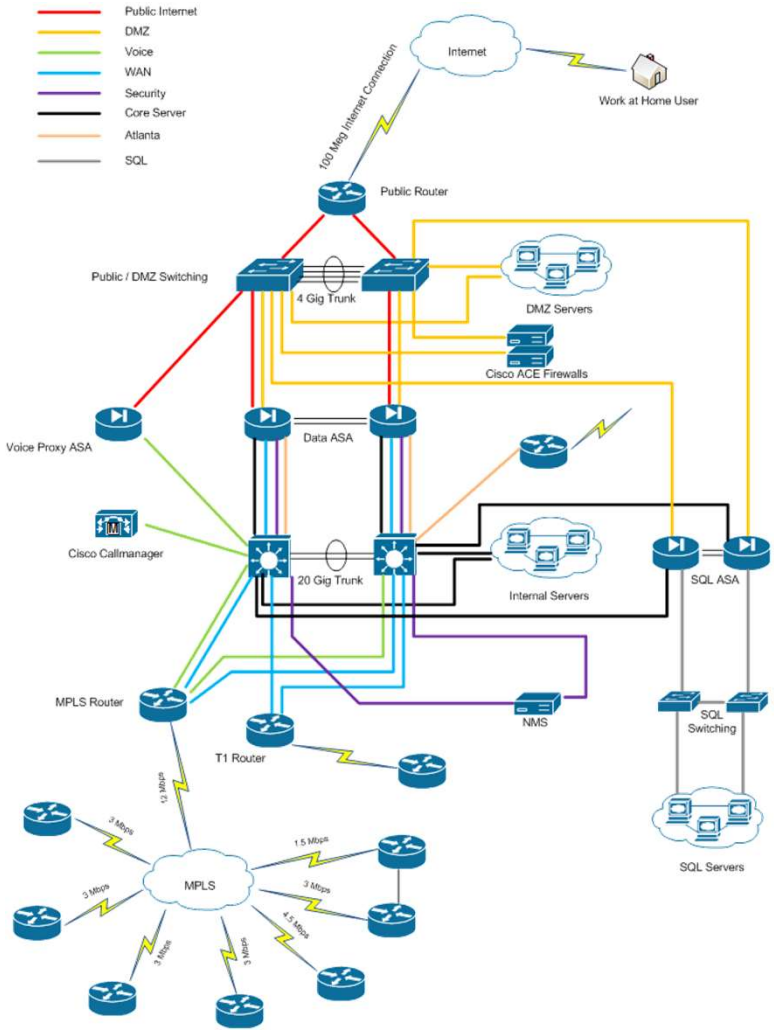
HTTPS://GITHUB.COM/AJAY63/DATAVIZ101

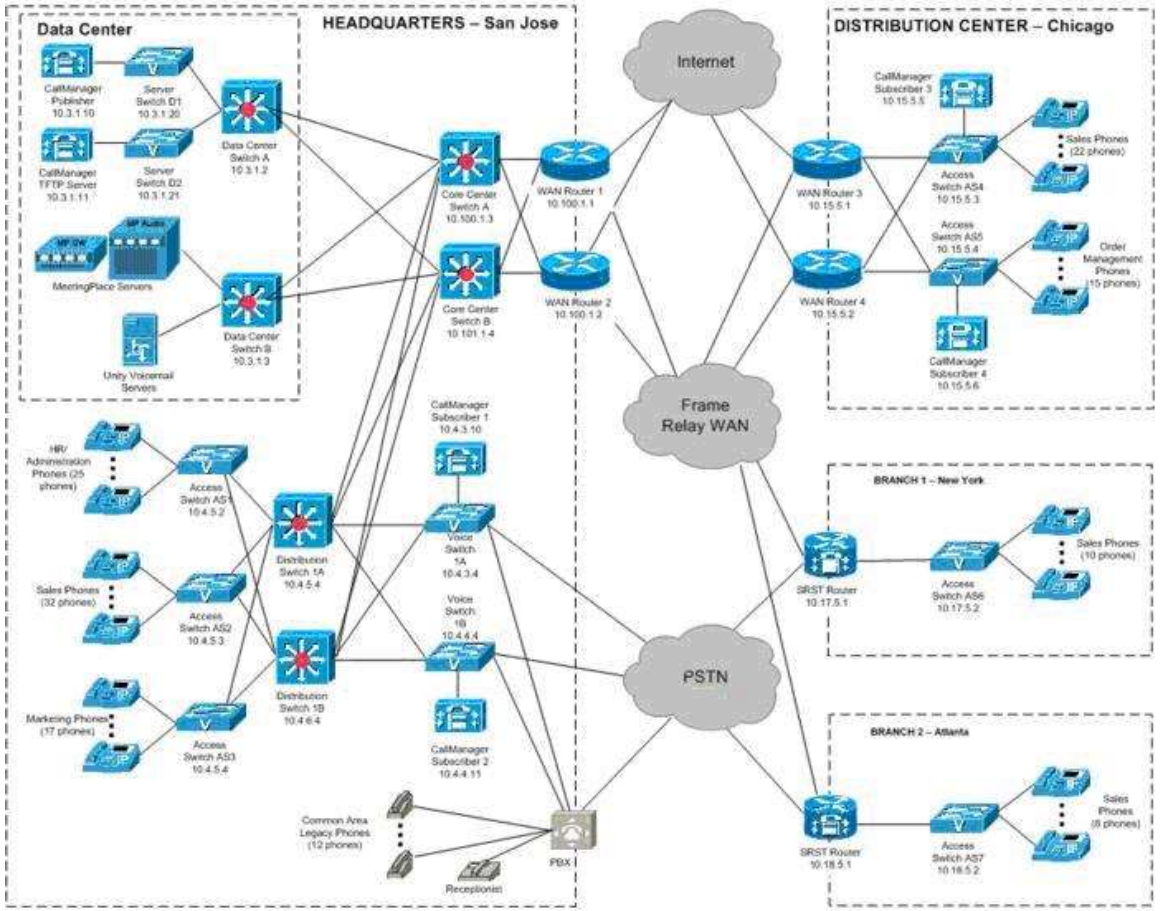
©2017 SecureSet Academy, Inc. | All Rights Reserved

