2.1.2 Threat Agents Overview

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

This lesson covers the following topics:

- Threat agent attributes
- Types of threat actors

Threat Agent Attributes

Understanding the attributes and tactics associated with threat actors will help you better identify and defend against them.

Attribute	Description
Internal vs. external	▪ *Internal threat agents* are authorized individuals that carry out an attack by exploiting their inherent privileges. This category includes employees (both current and former), janitors, security guards, and even customers. ▪ *External threat agents* are individuals or groups that attack a network from the outside and seek to gain unauthorized access to data.
Persistent vs. non-persistent	▪ The goal of persistent threats is to gain access to a network and retain access undetected. With this type of threat, attackers go to great lengths to hide their tracks and presence in the network. ▪ The goal of non-persistent threats is to get into a system and steal information. The attack is usually a one-time event. The attacker typically doesn't care if the attack is noticed. An advanced persistent threat (APT) is a type of persistent threat carried out by a nation state. An APT has the goal of continually stealing information without being detected. The tactics used are much more advanced than a traditional persistent threat.
Open-source intelligence (OSINT)	Before carrying out an attack, a threat actor typically gathers open-source intelligence (OSINT) about the target. OSINT is information that is readily available to the public and doesn't require any type of malicious activity to obtain. Sources of OSINT include the following: ▪ Media (newspapers, magazines, advertisements) ▪ Internet (websites, blogs, social media) ▪ Public government data (public reports, hearings, press conferences, speeches) ▪ Professional and academic publications (journals, academic papers, dissertations)

Types of Threat Actors

The following table describes the types of threat actors that you, as a security professional, need to be aware of.

Threat actor type	Description

Insider	An insider is any individual who has authorized access to an organization and either intentionally or unintentionally carries out an attack. The most common type of insider is a full-time employee; however, other inside actors include customers, janitors, security guards, and even former employees. Possible motives for an insider threat actor can include:
	▪ Disgruntlement with an employer
	▪ Bribery by a competitor
	▪ Personal financial gain
	Because insiders are one of the most dangerous and overlooked threats to an organization, you need to take the appropriate steps to protect against them.
	▪ Require mandatory vacations.
	▪ Create and follow onboarding and off-boarding procedures.
	▪ Employ the principal of least privilege.
	▪ Have appropriate physical security controls in place.
	▪ Require security awareness training that is tailored for the role of the employee (role-based awareness training). Typical roles include:
	  ▪ Data owner
	  ▪ System administrator
	  ▪ System owner
	  ▪ User
	  ▪ Privileged user
	  ▪ Executive user
	Sometimes an employee can become an insider threat actor without knowing it. This is known as an unintentional insider threat actor. Proper security training can help protect against unintentional insider threat actors.

White hat	A skilled hacker who uses knowledge and skills only for defensive purposes. A white hat hacker obtains explicit permission to interact a system or systems. These are the ethical hackers.
Black hat	This hacker is also very skilled, but uses 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 malicious like a black hat hacker.
Script kiddie	A script kiddie is an individual who carries out an attack by using scripts or programs written by more advanced hackers. Script kiddies typically lack the skills and sophistication of legitimate hackers. Script kiddies are usually motivated by the chance to impress their friends or garner attention in the hacking community. Because script kiddies lack knowledge and sophistication, their attacks often seek to exploit well-known vulnerabilities in systems. As such, defending against script kiddies involves keeping systems up-to-date and using standard security practices.
Hacktivist	A hacktivist is any individual whose attacks are politically motivated. Instead of seeking

	financial gain, hacktivists are looking to defame; shed light on; or cripple an organization or government. Often times, hacktivists work alone. Occasionally, they create unified groups of like-minded hackers. For example, the website wikileaks.org is a repository of leaked government secrets, some of which have been obtain by hacktivists.
Organized Crime	An organized crime threat actor consists of a group of cybercriminals whose main goal is financial gain. Attacks carried out by organized crime groups can last several months, are well-funded, and are extremely sophisticated. A common tactic used by organized crime is a targeted phishing campaign. Once access is gained, the group will either steal data and threaten to release it, or use ransomware to hold data hostage. Due to the level of sophistication and amount of funding, attacks from organized crime groups are extremely hard to protect against. In many cases, it's simply a matter of time until a data breach occurs or ransomware takes hold. Because of this, many companies that need immediate access to their data (such as hospitals and financial institutions) stockpile digital currency in case of an attack. Specific protections against organized crime threat actors include: ▪ Proper user security training ▪ Implementing email filtering systems ▪ Properly secure and stored data backups In July 2017, an organized crime group hacked HBO's network and stole a purported 1.5 terabytes of data. The group then demanded HBO pay it a hefty ransom in bitcoins, or it would release the data to the public.
Nation state	A nation state is the most organized, well-funded, and dangerous type of threat actor. There are two primary motives for nation state attacks (also called state-sponsored attacks). ▪ Obtaining information - some attacks seek to obtain sensitive information, such as government secrets. These attacks usually target organizations that have government contracts or the government systems themselves. Attacks motivated by information gathering are considered a type of APT, because the goal is to remain in the system undetected. ▪ Crippling systems - some attacks seek to cripple the target's network or infrastructure. For example, an attack could target a city's power grid or water system. In 2010, a malicious computer worm called Stuxnet was discovered. The worm was designed to target industrial centrifuges used by the Iranian nuclear program. Stuxnet is thought to be a state-sponsored attack because its code was so large and complex that it would have required huge amounts of funding and resources to create. Nation states use many attack vectors and unknown exploits. Defending against them involves building a comprehensive security approach that uses all aspects of threat prevention and protection.
Competitor	A competitor threat actor carries out attacks on behalf of an organization and targets competing companies. For example, a payment processing company could hire someone to carry out a DDoS attack on a competing payment processing company to force users to choose the attacker's product. The motive behind such attacks include financial gain, competitor defamation, or stealing industry secrets.

The term *hacker* is a catch-all term used to describe any individual who uses technical knowledge to gain unauthorized access to an organization.