Threat Actors

Objectives:

- 1.2 - Summarize fundamental security concepts
- 2.1 - Compare and contrast common threat actors and motivations
- 2.2 - Explain common threat vectors and attack surfaces

- **Threat Actors**
    - Threat Actor Motivations
        - Data Exfiltration
        - Blackmail
        - Espionage
        - Service Disruption
        - Financial Gain,
        - Philosophical/Political Beliefs
        - Ethical Reasons
        - Revenge
        - Disruption/Chaos
        - War
    - Threat Actor Attributes
        - Internal vs. External Threat Actors
        - Differences in resources and funding
        - Level of sophistication
    - Types of Threat Actors
        - *Unskilled Attackers*
            - Limited technical expertise, use readily available tools

  - *Hacktivists*
    - Driven by political, social, or environmental ideologies
  - *Organized Crime*
    - Execute cyberattacks for financial gain (e.g., ransomware, identity theft)
  - *Nation-state Actor*
    - Highly skilled attackers sponsored by governments for cyber espionage or warfare
  - *Insider Threats*
    - Security threats originating from within the organization
- *Shadow IT*
  - IT systems, devices, software, or services managed without explicit organizational approval
- Threat Vectors and Attack Surfaces
  - Message-based
  - Image-based
  - File-based
  - Voice Calls
  - Removable Devices
  - Unsecured Networks
- Deception and Disruption Technologies
  - *Honeypots*
    - Decoy systems to attract and deceive attackers
  - *Honeynets*
    - Network of decoy systems for observing complex attacks
  - *Honeyfiles*
    - Decoy files to detect unauthorized access or data breaches

        - *Honeytokens*
            - Fake data to alert administrators when accessed or used

- **Threat Actor Motivations**
    - There is a difference between the intent of the attack and the motivation that fuels that attack
        - *Threat Actors Intent*
            - Specific objective or goal that a threat actor is aiming to achieve through their attack
        - *Threat Actors Motivation*
            - Underlying reasons or driving forces that pushes a threat actor to carry out their attack
    - Different motivations behind threat actors
        - *Data Exfiltration*
            - Unauthorized transfer of data from a computer
        - Financial Gain
            - Achieved through various means, such as ransomware attacks, or through banking trojans that allow them to steal financial information in order to gain unauthorized access into the victims' bank accounts
        - Blackmail
            - Attacker obtains sensitive or compromising information about an individual or an organization and threatens to release this information to the public unless certain demands are met
        - Service Disruption
            - Some threat actors aim to disrupt the services of various organizations, either to cause chaos, make a political statement, or to demand a ransom

        - Philosophical or Political Beliefs
            - Attacks that are conducted due to the philosophical or political beliefs of the attackers is known as hacktivism
            - Common motivation for a specific type of threat actor known as a hacktivist
        - Ethical Reasons
            - Contrary to malicious threat actors, ethical hackers, also known as Authorized hackers, are motivated by a desire to improve security
        - Revenge
            - It can also be a motivation for a threat actor that wants to target an entity that they believe has wronged them in some way
        - Disruption or Chaos
            - Creating and spreading malware to launching sophisticated cyberattacks against the critical infrastructure in a populated city
        - *Espionage*
            - Spying on individuals, organizations, or nations to gather sensitive or classified information
        - War
            - Cyber warfare can be used to disrupt a country's infrastructure, compromise its national security, and to cause economic damage

- **Threat Actor Attributes**
    - 2 Most Basic Attributes of a Threat Actor
        - *Internal Threat Actors*
            - Individuals or entities within an organization who pose a threat to its security

    - *External Threat Actors*
      - Individuals or groups outside an organization who attempt to breach its cybersecurity defenses
  - Resources and funding available to the specific threat actor
    - Tools, skills, and personnel at the disposal of a given threat actor
  - Level of sophistication and capability of the specific threat actor
    - Refers to their technical skill, the complexity of the tools and techniques they use, and their ability to evade detection and countermeasures
    - In the world of cybersecurity, we usually classify the lowest skilled threat actors as "script kiddies"
      - *Script Kiddie*
        - Individual with limited technical knowledge
        - use pre-made software or scripts to exploit computer systems and networks
    - Nation-state actors, Advanced Persistent Threats and others have high levels of sophistication and capabilities and possess advanced technical skills
      - Use sophisticated tools and techniques

- **Unskilled Attackers**
  - *Unskilled Attacker (Script Kiddie)*
    - Individual who lacks the technical knowledge to develop their own hacking tools or exploits
    - These low-skilled threat actors need to rely on scripts and programs that have been developed by others
  - How do these unskilled attackers cause damage?
    - One way is to launch a DDoS attack

