FORTINET CERTIFIED FUNDAMENTALS Cybersecurity

Introduction to the Threat Landscape

Lesson Scripts

1.0

FORTINET Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

TABLE OF CONTENTS

Introduction to Cybersecurity Module

Introduction to Cybersecurity Overview Lesson

Welcome to the *Introduction to Cybersecurity* module.

Click **Next** to get started.

Cybersecurity is the collective methods, technologies, and processes that protect computer systems, networks, and the information they contain.

Note that cybersecurity is more than technology. In addition to technology, it is also the correct actions and behaviors of people that keep computer systems safe.

By the end of this module, you will be equipped with some of the fundamental conceptual knowledge of IT security. You will learn about the principles of information security that give direction to IT security professionals in their day-to-day activities. And you will have greater insight into the process of identifying what information needs protection and how much protection it requires. You will learn about the first-line of defense against cyberattacks. In addition, you will become familiar with some of the essential information security terms.

These topics include some of the critical knowledge that all cybersecurity professionals are expected to know, and upon which more specific technological information will be built.

Proceed to the first lesson to get started.

What is Cybersecurity Lesson

Welcome to the *What Is Cybersecurity* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe the terms cybersecurity, information security, and information systems security.
- Explain how IT security determines what information needs protecting.
- Explain the first line of defense against cyberattacks.

What is cybersecurity?

Cybersecurity is the practice of protecting computer networks, devices, and information from damage, loss or unauthorized access. It is important to note that cybersecurity protects digital information from cyberthreats. The protection of information means the preservation of confidentiality, integrity, and availability of information in the cyberspace.

Cybersecurity professionals act to protect servers, endpoints, databases, and networks by finding security gaps and misconfigurations that create vulnerabilities.

Cybersecurity can be divided into five categories: critical infrastructure security, application security, network security, cloud security, and the Internet of Things (IoT) security.

Note that other organizations may categorize the types of cybersecurity differently or label them differently. In addition to these five categories there are the people and processes that use technology to defend computer systems, networks, and the information therein.

These different categories reflect the extent that computer technologies have transformed the world.

From online management of gas pipelines or electrical grids to applications that allow you to buy and sell goods online to collaborating with work colleagues irrespective of geography to renting data storage in the cloud to tracking printer toner and maintenance, all of these technologies have transformed how people live and how they do business.

The digital transformation has realized enormous efficiencies, expanded unheard of conveniences, supplied omnipresent access to information, and exponentially increased productivity, which has grown wealth and improved the quality of life. For example, people living in remote areas of the world can access medical experts using computer technologies. Personal medical information can be collected locally and transferred to medical experts to assist in diagnosis and remedies. Without securing computer networks and the links that connect them, all of these advances are at risk.

Information security, also known as InfoSec, is the practice of protecting information. InfoSec includes the tools and processes used for preventing, detecting, and remediating attacks and threats to sensitive information, both digital and physical. InfoSec also includes documenting the processes, threats, and systems that affect the security of information. The nature of the information is inclusive and broad. It includes information stored electronically on a computer, or information laying on someone’s desk, or stored in a file cabinet. Information that might require protection could also include everything from mission-critical data to HR policies to legal contracts.

IT security scrutinizes all information within an organization in order to categorize and prioritize its sensitivity. Some information is labelled as unprotected, meaning that no controls are necessary, while some information is labelled as protected, meaning that some level of protection and control is required. Depending on the protected

information’s criticality, it could be labelled confidential, secret, or top secret. Each successive protected level requires more rigorous control and safeguards.

Information systems security is a part of InfoSec. It is defined as the protection of information systems against unauthorized access, modification, destruction, or the denial of access to authorized users. Information systems include the devices, computer networks, and physical locations that store or transmit sensitive information. The form of the information can be digital or physical.

Given what you now know about the terms discussed in this lesson, you can conclude that information systems security is a subset of InfoSec and cybersecurity is a subset of information systems security.

Given the importance of protecting this cyber infrastructure, which is vital to the continued prosperity and quality of life to much of the world, certain precautions can be taken. It starts with people and education. Numerous studies have identified human error as the leading cause of network and computer breaches. This situation can be addressed by educating people at work and at home to think before clicking and to help them identify phishing attacks and other common attack methods by bad actors.

Another first line of defense, both at work and at home is to prepare for disaster and plan for recovery. If you do regular backups of your data and these are kept safely offline, then should your data be deleted or corrupted by malware, or encrypted by ransomware, you can restore your data with the least amount of data loss and interruption.

Principles of Information Security Lesson

Welcome to the *Principles of Information Security* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- List the principles of information security.
- Describe the terms authentication, authorization, and accounting.

There is a triad of principles that constitutes the objectives of information security. These principles are confidentiality, integrity, and availability which form the letters C-I-A.

Private information must remain confidential. You need to know who is trying to access the information and whether or not they are authorized to access it.

You must also have assurance that the information is authentic, in other words has integrity. The information must be protected from an unauthorized change, and if it is altered then you must be alerted to this fact.

Last, authorized parties must have access to the information. Technologies, policies, and processes must be in place to ensure reliable availability. Together, these three principles constitute the CIA triad.

Conversely, Infosec works to prevent the disclosure and alteration of information. In addition, it strives to ensure that authorized parties are not denied information.

These characteristics, known as the DAD triad, are the opposite of the CIA triad.

Disclosure exposes confidential data to unauthorized parties.

The alteration of data, or the inability to test for alteration, makes the data untrustworthy.

Denial of information prevents legitimate and authorized agents from accessing data. An effective security solution, such as a network firewall, will help neutralize the DAD triad.

The three security terms that you should be conversant with are authentication, authorization, and accounting (AAA). Together, AAA constitutes a security framework that controls resources, enforces policies, and audits usage. The security framework plays a major role in network management and cybersecurity by screening users and keeping track of their activities while they are connected.

Authentication is the process of identifying and verifying a person or thing. As an identity and access management (IAM) tool, an AAA server compares a user's credentials with its database of stored credentials by checking if the username, password, and other authentication tools align with that specific user.

Authorization is the process of controlling access to resources. During authorization, a user can be granted privileges to access certain areas of a network or system. The areas and sets of permissions granted a user are stored in a database along with the user's identity. The user's privileges can be changed by an administrator.

Last, accounting in information technology is the record-keeping and tracing of agent activities on computer devices and networks. Accounting tracks information such as the length of time a user was logged in, the data they sent or received, their internet protocol (IP) address, the uniform resource identifier (URI) they used, and the different services they accessed. Accounting may be used to analyze user trends, audit user activity, and provide more accurate billing.

You have completed the lesson. You are able to:

- List the principles of information security.
- Describe the terms authentication, authorization, and accounting.

Threat Landscape Module

Threat Landscape Overview Lesson

Welcome to the *Threat Landscape* module.

Click **Next** to get started.

What is a threat landscape? A threat landscape is the collection of threats in a given context or domain and includes information about the perpetrators of the threats: the bad actors. In the context of cybersecurity, the threat landscape includes all known and possible threats to computer networks. The introduction of new technologies and methods ensures a dynamic landscape where evolving new threats arise on an ongoing basis.

Understanding the nature of the threats posed to your network arms you with the knowledge to counter and defeat attacks against computer systems.

The lessons in this Threat Landscape module provide an essential understanding of the following fundamentals necessary to achieve your goals.

You will be able to:

Identify the different types of bad actors and hackers by their motivations and tactics.

Different types of bad actors are more likely to attack certain verticals or types of businesses. For example, hospitals are big targets of cyber criminals who want to ransom valuable medical information to enrich themselves. A nation's department of defense is more likely to be attacked by other nation state threat actors, who are more interested in stealing state secrets than extracting money from their victims. Therefore, by knowing your enemy you are better equipped to counter their attacks.

You will be able to:

Describe attack vectors, cybersecurity threats, and the categories that cyberthreats fit into.

Understanding the classification of threats gives you insight into how attacks can be carried out. Again, this can help you to identify weaknesses in your environment and take precautions to reduce the attack surface.

You will be able to:

Define threat intelligence and explain how it is processed.

For information to be threat intelligence, it must be relevant, actionable, and contextual. If it is not all of these things, then it is not threat intelligence. However, this is also very situational, so what is intelligence for one organization may not be intelligence for another.

You will be able to:

Describe different attack frameworks, such as the Cyber Kill Chain and MITRE ATT&CK.

Attack frameworks give you a glimpse into the anatomy of a cyberattack. Understanding the chain of actions in an attack enables you to anticipate your enemy's actions and counter them. Also, frameworks like MITRE ATT&CK are rich in information and threat intelligence that you need to be an effective IT security professional.

Proceed to the first lesson to get started.

Threat Actors Lesson

Welcome to the *Threat Actors* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe the different types of bad actors and their motivations.
- Describe the different categories of hackers.