Data Visualization Introduction

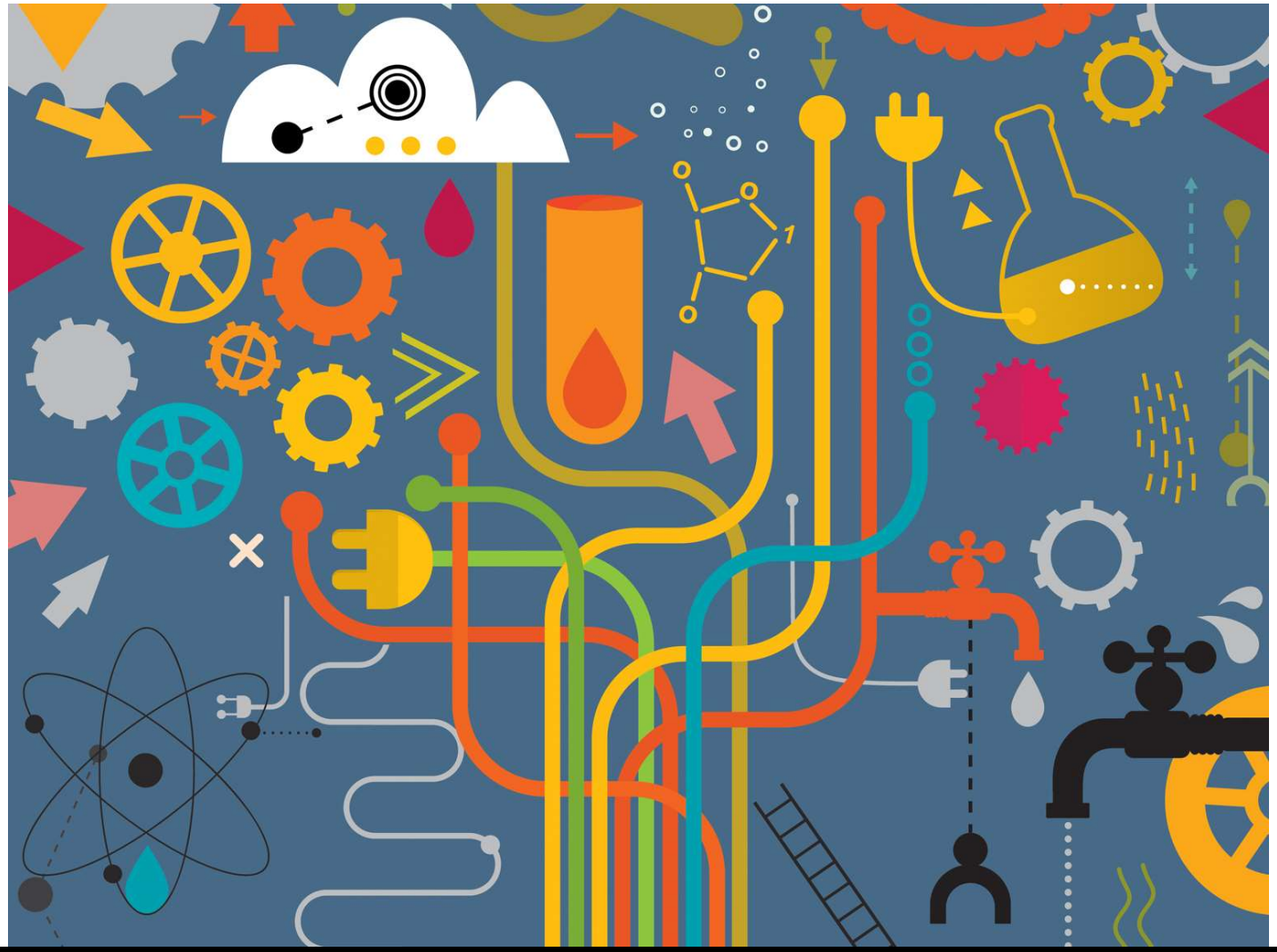


©2017 SecureSet Academy, Inc. | All Rights Reserved



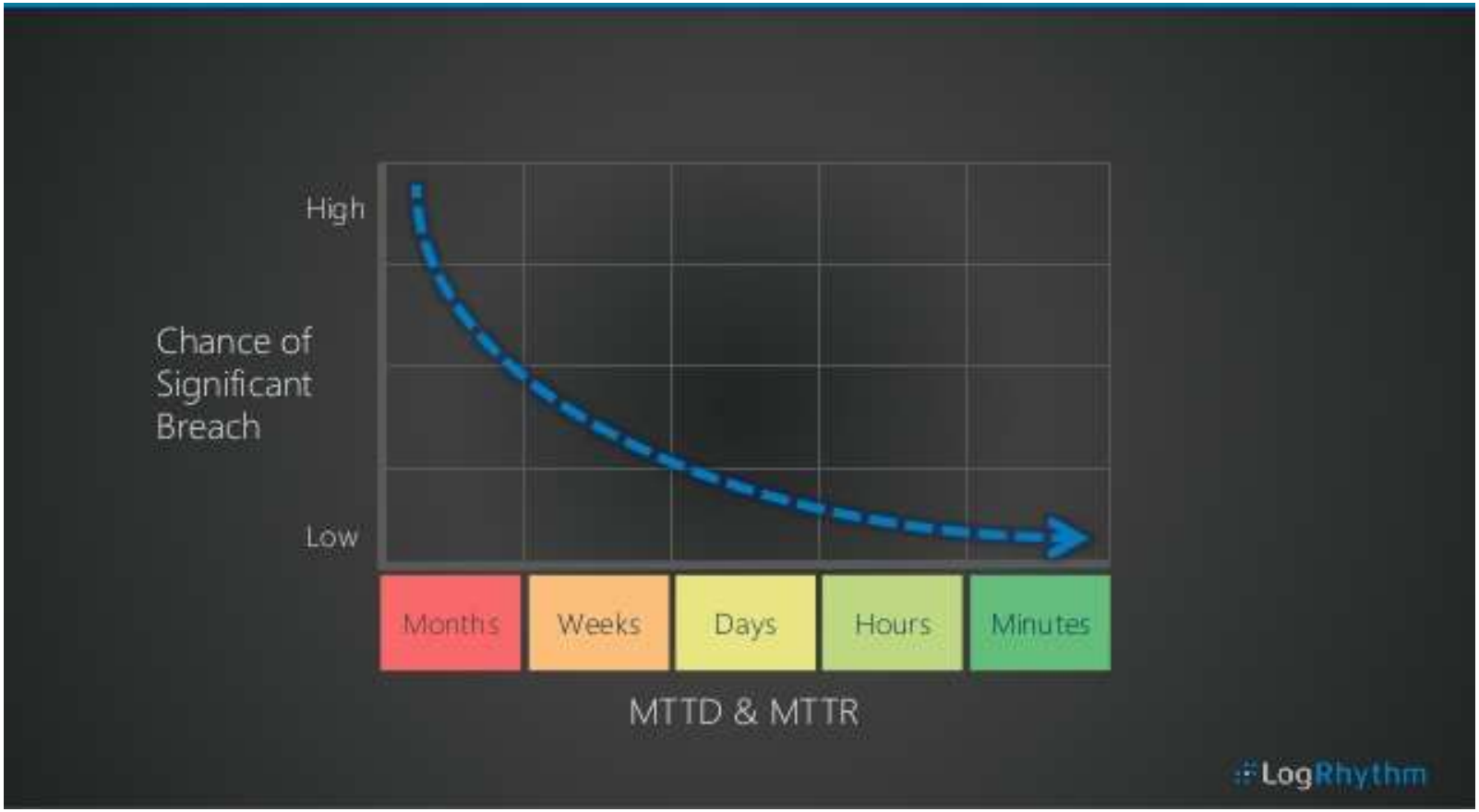


©2017 SecureSet Academy, Inc. | All Rights Reserved