        - An unskilled attacker can simply enter in the IP address of the system they want to target, and then click a button to launch an attacker against that target

- **Hacktivists**
    - *Hacktivists*
        - Individuals or groups that use their technical skills to promote a cause or drive social change instead of for personal gain
    - *Hacktivism*
        - Activities in which the use of hacking and other cyber techniques is used to promote or advance a political or social cause
    - To accomplish their objectives, hacktivists use a wide range of techniques to achieve their goals
        - Website Defacement
            - Form of electronic graffiti and is usually treated as an act of vandalism
        - Distributed Denial of Service (DDoS) Attacks
            - Attempting to overwhelm the victim's systems or networks so that they cannot be accessed by the organization's legitimate users
        - *Doxing*
            - Involves the public release of private information about an individual or organization

        - Leaking of Sensitive Data
            - Releasing sensitive data to the public at large over the internet
    - Hacktivists are primarily motivated by their ideological beliefs rather than trying to achieve financial gains

- Most well-known hacktivist groups is known as “Anonymous”
  - Anonymous
    - Loosely affiliated collective that has been involved in numerous high-profile attacks over the years for targeting organizations that they perceive as acting unethically or against the public interest at large

- **Organized Crime**
  - Organized cybercrime groups are groups or syndicates that have banded together to conduct criminal activities in the digital world
    - Sophisticated and well structured
    - Use resources and technical skills for illicit gain
  - In terms of their technical capabilities, organized crime groups possess a very high level of technical capability and they often employ advanced hacking techniques and tools
    - Custom Malware
    - Ransomware
    - Sophisticated Phishing Campaigns
  - These criminal groups will engage in a variety of illicit activities to generate revenue for their members
    - Data Breaches
    - Identity Theft
    - Online Fraud
    - Ransomware Attacks
  - Unlike hacktivists or nation state actors, organized cybercrime groups are not typically driven by ideological or political objectives
    - These groups may be hired by other entities, including governments, to conduct cyber operations and attacks on their behalf

        - Money, not other motivations is the objective of their attacks even if the attack takes place in the political sphere

- **Nation-state Actor**
    - *Nation-state Actor*
        - Groups or individuals that are sponsored by a government to conduct cyber operations against other nations, organizations, or individuals
    - Sometimes, these threat actors attempt what is known as a false flag attack
        - *False Flag Attack*
            - Attack that is orchestrated in such a way that it appears to originate from a different source or group than the actual perpetrators, with the intent to mislead investigators and attribute the attack to someone else
    - Nation-state actors possess advanced technical skills and extensive resources, and they are capable of conducting complex, coordinated cyber operations that employ a variety of techniques such as
        - Creating custom malware
        - Using zero-day exploits
        - Becoming an advanced persistent threats
    - *Advanced Persistent Threat (APT)*
        - Term that used to be used synonymously with a nation-state actor because of their long-term persistence and stealth
        - A prolonged and targeted cyberattack in which an intruder gains unauthorized access to a network and remains undetected for an extended period while trying to steal data or monitor network activities rather than cause immediate damage
        - These advanced persistent threats are often sponsored by a nation-state or its proxies, like organized cybercrime groups

- What motivates a nation-state actor?
  - Nation-state actors are motivated to achieve their long-term strategic goals, and they are not seeking financial gain

- **Insider Threats**
  - *Insider Threats*
    - Cybersecurity threats that originate from within the organization
    - Will have varying levels of capabilities
  - Insider threats can take various forms
    - Data Theft
    - Sabotage
    - Misuse of access privileges
  - Each insider threat is driven by different motivations
    - Some are driven by financial gain and they want to profit from the sale of sensitive organizational data to others
    - Some may be motivated by revenge and are aiming to harm the organization due to some kind of perceived wrong levied against the insider
    - Some may take actions as a result of carelessness or a lack of awareness of cybersecurity best practices
  - <u>Remember</u>
    - Insider threat refers to the potential risk posed by individuals within an organization who have access to sensitive information and systems, and who may misuse this access for malicious or unintended purposes
    - To mitigate the risk of an insider threat being successful, organizations should implement the following
      - Zero-trust architecture

            - Employ robust access controls
            - Conduct regular audits
            - Provide effective employee security awareness programs

- **Shadow IT**
    - *Shadow IT*
        - Use of information technology systems, devices, software, applications, and services without explicit organizational approval
        - IT-related projects that are managed outside of, and without the knowledge of, the IT department
    - Why does Shadow IT exist?
        - An organization's security posture is actually set too high or is too complex for business operations to occur without be negatively affected
    - *Bring Your Own Devices (BYOD)*
        - Involves the use of personal devices for work purposes