What is a bad actor? Bad actors, also known as threat actors, are persons who try to steal, sabotage, or stop you from using computer systems or accessing information that you are authorized to use and that is stored on or in transit between computing devices. There can be a myriad of motivations for their criminal behavior, and these different motivations not only influence their attack methods but provide insight into their character and beliefs. Bad actors can be grouped into types based on their character, motivations, and the common attack methods that they use. It's important to note that bad actors are NOT a homogeneous group.

While there are various types of bad actors who have different motivations that help explain their activities, you should not view a bad actor as a mysterious hooded character who works in a dark basement, in another country, or in another city. A bad actor could be anyone, located anywhere. It could be someone in a local coffee shop who is setting up a fake Wi-Fi access point to steal data, a disgruntled employee who is leveraging their employee status to gain deeper access to corporate data, someone in another country whose full-time job is to scam people from a call center, or it could be a teenager in your neighborhood who is curious about the freely available programs on the internet that makes distributing malware and ransomware as easy as a few clicks of the mouse.

The types of bad actors are explorer, hacktivist, cyberterrorist, cybercriminal, and cyberwarrior.

The explorer is perhaps the least nefarious of all the bad actor types.

Notoriety is the biggest motivator within this group. The explorer is curious about the kinds of weaknesses that exist on computer networks and strives to find and exploit them. They do not intend to inflict serious damage, but they might change a page on a website to embarrass someone or do something to advertise to the world how clever they are.

One method used by explorers and other bad actor types is called phishing. Essentially, they trick people into giving up personal information. An example of phishing is an email from a seemingly legitimate source to a broad group of people. The ingredients of a successful phishing attack are, one, to gain the trust of the recipient or at least to appear innocuous, and two, to manufacture an emergency to force the recipient to act. There are variants of phishing that can be deployed as well. Spear phishing also uses email, but the email is directed at a specific person or group. The explorer also might choose to call or text you, better known as smishing and vishing. While not using email, the same ingredients are required for the scheme to be successful. Phishing and its variants, however, are not exclusive to the explorer, and other bad actor types might use them for their own purposes.

Click the icons and buttons for more information.

Phishing Example:

A phishing email might state that some business demands the recipient's immediate attention and a link to the organization's site is provided for their convenience. The link, however, does not direct their browser to the legitimate site but rather takes them to a look-a-like rogue site. The rogue site provides the login page and the victim dutifully types their username and password. When the victim clicks submit the rogue site returns a message that their password was incorrect. A link is provided to the legitimate login page, the victim tries again, and this time logs in successfully. Because people often type their passwords quickly and sometimes make

mistakes, the victim may not be alerted to the fact that something fishy has transpired. But meanwhile, the bad actor has the victim's username and password and can now log in as them.

Unlike the self-interested explorer, hacktivists are fervent believers in an external cause. They are motivated by ideology or are animated by an emotive force. The hacktivists' idealism drives them to act collectively in common cause against an enemy.

While hacktivists may collectively crusade against a specific corporation, or go after political or social organizations that they feel did something bad, their extremism demands anonymity and online groups, by nature, are fragmented. A common strategy of hacktivists is to build a botnet in secret. To make a botnet, the hacktivist sets up a command-and-control (C&C) server that is accessible on the internet. This is a central coordination point for all the botnet nodes. Next, they craft malware that, once installed on some unsuspecting computers, waits patiently for instructions from the C&C server. The C&C server instructs thousands of botnet nodes to send messages to the targeted server, which becomes overwhelmed by requests and stops responding. This is called a distributed denial-of-service (DDoS) attack. Hacktivists lack the computer resources to make a successful DDoS attack, so they must gain control of thousands of other people's computers.

The cyberterrorist has more in common with the hacktivist than the explorer. Their motivation is also driven by ideology, but their violence is directed more broadly against a society. While hacktivists are content with punishing their enemies, cyber terrorists strive to intimidate and destabilize a society by destroying or disrupting computer or communication networks. They like to target online infrastructure, such as nuclear power plants, natural gas pipelines, and electrical power grids. This type of online infrastructure is called operational technology.

Like hacktivists, and unless they are sponsored by a nation state, they lack the resources to inflict catastrophic destruction and must beg, borrow, and steal technology to mount effective attacks. Unlike hacktivists, cyberterrorists operate more like a cohesive virtual army. They have structure and direction. They can deploy tactics such as DDoS to attack targets, but a favorite method is spear phishing. Once they have identified a person with extensive network privileges, they target them with a carefully planned social engineering campaign.

The motivation of a cybercriminal is more self-centered: They want money plain and simple. They achieve this goal by a combination of phishing, theft of identities or credit cards, which they use or sell on the black market, or ransomware. Ransomware is a type of malware that blocks access to computer information or systems until a ransom is paid.

Sometimes there can be multiple motivations for a group, or two or more bad actor types. For example, it would not be unusual for cybercriminals and cyberterrorists or cyberwarriors to collaborate on an attack or to exist within the same group. In the example of the 2021 cyberattack against Colonial Pipeline, the criminal organization's host country is suspected to have abetted or approved of the attack. This is an example of cybercriminals and cyberwarriors colluding.

Click the icon and button for more information.

Cyberwarriors are the least self-interested, but are nonetheless the most dangerous because they have the resources of a nation-state at their disposal. Cyberwarriors are motivated by the national interests of their home country. Whether cyberwarriors are good, bad or neutral depends on which nation-state they fight for. Their methods are vast and sometimes secret, and their missions include espionage, extortion, and embarrassment on the one hand, to using targeted cyberweapons to disrupt, damage, or destroy critical infrastructure on the other.

They like to leverage unpatched vulnerabilities in common operating systems and applications. These are known as zero-day exploits—presumably because when the exploit is launched, the vendor has zero days to fix the problem. Cyberwarriors do intensive research on these common operating systems and applications, finding weaknesses, bugs, and other behaviors that they can use to attack the enemy's computer systems. The weaknesses must remain a secret until they can be used because once they are known the vendor will issue a patch immediately.

Just as there are different types of bad actors, there are different categories of hackers, each identified by a symbolic color. The main categories are: white hat, black hat, grey hat, and blue hat.

A white hat is an ethical hacker who, with proper authorization, probes the network to identify vulnerabilities. In contrast, a black hat is a hacker who attacks a network for profit or to cause harm. A grey hat is a hacker who attacks a network, contradicting lawful and ethical behavior, but who does not have the same malicious intent as a black hat hacker. This category most closely aligns with the explorer bad actor. A blue hat hacker is a variant of a white hat. This category of hacker refers to outside computer security consulting firms that are employed for penetration testing of a system prior to its launch and with the intent to detect and close vulnerabilities.

You have completed the lesson. You are able to:

- Describe the different types of bad actors and their motivations.
- Describe the different categories of hackers.

Cybersecurity Threats Lesson

Welcome to the *Cybersecurity Threats* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe cybersecurity threats and list examples.
- List the main cyberthreat categories.
- Describe the attack vectors profiled.

What is a cybersecurity threat? A cybersecurity threat is an action exploiting a vulnerability that results in harm to a network or computer system.

Bad actors are the instigators of cybersecurity threats. They exploit different attack vectors to achieve their goals. Broadly speaking, an attack vector is a method used by a bad actor to illegally access or inhibit a network, system, or facility. You can deduce that cybersecurity threats are a subset of attack vectors. What is meant by method? Specifically, the method is how a vulnerability is exploited. There are three components that comprise an attack vector: (1) the vulnerability, (2) the mechanism or object that exploits the vulnerability, and (3) the pathway to the vulnerability.

Here are a couple of examples. Diego receives an email from a colleague asking him to review an attached document. He saves the document to his hard drive and opens it. Unbeknownst to Diego, the sender was not really his colleague and the document installed malware onto his computer. In this example, the vulnerability is the user, the mechanism is the malware and the socially engineered message that convinced him to download the document, and the pathway is the email.

In another example, an authorized person is entering a server room, which is a restricted zone. He notices a technician laden with boxes and computer equipment loitering outside. She explains that she needs to upgrade some equipment but forgot her access pass. Although, the authorized person doesn't recognize her, she sounds convincing and he wants to be helpful, so he opens the door and she passes through. While in the server room she discretely connects a USB device to one of the servers that installs malware. In this example, the vulnerability was the authorized person and an unprotected server. The mechanism was the malware and the situation used to convince the man to allow her access to the server room. The pathway was the door into the server room and the USB device that released the malware.

As you see from these two examples, attack vectors can be divided into electronic social engineering, physical social engineering, and technical, which includes vulnerabilities such as computer misconfiguration. You may have noticed in this last scenario that there were multiple attack vectors. The bad actor first needed to access the facility before she acquired access to the server room, and the server infection was merely the first stage in a chain of events that may include reconnaissance and the exfiltration of data. The preparation of an attack campaign is sometimes referred to as an attack path. An attack path is the chain of events that occurs when attack vectors are exploited.