©2017 SecureSet Academy, Inc. | All Rights Reserved

MTTD - MTTR

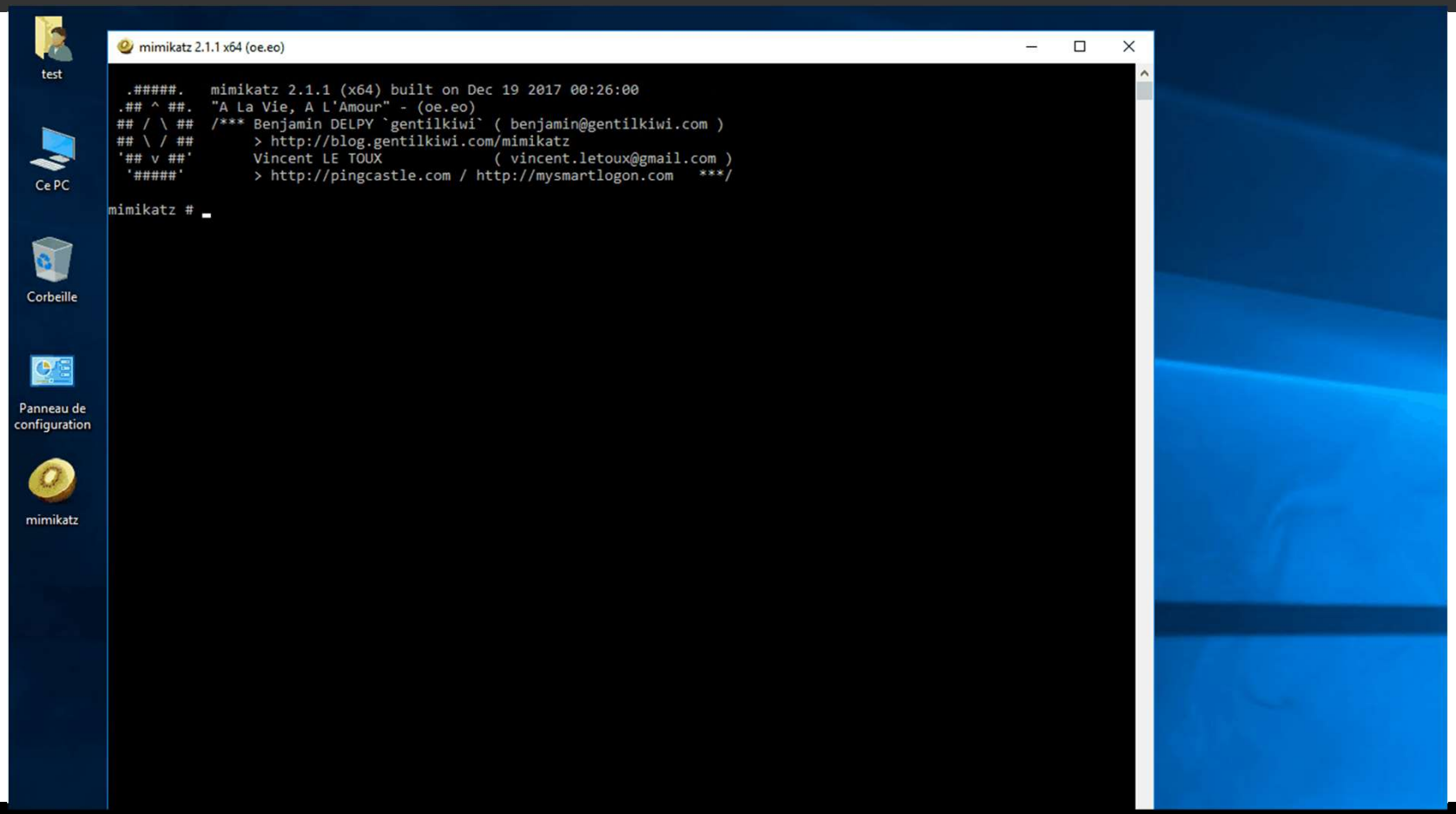


©2017 SecureSet Academy, Inc. | All Rights Reserved

Dwell Time and Metrics

©2017 SecureSet Academy, Inc. | All Rights Reserved

Ain't nobody got time for that...