- **Threat Vectors and Attack Surfaces**
    - *Threat Vector*
        - Means or pathway by which an attacker can gain unauthorized access to a computer or network to deliver a malicious payload or carry out an unwanted action
    - *Attack Surface*
        - Encompasses all the various points where an unauthorized user can try to enter data to or extract data from an environment
        - Can be minimized by
            - Restricting Access

        - Removing unnecessary software
        - Disabling unused protocols
- Think of threat vector as the "how" of an attack, whereas the attack surface is the "where" of the attack
- Several different threat vectors that could be used to attack your enterprise networks
    - Messages
        - Message-based threat vectors include threats delivered via email, simple message service (SMS text messaging), or other forms of instant messaging
        - Phishing campaigns are commonly used as part of a message-based threat vector when an attacker impersonates a trusted entity to trick its victims into revealing their sensitive information to the attacker
    - Images
        - Image-based threat vectors involve the embedding of malicious code inside of an image file by the threat actor
    - Files
        - The files, often disguised as legitimate documents or software, can be transferred as email attachments, through file-sharing services, or hosted on a malicious website
    - Voice Calls
        - *Vhishing*
            - Use of voice calls to trick victims into revealing their sensitive information to an attacker

- Removable Devices
    - One common technique used with removable devices is known as baiting
        - *Baiting*
            - Attacker might leave a malware-infected USB drive in a location where their target might find it, such as in the parking lot or the lobby of the targeted organization
- Unsecure Networks
    - Unsecure networks includes wireless, wired, and Bluetooth networks that lack the appropriate security measures to protect these networks
    - If wireless networks are not properly secured, unauthorized individuals can intercept the wireless communications or gain access to the network
    - Wired networks tend to be more secure than their wireless networks, but they are still not immune to threats
        - Physical access to the network infrastructure can lead to various attacks
            - MAC Address Cloning
            - VLAN Hopping
    - By exploiting vulnerabilities in the Bluetooth protocol, an attacker can carry out their attacks using techniques like the BlueBorne or BlueSmack exploits
        - *BlueBorne*
            - Set of vulnerabilities in Bluetooth technology that can allow an attacker to take over devices, spread malware, or even establish an on-path attack to intercept communications without any user interaction

                - *BlueSmack*
                    - Type of Denial of Service attack that targets Bluetooth-enabled devices by sending a specially crafted Logical Link Control and Adaptation Protocol packet to a target device

- **Outsmarting Threat Actors**
    - One of the most effective ways to learn from the different threat actors that are attacking your network is to set up and utilize deception and disruption technologies
    - *Tactics, Techniques, and Procedures (TTPs)*
        - Specific methods and patterns of activities or behaviors associated with a particular threat actor or group of threat actors
    - *Deceptive and Disruption Technologies*
        - Technologies designed to mislead, confuse, and divert attackers from critical assets while simultaneously detecting and neutralizing threats
        - *Honeypots*
            - Decoy system or network set up to attract potential hackers
        - *Honeynets*
            - Network of honeypots to create a more complex system that is designed to mimic an entire network of systems
                - Servers
                - Routers
                - Switches
        - *Honeyfiles*
            - Decoy file placed within a system to lure in potential attackers

        - *Honeytokens*
            - Piece of data or a resource that has no legitimate value or use but is monitored for access or use
    - Some disruption technologies and strategies to help secure our enterprise networks
        - Bogus DNS entries
            - Fake Domain Name System entries introduced into your system's DNS server
        - Creating decoy directories
            - Fake folders and files placed within a system's storage
        - Dynamic page generation
            - Effective against automated scraping tools or bots trying to index or steal content from your organization's website
        - Use of port triggering to hide services
            - *Port Triggering*
                - Security mechanism where specific services or ports on a network device remain closed until a specific outbound traffic pattern is detected
        - Spoofing fake telemetry data
            - When a system detects a network scan is being attempted by an attacker, it can be configured to respond by sending out fake telemetry or network data

Physical Security

Objectives:

- 1.2 - Summarize fundamental security concepts
- 2.4 - Analyze indicators of malicious activity

- **Physical Security**
  - *Physical Security*
    - Measures to protect tangible assets (buildings, equipment, people) from harm or unauthorized access
  - Security Controls
    - Fencing and Bollards
      - *Bollards*
        - Short, sturdy vertical posts controlling or preventing vehicle access
      - *Fences*
        - Barriers made of posts and wire or boards to enclose or separate areas
    - Brute Force Attacks
      - Forcible entry
      - Tampering with security devices
      - Confronting security personnel
      - Ramming a barrier with a vehicle
    - *Surveillance Systems*
      - An organized strategy to observe and report activities
      - Components
        - Video surveillance

