2.2.2 Threat Actor Type Facts

A threat actor is a person or organization that poses a threat to an organization's security. This can be an inside or external threat. Some threats aren't even malicious; they can be caused by internal negligence.

This lesson covers the following topics:

- Threat actor types
- Advanced persistent threat
- Threat modeling

Threat Actor Types

Threat actors generally fall into different categories based on their skills and motivation.

Type	Description
White hat	This is a skilled hacker who uses their skills and knowledge for defensive purposes only. A white hat hacker will only interact with a system that they have explicit permission to access. These are the ethical hackers.
Black hat	This hacker is also very skilled, but uses their knowledge and skills for illegal or malicious purposes. A black hat is also known as a cracker. They are highly unethical.
Gray hat	The gray hat hacker falls in the middle of the white hat and black hat hackers. The gray hat may cross the line of what is ethical, but usually has good intentions and isn't being malicious like a black hat hacker.
Suicide hacker	A hacker who is only concerned with taking down their target for a cause. This hacker has no concern with being caught or going to jail--their only concern is their cause.
Cyber terrorist	This hacker is motivated by religious or political beliefs and wants to cause severe disruption or widespread fear.
State sponsored hacker	A hacker that works for a government and attempts to gain top-secret information by hacking other governments.
Hacktivist	A hacker whose main purpose is to protest and get their views and opinions out there. Hacktivists often deface websites or use denial-of-service attacks.
Script kiddie	This person is extremely unskilled and uses tools and scripts that real hackers have developed.

Advanced Persistent Threat

Regardless of the hacker's motivation and skill set, one goal for many hackers is to execute what's known as an Advanced Persistent Threat (APT). An APT is a stealthy attack that gains access to a network or computer system and remains hidden for an extended period of time. This means that the hacker can keep going back undetected for quite a while.

Threat Modeling

Threat modeling is the process of analyzing the security of the organization and determine security holes. Once a threat model is put together, the organization can begin securing its systems and data.