HAFTA 1 ANKACORE26 ÖDEV : Dijital Savaş Alanı ve CTI (Tehdit İstihbaratı)

Bölüm A1) Ağ ve Çevre Güvenliği (Sınır Hattı)

Sınır hattı saldırganın içeriye ilk adım atacağı noktadır henüz içeriye girmemeiştir fakat bir açık arıyor demektir tam buraya girdiğinde devreye Firewall ve IDS/IPS ler girer . Bunlar aynı kapıdır fakat farklı pozisyonlara açılır. Sınır hattında Firewall trafiği kurallara göre eleyerek gürültüyü azaltır. IDS/IPS aynı noktada durur ama “kurala uyan fakat niyeti şüpheli” davranışları izler, gerektiğinde müdahaleye zemin hazırlar. Buna rağmen içeri sızan bir tehdit olduğunda, ağın içinde konumlanan NDR devreye girer ve trafiğin içeriğine değil **davranışın ağ üzerindeki etkisine** bakarak anormallikleri yakalar.

Firewall nerden gireleceğini tespit eder IDS bir süre sadece izler çünkü hata büyük bir maliyete neden olabilir o sadece bir şey gördüğünü söyler kararı sisteme bırakır. IPS devreye gireceği zamansa desen nettir bir anormallik kesin olarak görülüyordur ve bu anda izleyen sistem müdahale eden sisteme dönüşür.

Görünmeyeni Gören Katman : NDR

Saldırganın trafiği meşru hale getirecek bir açık (bir sıfır gün açığı,VPN hesabı ele geçirmesi gibi) bulduktan sonra hedefine ulaşmasını engelleyen katmandır.

Saldırgan içerdedir. Firewall ve IDS’in “kim geliyor?” sorusundan sonra, NDR **“içeride ne oluyor?”** sorusunu sorar. NDR içerideki davranışları inceleyerek normal ve anormali ayırır. Kısacası NDR saldırgan içeri girdikten sonra ne yapamaya çalıştığını anlamaya çalışan segmenttir.

Bölüm A2) Uç Nokta Savunmasının Aşılması

Bu nokta da saldırgan fiilen bir ağı geçmiş ve laptop veya sunucuya ulaşmış demektir.Son kale savunması burada AV ve EDR ile başlar. Antivirüs bilinen bir zararlı imza , yaygın bir malware gibi görünür saldırılarda devamlıdır fakat kritik saldırılar, zero day açıkları gibi saldırılarda daha işlevsizdir. EDR ise yan hareketleri tespit eder ve diğer endpoint’ler için alarm üretir yani durum davranışsal farklılıklar olduğundan saldırılar daha net fark edilebilir. Dosya temelli kontrol saldırıyı kaçırır fakat davranış analizi saldırıyı yakalar. Yani son kaleyi EDR korur denilebilir.

Dosyasız saldıralarda disk üzerinde zararlı bir dosya bulunmaz bu yüzden AV bu nokta da kör kalır. Saldırı RAM içerisinde çalışır EDR de bu noktada process zincirlerini izleyerek Anormal davranışları tespit eder ve saldırı modelini yakalar ve müdahale eder.

Bölüm A3) Operasyon Merkezi ve Görünürlük

Bir saldırı girişimi başladığında, SOC, SIEM ve SOAR arasındaki ilişki beynin refleks sistemi gibi çalışır. SIEM girilen binlerce log arasından bir filtreleme yapar ve veriyi anlamlandırır, SOC analisiti karar ve analiz yapısını düzenler, son olarak SOAR müdehale ve savunma mekanizmasını devreye sokar.

Bölüm A4) Genişletilmiş ve Yönetilen Hizmetler

XDR (Genişletilmiş Tespit ve Yanıt), güvenlik araçları arasındaki duvarları yıkar.
Parçalı Bakış (Eski): EDR sadece bilgisayara, NDR sadece ağ trafiğine, Cloud Security ise sadece buluta bakar. Saldırgan bu boşluklardan sızar.
XDR Bakışı (Yeni): XDR, tüm bu farklı platformlardan gelen verileri tek bir havuzda toplar.

Örnek: Saldırgan önce bir bulut hesabına sızar (**Cloud**), oradan bir sunucuya atlar (**EDR**) ve ağ üzerinde hareket eder (**NDR**). XDR, bu üç farklı izi tek bir "saldırı hikayesi" olarak birleştirir.

MDR (Yönetilen Tespit ve Yanıt), bir hizmet ve uzmanlık modelidir. Öreneğin bir şirketin 7/24 alarm izleyecek, gelişmiş tehditleri avlayacak 10-15 kişilik uzman bir SOC ekibi kurması çok maliyetli ve zordur MDR bu soruna şöyle bir çözüm üretir : Şirket, teknolojiyi (XDR/SIEM) kurar ancak "direksiyonu" dışarıdaki profesyonel bir ekibe bırakır. Böylece hem 7/24 izleme sağlanır hem basit bir saldırı bile anında tespit edilir hem de saldırı olduğu an müdahale edilerek sorun giderilir. XDR en gelişmiş radar sistemini verirken MDR ise o radarı kullanacak ve uçağı yere indirecek tecrübeli pilotları sağlar.

