* **Classifying Cybersecurity Threats:**
  + **Internal vs. External:**
    - We most often think about the threat actors who exist outside our organization: competitors, criminals, and the curious. However, some of the most dangerous threats come from within our own environments.
  + **Level of Sophistication:**
    - Threat actors vary greatly in their level of cybersecurity sophistication and capability.
  + **Resources/Funding:**
    - Just as threat actors vary in sophistication, they also vary in the resources available to them. Some may have limitless funding or have only spare time.
  + **Intent/Motivation:**
    - Attackers also vary in their motivation and intent. So may just do it because it’s fun, while others look to gain something.
* **The Hats Hackers Wear:**
  + **White-Hats:**
    - Authorized attackers who act with authorization and seek to discover security vulnerabilities with the intent of correcting them.
  + **Black-Hats:**
    - Unauthorized attackers with malicious intent.
  + **Gray-Hats:**
    - Semi-authorized attackers who act without proper authority but do so with good intent of correcting any vulnerabilities.
      * Good intent does not mean ethical or legal, and these individuals can still be arrested.
* **Threat Actors:**
  + **Script Kiddies:**
    - People who use hacking techniques but have limited skill. They rely almost entirely on automated tools they download from the Internet. They have little knowledge of how their attacks actually work and simply seek out convenient targets.
    - Their limited skill does not make them any less dangerous however, as the tools they use are still powerful and will create problems if your services are vulnerable to that type of attack. Additionally, they are less discriminate of who they attack, making low profile targets susceptible to these attacks. There additionally are many these individuals.
    - Fortunately, they still lack skill, time, and resources, so are not very effective at what they do.
  + **Hacktivists:**
    - Use hacking to accomplish some activist goal.
      * They may deface a company with policies they disagree with or attack a network for political issues.
      * The defining characteristics of these hackers is that they believe what they are doing is for the greater good, even if their activity violates the law.
      * Their skills vary between Script Kiddies to Industry Professionals, and their resources also vary greatly as well. Some Hacktivists are alone, while others are in groups.
      * The most popular organized **Hacktivist Group is Anonymous**.
      * **Edward Snowden** can also be considered an Insider Hacktivist.
* **Criminal Syndicates:**
  + Organized crime that most often is motivated simply by financial gain. They typically want to remain low-key, to draw as little attention to themselves as possible.
  + In their **2019 Internet Organized Crime Threat Assessment (IOCTA**), the **European Union Agency for Law Enforcement Cooperation (EUROPOL)** found that organized crime groups were active in the following categories:
    - **Cyber-Dependent Crime:**
      * Includes **ransomware, data compromise, distributed denial-of-service (DDoS) attacks**, website defacement, and attacks against critical infrastructure.
      * **Child Sexual Exploitation:**
        + Includes child porn, abuse, and solicitation.
      * **Payment Fraud:**
        + Credit card fraud and business email compromises.
      * **Dark Web:**
        + Activity including the sale of illegal goods and services.
      * **Terrorism:**
        + Support, including facilitating the actions of terrorist groups online.
      * **Cross-Cutting Crime Factors:**
        + Including social engineering, money mules, and the criminal abuse of cryptocurrencies.
  + These organized crime groups tend to range between moderately skilled to highly skilled.
    - Some groups do consist of script kiddies, but they tend to be caught quickly.
  + These groups also tend to have more resources compared to hacktivists and script kiddies as this can be seen as a “business” where it takes money to make money.
* **Advanced Persistent Threats (APTs)**
  + In the recent years, a great deal of attention has been given to State Actors hacking into either foreign governments or corporations. The security company Mandiant created the term APTs to describe a series of attacks first traced to sources connected to the Chinese military.
    - These attacks are now found to be perpetrated by every technologically advanced country and have two characteristics.
      * These attacks are advanced and persistent, something that can only be done with a group of individuals who have great skill and access to many resources.
  + Typically motivated by political and economic reasons, but sometimes espionage.
  + **Zero-Day Attack:**
    - Whenever APT attacks find vulnerabilities in a system, they typically keep quiet about, and keep note of it in a list of known vulnerabilities. Thus, whenever it is time to abuse the vulnerability, only the attacker is aware of it and can abuse the vulnerability with no resistance. Thus, the attack is called a Zero-Day Attack because there were Zero days to respond to the attack since no one knew it existed in the first place.
