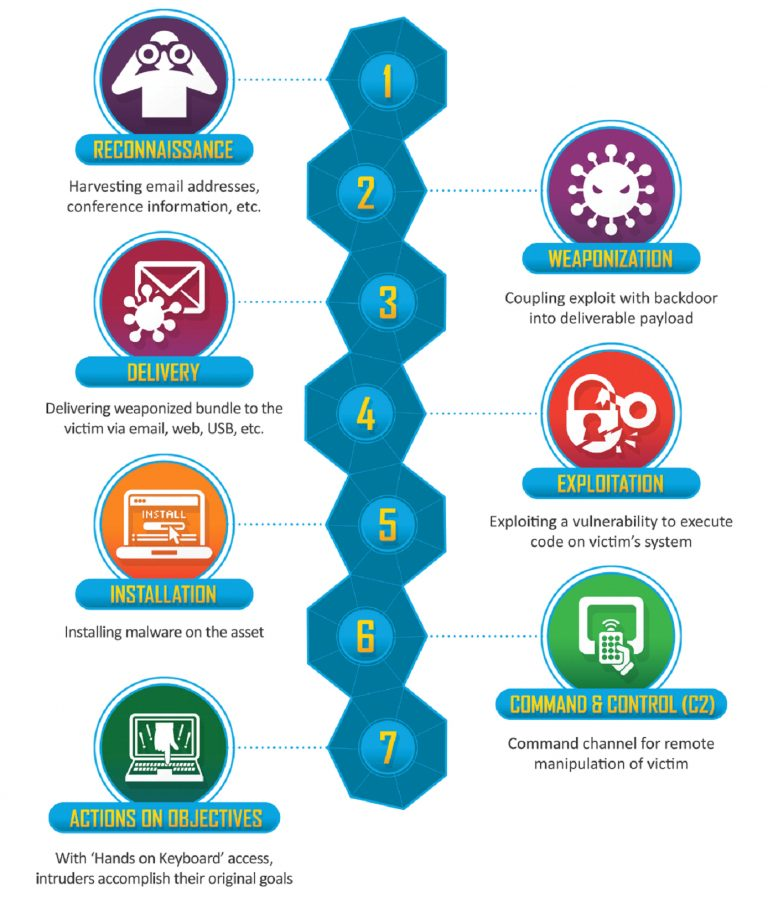
**Task 1: Explain cyber kill chain stages.**

Kill chain, bir düşmanı hedef almak ve düşmanı etkilemek amacı ile kullanılan bir süreçtir. Aslında ölüm zinciri ya da saldırı aşamaları olarak tanımlanabilecek askeri bir konsepttir. Kaldı ki , ABD askeri hedefleme doktrini bu sürecin adımlarını bulma (find), sabitleme (fix), izleme (track), hedefleme (target) angaje etme (engage) ve değerlendirme (assess) (F2T2EA) olarak tanımlamıştır. ABD Savunma Bakanlığı bu süreci örnek olarak düşman hedeflerinin bulunması, konumlarının tespit edilmesi, izleme ve gözleme faaliyeti, istenen etkiyi yaratmak için uygun silah veya araçla hedeflenmesi, düşmanın angaje edilmesi ve etkilerin değerlendirilmesi gibi bir süreç olarak belirtmiştir. Bu süreci bir zincir olarak uçtan uca bir süreç olarak belirtilmiş çünkü aşamalardaki herhangi bir eksikliğin tüm süreci kesintiye uğratacağı belirtilmiştir.

Locheed Martin firması 2011 yılında bu konsepti geliştirerek özellikle siber alana uygun olacak yeni bir kill chain metodolojisi ortaya koymuştur. Saldırganın güvenilen bir ortama giriş için bir payload geliştirmesi, bu ortam içerisinde bir varlık kurması ve bu varlık üzerinden amaçlarına yönelik olarak eylemlerde bulunması ki bu hareketler ortam içerisinde yatay hareketlerde bulunmak veya ortamdaki sistemin gizliliğini, bütünlüğünü ve erişebilirliğini ihlal edilmesi gibi kısaca bir tanım yapılabilir. Cyber Kill Chain, keşif (reconnaissance), silahlanma (weaponization), iletme(delivery) , sömürme (exploitation), yükleme (installation), komuta kontrol (command and control C2) ve amaçlara yönelik eylemler (actions on objectives) adımlarını içeren 7 aşamalı bir modeldir.

Siber ölüm zinciri aslında bir siber saldırının yaşam döngüsüdür. Siber saldırıyı anlamak ve savunma stratejileri geliştirmek için önemli rol oynamaktadır.



Cyber Kill Chain aşamaları şu şekildedir.

