Types of threat actors

Anticipating attacks is an important skill you'll need to be an effective security professional. Developing this skill requires you to have an open and flexible mindset about where attacks can come from. Previously, you learned about **attack surfaces**, which are all the potential vulnerabilities that a threat actor could exploit.

Networks, servers, devices, and staff are examples of attack surfaces that can be exploited. Security teams of all sizes regularly find themselves defending these surfaces due to the expanding digital landscape. The key to defending any of them is to limit access to them.

In this reading, you'll learn more about threat actors and the types of risks they pose. You'll also explore the most common features of an attack surface that threat actors can exploit.

Threat actors

A **threat actor** is any person or group who presents a security risk. This broad definition refers to people inside and outside an organization. It also includes individuals who intentionally pose a threat, and those that accidentally put assets at risk. That's a wide range of people!

Threat actors are normally divided into five categories based on their motivations:

- **Competitors** refers to rival companies who pose a threat because they might benefit from leaked information.
- **State actors** are government intelligence agencies.
- **Criminal syndicates** refer to organized groups of people who make money from criminal activity.
- **Insider threats** can be any individual who has or had authorized access to an organization's resources. This includes employees who accidentally compromise assets or individuals who purposefully put them at risk for their own benefit.
- **Shadow IT** refers to individuals who use technologies that lack IT governance. A common example is when an employee uses their personal email to send work-related communications.

In the digital attack surface, these threat actors often gain unauthorized access by hacking into systems. By definition, a **hacker** is any person who uses computers to gain unauthorized access to computer systems, networks, or data. Similar to the term threat actor, hacker is also an umbrella term. When used alone, the term fails to capture a threat actor's intentions.

Types of hackers

Because the formal definition of a hacker is broad, the term can be a bit ambiguous. In security, it applies to three types of individuals based on their intent:

1. Unauthorized hackers
2. Authorized, or ethical, hackers
3. Semi-authorized hackers

An unauthorized hacker, or unethical hacker, is an individual who uses their programming skills to commit crimes. Unauthorized hackers are also known as malicious hackers. Skill level ranges widely among this category of hacker. For example, there are hackers with limited skills who can't write their own malicious software, sometimes called *script kiddies*. Unauthorized hackers like this carry out attacks using pre-written code that they obtain from other, more skilled hackers.

Authorized, or ethical, hackers refer to individuals who use their programming skills to improve an organization's overall security. These include internal members of a security team who are concerned with testing and evaluating systems to secure the attack surface. They also include external security vendors and freelance hackers that some companies incentivize to find and report vulnerabilities, a practice called **bug bounty** programs.

Semi-authorized hackers typically refer to individuals who might violate ethical standards, but are not considered malicious. For example, a **hacktivist** is a person who might use their skills to achieve a political goal. One might exploit security vulnerabilities of a public utility company to spread awareness of their existence. The intentions of these types of threat actors is often to expose security risks that should be addressed before a malicious hacker finds them.

Advanced persistent threats

Many malicious hackers find their way into a system, cause trouble, and then leave. But on some occasions, threat actors stick around. These kinds of events are known as advanced persistent threats, or APTs.

An **advanced persistent threat (APT)** refers to instances when a threat actor maintains unauthorized access to a system for an extended period of time. The term is mostly associated with nation states and state-sponsored actors. Typically, an APT is concerned with surveilling a target to gather information. They then use the intel to manipulate government, defense, financial, and telecom services.

Just because the term is associated with state actors does not mean that private businesses are safe from APTs. These kinds of threat actors are stealthy because hacking into another government agency or utility is costly and time consuming. APTs will often target private organizations first as a step towards gaining access to larger entities.

Access points

Each threat actor has a unique motivation for targeting an organization's assets. Keeping them out takes more than knowing their intentions and capabilities. It's also important to recognize the types of attack vectors they'll use.

For the most part, threat actors gain access through one of these attack vector categories:

- **Direct access**, referring to instances when they have physical access to a system
- **Removable media**, which includes portable hardware, like USB flash drives
- **Social media platforms** that are used for communication and content sharing
- **Email**, including both personal and business accounts
- **Wireless networks** on premises
- **Cloud services** usually provided by third-party organizations
- **Supply chains** like third-party vendors that can present a backdoor into systems

Any of these attack vectors can provide access to a system. Recognizing a threat actor's intentions can help you determine which access points they might target and what ultimate goals they could have. For example, remote workers are more likely to present a threat via email than a direct access threat.

Key takeaways

Defending an attack surface starts with thinking like a threat actor. As a security professional, it's important to understand *why* someone would pose a threat to organizational assets. This includes recognizing that every threat actor isn't intentionally out to cause harm.

It's equally important to recognize the ways in which a threat actor might gain access to a system. Matching intentions with attack vectors is an invaluable skill as you continue to develop an attacker mindset.