©2017 SecureSet Academy, Inc. | All Rights Reserved

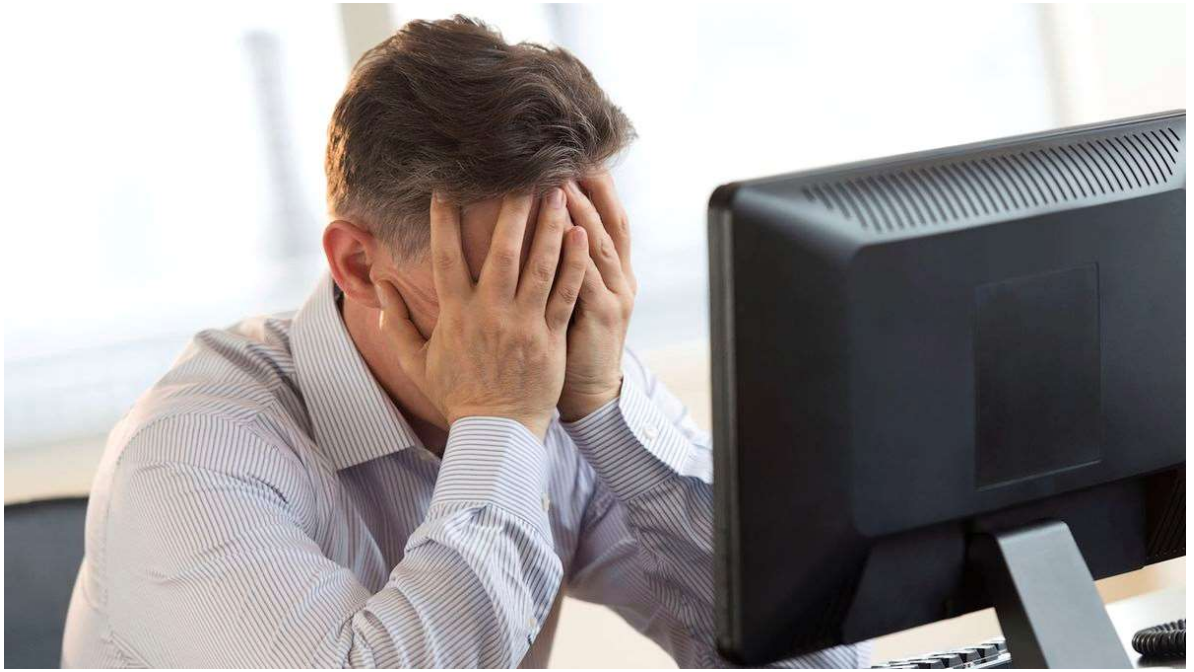
Zero Days

©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

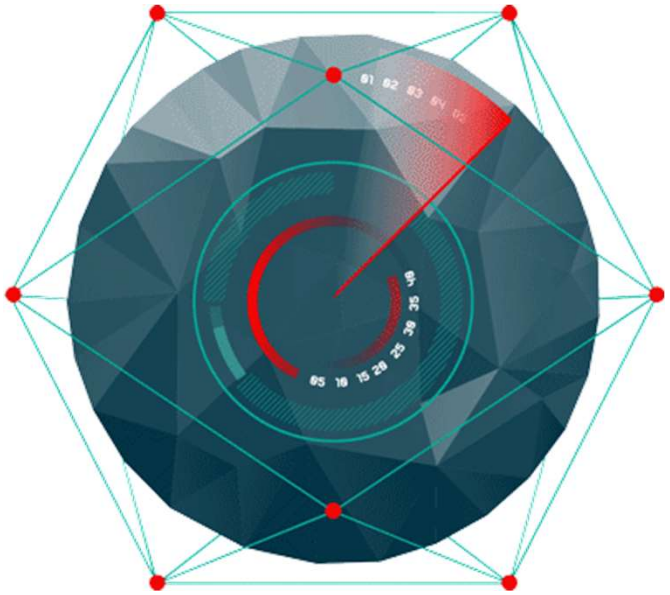


©2017 SecureSet Academy, Inc. | All Rights Reserved

Benefits of Hunting

©2017 SecureSet Academy, Inc. | All Rights Reserved

Automation



©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

