

Visualization Design Challenge

Overview

It's time for you to put what you've learned to the test! After completing the 3 modules, we want you to design your own display tool that will help you better understand how professionals make the invisible visible and will help you get to know the different parts of the "Threat Unseen Cybersecurity Challenge."

To complete this challenge, you can print out this document and write directly in it or you can sketch your thoughts in a separate notebook. Engineers constantly document their thoughts and processes.

Objective: Design a visualization tool that will alert you to a potential cyber attack.

Step 1: Decide what you want to measure

A. Review your answers to the questions in *Module 1: Observation* and *Module 2: Measurement* to help you decide what grid assets and measurements to take a closer look at.

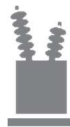
B. Determine the grid asset that you think is most important to your community

- a) Generator/battery
- b) Substations
- c) Residential area/Industrial area (circuit breakers, outlets, and switches)

a.



b.



c.



For example, if you think that the biggest threat to the power grid is an attack on a substation then that is probably where you want to focus your observation.

C. Decide who or what the biggest threat to that grid asset is.

- a. Review the Investigative Files, what assets do the different hackers tend to attack?
- b. What methods do they use to do it?

What you find can help you determine what you want to measure.

Example A

We found this phrase in the Investigative Files and decided that this might be a significant threat:

coordinated attacks using multiple tactics such a port scan tactics

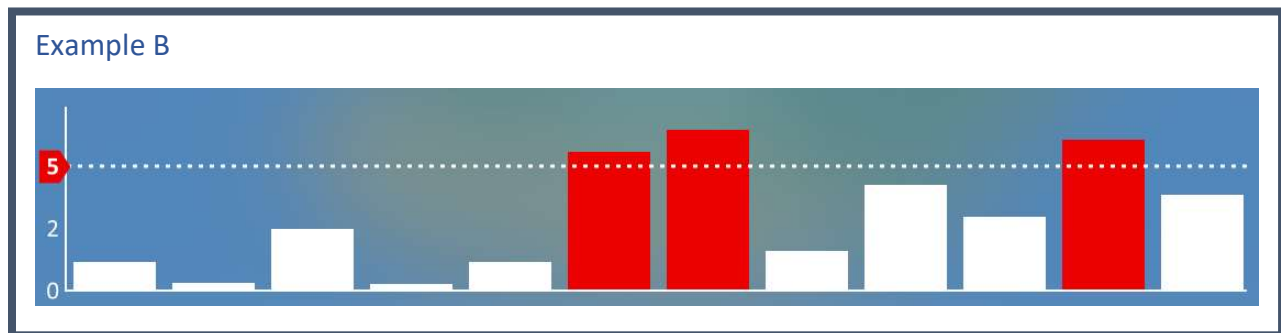
D. Pick 1 of the 5 critical measurement types from *Module 2: Measure* that you would like to keep an eye on.

- a) Generator Output
- b) Power Load
- c) Breaker Operation
- d) Password Attempts
- e) Port Scans

If you think that a huge decrease in power production from a generator is the best indicator of an attack, then you would want to measure Generator Output. On the other hand, if you think a high amount of Password Attempts signals a bigger problem, you should focus on that.

E. Determine what relationship you want to measure based on what you want to learn about what's happening at that grid asset.

In our example below, we've decided to measure the number of port scans over a period of time. Notice the number of port scans is on the vertical column to the left of the bar graph. To the right of that, each bar represents a certain period of time; for example the left most bar could be scans between 1:00AM-1:15AM and each bar could be a 15 minute range after that.



You could decide to compare the number of port scans at different locations or investigate the relationship between port scans and the time of day. It really all depends on what you think will give you the information you need.

Step 2: Determining “Normal State” vs “Alarm State”

F. Set a number range for what's normal and what would signal an alarm or alert.

Although you won't know what numbers are normal and which are not in the “cyber security world” any range of numbers will do. The point is simply to show the difference between what would be normal and what is not so that you'll be able to identify a possible cyber attack quickly and accurately.

Look at Example B, above. Our normal range is between 0-4, and our alarm range is anything above 5.

Step 3: Sketch out your Visualization Tool

G. Review what you want to measure and where you want to measure it.

Grid Asset	Measurement Type	Measurement Relationship

Example C

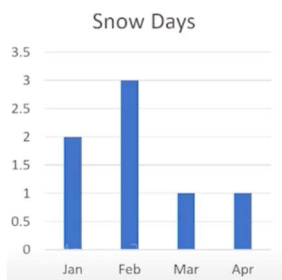
Grid Asset	Measurement Type	Measurement Relationships
Substation	Number of Port Scans	Number of Port Scans over time

H. Select the best visualization tool for the measurement you chose.

In *Module 2: Measurement* and *Module 3: Visualization*, we review different tools that best display those measurements.

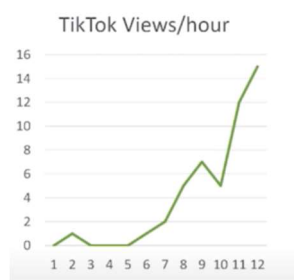
Bar Chart

Display & compare sets of numerical data



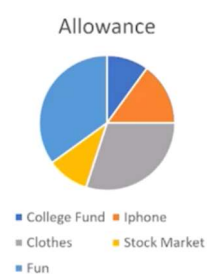
Line Graph

Show change over time



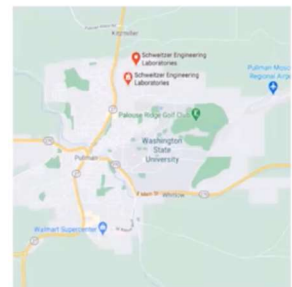
Pie Chart

Show all parts of a whole



Geospatial View

Show information with respect to actual locations



I. Sketch your visual display.

a. Include the principles of display design in your own design.

In *Module 3: Visualization*, we described three principles of design that you should incorporate into your own design. Review these to help you as you create your visual display.

1. Pictorial Realism
2. Situational Awareness
3. Progressive Disclosure

b. Sketch out a visual display that can show you the difference between a normal state and an “alarm state.” This “alarm state” will signal to you that something bad might be happening. Do that in the space below or in your own notebook.

c. Keep it “sketchy.” No need for a polished design. Add notes and other symbols to describe your idea.

Conclusion

Nice going! You’re on your way to helping make the invisible visible! We’d love to see your designs. To see how a professional does it, you’ll be able to utilize the visual display tool that Bryan created in the Threat Unseen: Cybersecurity Session

Please send your sketches to your teachers, they will pass the sketches on to us, and we will enter you in a drawing to win a prize!