Bölüm B) Temel Sözlük ve Kavran Ağı

1-Temel Yapı Taşları ve Ağ

Transistör ve işletim sistemi arasındaki bağlam: Transistör elektrik akımını geçiren 3 yarı iletkenin bir araya gelmesiyle oluşmuş bir mikro anahtardır. Bu basit ama bir araya geldiğinde karmaşık bir algoritma yapısı oluşturan mikroskobik anahtarlar günümüz işletim sistemlerinin çalışma mantığının temelini oluşturur.

OSI ve TCP/IP karşılaştırması: OSI modeli daha teorik ve 7 katmanlı bir sistem TCP/IP modeli ise 4 katmandan oluşan OSİ modelinin daha yalın halidir bu yüzden daha hızlı bir veri akşı sağlamak istediğimiz günümüz internet dünyasında TCP/IP modeli en pratik ve kullanışlı yoldur.

Kriptografinin önemi: Modern güvenlik pratiklerinde şifreleme + doğrulama = veri güvenliği için temel oluşturur. Veriyi sadece şifrelediğimiz de onu yetkisiz kişilerin

erişiminden korumuş oluruz bunun yanında şifreleme yapmak verinin yolda değiştirilip değiştirilmediğini de tespiti için önemlidir. Böylece veri bütünlüğü de sağlanmış olur.

2-Saldırı Vektörleri

Bir sistemi hacklemek yerine insanı hacklemek daha kolaydır çünkü insan duygularının etkisinde kalıp hatalar yapabilir , manipüle edilebilir ve normalde yapmayacağı herhangi bir şeyi yapabilir.

Email soofing ve phising:

E-mail spoofing , saldırganın sahte bir e –mail hazırlayıp üzerinde değişiklikler yaparak görünürde onu güvenilir gibi e – mail gibi göstermesidir.

Phising ise saldırganın kullanıcıyı kandırarak ondan bilgi çalmasıdır. E-mail yada link kullanılabilir.

Malware ve Ransomware:

Malware sistemlere zarar vermek için tasarlanmış tüm zararlı yazılımların genel adıdır. Ransomeware ise bu geniş ailenin verileri şifreleyerek bunlara erişim için fidye talep eden özelleşmiş , şantaj odaklı bir üyesidir.

Zero day açığının savunma tarafı için önemi: Zero day açığı henüz geliştiricinin bilmediği bir açığın tespitidir bu yüzden ortada hiç bir koruma mevcut değilken bir saldırı gerçekleşirse savunma tarafı hiç birşey yapamaz, yapsa da geç kalınmış olur.

3-Savunma Mekanizmaları

Güvenlik açığı ve Güvenlik güncellemeleri (patch): Bir güvenlik açığı yazılım da yada sistemdeki bir açıktır . Path ise yazılımcının hatalı veya açık kodu düzelttiği güncellemelerdir.Bunlar saldırganın gireceği kapıları kapatan birer onarım paketidir.

Kimlik ve erişim için 2FA: Verileri güvende tutmak için tek başına parola yeterli değildir çünkü çalınabilir yada tahmin edilebilir. İki faktörlü kimlik doğrulaması kişiye özel bir veri yada sadece kişinin erişim sağlayacağı bir bilgi olduğundan dolayı saldırganın her iki katmanı aynı anda ele geçirme ihtimalini imkansıza yakın hale getirir.

Tünelleme ve gizlilik VPN, SSL/TLS: VPN cihaz ile sunucu arasında şifreli bir tünel oluşturur. Trafiğinizin dışardan izlenmesini engeller fakat sizi internette tamamen görünmez kılmaz. SSL/TLS protokolü ise bu tünelin içindeki verilerin uçtan uca güvenli ve doğrulanmış şekilde taşınmasını sağlayan şifreleme motorudur.

4-Standartlar ve Süreçler

Zafiyet taraması ve pentest: Zafiyet taraması genel kapsamlı ve yüzeysel olarak otomatik araçlarla yapılan, bilinen açıkları arayan hızlı bir röntgen çekme işlemidir.

Pentest yani sızma testi bir uzman tarafından bu zafiyetleri saldırgan bakış açısıyla test eden derin ve hedef odaklı bir taramadır. Sistemi manuel olarak test eder.

Regülasyonlar (ISO,NIST,GDPR): Bu standartlar teknik birer araçtan ziyade, güvenliği sürdürülebilir kılan kurumsal birer yönetim anlayışı ve disiplin çerçevesidir. Bir mühendis bu standartları bilmelidir çünkü güvenli bir sistem inşa etmek sadece kod yazmak değil, o sistemin yasal ve etik sınırlar içerisinde yönetilmesini sağlamaktır.