Cybersecurity threats can be divided into four categories: social engineering, malicious software (known as malware), unauthorized access to physical places or computer systems, and system design failure.

Social engineering is the act of using psychological manipulation to trick people into taking some action that is contrary to their best interests, such as disclosing confidential information. The ingredients of a successful social engineering attack usually involve gaining the trust of the victim and then compelling them to act.

Malware is software that is designed to disrupt, damage, or gain unauthorized access to a computer system.

Unauthorized physical access could be a bad actor following an authorized person through a door after they have swiped their badge. This is known as tailgating. Unauthorized digital access could be a bad actor looking over someone's shoulder as they type their credentials.

System design failure is a security flaw in a computer system or application that the bad actor exploits to gain access to a computer system. There are many examples of cyberattacks that fall into one or more of these categories.

Attack vectors can be categorized in several ways and are often combined with other vectors to achieve the desired result. For example, a distributed denial-of-service (DDoS) attack involves a command and control (C&C) server signaling to thousands of infected computers to send requests to a targeted server at the same time. However, before a DDoS attack can be invoked, the bad actor must first infect thousands of computers. How do they do that? One common method is phishing. The bad actor can send a phishing email to millions of unsuspecting users, and some of those users will click on the link provided that will install malware on their computers.

Other forms of phishing, such as whale phishing or spearphishing, may not be suitable for setting up a DDoS botnet, or farm of infected computers, but they would be suitable for installing Trojan horse malware or ransomware on a specific individual's computer. Whale phishing is a phishing attack aimed at a high-value target, such as a CEO or CFO of an organization. These individuals are targets because they have access privileges to servers and databases, which the bad actor wants access to. The email is carefully crafted to be plausible and personalized to ensure the target is not alerted to the scam. Within the email could be an attached document or a link. Once opened, the document appears entirely harmless, but behind the scenes malware is installed on the target's computer. This is known as a Trojan horse attack. From there, the malware can leverage the individual's network privileges to access and infect other computers. The initial targeted computer is merely the access point to the network in a multi-staged attack.

Click the underlined terms for more information.

As you can see, some attack vectors, such as phishing, are used to exploit a weakness to gain a foothold in a computer system, while other attack vectors, such as DDoS, ransomware, and Trojan horse, are used during the post-exploit stage. The exploited weakness can be human, computer technology, or a combination of the two. In the case of phishing, the weakness is human nature. It is a default trait of human nature to trust, especially if a request seemingly comes from an official source or if you know the person or thing who is making the request.

An example of exploiting computer technology during the pre-exploit stage is the birthday attack. This attack exploits a weakness in some hashing algorithms, which are often used to protect passwords. Last, a brute force attack is typically a method to steal someone's credentials. It involves simply trying every possible combination until the bad actor guesses correctly, but success relies on the targeted individual using a weak password. This type of attack is pre-exploit and relies on human fallibility.

If you were a network administrator, you could neutralize this attack by implementing a strong password policy. As this suggests, there are many counteractions that you can take against the listed attack vectors. Throughout this course, you will be introduced to more attack vectors deployed by bad actors and the measures used to counter them.

Click the underlined term for more information.

You have completed the lesson. You are able to:

- Describe cybersecurity threats and list examples.
- List the main cyberthreat categories.
- Describe the attack vectors profiled.

Threat Intelligence Lesson

Welcome to the *Threat Intelligence* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define threat intelligence.
- Describe the formatting standards for threat intelligence.
- Describe the steps for processing threat intelligence.

What is threat intelligence? According to Gartner, threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

This definition tells you that threat intelligence possesses three requisite characteristics. Threat intelligence is Information that is relevant, actionable, and contextual. Threat intelligence must be relevant to your organization. For example, if you receive information that there is a new computer virus that exploits a vulnerability in macOS, but your organization does not use Apple products, then this information is not relevant to your organization. While it would be relevant to an organization that uses Apple products, it does not qualify as threat intelligence for your organization.

Threat intelligence must be actionable, meaning that the intelligence provides sufficient information for you to take steps to protect your organization. For example, if you learned that the bad actor group Dynamite Panda had just launched a new campaign of attacks against medical facilities, this alone does not provide you with enough information to act upon.

Threat intelligence must be contextual, meaning that there is enough information to enable an intelligence analyst to assess the threat. The macOS vulnerability mentioned earlier is a good example. While a vulnerability in macOS could be a cause for concern, if your organization is properly managing and scanning its network assets, the security team should be able to quickly determine whether there are any macOS devices anywhere on the network. If none exist, then there is most likely no threat to the organization from the vulnerability. It is that additional context—knowledge network assets—that can turn information into threat intelligence. The Dynamite Panda story example can also support this point. The information that this bad actor group exclusively targets specific US verticals becomes threat intelligence because it helps you to assess the threat to your own organization. When viewed or considered on their own, many pieces of information do not amount to threat intelligence. However, when considered along with other, additional information, that initial piece of information can become threat intelligence.

Where do you find threat intelligence? There are a myriad of sources, both external and internal. An internal source of threat intelligence is the information gathered by your organization’s own IT security team. More specifically, internal sources come in the form of server logs, network device logs, past incident reports, captured network traffic, penetration test results, and more. This raw data is organized and contextualized into information, and some of that information is relevant, actionable, and contextual, which makes it threat intelligence.

Externally, threat intelligence can come from a variety of sources and the information is often free. Some external sources of threat intelligence are government sites, such as the Department of Homeland Security, the FBI, and the National Institute of Standards and Technology (NIST) in the United States. These sites generally do not provide specific intelligence about individual malware, but they do offer useful advice about how to protect yourself from attacks, such as ransomware, and timely information about trending scams and attack methods.

Intelligence can come from private sources, such as the SANS Institute and FortiGuard, the Fortinet research and threat intelligence service. Some FortiGuard services are offered by subscription, but much of the threat intelligence found on the FortiGuard website is available for free. It describes how individual malware variants work and uses a severity rating system to rank the danger that these variants pose. Organizations can use this information to prioritize resources to counter the most dangerous threats.

There is also the Common Vulnerability Scoring System (CVSS). CVSS is a free and open industry standard used to assess computer system vulnerabilities. A CVSS assessment produces a numeric score to rate severity. The score, which rates the vulnerability from zero to ten—ten being the most severe—is computed using different sets of metrics. The metrics include factors, such as how exploitable the vulnerability is, how the vulnerability impacts systems, and how effective mitigation efforts are against new exploits as the campaign progresses. For a more detailed description of these metrics, search for common vulnerability scoring system in nvd.nist.gov/vuln-metrics/cvss.

CVSS is an example of open-source intelligence (OSINT). If you search the internet for OSINT, you will discover many other sources of free threat intelligence.

Another invaluable public source for cyberthreat intelligence is MITRE ATT&CK. MITRE ATT&CK freely shares a knowledge base of adversary tactics and techniques.

Finally, there are verticals that share threat intelligence. For example, banks in Brazil share their threat intelligence with each other. There are also other threat intelligence services and tools, including open-source intelligence, like Maltego and the MISP project.

There are also some recognized standards that help to share and describe cyberthreats in a language that is understood by the cyber intelligence community. One standard is called structured threat information expression (STIX). Another is called trusted automated exchange of indicator information (TAXII).

STIX is defined as a collaborative, community-driven effort to define and develop a structured language to represent cyberthreat information. It provides information about bad actors, incidents that have occurred, indicators of compromise (IoC), and the tactics and exploits used to carry out attacks. STIX also recommends actions to mitigate the incidents that it reports.

TAXII is an application protocol for exchanging cyber threat intelligence (CTI) over HTTPS. It defines a RESTful API and a set of requirements for TAXII clients and servers. By using standardized services, messages, and message exchanges, TAXII eliminates the need for customized point-to-point exchange implementations and facilitates the sharing of vital CTI. As the diagram shows, an organization that is a TAXII client can request information and publish new threat intelligence to a TAXII server, which then can be shared with other subscribers.

Click the underlined term for more information.

While knowing where to collect threat intelligence is a good first step, knowing how to use the threat intelligence is arguably more important, because inert information is worthless. There is a process that you can follow to convert mass data into purposive threat intelligence that can be acted upon.

First, identify the primary threats to your network; that is, those threats that are the most vital to stop. Because there is an inexhaustible volume of cyberthreats, it is impossible to stop them all, and to attempt to do so would dangerously disperse and diminish cyber defenses. Websites such as CVSS and FortiGuard will help you answer this question, because they provide intelligence about the most current threats with their severity ratings. But relevant threats may also be determined by your organization’s vertical or business. For example, if you are protecting a hospital from cyberattacks, then ransomware is likely high on the list of attack methods employed by threat actors. On the other hand, if you are defending the Department of Defense, then attacks involving exfiltration are more likely.