            - Security guards
            - Lighting
            - Sensors
        - *Access Control Vestibules*
            - Double-door system electronically controlled to allow only one door open at a time
            - Prevents piggybacking and tailgating
        - Door Locks
            - Padlocks
            - Pin and tumbler locks
            - Numeric locks
            - Wireless locks
            - Biometric locks
            - Cipher locks
            - Electronic access control systems
        - Access Badges
            - Use of Radio Frequency Identification (RFID) or Near Field Communication (NFC) for access

- **Fencing and Bollards**
    - Fencing and bollards stand out as some of the most primitive tools that are employed to safeguard assets and people
    - *Fence*
        - Structure that encloses an area using interconnected panels or posts
        - In terms of physical security, fences serve several purposes
            - Provides a visual deterrent by defining a boundary that should not be

violated by unauthorized personnel

        - Establish a physical barrier against unauthorized entry
        - Effectively delay intruders which helps provide our security personnel a longer window of time to react

    - *Bollards*
        - Robust, short vertical posts, typically made of steel or concrete, that are designed to manage or redirect vehicular traffic
    - Fencing is considered to be more adaptable and well-suited for safeguarding large perimeters around the entire building
    - Bollards are really designed to counter vehicular threats in a specific area instead

- **Attacking with Brute Force**
    - *Brute Force*
        - Type of attack where access to a system is gained by simply trying all of the possibilities until you break through
    - In terms of physically security, brute force focuses on the following
        - *Forcible Entry*
            - Act of gaining unauthorized access to a space by physically breaking or bypassing its barriers, such as windows, doors, or fences
            - Use high-strength doors with deadbolt locks, metal frames, or a solid core
        - Tampering with security devices
            - Involves manipulating security devices to create new vulnerabilities that can be exploited
            - To protect against tampering with security devices, have redundancy in physical security measures

- Confronting security personnel
    - Involves the direct confrontation or attack of your organization's security personnel
    - Security personnel should undergo rigorous conflict resolution and self-defense training to mitigate risks
- Ramming barriers with vehicles
    - Uses a car, truck, or other motorized vehicle to ram into the organization's physical security barriers, such as a fence, a gate, or even the side of your building
    - Install bollards or reinforced barriers to prevent vehicles from driving into your facilities

- **Surveillance Systems**
    - *Surveillance System*
        - Organized strategy or setup designed to observe and report activities in a given area
    - Surveillance is often comprised of four main categories
        - Video Surveillance
            - Can include the following
                - Motion detection
                - Night vision
                - Facial recognition
            - Remote access
            - Provides real-time visual feedback
            - A wired solution security camera is physically cabled from the device back to the central monitoring station

        - A wireless solution relies on Wi-Fi to send its signal back to the central monitoring station
        - *Pan-Tilt-Zoom (PTZ) System*
            - Can move the camera or its angle to better detect issues during an intrusion
        - Best places to have cameras
            - Data center
            - Telecommunications closets
            - Entrance or exit areas
        - Cameras should be configured to record what they're observing
    - Security Guards
        - Flexible and adaptable forms of surveillance that organizations use
        - Helps to reassure your staff or your customers that they are safe
    - Lighting
        - Proper lighting is crucial for conducting effective surveillance using both video and security guards
        - If you create well-lit areas, this can deter criminals, reduce shadows and hiding spots, and enhance the quality of your video recordings
    - Sensors
        - Devices that detect and respond to external stimuli or changes in the environment
        - There are four categories of sensors
            - Infrared Sensors
                - Detect changes in infrared radiation that is often emitted by warm bodies like humans or animals

        - Pressure Sensors
            - Activated whenever a specified minimum amount of weight is detected on the sensor that is embedded into the floor or a mat
        - Microwave Sensors
            - Detect movement in an area by emitting microwave pulses and measuring their reflection off moving objects
        - Ultrasonic Sensors
            - Measures the reflection of ultrasonic waves off moving objects

