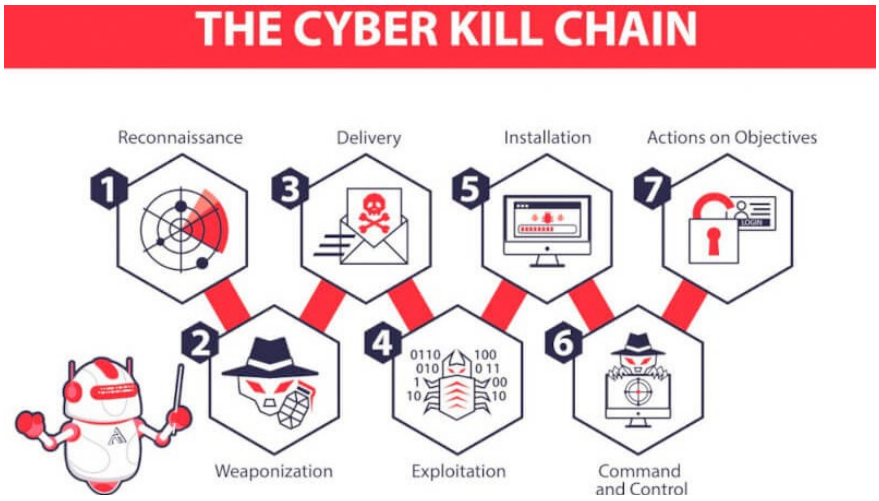
What is Cyber ??Kill Chain and its stages of operation

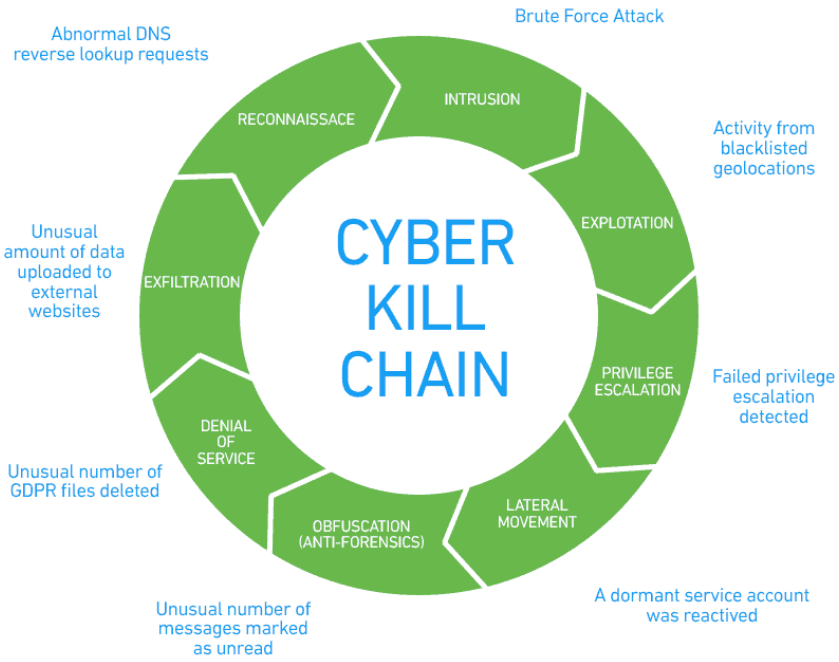
Cyber ??Kill Chain is a cybersecurity model developed by Lockheed Martin that consists of eight stages from information gathering to the attacker stealing data.



Many businesses today use Cyber ??Kill Chain to detect and prevent cyber attacks. If you are also interested in this cyber security model and want to apply it to your system, follow the article below of ***TipsMake*** .

What is Cyber ??Kill Chain?

Cyber ??Kill Chain is a cybersecurity model developed by Lockheed Martin that includes eight stages from information gathering to data theft. Cyber ??Kill Chain provides deeper insight into each stage of a cyber attack. Security professionals will gain a better understanding of hacker tactics, processes, and approaches.



What is Cyber ??Kill Chain?

How does Cyber ??Kill Chain work?

The Cyber ??Kill Chain outlines the sequence of steps an attacker typically takes to execute a cyber attack. This model provides an objective view. Instead of viewing an attack as a single, large-scale event, the Kill Chain breaks it down into stages, from initial information gathering to the final act of stealing data or compromising a system.

By understanding the progression of a cyberattack, security professionals can design defenses and find ways to detect and counter attackers' moves as early as possible. The sooner attacks can be stopped, the less damage a business will suffer.

8 Stages of the Cyber ??Kill Chain

Cyber ??Kill Chain is divided into eight different stages, each stage plays an important role, those 8 stages are:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. DoS-Denial of Service
8. Exfiltration

Reconnaissance

In the Reconnaissance phase, attackers gather information about the target organization. They may use automated scanners to find vulnerabilities and weak points that can be exploited. Attackers will attempt to identify and investigate existing security systems, such as firewalls, intrusion prevention systems, and authentication mechanisms.

Attackers can collect information using methods such as scanning the system for security vulnerabilities, sending fake emails to get victims to provide information such as usernames, account passwords, etc. The more information collected during this stage, the more likely the cyber attack will be successful.

Weaponization

In the Weaponization phase, based on the information collected in the previous phase, the hacker will create or modify malware to best exploit the target's weaknesses.

Delivery

Once the malware is built, the hacker will try to launch the attack. One of the most common methods is to use Social Engineering such as phishing to trick users into giving them information. Hackers can also penetrate by exploiting vulnerabilities discovered in stage 1 or using public wifi because the wifi here is not well secured.

Exploitation

Once the hackers gain access, they use their access to move laterally from system to system. Their goal is to find sensitive information, install additional tools, modify security certificates, and create new script files for criminal purposes.

Installation

If the exploitation phase is successful, the attacker will proceed to install malware. This gives them control over more systems and accounts.

Command and Control

Once hackers have taken control of a large number of systems, they create a control center that allows them to operate remotely. During this stage, they use obfuscation to cover their tracks and avoid detection. They also use denial of service attacks to distract security experts from their real target.

Actions on Objectives

At this stage, the hacker will take steps to achieve his primary goal, which may include attacking the supply chain, stealing data, encrypting data, or destroying data.

Exfiltration

While Lockhead Martin's original Cyber ??Kill Chain consisted of just seven steps, many cybersecurity experts have now expanded it to eight steps to account for hackers monetizing their attacks, such as using ransomware to extract money from victims or selling sensitive data on the dark web.

Benefits of Understanding Cyber ??Kill Chain

Cyber ??Kill Chain helps cybersecurity professionals:

1. Identify threats at every stage of the cyber attack chain.
2. Prevent unauthorized access from outside
3. Protect privileged accounts, data, and systems.
4. Regularly patch and upgrade old hardware and software.
5. Train employees how to spot phishing emails.
6. Explore and react quickly to horizontal movement.
7. Prevent ongoing cyber attacks.

Conclude

Cyber ??Kill Chain is an important tool in understanding and combating cyber attacks. Putting this model into practice not only helps protect information and digital assets, but also improves the ability to respond to future cyber threats.