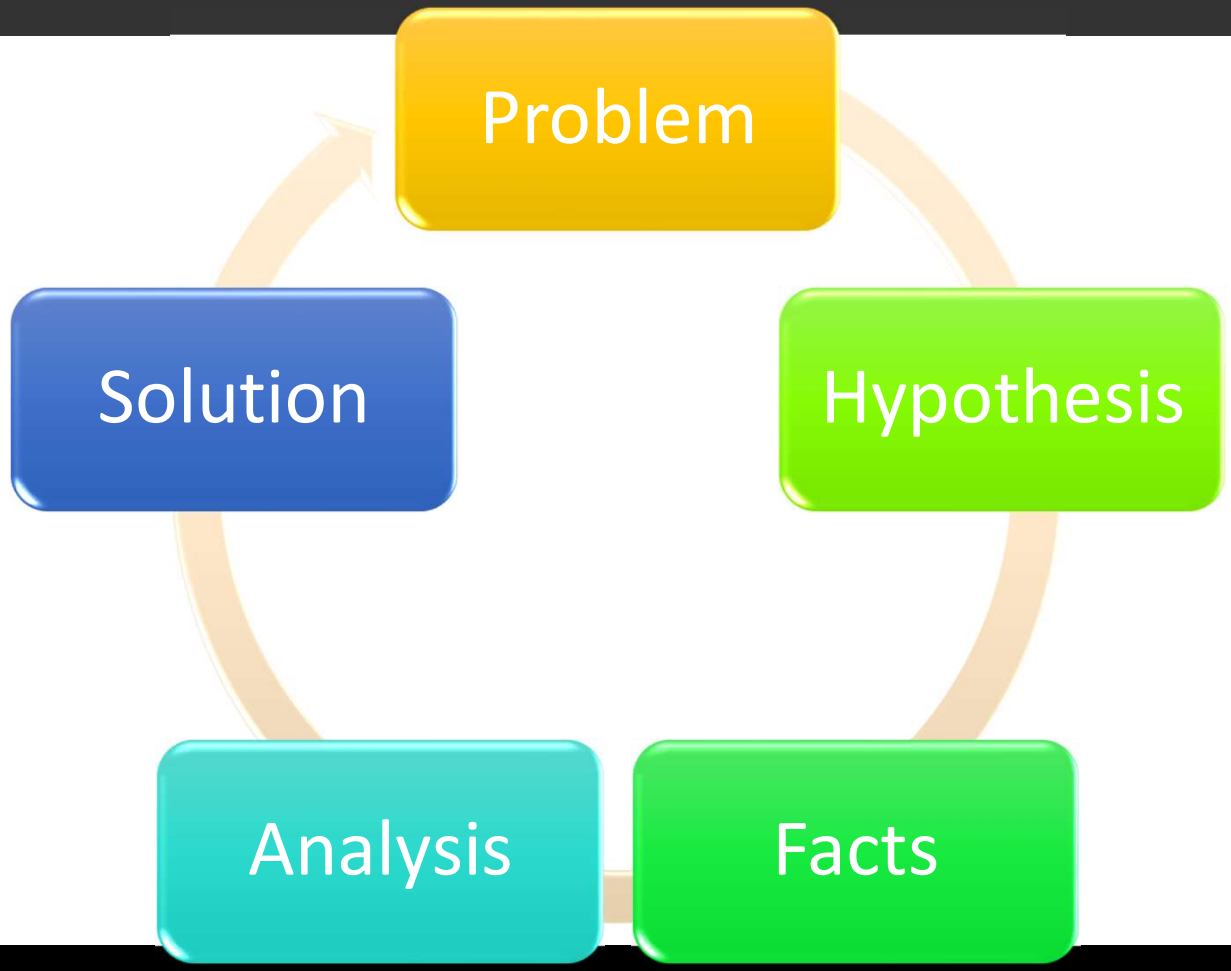
- Initial Assets to HUNT on
- Guidance from MGT on Priority of Assets
- Cyber Risk Assessment

©2017 SecureSet Academy, Inc. | All Rights Reserved

THINK

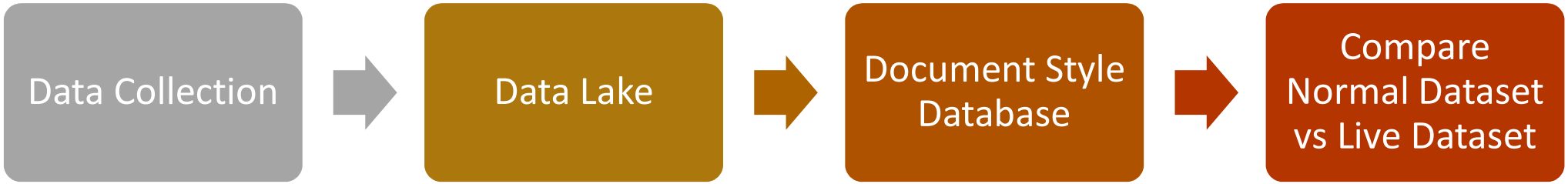
©2017 SecureSet Academy, Inc. | All Rights Reserved

Analysis



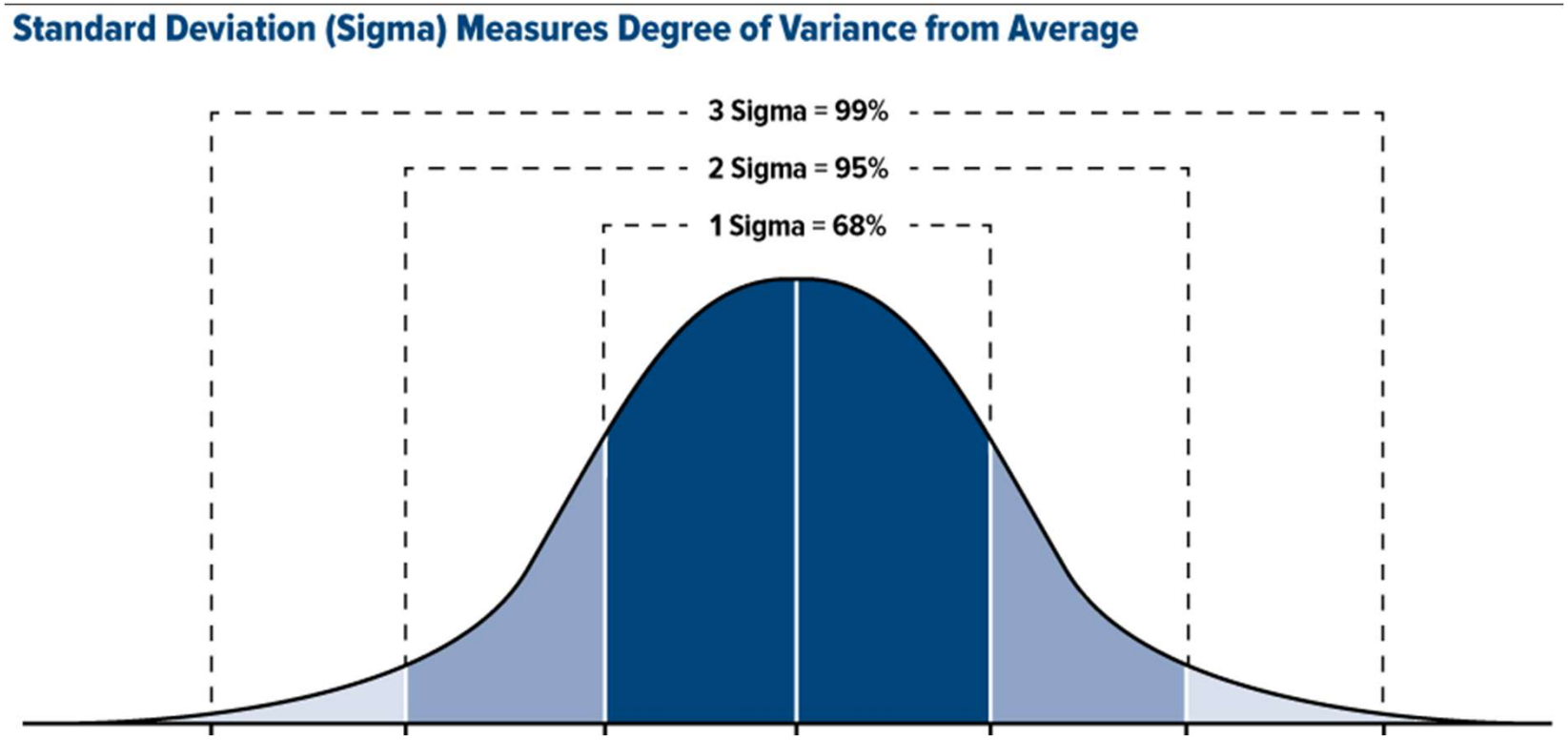
©2017 SecureSet Academy, Inc. | All Rights Reserved

