Principles of Science in Cybersecurity

Gabriel Canfield
June 1, 2025

A strong base to go off of for logical thinking and analysis in cybersecurity is the principles of science. The principles of science can help professionals in the cybersecurity industry make correct and informed decisions when they are face to face with an incident they need to resolve. There are many principles of science, those being objectivity, empiricism, parsimony, skepticism, and tentativeness.

- **Objectivity:**
  The idea of making decisions that are based on facts. When you are relating that to cybersecurity, it is extremely important because you need to be focused when going over logs or certain alerts.
- **Empiricism:**
  This principle takes a focus on the use of observation and experience to understand types of problems. Professionals in the cybersecurity world rely more on network traffic, logs of attempted logins, or behavior of certain malware in order to have a better understanding of threats. This can improve their decision making.
- **Parsimony:**
  Parsimony is the idea of picking the most simple explanation that can fit the factual evidence. Examples of this would be someone not being able to log in, and the reason would most simply be forgetting a password instead of something extremely technical.
- **Skepticism:**
  This principle bases everything on factual evidence over assumptions. It describes someone that doesn't take something as true without strong evidence. This can be used through cybersecurity with things such as phishing emails or dangerous links. With people being skeptical, it forces them to look into things more and find possible suspicious angles.
- **Tentativeness**
  This principle means that you have an understanding that our knowledge can change with new evidence. This is very important because threats always change and evolve, and professional analysts in cybersecurity must be flexible and update their methods as threats update.

All in all, each of these principles strengthen cybersecurity by promoting critical thinking, problem solving, and constant learning.

References

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Sommers, J. (2017). The scientific method and cybersecurity: Improving analytical thinking. *Journal of Cybersecurity Education*, 2(1), 45–56.