Second, assemble threat information from your internal and external sources. Third, process this information. This might involve focusing on information that is most relevant to the primary threats that you identified in the first step. Processing will also likely entail defining baselines of normalcy in network activities. The purpose of this is to help you recognize abnormal network activities. By separating the noise from the signal–eliminating the inconsequential data–you are better able to focus on and process the relevant information. Fourth, analyze the information and look for indicators of compromise (IoC). Fifth, disseminate your analysis, along with any new information, to friends and partners. This effort is facilitated by STIX and TAXII. And sixth, implement lessons learned during the process. Does the information alter which threats you consider the most dangerous to your organization? Does it affect what information you are collecting, or how you are processing and analyzing the information?

As you can see, the process functions as a continuous loop.

You have completed this lesson. You are now able to:

- Define threat intelligence.
- Describe the formatting standards for threat intelligence.
- Describe the steps for processing threat intelligence.

Attack Frameworks Lesson

Welcome to the *Attack Frameworks* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe the cyber kill chain.
- List and explain the stages of the Cyber Kill Chain.
- Explain the benefits of the MITRE ATT&CK matrix.

To better understand and defend against cyberattacks, it is helpful to examine the various frameworks that have been developed to classify and analyze them. These frameworks provide a structure for identifying the different stages of attack, discerning the different tactics used during those stages, analyzing their impact, and developing strategies for prevention and response.

Attack frameworks were developed in response to cyberattacks that were more sophisticated and protracted than in the past. These types of attacks, which can involve extended periods of surveillance and planning before methodically attacking a targeted computer network, are often referred to as advanced persistent threats (APTs). While attack frameworks embody extensive knowledge about attackers' tactics and techniques, they are more than a knowledge base. Rather, you should view attack frameworks as a toolbox for cybersecurity professionals to enhance an organization's security posture.

Lockheed Martin's Cyber Kill Chain and MITRE ATT&CK are only two of several cyberattack frameworks in the industry. You are likely to use at least one of these frameworks during a career in cybersecurity.

One of the most widely used frameworks for analyzing cyberattacks is the Cyber Kill Chain, developed by Lockheed Martin in 2011. The Cyber Kill Chain is a seven-step model that describes the stages of a cyberattack, from the initial reconnaissance and weaponization of the attack method to the final exploitation and exfiltration of data.

The first step in the Cyber Kill Chain is reconnaissance, in which the attacker gathers information about the target and its vulnerabilities. This may involve using tools such as search engines, social media, and other open sources to gather intelligence about the target organization and its systems.

The second step is weaponization, in which the attacker creates a payload or exploit that can be delivered to the target. This may involve creating malware or other malicious code, such as a virus or Trojan horse, and packaging it in a way that is difficult to detect. For example, this could be an innocuous-looking but infected Microsoft Word document that is intended to be delivered by way of a phishing email.

The third step is delivery, in which the attacker delivers the payload to the target. This may involve sending an email with a malicious attachment, or exploiting a vulnerability in a website to inject the payload into the target's system.

The fourth step is exploitation, in which the attacker uses the payload to gain access to the target's systems or data. This may involve executing the payload to exploit a vulnerability in the target's software or operating system, or using the payload to gain access to the target's network.

The fifth step is installation, in which the attacker establishes a foothold within the target's systems. This may involve installing a rootkit or other malicious software that allows the attacker to maintain access to the target's systems even if the initial payload is detected and removed.

Click the underlined words for more information.

The sixth step is command and control, in which the attacker establishes a means of communication with the compromised systems. This may involve setting up a command-and-control server or using other methods to communicate with the compromised systems remotely.

The final step in the Cyber Kill Chain is exfiltration, in which the attacker extracts the data or other assets that were the goal of the attack. This may involve copying sensitive data to a remote location or using the compromised systems to launch further attacks on other targets.

Lockheed Martin's Kill Chain has done much to advance the understanding of the incremental stages of a cyberattack. However, it makes some assumptions that reduce its effectiveness. One major disadvantage of the Cyber Kill Chain is that it assumes that the origin of an attack is external to the network. Also, the kill chain methodology aims to reinforce traditional defense methods. Other cyberattack frameworks arose, in part, because of limitations in the Cyber Kill Chain.

In 2013, the MITRE Corporation published the adversarial tactics, techniques, and common knowledge or MITRE ATT&CK guideline. The guideline classified and described cyberattacks and intrusions. So, like the Cyber Kill Chain, it will help you to understand the attacker's methodology, but MITRE is more than that. It is a constantly evolving resource that provides a common language and approach for understanding and mitigating cyberattacks. The matrix is organized into a series of "techniques" that describe specific tactics and methods used by attackers to compromise systems and steal or manipulate information. These techniques are grouped into categories based on the type of attack or activity being performed, such as "Initial Access", "Execution", and "Defense Evasion".

One of the key benefits of the MITRE ATT&CK matrix is that it provides a common language and framework for discussing and analyzing cyber threats. This allows organizations to communicate and coordinate their efforts to prevent and respond to attacks more effectively. The matrix also helps organizations to identify and prioritize the most critical threats and vulnerabilities by mapping them to the appropriate techniques and categories.

The matrix is also a valuable resource for security professionals because it provides a comprehensive overview of the tactics, techniques, and procedures (TTPs) used by attackers. This allows security teams to better understand the methods and motivations of attackers, and to design and implement countermeasures to prevent or mitigate attacks more effectively.

You have completed the lesson. You are able to:

- Describe the Cyber Kill Chain.
- List and explain the stages of the Cyber Kill Chain.
- Explain the benefits of the MITRE ATT&CK matrix.

Social Engineering Module

Social Engineering Overview Lesson

Welcome to the introduction to the *Social Engineering* module.

Click **Next** to get started.

What is social engineering? Understood in the context of information security, it is the act of manipulating people to gain advantage, often at the expense of those targeted.

All social engineering attacks are designed to benefit the attacker. Most successful social engineering attacks are detrimental to their victims. Social engineering attacks can result in a loss of confidential data, blackmail or embezzlement, disruption or damage to a network, the denial of network services, the alignment of the target's opinion with the attacker's as a result of manipulation, or some combination of all of these outcomes.

There are many different methods—physical and digital—of social engineering attack. Some examples of those methods include, a bad actor convincing a target to allow them access to a restricted area, or an email sent to a target convincing them to click a provided link. In both examples, manipulation is the means used to get the desired action from the targeted individual. Social engineering works because people are vulnerable to manipulation. How do you protect yourself from such attacks?

By being educated about and more alert to social engineering techniques, you will be less likely to fall victim to this type of attack.

The lessons in the Social Engineering module provide an essential understanding of the fundamentals necessary to achieve your goals.

You will be able to:

Describe the different methods of social engineering.

You have already seen two examples, but there are many more methods and techniques used by bad actors to achieve their goals.

You will be able to:

Describe the attack vectors, methods, and threat indicators associated with insider threats.

Bad actors rely on your complacency to enact their plans, and the more secure you feel, the happier bad actors are. Feelings of security, however, are deceptive. You may feel the most secure around those with whom you work, and this may cause you to let down your guard. Still, you can be certain that bad actors will take advantage of this.

And you will be able to:

Describe fraud, scams, and influence campaigns.

Fraud and scams are generally short-term transactions intended to swindle people out of their money. In contrast, influence campaigns can be protracted and sophisticated operations that affect people's opinions, or even their morale. Although the purposes of fraud, scams, and influence campaigns can be different from phishing, baiting, or watering hole attacks, they all rely on psychological manipulation to forward the advantage of the instigator, and often at the expense of the human targets, which is social engineering.

Proceed to the first lesson to get started.

Social Engineering Techniques Part A Lesson

Welcome to the *Social Engineering Techniques, Part A* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Explain social engineering.
- Describe the different methods of social engineering.

What is social engineering? Social engineering is a term that you have been introduced to already but, given its importance, it is worth revisiting. According to one source, social engineering remains a leading cause of network breaches. Social engineering refers to a wide range of attacks that leverage human emotions to manipulate a target. The attack may incite the target to action or inaction. Ultimately, social engineering aims to steer the target in a direction prescribed by the orchestrator and often to the detriment of the target. Examples of social engineering goals include disclosing confidential information, transferring money, and influencing a person or persons to think in a certain way.

Two important characteristics of social engineering are:

- One, the aim is to achieve an outcome desirable to the orchestrator, and
- Two, the method is emotional manipulation.

To spot a social engineering attack, look for the following signs:

- An emotional plea that leverages fear, curiosity, excitement, anger, sadness, or guilt
- A sense of urgency around the request, and
- An attempt to establish trust with the recipient

Take caution when you receive a message that has any of these attributes. Don't allow a bad actor to pull your strings. The bad actor has devised a play and he intends you to play the tragic role. Don't do it!