Identifying and preparing Normal



©2017 SecureSet Academy, Inc. | All Rights Reserved

What is NORMAL



©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

©2017 SecureSet Academy, Inc. | All Rights Reserved

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.

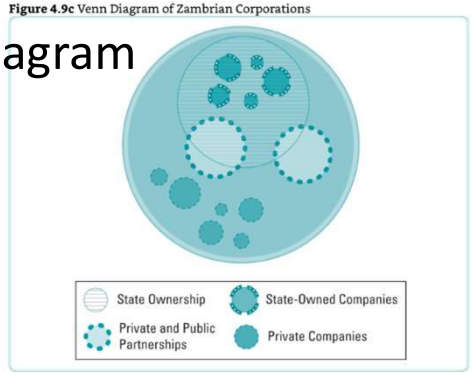
©2017 SecureSet Academy, Inc. | All Rights Reserved

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%**

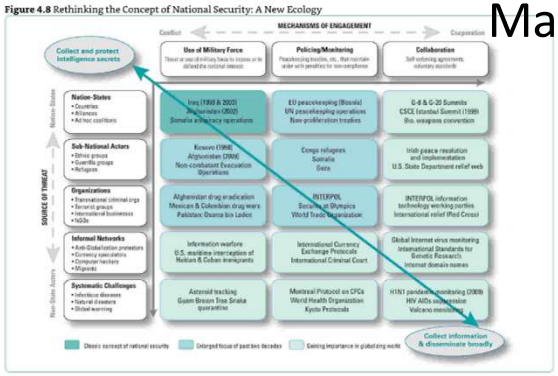
Venn Diagram

Figure 4.9c Venn Diagram of Zambrian Corporations

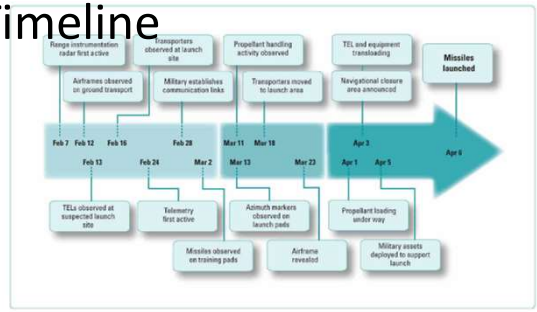


Matrices

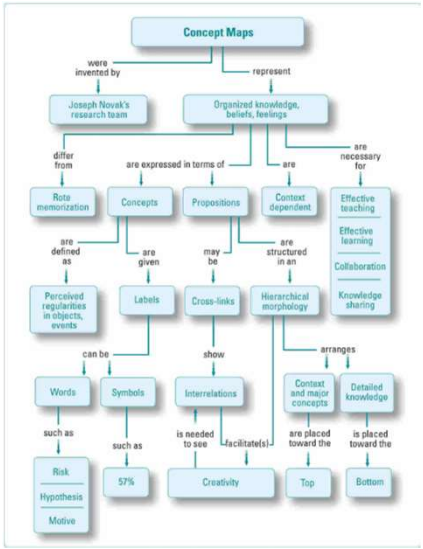
Figure 4.8 Rethinking the Concept of National Security: A New Ecology



