In general, an ethical hacker is a soldier in the arms race between cybersecurity experts and those who want to attack systems. But there is a little more to it than that. In an earlier piece, we talked about this as an emerging industry, and demand for ethical hackers since then has only grown.

First and foremost, a lot of experts describe three types of hackers:

White hat hackers are engaged in attacking systems on behalf of the people who run or own those systems.

Gray hats sort of exist in the middle of the whole conflict. They are often described as mercenaries and work for whoever gives them an incentive.

Black hats are malicious hackers who are trying to attack a system for profit or for other motives.

Demand for ethical hackers has only grown as cybersecurity becomes a more prominent concern for organizations across the globe.

While the specifics this job role entails can vary from position to position and company to company, in general, ethical hacking involves trying to break into an organization's system so vulnerabilities can be fixed before malicious hackers exploit them.