Click the icon for more information.

Perhaps the most famous social engineering bad actor is Frank Abagnale. His criminal life was depicted in the movie Catch Me If You Can and in an autobiography by the same name. The book and movie reveal how Abagnale successfully impersonated a doctor, lawyer, and airplane pilot to gain people's trust and take advantage of them.

In 2011, an attacker compromised the network of a well-respected security company by sending phishing emails to groups of employees, using a method known as spear phishing. The emails had an Excel spreadsheet attached. The spreadsheet had malicious code embedded in it, which exploited a vulnerability in Adobe Flash to install a backdoor into the host computer. Unfortunately, at least one employee opened the attachment. It only takes one.

As you can see from these two examples, there are many methods or attack vectors that a bad actor can use to execute a social engineering attack. A social engineering bad actor can speak to the human target directly, like Frank Abagnale, or communicate through email, or through some other method. In this lesson, you will learn the different methods of a social engineering attack.

You are already familiar with the term phishing, and you likely have experience with phishing emails. Hopefully you were not a victim of one. The two important characteristics of phishing are that it exploits email as the attack vector and that it targets anyone with an email address. The attack is indiscriminate, insofar as who receives the

email. Phishing is simply malicious spam that is sent to as many people as possible with the hope that at least one will be taken in. However, phishing can also have a categorial meaning—it can be used to refer to all electronic social engineering attacks, such as spear phishing, whaling, smishing, and vishing.

There are many variants of phishing, some of which could be a part of a sophisticated campaign and may demand research and reconnaissance on the part of the attacker. Spear phishing and whaling fit into this category. Both spear phishing and whaling can be described as a social engineering attack that uses email to target a specific individual or group with the intent of stealing confidential information or profiting in some way. Like phishing, spear phishing and whaling use email as the attack vector, but with specific targets in mind.

Click the icons to review the different descriptions of phishing types.

What, then, is the difference between spear phishing and whaling? In a spear phishing attack, the bad actor targets an individual or category of individuals with lower profiles, such as the employees at that security company. In a whaling attack, the bad actor targets high-ranking individuals within an organization. When creating a whaling email, the attacker often does research on their target so that they can personalize the email in order to gain their target's trust.

The extra work very often pays off because executives and board members can be just as susceptible to an email attack as those who work for them. One of the most successful whaling attacks, and indeed one of the most successful social engineering attacks of all time, was conducted against a Belgian bank. The CEO of the bank didn't even know he had been compromised until after a routine internal audit disclosed that the attackers escaped with over 70 million euros. The attackers have never been caught or brought to justice.

Since the introduction of email as a ubiquitous means of communication, other methods have become popular, such as instant messaging, live chat, and SMS or text messaging. These methods can also act as threat vectors for a social engineering attack in the same way that email is used. A phishing-type attack that uses these media is known as smishing. Its name is derived from combining SMS with phishing.

Other social engineering attacks can take place over a telephone or mobile device. These types of attacks are named vishing. Its name is derived from combining voice and phishing. In March 2019, the CEO of a UK energy provider received a phone call from someone who sounded exactly like his boss. Fraudsters are known to use AI voice technology to impersonate other people. The call was so convincing that the CEO ended up transferring $243,000 to a "Hungarian supplier", which was a bank account belonging to the bad actor.

These types of attacks are identical to phishing, spear phishing or whaling, except that the attack vectors are different. They can also be equally profitable.

In 2020, a group of hackers took control of 130 accounts on a well-known social media platform, including those belonging to several celebrities. They downloaded users' data, accessed direct messaging, and made tweets requesting donations to a Bitcoin wallet. Within minutes, the bad actors had grossed $110,000 through 320 transactions. While the method used to take control of these accounts remains unknown, it is speculated that employees of the media platform were tricked into revealing account credentials, which allowed access to these accounts.

Social engineering bad actors use other tactics that are not restricted to any one attack vector. They could use email, messaging, voice, or even speak to the target face-to-face. One tactic is called *quid pro quo*, a Latin phrase that means "one thing for another". In the context of social engineering, a quid pro quo attack is when a bad actor offers a service, usually tech support, in exchange for access to information, such as user credentials.

Pretexting is another attack tactic. It involves a situation, or pretext, devised to invoke an emotional response from the target. Here is a real-life example. The target, a grandfather, receives a telephone call from someone who claims to be a police officer—the bad actor. The police officer tells the grandfather that his grandson has been arrested for possession of narcotics. The police officer also tells the grandfather that his grandson resisted arrest and that, during the ensuing fight, his grandson's nose was broken. The police officer then puts the grandson—

another bad actor—on the phone, who sobs and pleas for the grandfather to post bail. The grandson's voice doesn't sound quite right to the grandfather, but he reasons that his grandson is sobbing and has a broken nose, after all. Fortunately, the grandfather decides to hang up and phone the grandson's parents to verify if the story is true.

Another tactic used by bad actors is *baiting*. Baiting can take a number of forms and is similar to phishing. Baiting can occur in the form of an email, text, or telephone call claiming that you have won a prize or that you qualify for a rebate. Baiting relies on positive emotions, such as a reward, to entice you to act. A baiting attack can also be subtle. For example, a bad actor leaves a USB memory stick in a public place, such as the parking lot, lobby, or washroom of the targeted organization. An intriguing label, such as "managers' salaries and compensation" would be affixed to the drive. The bad actor is relying on you to be overcome with curiosity and to connect the USB drive to your computer. When you do, the malware on the USB drive installs a backdoor on your computer and the bad actor now has a gateway into the network.

Click the icons to review the social engineering attacks.

You have completed the lesson. You are now able to:

- Explain social engineering.
- Describe the different methods of social engineering.

Social Engineering Techniques Part B Lesson

Welcome to the *Social Engineering Techniques, Part B* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Explain social engineering.
- Describe the different methods of social engineering.

In the Social Engineering Techniques, Part A lesson, bad actors initiated actions against targets. In this lesson, the social engineering attacks are less intrusive, and some of them could even be described as clandestine. The social engineering methods described here all depend on you going to the bad actor, or at least this is how it is made to appear.

You are surfing the internet when a warning appears. The warning states that your computer is infected by malware and that to clean your computer, you should download the antivirus software using the provided link. If this has ever happened to you, then you've experienced a scareware attack. The antivirus software that is being offered, either for free or at a cost, is very likely fake or malware. A scareware attack is also known as a rogue attack.

In a watering hole attack, the attacker might compromise a site that is likely to be visited by a particular target group. Bad actors are known to exploit social media sites, such as Facebook and LinkedIn, to start and groom relationships with targets.

This also applies to the physical world, where a bad actor or agent would orchestrate a chance encounter at a place that the target is known to frequent. If the agent is talented, they can develop this initial contact into a relationship that they can exploit. In cinematography, a good example of an orchestrated encounter can be seen in the movie *Red Sparrow* where the female agent, played by Jennifer Lawrence, goes to swim at a public pool where she knows she could meet her target. Her attractiveness ensures that he will approach her, instead of her engaging him, which might cause suspicion.

Click the icons for more information.

This leads to another type of attack that has its origins—as least in terms of popular culture—in the world of espionage. This type of attack is known as a honeypot trap. The secret services of some nations recruit beautiful, educated women and groom them to act as professional temptresses. As per the previous example, the agent is the honeypot, and the public pool is the watering hole.

In cybersecurity, white hat analysts can apply the same concept to strengthen network defenses. A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities. Then, analysts can study the attacker's tactics and use what they learn to improve network security. Many network security companies sell honeypot systems. The name of the Fortinet honeypot product is FortiDeceptor.

The last social engineering attack method covered in this lesson is called tailgating. Tailgating involves a bad actor following someone with security clearance into a secure building or an access-controlled room. The bad actor, or tailgater, relies on the courtesy or sympathy of the target to gain access. For example, the target might hold a door open for someone who is following behind them, not knowing that person has malicious intent. Or perhaps the bad actor approaches their target pretending to be burdened with parcels and needing help to open the door. Or perhaps the attacker claims that they forgot their security pass.

While it is professional and correct to be courteous, if you don't recognize the person or know their security status, then ensure that you involve reception or security to help the individual. To be clear, if a tailgater slips through the door without you noticing, then this does not qualify as social engineering. There must be psychological manipulation between the attacker and the target for an attack to be considered social engineering. An attack can be physical, such as tailgating; active, such as whaling and pretexting; or subtle, such as baiting.

Click the icons for more information.

In real life, bad actors often rely on several methods and attack vectors to achieve their ends. As the attack campaign progresses, and new targets of opportunity arise, the tactics and methods used by bad actors might evolve and change. Think of social engineering techniques and various malware types, such as ransomware, Trojan horse, backdoor, worm, bot, and zero-day attacks, as tools in a toolbox, which an attacker can use as the situation requires. Just like a carpenter needs more than a hammer to do their job, a cyberattacker requires different tools and techniques to do theirs.

