In general, an ethical hacker is a soldier in the arms race between cybersecurity experts and those who want to attack systems.

Types of Hacking and Ethical Hacking in Particular

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

White hats. White hat hackers are engaged in attacking systems on behalf of the people who run or own those systems. In other words, they're trying to use hacking techniques to find vulnerabilities they can fix, keep malicious hackers out and to prevent certain kinds of system damage or compromise.

Gray hats. 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. Gray hats may vacillate between working as security experts and working as malicious hackers in independent lone wolf operations or criminal rings.

Black hats. Black hats are malicious hackers who are trying to attack a system for profit or for other motives. They generally seek the destruction of corporate or government systems or other networks. Some are disgruntled former employees, others are cybercriminals. All of them are active threats!

The problem, though, is that intent is sometimes in the eye of the beholder. What if there is no contract? When someone hacks a system, how does law enforcement know that they're doing it ethically? Without the documentation and agreements, they may not.

In recent times, when a lot of financial value is floating around the internet, it's even more important to pin down an ethical hacker's job role and incentivize people to act ethically.

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