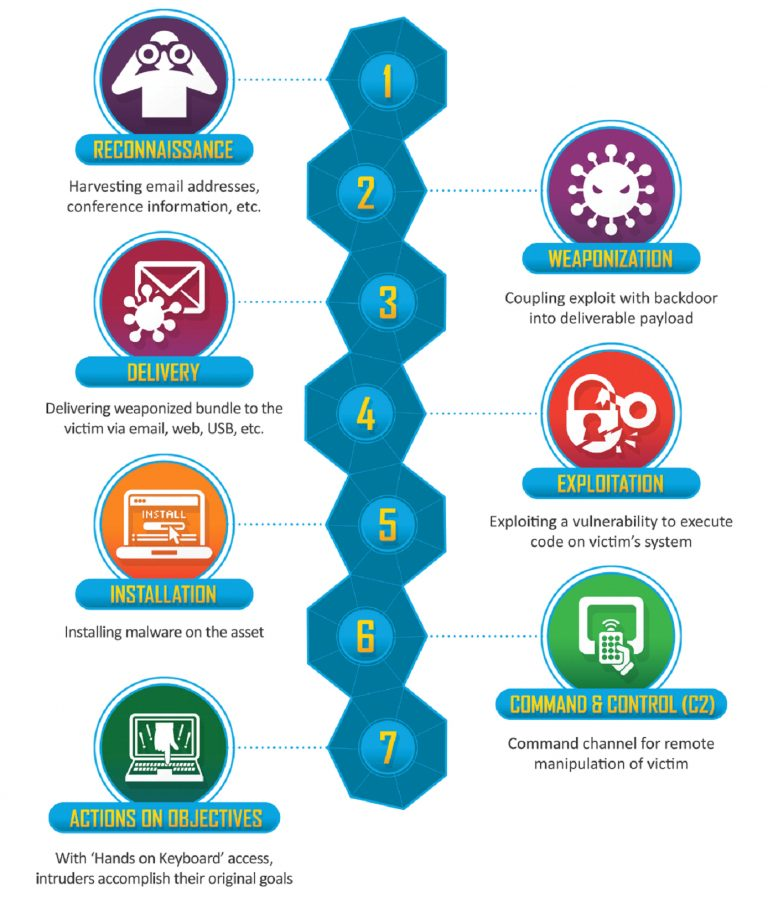
**Task 1: Explain cyber kill chain stages.**

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.

Cyber Kill Chain siber saldırı aşamalarını keşiften son amaca kadar açıklayan bir modeldir. Her ne kadar Cyber Kill Chain sıklıkla kullanılan bir framework olsa da organizasyonların siber tehditleri anlamak ve yanıtlamak için kullanabilecekleri alternatif frameworkler bulunmaktadır. Hali hazırda Cyber Kill Chain dışında kullanılan bazı frameworkler aşağıda çıkarılmıştır.

MITRE ATT&CK : MITRE ATT&CK çerçevesi, siber ortamda saldırganların izleyebileceği eylemleri ve taktikleri açıklayan kapsamlı bir bilgi tabanıdır. "ATT&CK," "Saldırgan Taktikleri, Teknikleri ve Ortak Bilgi" anlamına gelir. Çeşitli siber saldırı yaşam döngüsü aşamalarını kapsar ve siber saldırganların davranışlarını anlamak ve kategorize etmek için yapılandırılmış bir yol sağlar. Bu çerçeve, tehdit istihbaratını geliştirmek, savunma stratejilerini güçlendirmek ve olay yanıtını iyileştirmek amacıyla siber güvenlik alanında geniş bir şekilde kullanılmaktadır.

Diamond Model: Diamond Model, kuruluşların siber tehditleri analiz etmelerine ve anlamalarına yardımcı olan bir kavramsal çerçevedir. Model, saldırganlar, altyapı, yetenekler ve kurbanlar olmak üzere dört temel bileşeni inceleyerek siber tehdit peyzajının kapsamlı bir görünümünü sunar. Saldırganlar, tehdit aktörlerini, motivasyonlarını ve taktiklerini temsil eder; altyapı, kullandıkları araçları ve kaynakları içerir; yetenekler, teknik ve operasyonel becerilerini ifade eder; ve kurbanlar, siber saldırıların hedefidir. Cyber Security Diamond Model, bu yönleri inceleyerek kuruluşların durumsal farkındalıklarını artırmalarına, hedefe yönelik savunma stratejileri geliştirmelerine ve siber güvenlik alanındaki sürekli değişen koşullara karşı olay yanıt yeteneklerini iyileştirmelerine olanak tanır.

Mandiant Attack Life Cycle Framework : Mandiant Attack Life Cycle Framework, siber tehditleri anlama ve onlara yanıt verme konusunda stratejik bir yaklaşımdır. Ünlü bir siber güvenlik şirketi olan Mandiant tarafından geliştirilen bu çerçeve, siber saldırı yaşam döngüsünü başlangıçtan sona kadar farklı aşamalara ayırır; bu aşamalar arasında ilk saldırı, iç keşif, kimlik bilgisi erişimi, keşif ve yanal hareket, veri toplama, dışa çıkarma ve etki bulunmaktadır. Her aşama, bir siber saldırının ilerlemesinde kritik bir adımı temsil eder. Bu aşamaların kapsamlı bir şekilde haritalanmasıyla, kuruluşlar güvenlik olaylarını daha iyi tespit edebilir, analiz edebilir ve azaltabilir. Mandiant Attack Life Cycle Framework, siber güvenlik uzmanlarına olay yanıt yeteneklerini geliştirmeleri, evrilen tehditlere karşı proaktif savunma sağlamaları ve genel siber dirençlerini güçlendirmeleri konusunda olanak tanır.z