The following story is a real-life example of a successful social engineering attack carried out by a blue hat penetration testing team. The penetration team analyst, who reported the results at the RSA Europe security conference in 2012, did not disclose the name of the organization, but did reveal that the organization specializes in cybersecurity.

The team began preparing for the attack by building a credible online identity on LinkedIn for an attractive fictitious woman named Emily Williams. The team also set up information about her on other websites so people would be able to match the information on her social media profiles with the information obtained through Google searches. This meant that fabricated profiles set up on Facebook and other social media sites were used to corroborate the information found on LinkedIn. They even posted on some university forums using her name. According to her fake social media profiles, she was a 28-year-old MIT graduate with ten years' experience who claimed to have just been hired by the targeted organization.

Within the first 15 hours, Emily Williams had 60 Facebook friends and 55 LinkedIn connections with employees from the targeted organization and its contractors. After 24 hours, she had three job offers from other companies. Soon, she received LinkedIn endorsements for skills, and men working for the targeted organization offered to help her get started faster in her alleged new job. The team, acting as Emily, was able to manipulate the men into providing her with a work laptop and network access while skirting proper channels and normal procedures. In fact, she was granted more network privileges than she normally would have received as a new hire.

The penetration team decided not to use the laptop and network access, but rather to continue their social engineering assault on the organization. Around the Christmas holidays, the team created a site with a Christmas card and posted a link to it on Emily's social media profiles. People who visited the site were prompted to execute a signed Java applet that opened a reverse shell back to the attack team, by way of an SSL connection. Once they had a shell, the team used privilege escalation exploits to gain administrative rights and was able to sniff passwords, install other applications, and steal documents containing sensitive information.

Even though it was not part of the plan, contractors for the targeted organization also were deceived by the Christmas card attack, including employees from antivirus companies. At least one of the victims was a developer with access to source code. It might have been possible to compromise the source code that was being written for the targeted organization, which would have made detecting an attack on the organization even more difficult.

Click on the identified icons for more information.

Through Facebook, the penetration team learned from two employees that the head of information security at their organization was about to celebrate his birthday. While that individual did not have any social media exposure, the penetration team sent him an email with a birthday card that appeared to come from one of the two employees who had been talking about the event on Facebook. After he clicked the link in the malicious birthday card, his

computer became infected with malware, and because of his elevated privileges within the organization, much of the network and sensitive information became compromised too.

However, the team did not focus solely on high-profile individuals. The Emily Williams attack started by targeting low-level employees, like sales and accounting staff. By connecting to or befriending these employees first, the team gained credibility and increased trust, thereby making inroads with the higher-ranking individuals easier. As the social network around Emily Williams grew, the attack team was able to target more technical people, security people, and even executives.

In short, the penetration testing team's success confirmed that even technically sophisticated organizations can fall victim to social engineering attacks.

You have completed this lesson. You are now able to:

- Explain social engineering.
- Describe the different methods of social engineering.

Insider Threat Lesson

Welcome to the *Insider Threat* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define insider threat.
- Explain the different types of insiders.
- Describe the different threat vectors and methods used by or against insiders.
- Describe the threat indicators of insider threats and mitigation methods.

When addressing cybersecurity, organizations tend to focus on external threats. However, given that a significant number of security breaches are due to insiders, cybersecurity teams should address insider threats through initiatives such as employee awareness training. But what is an insider threat?

An insider threat is an individual or individuals who work for an organization or have authorized access to its networks or systems and who pose a physical threat or cyberthreat to the organization. The insider is typically a current employee, but it could also be a former employee, contractor, business partner, board member, or even an imposter who gains access to sensitive information or network privileges.

Click the icon for more information.

There are different ways to categorize insider threats and assign them names, but essentially there are two main groups: those who unintentionally assist bad actors because of human error, poor judgement, or carelessness and those on the inside who act maliciously. The first group could be named negligent, and the second group malicious. These two categories can be further subdivided.

The principal goals of malicious insider threats, sometimes called turncloaks, include espionage, fraud, intellectual property theft, and sabotage. Here is an example: In 2020, a former executive of company A stole trade secrets from its self-driving-car division and handed them to his new employer. He was sentenced to 18 months in prison.

Malicious insider threats can be divided into three types: moles, collaborators, and lone wolves. Lone wolves may seem as harmless as sheep, but they harbor malicious intent. And as the name implies, lone wolves work independently and without outside influence. Collaborators are authorized users who work with a third party. The third party may be a competitor, nation-state, organized criminal network, or an individual. A third type of malicious insider is an outsider who has gained access to the organization's network. They may gain access to the organization by posing as a vendor, partner, contractor, or employee. This type of malicious insider is known as a mole. The Emily Williams attack, discussed in the Social Engineering Techniques, Part B lesson, is an example where a mole was used. In the attack, Emily Williams gained access to the targeted organization's network by posing as an employee.

Click the icon for more information.

The more benign, yet equally dangerous category, is the careless insider who inadvertently helps a bad actor. They fall victim to phishing and other social engineering attacks. The careless insider category can be subdivided into two groups: pawns and goofs. A pawn is an authorized user who has been manipulated into unintentionally helping the bad actor, often through social engineering techniques, like tailgating or spear phishing. An example of a pawn is the head of information security who was duped by a digital birthday card in the Emily Williams attack. A goof is an insider who deliberately takes potentially harmful actions but harbors no malicious intent. This type of

insider could be described as arrogant, ignorant, or incompetent, and one who refuses to recognize the need to follow security policies and procedures.

Malicious agents use many methods and attack vectors against the careless insider. The attack vector can be physical. Methods used against a physical attack vector include *tailgating* or piggybacking, *shoulder surfing*, *dumpster diving*, and *eavesdropping*. Tailgating, or piggybacking, is a type of engineering attack in which an unauthorized person gains physical access to a restricted area by following someone who is authorized. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Dumpster diving is looking for information in someone else's garbage or recycle bin. Dumpster diving can also occur in a general access area, such as a printing room where confidential information is printed and not immediately retrieved. Eavesdropping in a physical setting could be listening in on a conversation where confidential information is discussed. Digitally speaking, eavesdropping refers to network snooping or sniffing, which occurs when a malicious actor exploits an insecure or vulnerable network to read or steal information as it travels between two devices. Eavesdropping occurs more commonly in wireless communications than on Ethernet networks because wireless networks are more accessible.

Within digital attack vectors, a plethora of methods, including spear phishing attacks and whaling attacks, are used to hoodwink careless insiders. In other attack vectors, such as messaging or telephoning, insiders can be victims of smishing, vishing, or pretexting. In the social media attack vector, watering hole attacks can be used. These are terms that you should already be familiar with from previous lessons.

Click the icons to review their definitions.

An insider attack can be more difficult to detect than an external attack. In part, this is because an insider has access to and knowledge about the network that an external attacker likely does not. However, there are behavioral and digital indicators that can help you to detect a possible insider threat.

If an insider appears to be dissatisfied with the organization, appears to hold a grudge against the organization, or starts to take on more tasks with excessive enthusiasm, these could be indicators of a potential insider threat. Context is everything. There are go-getter or type A personalities who aggressively take on new challenges. However, if an employee's behavior changes appreciably without some logical explanation, then this may be a threat indicator. Routine violations, open contempt of organization policies, or attempts to circumvent security are also possible behavioral indicators of an insider threat.

Anomalous activity at the network level is a digital indicator. Several activities are trackable, such as:

- Activity at unusual times, such as logging into the network at 4 AM, or always working late.
- Volume of traffic, such as transferring unusual amounts of data within the network.
- Type of activity, such as accessing resources that are atypical or not needed for the insider's job.

You should also be alerted to digital activities, such as:

- Repeated requests for access to systems not relevant to their job function.
- Using unauthorized devices, such as USB drives.
- Network crawling and deliberate searches for sensitive information.
- Emailing sensitive information outside the organization.

Your behavior as a person working for an organization can either jeopardize or enhance security. To help make your organization more secure, follow this list of recommendations:

- Learn your organization's security policies.
- Do not take shortcuts around security protocols.
- Do not leave login credentials exposed.
- Do not allow tailgating.

- Do not store confidential digital documents unencrypted or leave physical documents unsecured.
- Do not disable endpoint security and controls. Do not share proprietary or confidential information with unauthorized individuals.
- Patch your devices as soon as OS and software updates are available.

There are measures that you can take to protect your organization's assets from internal threats. First, identify your organization's critical assets, both logical and physical. These include networks, systems, confidential data, facilities, and people. Rank and prioritize each asset and identify the current state of each asset's protection. By prioritizing the assets, you can focus on securing the most important assets first.

