threat landscape

It is the collection of threats in a given context or domain.

The threat landscape means the entire scope of potential and recognized cybersecurity threats affecting user groups, organizations, specific industries, or a particular time.

All known and possible threat to computer networks.

Threat Actors

A cybersecurity threat actor, defined as an individual, group, organization, or entity engaged in activities designed to compromise computer systems, networks, data, or information, can have various motivations, skills, and resources and employ several tactics, techniques, and procedures to achieve their objectives.

Attack Frame Work gives you a glimpse into the category of a cyberattack.

Types of Bad Actors

What is a Bad Actor?

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.

Bad actors can be grouped into types based on their character, motivations, and the common attack they use.

Use image here from ./Images/ bad\_actotrs.jpg

and make it at the center

1. The explorer

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

Notoriety is the biggest motivator within this group.

One method Used by explorer is phishing and its variant, however are not exclusive to the explorer, and other bad actors types might uses them for own purpose.

Use image here from ./Images/fishing\_variants.jpg and make it at the center

Phishing:

Phishing: The most general term. Phishing attacks attempt to trick victims into revealing personal information, clicking malicious links, or downloading malware. Phishing attacks can occur via email, phone calls, text messages, or even social media. And it has many variant

* Spear Phishing is a type of email attack in which a specific person or organization is targeted.
* Whaling: Whaling is also a type of phishing attack. In this attack high level personnel of an organization such as CEO, COO, CTO are targeted. Attackers send emails or text messages that seem legitimate but contain malicious links.
* Vishing: fraudulent phone calls that induce you to reveal personal information.
* Smishing: fraudulent text messages meant to trick you into revealing data.

1. The Hacktivist

They are motivated by ideology or are animated by an emotive force.

They act collectively in common to cause against an enemy.

They collectively crusade against a specific corporation, or go after political or social organizations that they feel did something bad.

A common strategy of hacktivist is to build a botnet in secret. To make a botnet the hacktivist set up a command –and -control server (C & C Server ) that is accessible to the internet. This is the central coordination point for all botnet nodes and the botnet wait for instructions from the C&C server.

Use image here from ./Images/DDOS.jpg and make it at the center

1. The cyberterrorists

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.

1. The Cybercriminal

There motivation is self-centered . they want money plain and simple.

1. The cyberwarrior

Are the most least self-interested but are nonetheless the most dangerous because they have a resource of nation-state at their disposal .

They are motivated by the national interest of their home contry

Categories of Hackers

Use image here from ./Images/DDOS.jpg and make it at the center

Cybersecurity threats

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, damage, disrupt computing systems.

An attack vector

An attack vector, or threat vector, is a way for attackers to enter a network or system.

There are three components that comprise an attack vector:

Use image here from ./Images/ parts\_of\_attack\_vector.jpg

and make it at the center

Main Cybersecurity Threats

Use image here from ./Images/main\_cybersecurity\_threats.jpg and make it at the center

A tailgating attack is a physical security threat in which an attacker gains access to a secure area. This is accomplished by following someone with legitimate access to the space, such as an employee.

Threat Intelligence is a crucial component of cybersecurity that involves gathering, analyzing, and interpreting information about potential or current cyber threats. It helps organizations understand the tactics, techniques, and procedures (TTPs) used by threat actors to target their systems and data.

There are myriad of resource for a Threat Intelligence, Internal, External, Government, Private and Open source intelligence (OSINT) and MITRE ATT&CK.

MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally recognized framework that provides a comprehensive knowledge base of adversarial tactics and techniques used by cyber threat actors during various stages of a cyber attack.

CVSS stands for Common Vulnerability Scoring System. It's an industry-standard method for assessing the severity of security vulnerabilities in computer systems. Imagine it as a rating system that helps prioritize which security holes to patch first!

Processing Threat Intelligence

Use image here from ./Images/processing\_threat\_intelligence.jpg and make it at the center

Use image here from ./Images/ processing\_threat\_intelligence 2.jpgand make it at the center

Advanced Persistent Threat (APT)?

An advanced persistent threat (APT) is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period.

Attack framework

Attack framework is a toolbox for cybersecurity professional to enhance organization posture.

The Cyber Kill Chain and MITRE ATT&CK are two foundational frameworks in cybersecurity that help us understand and defend against cyberattacks.

Use image here from ./Images/cyber\_kill\_chain and make it at the centre

for information to qualify as threat intelligence, it should possess the following three qualities:

* Relevance: It should be applicable and specific to the organization's environment and potential threats.
* Context: It should provide a deeper understanding of the threat landscape, including tactics used by threat actors.
* Actionability: It should offer practical guidance or recommendations to mitigate or respond to the identified threats.