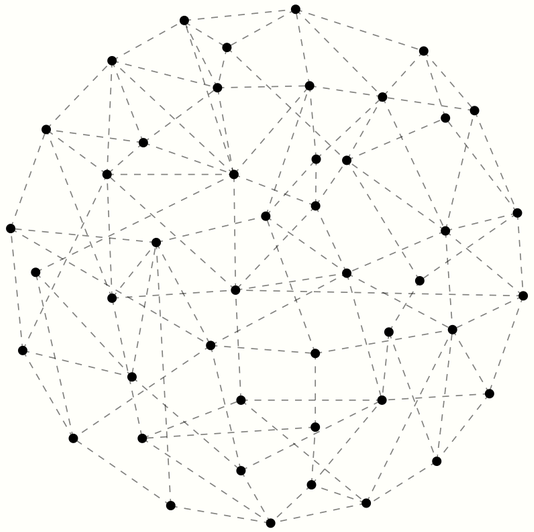
THE PRINCIPLES OF SCIENCE & CYBERSECURITY



Relativism

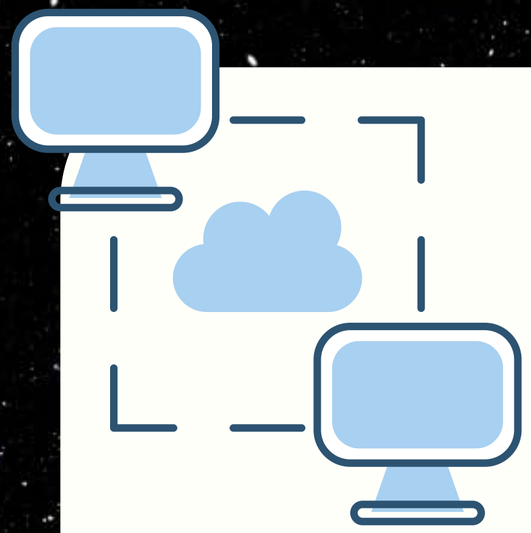
An event or concept can be explained in relation to other events or concepts.

As a Cybersecurity professional it is important to understand that the emergence of new technology can cause a relative changes in the cyberspace, security protocols, business processes, etc.

Objectivity

***Being objective in the pursuit of knowledge*.**

As a Cybersecurity professional it is important to be objective in comparing and selecting different cyber related solutions. For example when deciding whether hosting servers on site or outsourcing to the cloud, it is important to be objective and select the best solution that fits the requirement of the business.



Parsimony

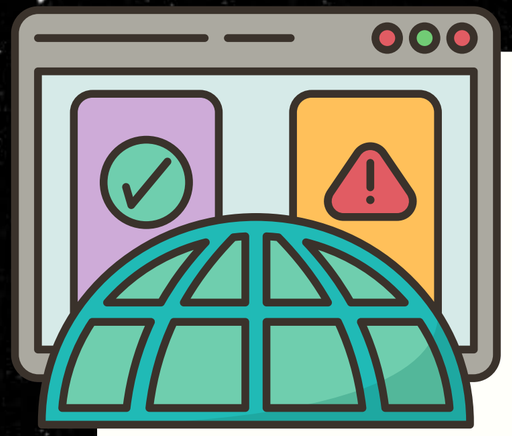
Explaining a concept as simple as possible

As a Cybersecurity professional it is important to be able to communicate complex processes in simplest way possible.
For example when explaining end-to-end communication between two network devices, the TCP/IP Model that contains four layers is the simplest way to do so.

Empiricism

Explaining a phenomena with empirical data rather than guessing

As a Cybersecurity professional it is important to be able to create solutions based on reliable gathered data.
For example when responding to cybersecurity breach, it is important to analyze event logs and system files and processes to identify the threat rather than just guessing.



Ethical Neutrality

Remaining ethical in pursuit of knowledge

As a Cybersecurity professional it is important to remain ethical in conducting cyber related tasks.

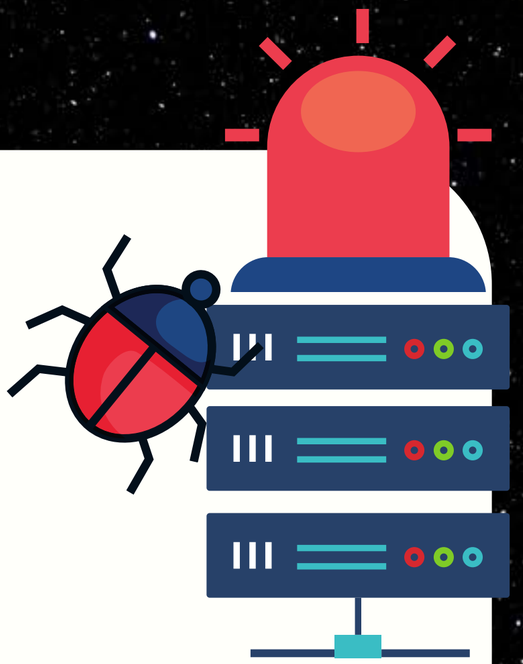
For example when conducting penetration testing it is important to abide by the agreed scope, terms, and parameters of the contract.

Determinism

An event can be determined based on previous events

As a Cybersecurity professional it is important to understand that certain events are bound to happen if an opportunity is provided.

For example if a known vulnerability is left unpatched, the vulnerability can and will be exploited.



JOURNAL #2

CYSE201S

ENNIO CRUZ