Tools like machine learning (ML) applications can help analyze the data stream and prioritize the most relevant alerts. You can use digital forensics and analytics tools, such as user and event behavior analytics (UEBA) to help detect, analyze, and alert the security team to any potential insider threats. User and device behavior analytics can establish a baseline for normal data access activity, while database activity monitoring can help identify policy violations.

Deploy tools that monitor user activity as well as aggregate and correlate activity information from multiple sources. Deception software, such as FortiDeceptor by Fortinet, establishes traps to attract malicious insiders and tracks their actions to better understand their intentions. The information gathered by a honeypot solution can be shared with other intelligence to improve detection and to mitigate attacks and breaches.

Define, document, and disseminate the organization's security policies. Then, provide training to those who work for your organization, and follow up with testing to ensure comprehension. This prevents ambiguity and establishes a foundation for enforcement. They should recognize their responsibility to comply and respect the organization's security policies.

This is a good segue to the final recommendation: Promote a culture of security awareness. Promoting a security-aware culture is key to mitigating the insider threat. Instilling the right beliefs and attitudes combats negligence and reduces the opportunity for malicious behavior.

You have completed the lesson. You are now able to:

- Define insider threat.
- Explain the different types of insiders.
- Describe the different threat vectors and methods used by or against insiders.
- Describe the threat indicators of insider threats and mitigation methods.

Fraud, Scams, and Influence Campaigns Lesson

Welcome to the *Fraud, Scams, and Influence Campaigns* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe fraud, scams, and influence campaigns.
- List examples of cyber fraud and cyber scams.
- Describe how a typical online influence campaign unfolds.

Increasingly, the internet has become a platform for bad actors to stage large-scale fraud, scams, or malevolent influence to sway people to a particular point of view. The methods used to achieve the sordid goals of fraud and scams often involve social engineering techniques, such as phishing, coupled with malware. In this lesson, you will also learn about influence campaigns, which is a social media technique to spread ideas and manipulate others.

What is cyber fraud? Cyber fraud is a social engineering technique, malware, or other type of deception that is used to defraud or take advantage of a person or organization for financial or personal gain.

What are cyber scams? Cyber scams are a type of fraud, but they are generally classified as petty or not as serious as cyber fraud. This is not to suggest that cyber scams are trivial, however. According to the FBI, elderly Americans lose more than three billion dollars annually to various types of scams. Senior citizens are often targeted because they are more trusting than younger adults and they have a lifetime of savings to prey upon.

Fraud and scams are criminal activities that use the same threat vectors and methods you have seen in previous lessons.

Examples of cyber fraud and cyber scams include the following:

- Copycat government websites—Bad actors use phishing, spear phishing, or other variant to provide a link to a fake government site, usually with the intention of stealing the user's credentials or credit card information.
- Dating and romance scams—Bad actors leverage legitimate dating websites, social networks, and chat rooms to get personal details or money from people.
- Holiday fraud—Bad actors offer customers online holidays and accommodations that are not available or do not exist.
- Mandate fraud—This type of fraud occurs when a bad actor hacks an email transaction, such as one between a customer and a vendor. The bad actor then, sends a duplicate invoice with the bad actor's bank account information, and requests payment.
- Pharming—Bad actors redirect traffic from a legitimate website to a fake one, such as an e-commerce or banking site.
- Greeting card scams—This type of fraud involves sending a malicious greeting card to a person on their birthday, or during an important holiday, such as Christmas or Easter.

What are online influence campaigns? Influence campaigns are large-scale efforts to shift public opinion. Such campaigns are generally executed in bad faith and seek to promote a false narrative. These campaigns are often carried out by groups with high levels of capability, up to and including nation-state actors.

This is how an influence campaign might unfold: (1) The bad actor creates fake user accounts on social media platforms. (2) The bad actor creates content to promote a given narrative. (3) They post this content as fake users

on numerous social media sites. (4) Real people see the content and begin to share it. (5) After reaching a certain threshold, mass media picks up the story, further amplifying the narrative.

This is the strength of influence campaigns. With little cost and effort, the bad actor can manipulate the opinions of hundreds of thousands of people. The nature of social media allows the bad actor to operate secretly and without fear of being identified as the source of the attack.

Publicly attacking an adversary is likely to result in undesirable consequences, but secretly turning public opinion against them is harder to prove and harder to retaliate against. Consider this scenario. Two restaurant owners are bitter rivals. Restaurant owner A uses anonymous social media accounts to spread disinformation about restaurant owner B. Restaurant owner A claims that restaurant owner B refused to hire an individual based on that individual's race. Others jump onto social media, demand retribution, and boycott the restaurant. If restaurant owner B accuses their rival of circulating lies, this could easily backfire and further provoke the virtue-signaling mob. Regardless of what restaurant owner B does—remains silent, denies the accusation, or accuses their rival of foul play—it's a losing proposition. On the other hand, if someone openly makes a false claim or accusation, then the victim can take legal recourse, putting the reputation of the accuser at stake.

Influence campaigns can also be a part of hybrid warfare, as conducted by "psyops", a division of the military. In this scenario, traditional warfare tactics are combined with political strategy and cyber warfare, which can include hacking, social engineering, influence campaigns, and promoting fake news. In hybrid warfare, the objective of influence campaigns is to weaken the enemy's resolve by sowing confusion and division.

You have completed the lesson. You are now able to:

- Describe fraud, scams, and influence campaigns.
- List examples of cyber fraud and cyber scams.
- Describe how a typical online influence campaign unfolds.

Malware Module

Malware Overview Lesson

Welcome to the *Malware* module.

Click **Next** to get started.

What is malware? The term malware is short for malicious software that disrupts, damages, or gains unauthorized access to a computer. Bad actors design malware to perform various tasks, such as modifying the behavior of a program, spying on people using the infected computer, exfiltrating data, encrypting important information and then demanding a ransom, or denying users access to a system. The purpose of each type of malware depends on the objectives of bad actors. And, an attack campaign may use multiple types of malware that are designed to complete specific tasks at each stage of the attack. Understanding the different types of malware, their characteristics, and their uses, will help you to prepare for cyberattacks against your computer and network. The lessons in this module provide an essential understanding of the following fundamentals necessary to achieve your goals.

Categorize and describe the different types of malware in the threat landscape, such as viruses, worms, and ransomware.

One important feature of a virus is that it is not self-activated; in other words, it requires a user to invoke it. In contrast, a worm self-activates and does not need a user to invoke it on the targeted computer. Ransomware denies users access to information, usually by encrypting it. In contrast, spyware reports user behavior to an external party. Each malware type has different traits and purposes.

You will also be able to:

Describe what an attack vector is, and how it is composed of three essential parts: a mechanism, a pathway, and a vulnerability.

You will also be able to:

Explain how different types of malware and mechanisms exploit computers.

Wherever there's a pathway to a vulnerability, you can be certain that a bad actor will develop a mechanism to exploit it. Bad actors attempt to manipulate users using various social engineering methods, or exploit weaknesses or misconfigurations on devices.

Becoming knowledgeable about how attacks are staged and how malware works will help you to defend yourself from becoming a victim of a cyberattack.

Proceed to the first lesson to get started.

Malware Types Lesson

Welcome to the *Malware Types* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define malware.
- Describe the traits of a computer virus.
- Describe the different types of computer viruses and malware.

Has your computer ever behaved oddly? Perhaps its performance has suddenly and inexplicably slowed, or unwanted pop-up windows appear, or applications crash or start by themselves. You may think that there is a ghost in the machine, but it's more likely that malware has infected your computer.

If malware infects your computer, its behavior may change abruptly and without any obvious reason. Some common symptoms of computer infection are:

- Computing devices suddenly become sluggish or unresponsive.
- Unwanted pop-up windows appear in an application or web browser. These are telltale signs that malware, virus, or spyware is affecting your device.
- Applications unexpectedly close by themselves. This likely means that the software has been infected with some form of virus or malware.
- Applications fail to load when selected from the Start menu or desktop icon. Computer malware causes computers to act in a variety of strange ways, which may include opening files by themselves, displaying unusual error messages, or entering characters randomly.
- Applications crash or log the user out.
- System crashes and the computer itself inexplicably shutting down.
- Emails in your outlook that you didn't send. Hackers use other people's email accounts to spread malware and carry out wider cyberattacks. Emails in your outbox that you didn't send can be a sign of an infection.
- Unexplained changes to a computer, such as your system's homepage being modified or your browser settings being updated, are signs of the presence of malware.

Now that you know the symptoms of computer infection, the next step is to learn to describe and categorize the different types of malware.

While malware is malicious software that disrupts, damages, or gains unauthorized access to a computer system, a computer virus is malware with additional traits. Norton.com defines a computer virus as "…a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data."

Computer viruses have several defining traits that you should be aware of. First, computer viruses must be invoked by a user, second, they insert themselves in or attach themselves to legitimate applications, and third, they are designed to spread the infection to other applications and computers on the network.