- **Bypassing Surveillance Systems**
    - Some of the different methods used by attackers to bypass your organization's surveillance systems
        - Visual Obstruction
            - Blocking the camera’s line of sight
            - Can involve the following
                - spraying paint or foam onto the camera lens
                - placing a sticker or tape over the lens
                - positioning objects like balloons or umbrellas in front of the camera to block its view
        - Blinding Sensors and Cameras
            - Involves overwhelming the sensor or camera with a sudden burst of light to render it ineffective for a limited period of time
        - Interfering with Acoustics
            - Acoustic systems are designed to listen to the environment to detect if

            someone is in the area or to eavesdrop on their conversations
            - Jamming or playing loud music to disrupt the microphone's functionality
        - Interfering with Electromagnetic
            - *Electromagnetic Interference (EMI)*
                - Involves jamming the signals that surveillance system relies on to monitor the environment
        - Attacking the Physical Environment
            - Exploit the environment around the surveillance equipment to compromise their functionality
    - Physical tampering, like cutting wires or physically disabling devices, is an effective strategy to bypass surveillance systems
    - Modern systems are equipped with countermeasures to help protect surveillance systems

- **Access Control Vestibules**
    - *Access Control Vestibules*
        - Double-door system that is designed with two doors that are electronically controlled to ensure that only one door can be open at a given time
    - These access control vestibules can also help prevent piggybacking and tailgating
        - *Piggybacking*
            - Involves two people working together with one person who has legitimate access intentionally allows another person who doesn't have proper authorization to enter a secure area with them
        - *Tailgating*
            - Occurs whenever an unauthorized person closely follows someone through the access control vestibule who has legitimate access into the

        secure space without their knowledge or consent
    - The key difference between Piggybacking and Tailgating
        - Piggybacking uses social engineering to gain consent of the person with legitimate access
        - Tailgating doesn’t use or obtain the consent of the person with legitimate access.
  - Access control vestibules are usually integrated with electronic badges and operated by a security guard at the entrance to a secure facility or office building
    - Badges contain
      - RFID (Radio-Frequency Identification)
      - NFC (Near-field Communication)
      - Magnetic strips
  - Security guards are often at access control vestibules because they provide
    - Visual deterrent
    - Assistance
    - Check identity
    - Response

- **Door Locks**
  - *Door Locks*
    - Critical physical security control measure designed to restrict and regulate access to specific spaces or properties, preventing unauthorized intrusions and safeguarding sensitive data and individuals
  - Types of Door Locks
    - Traditional Padlocks
      - Easily defeated and offer minimal protection

- Basic Door Locks
  - Vulnerable to simple techniques like lock picking
- Modern Electronic Door Locks
  - Utilize various authentication methods for enhanced security
  - Authentication Methods
    - Identification Numbers
      - Require entry of a unique code, providing a balance of security and convenience
    - Wireless Signals
      - Utilize technologies like NFC, Wi-Fi, Bluetooth, or RFID for unlocking
    - Biometrics
      - Rely on physical characteristics like fingerprints, retinal scans, or facial recognition for authentication
      - Biometric Challenges
        - *False Acceptance Rate (FAR)*
          - Occurs when the system erroneously authenticates an unauthorized user
          - Lower FAR by increasing scanner sensitivity
        - *False Rejection Rate (FRR)*
          - Denies access to an authorized user. Increasing sensitivity can increase FRR
        - *Crossover Error Rate (CER)*
          - A balance between FAR and FRR for optimal authentication effectiveness

- Some electronic door locks use multiple factors, such as an identification number and fingerprint, to increase security
- *Cipher Locks*
  - Mechanical locks with numbered push buttons, requiring a correct combination to open
  - Commonly used in high-security areas like server rooms
- Secure entry areas in office buildings, often using electronic access systems with badges and PINs for authentication

- **Access Badge Cloning**
  - Radio Frequency Identification (RFID) and Near Field Communication (NFC) are popular technologies used for contactless authentication in various applications
  - *Access Badge Cloning*
    - Copying the data from an RFID or NFC card or badge onto another card or device
  - How does an attacker clone an access badge?
    - Step 1: Scanning
      - Scanning or reading the targeted individual's access badge
    - Step 2: Data Extraction
      - Attackers extract the relevant authentication credentials from the card, such as a unique identifier or a set of encrypted data
    - Step 3: Writing to a new card or device
      - Attacker will then transfers the extracted data onto a blank RFID or NFC card or another compatible device
    - Step 4: Using the cloned access badge
      - Attackers gain unauthorized access to buildings, computer systems, or even make payments using a cloned NFC-enabled credit card

- Access badge cloning is common because of its
    - Ease of execution
    - Ability to be stealthy when conducting the attack
    - Potentially widespread use in compromising physical security
- How can you stop access badge cloning?
    - Implement advanced encryption in your card-based authentication systems
    - Implement Multi-Factor Authentication (MFA)
    - Regularly update your security protocols
    - Educate your users
    - Implement the use of shielded wallets or sleeves with your RFID access badges
    - Monitor and audit your access logs