* **Insiders:**
  + Insider attacks occur when an employee, contractor, vendor, or other individual with authorized access to information and systems uses that access to wage an attack against the organization.
    - These attacks typically aim at disclosing confidential information but can include actions to disrupt business processes.
  + Insiders can be of any skill level and usually have a motivation related to activism, money, or they are just pissed because they are going to get laid off.
    - Most insider attacks could be behaviorally tracked, which is why cybersecurity teams should work with HR to identify possible threats.
  + **The Threat of Shadow IT:**
    - There are times when employees resort to unapproved technology in order to do their job better. One popular instance was when employees would use Dropbox to sync their work content between business and personal devices. Something like this has zero malicious intent and is done to try to benefit the company, and this phenomenon is known as Shadow IT. But Shadow IT poses many security issues as possibly sensitive data becomes accessible to unapproved vendors.
* **Competitors:**
  + Competitors may engage in corporate espionage designed to steal sensitive information for your organization and use it to their own business advantage.
    - This may include theft of customer information, stealing proprietary software, identifying confidential product development plans, or gaining access to any other information that would benefit the competitor.
    - In some cases, competitors may get an insider to retrieve information from within your company.
      * Insider information is sometimes sold on the dark web as well.
* **Threat Vectors:**
  + The means that threat actors use to obtain access to an information system.
  + Email and Social Media:
    - **Email is one of the most exploited threat vectors**, containing phishing and spam messages which are a simple way to gain access to an organization’s network.
      * They can be employed against many people easily, and only need one person to fall victim.
    - **Social Media** can also be used similarly, but additionally provides information about users that can aid in other types of attacks.
  + **Direct Access:**
    - Attackers may attempt to gain direct access to an organization’s network by physically entering the organization’s facilities.
      * They may enter public areas and possible connect to unsecured network jacks on the wall or do some other stuff.
      * They may also gain access to unsecured computer terminals and network devices.
        + Security professionals must assume that an attacker who is able to physically touch a component will be able to compromise that device and use it for malicious purposes.
  + **Wireless Networks:**
    - Provide an easier path into an organization’s network as attackers don’t need physical access to a facility and can just sit in the parking lot to access the network. This means they MUST still be near the organization’s facility.
  + **Removable Media:**
    - Attackers may physically input or throw around some USBs around a parking lot hoping someone will input the USB into a computer, thus compromising it.
  + **Cloud:**
    - Attackers routinely scan popular cloud services for files with improper access controls, systems that have security flaws, or accidentally publish **API keys and passwords.** 
      * The vulnerabilities that organizations face bear similarities to those found in on-premises environments.
  + **Third-Party Risks:**
    - Sophisticated attackers may attempt to interfere with an organization’s IT supply chain, gaining access to devices at the manufacturer or while the devices are in transit from the manufacturer to the end user.
      * Devices could be tampered with and installed with malware or backdoors.
    - Other security issues may arise as collaborating with third parties now means any security flaws the third party has may impact your own security as well.
    - Issues also arise if the third-party stops supporting certain services, leading to no more security updates.
* **Threat Data and Intelligence:**
  + **Threat Intelligence:**
    - The set of activities and resources available to cybersecurity professionals seeking to learn about changes in the threat environment.
      * It is important to be familiar with current threats as you won’t be able to defend against it if you don’t know it.
  + **Predictive Analysis:**
    - Something that can be achieved through threat intelligence where you identify risks to an organization.
  + There are many sources of threat intelligence such as open-source intelligence **(OSINT)** that can be gathered from publicly available sources to commercial services that provide proprietary or closed-source intelligence information.
    - An increasing number of products and services have the ability to consume threat feed data, allowing you to leverage it throughout your infrastructure and systems.
    - **Threat Feeds** are intended to provide up-to-date detail about threats in a way your organization can leverage, and usually include technical details about a threat such as IP addresses, hostnames and domains, email addresses, URLs, file hashes, file paths, CVE numbers, and other details about a threat.
  + **Vulnerability Databases:**
    - An essential part of an organization’s threat intelligence program where reports of vulnerabilities can be recorded.