Knowing these will help you to distinguish between malware that is a virus and malware that is not.

Many types of viruses possess these traits yet do very different things. The following is a list of some common virus types:

A resident virus propagates itself by infecting applications as they are opened by a user.

A non-resident virus infects executable files when applications are not running.

A multipartite virus uses multiple methods to infect and spread across computers. It typically remains in the computer's memory to infect the hard disk, then spreads and infects more drives by altering the content of applications.

A direct action virus accesses a computer's main memory and infects all applications, files, and folders located in the autoexec.bat path or the autostart registry path, before deleting itself. This virus typically alters the performance of a system and can destroy all data on the computer's hard disk and any USB device attached to it.

A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files, but it can be hugely damaging to computer users, who often will not be able to restore their homepage or search engine. It can also contain adware that causes unwanted pop-up windows and ads.

Overwrite viruses are extremely dangerous. They can delete and replace data with their own file content or code. Once files are infected, they cannot be replaced, and the virus can affect Windows, DOS, Linux, and macOS systems. The only way this virus can be removed is by deleting all the files it infected.

A web scripting virus attacks web browser security, enabling a hacker to inject malicious code into web pages, or client-side scripting. Client-side scripting simply means running scripts, such as JavaScript, on the client device, usually within a browser. This allows cybercriminals to attack major websites, such as social networking sites, email providers, and any site that enables user input or reviews. Attackers can use the virus to send spam, commit fraudulent activity, and damage server files.

A file infector is one of the most common computer viruses. It overwrites files when they are opened and can quickly spread across systems and networks. It largely affects files with .exe or .com extensions.

Network viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover because the virus can hide on any computer on an infected network. These viruses can easily replicate and spread by using the internet, and transfer to devices connected to the network.

A boot sector virus targets a computer's master boot record (MBR). The virus injects its code into a hard disk's partition table, then moves into the main memory when a computer restarts.

Aside from viruses, there are other types of malware that do not share all the traits of a virus. For example, worm malware does not need a host system and can spread between systems and networks without user action, whereas a virus requires a user to execute its code. Here are some other types of malware that are not viruses:

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed. A rootkit often masks its existence or the existence of other software. It operates near or within the kernel of the operating system, but it cannot self-replicate or spread across systems. A DLL injection attack allows the attacker to execute malicious code by replacing legitimate DLL files with malicious ones. This type of attack is difficult to detect and prevent because it often involves the use of legitimate files and processes. Similarly, a driver manipulation attack changes or replaces driver software that allows the operating system to communicate with hardware devices.

A keylogger is a computer program that records every keystroke made by a computer user, with the purpose of gaining fraudulent access to passwords and other confidential information. Keyloggers are a type of spyware, which is malware designed to spy on victims. Because they can capture everything you type, keyloggers are one of the most invasive forms of malware.

A potentially unwanted program (PUP) is a program that may be unwanted, despite the possibility that a user consented to download it. PUPs include spyware, adware, and dialers, and are often downloaded in conjunction with a program that the user wants.

Spyware is malware that obtains covert information about a user's computer activities by transmitting data secretly from the hard drive. Spyware is a type of malware that collects personal information and gathers data about a user without consent.

Adware is a form of malware that hides on a device and displays ads. Some adware also monitors a user's online behavior so it can target them with specific ads.

A dialer is a malicious program that is installed on a computer and tries to use the dialing features, often running up expensive phone bills for the victim. A dialer is unlike other types of spyware, though it is sometimes included with free software downloads.

Adversarial machine learning is a technique used in machine learning to fool or misguide a neural network with malicious input. Adversarial artificial intelligence uses specialized inputs created for the purpose of confusing a neural network, resulting in the misclassification of an input. These notorious inputs can be indistinguishable to the human eye but cause the network to fail to correctly identify an image.

Ransomware is a type of virus that encrypts or prevents access to the information on a computer and restores access only after the user pays a ransom.

A Trojan horse virus is a virus disguised to look like something it is not. For example, viruses can be hidden within unofficial games, applications, file-sharing sites, and bootlegged movies. A remote access Trojan (RAT) virus is Trojan malware that can remotely control an infected computer.

A dropper is a type of Trojan horse that is designed to install malware on a computer. Once the dropper is installed, two things can happen: The dropper installs the embedded malware, or the dropper downloads the malware to the targeted computer.

Rogue security software, also known as rogueware or scareware, misleads a user into believing that there is malware on their computer and then prompts them to pay for antimalware, which is either fake or malware.

Botnet malware controls its infected host through a command and control (C&C) server. An infected computer is named a bot, or robot, and a collection of infected computers is known as a botnet.

Cryptojacking is the illegal use of computing resources to mine cryptocurrency. Attackers use malware or scripting to hijack a computer. For example, Coinhive was a cryptocurrency mining service that allowed website owners to embed JavaScript code on their websites, which hijacked the resources of connected computers for cryptomining purposes. This type of exploit is called in-browser mining.

You have completed this lesson. You are now able to:

- Define malware.
- Describe the traits of a computer virus.
- Describe the different types of computer viruses and malware.

Malware Attack Vectors and Methods Lesson

Welcome to the *Malware Attack Vectors and Methods* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Distinguish the difference between an attack vector and an attack surface.
- Describe the three components of an attack vector.
- Describe examples of attack vector malware and its mechanisms.

What is an attack vector? An attack vector, also known as a threat vector, is a method that a bad actor uses to illegally access or inhibit a network, system, or facility. An attack vector can refer either to a specific method of attack, or to a category of attack. For example, social engineering is a category of attack vector, and it consists of many attack types. As you saw in a previous lesson, bad actors can tailgate to access restricted areas, or spear phish a user to exploit their network privileges. Remember that an attack vector has three components: a vulnerability, a mechanism, and a pathway. The pathway enables a mechanism to access the target.

Learning the difference between an attack vector and an attack surface is also important. While an attack vector is the method used to attack a target, an attack surface represents the total number of entry points that the vector creates to gain unauthorized access to the target. In addition, the attack surface can expand or contract due to circumstances. In this graphic, the targeted person is the attack surface and is exposed to various assassination methods. The entire individual is the attack surface. The person could reduce their vulnerability, or attack surface, by wearing a helmet and Kevlar vest. In another example, a password policy requirement is a factor in the attack surface. More stringent password requirements cause the attack surface to contract, and lenient requirements cause the attack surface to expand. One of the objectives of IT security is to reduce the attack surface of the network.

Although attack vectors can be physical or electronic, this lesson focuses on only attack vectors involving malware. Social engineering attacks infect computers with different types of malware, as seen in the previous lesson. The following are two examples of malware attack vectors:

Watering holes are pathways that bridge mechanisms to vulnerabilities. For example, a bad actor compromises a digital meeting place. Users are more vulnerable to manipulation in a familiar environment such as a social media site, so they are more likely to click on links or download an amusing cat video that serves as a Trojan horse for malware.

Malware takes control of a computer, making it into a robot, or bot for short. Another term for bot is zombie. The bad actor controls the computer using a command-and-control (C&C) server, which sends commands to systems compromised by bot malware, and then receives stolen data. A collection of computers controlled by a C&C server is called a botnet. Botnets can have many purposes, for example, to harvest information from infected machines, to send spam and phishing emails, or to attack web services. An attack by a botnet against a server with the intent of making it inaccessible is known as a distributed denial-of-service (DDoS) attack. In this case, the mechanism of the attack vector is the botnet, the pathway is the internet, and the vulnerability is the targeted server.

When a bad actor finds a pathway to a vulnerability, they can install malware or deploy a malicious mechanism. Here are some examples of clandestine mechanisms and exploitation methods used by bad actors:

A backdoor is an unauthorized way of gaining access to a computer.

A logic bomb is a piece of malicious code left lying in wait on a computer that will execute under specific conditions.

An Easter egg is a hidden feature or a piece of code left behind by developers. In some cases, an Easter egg can leave your network and data exposed to bad actors.

Droppers are programs designed to extract other files from their own code. Typically, droppers extract several files onto a computer to install a malicious program package. Droppers can also have other functions.

A downloader is a type of Trojan horse that installs itself on a computer, and waits until an internet connection becomes available to connect to a remote server or website. It then downloads additional programs (usually malware) onto the infected computer.

Shellcode is a set of instructions in software that execute a command to take control of or exploit, a compromised computer.

Code injection is the term used to describe attacks that inject code into an application. The injected code is interpreted by the application, changing the way a program executes. Code injection attacks typically exploit an application vulnerability that allows the processing of invalid data.

You have completed this lesson. You are now able to:

- Distinguish the difference between an attack vector and an attack surface.
- Describe the three components of an attack vector.
- Describe examples of attack vector malware and its mechanisms.