Timeline

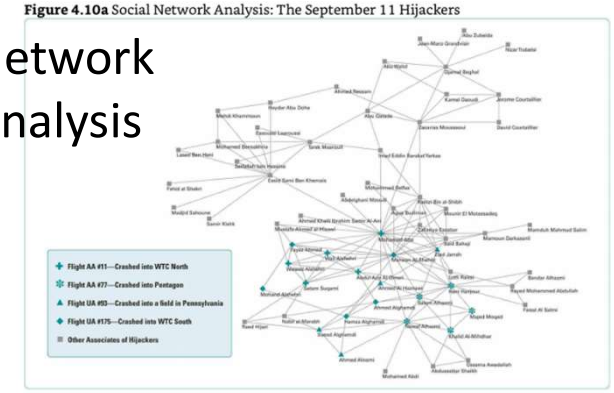


Concept Map



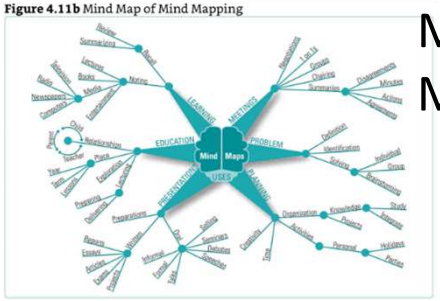
Network Analysis

Figure 4.10a Social Network Analysis: The September 11 Hijackers



Mind Map

Figure 4.11b Mind Map of Mind Mapping



What is NORMAL

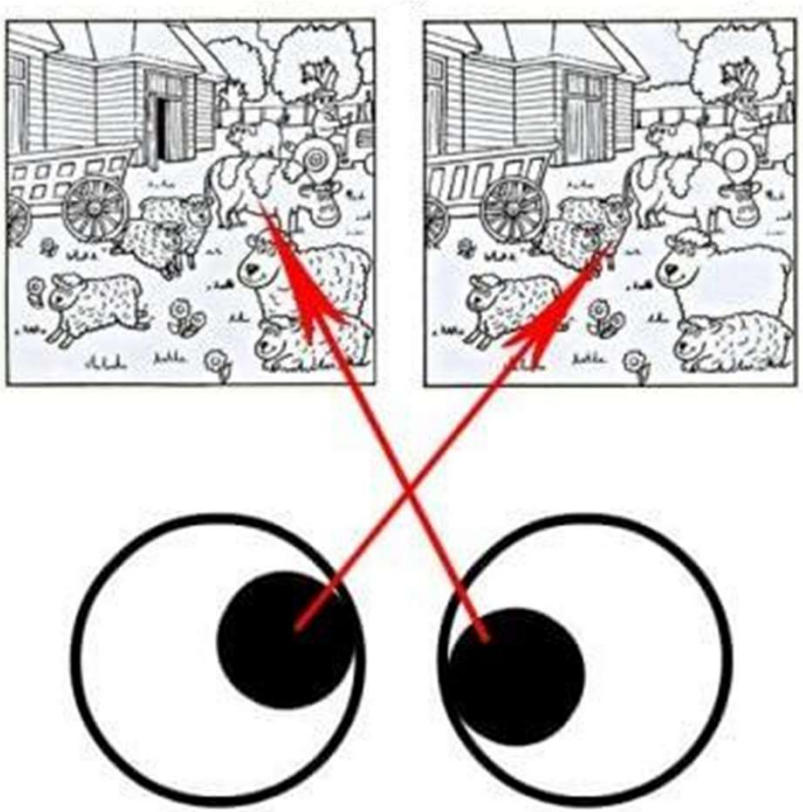
Lets do some Data Visualization 101 Exercises

LABS

1. DIFF with wetware
2. DIFF with words
3. DIFF with data

©2017 SecureSet Academy, Inc. | All Rights Reserved

Visualizations side by side by using stereoscopy



©2017 SecureSet Academy, Inc. | All Rights Reserved

What is DIFF?

DIFF

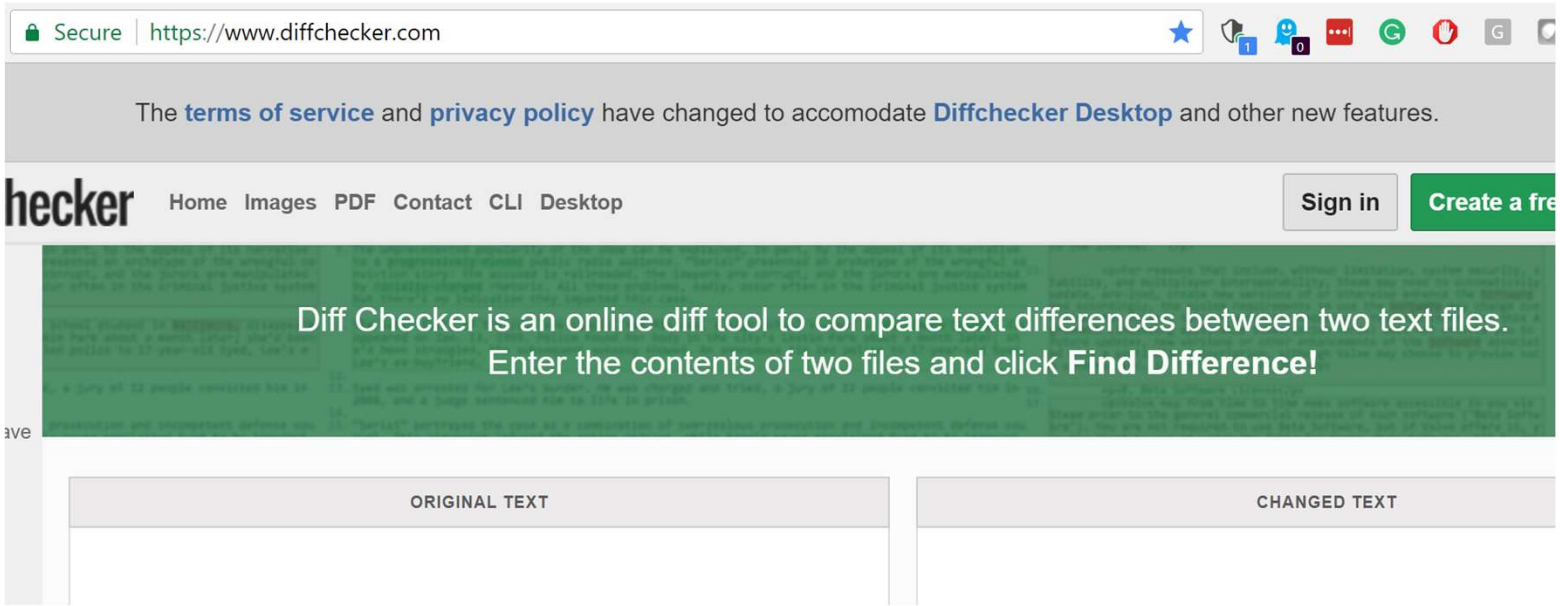
https://en.wikipedia.org/wiki/Diff_utility

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]