  + **Indicators of Compromise (IoCs):**
    - Something that can be provided with from threat intelligence sources. These are telltale signs that an attack has taken place and may include file signatures, log patterns, and other evidence left behind by attackers.
    - IoCs may also be found in file and code repositories that offer threat intelligence information.
* **Open-Source Intelligence (OSINT):**
  + Threat intelligence that is acquired from publicly available sources.
    - Many organizations have recognized how useful open sharing of threat information can be, and OSINT has become broadly available.
    - A number of sites maintain extensive lists of OSINT sources:
      * Senki.org
      * Open Threat Exchange
      * MISP Threat Sharing project
      * Threatfeeds.io
    - There are additionally government and public sources of threat intelligence data.
      * **Cybersecurity and Infrastructure Security Agency (CISA)**
      * **U.S. Department of Defense Cyber Crime Center**
      * **CISA’s Automated Indicator Sharing (AIS) Program**
    - **Dark Web:**
      * A network run over standard Internet connections but using multiple layers of encryption to provide anonymous communications.
* **Proprietary and Closed-Source Intelligence:**
  + Closed-source intelligence is typically used by commercial security vendors, government organizations, and other security-centric organizations. They used their own information gathering and research, use custom tools, and typically keep their information closed off to sell or license it, or if they don’t want threat actors to be aware that the threat is known.
* **Threat Maps:**
  + They provide a geographic view of threat intelligence.
    - Many security vendors offer high-level maps that provide real-time insight into the cybersecurity threat landscape, which help gain insight into the sources of attacks aimed directly at their network.
      * Unfortunately, geographic attribution is unreliable because attackers often relay their attacks through cloud services and other compromised works, hiding their true geographic location.
* **Assessing Threat Intelligence:**
  + Regardless of the source of your threat intelligence information, you need to assess it. You need to consider a few factors:
    - **Is it timely?**
      * A feed that is operating on delay can cause you to miss a threat, or to react after the threat no longer is relevant.
    - **Is the information accurate?**
      * Can you rely on what it says, and how likely is it that the assessment is valid? Does it rely on a single source or multiple sources? How often are those sources correct?
    - **Is the information relevant?**
      * If it describes the wrong platform, software, or reason for the organization to be targeted, the data may be very timely, very accurate, and completely irrelevant to your organization.
  + **One way to summarize the threat intelligence assessment data is via a Confidence Score.**
    - A lot of threat intelligence usually start with low scores, and low scores does not mean the info is not useful. It just means it shouldn’t be fully trusted, until the threat intelligence is consistently achieving all factors above.
* **Threat Indicator Management and Exchange:**
  + Managing threat information at any scale requires standardization and tooling to allow the threat information to be processed and used in automated ways. Indicator management can be much easier with a defined set of terms.
    - **Structured Threat Information eXpression (STIX):**
      * An **XML** language / structured markup language that in its current form, STIX 2.0, defines 12 domain objects including attack patterns, identities, malware, threat actor, and tools.
      * While STIX used to be sponsored by the **DoD**, it is now under the Organization for the **Advancement of Structured Information Standards (OASIS)**
    - **Trusted Automated eXchange of Indicator Information (TAXII) Protocol:**
      * A companion to STIX, intended to allow cyber threat information to be communicated at the application layer via **HTTPS**, and was designed to support STIX data exchange.
    - **Open Indicators of Compromise (OpenIOC) Format:**
      * Like STIX as it is an XML-based framework, developed by Mandiant and uses Mandiant’s indicators for its base framework.
* **Public and Private Information Sharing Centers**
  + In addition to threat intelligence vendors and resources, threat intelligence communities have been created to share threat information.
    - **Information Sharing and Analysis Centers (ISACs)** for example help share threat information and provide tools and assistance to their members. Introduced in the U.S. to protect critical infrastructure.
* **Conducting Your Own Research:**
  + Vendor security information websites.
  + Vulnerability and threat feeds from vendors, government agencies, and private organizations.
  + Academic journals and technical publications, such as **Internet Request for Comments (RFC) documents**. RFC documents are particularly informative because they contain the detailed technical specifications for Internet protocols.
  + Professional conferences and local industry group meetings.
  + Social media accounts of prominent security professionals.
  + **Tactics, Techniques, and Procedures (TTPs)**, which are like guides on how threat actors perform a hack.