1. ****Keşif** (Reconnaissance) :** Saldırganın hedef sistem ile ilgili olarak bilgi toplama aşamasıdır. Amacı genellikle sisteme sızma yöntemlerinin tespit edilmesidir.
2. ****Silahlandırma** (Weaponization):** Keşif aşamasında sisteme giriş noktalarının belirlenmesi soonrası bu noktalara hangi atak vektörünü kullanacağına saldırgan bu aşamada karar verir.
3. ****Teslimat** (Delivery):** Hazırlanan zararlı yazılımın hedef sisteme iletildiği aşamadır. İletim yöntemi bu aşamada seçilmektedir.
4. ****Sömürü** (Exploitation):** Saldırganın silahlanma aşamasında oluşturmuş olduğu atak vektörünü kullanarak hedef sistemdeki zafiyeti sömürdüğü aşamadır. Amaç zararlının sistem üzerinde çalışmasını sağlamaktır.
5. ****Kurulum (Installation):**** sistem üzerinde başarılı bir şekilde çalıştırılan yazılımın kalıcı bir tehdit haline gelmesi için sisteme kendini yüklemelidir. Bu aşamada saldırgan için sistemi kontrol etmesinin önü açılmaktadır. Yükleme aşamasının amacı zararlının sistemde kalacağı süreyi mümkün oldukça artırmaktır.
6. ****Komuta ve Kontrol (C2)** (Command & Control):** Hedef sistemin uzaktan kontrol edildiği aşamadır. Daha önce belirlenen haberleşme kaynağı ile genellikle şifreli haberleşme yöntemleri ile bağlantı kurulur. Bu aşamada hedef sistem ele geçirilmiş durumdadır.
7. ****Amaçlara Yönelik Eylemler (Actions on Objectives):** Saldırgan sistemi ele geçirmesi ile birlikte amacına ulaşmak için çeşitli eylemler gerçekleştirir. Bu eylemlere örnek olarak veri kaçırma, silme veya başka bir sisteme saldırı verilebilir. Saldırganın asıl hesefine ulaşabilmek için gerçekleştirdiği tüm eylemler bu aşamada değerlendirilir.**

Bir Cyber Kill Chain örneği verecek olursak ;

Keşif : Hedefe ait eposta adreslerinin tespiti.

Silahlanma : Zararlı içeren doc dosyası hazırlanması.

İletme : E-posta yolu ile zararlının hedefe gönderilmesi.

Sömürme : CVE-2017-8570 zafiyetinin istismar edilmesi.

Yükleme : Zararlının kendini sistem dosyalarına eklemesi.

Komuta & Kontrol : HTTPS üzerinden xx.xx.xx.xx ile haberleşme.

Eylem : Kurumsal verilerin C2’ya gönderilmesi ve şifrelenmesi.

**Task 2: In which stage of the cyber kill chain is malware developed?**

Kötü amaçlı yazılımın geliştirilmesi genellikle "Silahlandırma" aşamasında icra edilmektedir. Bu, saldırganların zayıflıkları sömürmek ve hedef sistemi tehlikeye atmak için ihtiyaçları olan araçları oluşturdukları veya temin ettikleri aşamadır.

Task 3: Investigate the alternative frameworks.

The Cyber Kill Chain is a model that outlines the stages of a cyber attack, from initial reconnaissance to data exfiltration. While the Cyber Kill Chain is a widely recognized framework, there are alternative models and frameworks that organizations may use to understand and respond to cyber threats. Here are a few alternatives:

1. **MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge):**
   * MITRE ATT&CK is a comprehensive knowledge base that describes the actions and behaviors of cyber adversaries across various stages of an attack.
   * It provides a matrix of tactics and techniques used by adversaries, making it a valuable resource for understanding and mapping out threat actor behaviors.
2. **Diamond Model:**
   * The Diamond Model of Intrusion Analysis is an alternative approach that focuses on four key elements: adversary, infrastructure, capabilities, and victim.
   * It emphasizes the relationships between these elements to provide a more holistic view of cyber threats.
3. **OODA Loop (Observe, Orient, Decide, Act):**
   * The OODA Loop is a decision-making process that stands for Observe, Orient, Decide, and Act. While not explicitly a cyber threat model, it can be applied to understand and respond to evolving threats in a more dynamic way.
4. **NIST Cybersecurity Framework:**
   * Developed by the National Institute of Standards and Technology (NIST), this framework provides a set of guidelines for improving the cybersecurity posture of an organization.
   * It consists of five core functions: Identify, Protect, Detect, Respond, and Recover.
5. **Pentagon of Cyber Security:**
   * The Pentagon of Cyber Security is a model that includes five key components: People, Processes, Technology, Intelligence, and Integration.
   * It emphasizes the importance of a holistic approach to cybersecurity that goes beyond just technology.
6. **Prevent, Detect, Respond, Recover (PDRR):**
   * This framework focuses on the key stages of preventing, detecting, responding to, and recovering from cyber incidents.
   * It is a simplified model that aligns with the key activities organizations need to perform to manage and mitigate cyber threats.
7. **Cybersecurity Kill Chain (Lockheed Martin):**
   * Lockheed Martin's version of the Cyber Kill Chain is a refinement of the original model, often with additional stages like "Reconnaissance" and "Actions on Objectives."

When choosing a framework, it's essential to consider the specific needs and context of your organization. Some organizations may prefer a more detailed and technical approach, while others may opt for a broader, risk-based framework. Ultimately, a combination of these frameworks may be used to provide a more comprehensive understanding of cyber threats and enhance the overall cybersecurity posture.