©2017 SecureSet Academy, Inc. | All Rights Reserved

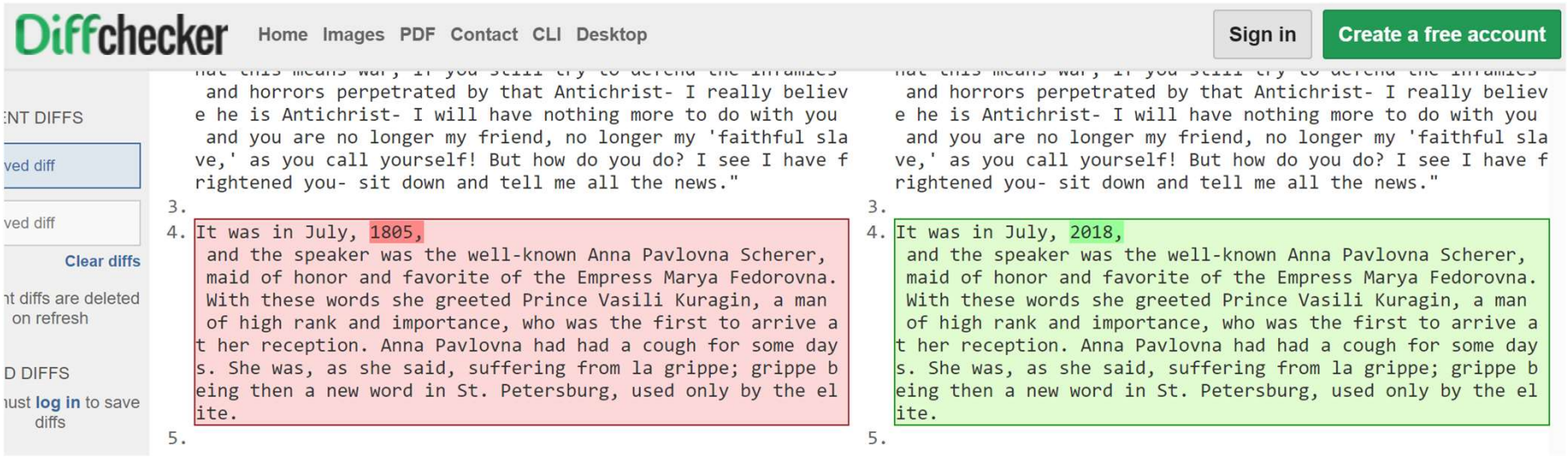
ONLINE WORD DIFF TOOLS

https://www.diffchecker.com/



©2017 SecureSet Academy, Inc. | All Rights Reserved

What is different from NORMAL



©2017 SecureSet Academy, Inc. | All Rights Reserved

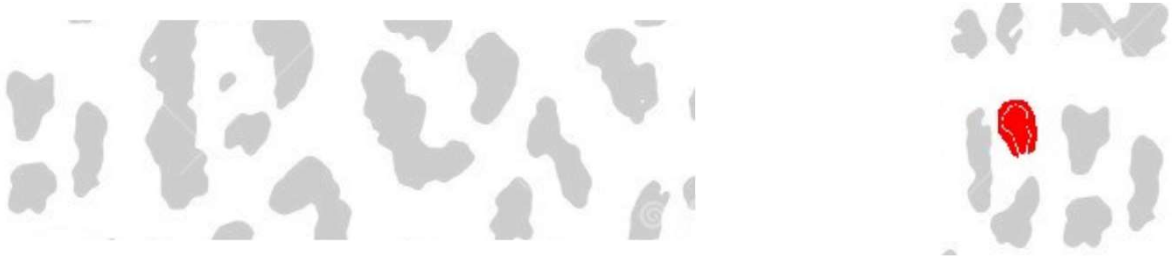
ONLINE IMAGE DIFF TOOLS

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

©2017 SecureSet Academy, Inc. | All Rights Reserved

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.



©2017 SecureSet Academy, Inc. | All Rights Reserved

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.

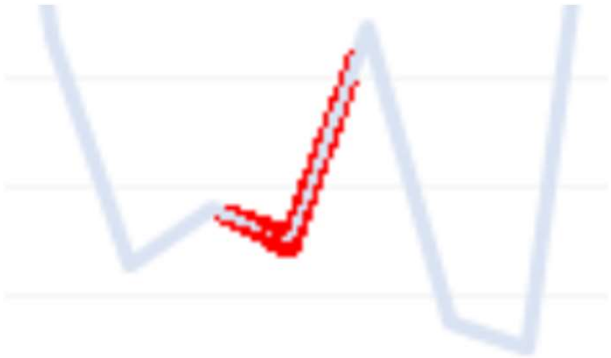
Let's compare DownSlope1 with DownSlope3.

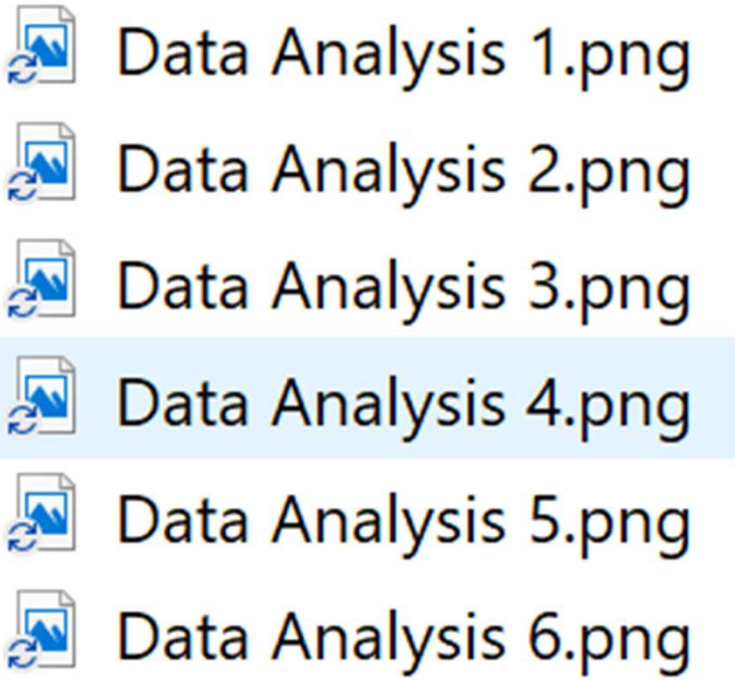
WOAH, check out the RED!

©2017 SecureSet Academy, Inc. | All Rights Reserved

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?





©2017 SecureSet Academy, Inc. | All Rights Reserved

HUNT Analyst

©2017 SecureSet Academy, Inc. | All Rights Reserved