Cyber Kill Chain: An Overview

The Cyber Kill Chain is a model used in cybersecurity to understand the stages of cyber attacks and develop defense strategies. Originating from Lockheed Martin, this concept aims to sequence the stages of attacks, identifying when defense mechanisms can be deployed. Here are the stages of the Cyber Kill Chain:

1-Reconnaissance: Attackers gather information about the target system or organization. Information is often collected through social media, open sources, or other methods. The information is collected from publicly available sources, social media, or even through direct interactions with employees.

2-Weaponization: Attackers use the gathered information to prepare attack tools. This stage may involve the creation of malicious software.

3-Delivery: Prepared attack tools are delivered to the target system or network. This can occur through email attachments, malicious links, or other methods.

4-Exploitation: Attackers exploit security vulnerabilities in the target system during the delivery stage to gain unauthorized access.

5-Installation: Attackers establish a permanent presence in the system by creating a persistent entity. This involves the placement of malicious software and tools.

6-Command and Control: Attackers set up their own command and control infrastructure to maintain control over the compromised system. This allows them to send commands, receive data, and maintain control over the infiltrated environment without being easily detected.

7-Actions on Objectives: Attackers carry out actions aligned with their primary objectives. This stage may involve data theft, system disruption, or other malicious activities.

Understanding these stages of the Cyber Kill Chain helps organizations enhance their defense strategies and effectively prevent attacks. This model guides organizations in identifying security measures to detect and prevent attacks more efficiently.