BÖLÜM A: Savunma Mimarisi ve Teknoloji Entegrasyonu

1.Ağ ve Çevre Güvenliği:Ağ ve Uç Nokta Ayrımı: Ağ güvenliği; teknoloji, erişim kontrolü, şifreleme ve segmentasyonun yanı sıra çevre güvenliğini de kapsarken, uç nokta güvenliği sadece teknoloji, şifreleme ve erişim kontrolü odaklıdır.

Firewall İşleyişi: Net kurallar çerçevesinde IP, port ve servis odaklı çalışan Firewall'lar, ağ trafiğinin birincil güzergahıdır; ancak IPS'ten farklı olarak HTTP/HTTPS içeriklerini (request) filtrelemezler.

IDS (Saldırı Tespit Sistemi): Ana trafik akışının dışında konumlanan IDS, trafiğin kopyasını izleyerek potansiyel tehditleri ve protokol tutarsızlıklarını raporlar; veri iletimine doğrudan müdahale etmeden sadece uyarı ve alarm üretir.

IPS (Saldırı Önleme Sistemi): Trafiğin direkt yolunda bulunan ve güvenlik duvarından sonra yerleştirilen IPS, tehditleri otomatik eylemlerle (engelleme, bağlantı sıfırlama) durdurarak güvenlik açıklarını kapatır.IDS sistemleri, trafiği çift yönlü bir akışta izlediğinden, ağın operasyonel akışını aksatmaz. Buna karşılık, IPS sistemleri ağ performansını daha önemli ölçüde etkileyebilir.IDS'te yanlış bir alarm sadece gereksiz bir bildirim oluştururken, IPS'te yanlış bir tespit meşru trafiğin engellenmesine ve potansiyel olarak iş sürekliliğinin kesintiye uğramasına neden olabilir.Özellikle IPS sistemleri, ağ trafiğini aktif olarak işlediği için ağ performansını etkileyebilir. Yüksek trafik hacmine sahip ortamlarda, performans darboğazlarını önlemek için uygun donanım kapasitesi sağlanmalıdır.

iş birliği

Birlikte çalışabilirler. Ağ trafiği ilk önce firewall den geçer firewall verileri ıp, servis ve portuna bakarak gerekli güvenlik önlemlerini alır tehditlere karşı sonrasında ıds veri akoışını kopyalayarak kontrol eder ve IPS de kendisi üzerinden geçen ağ trafiğini kontrol eder ve gerekirse eylemlerde bulunur.

.....

Sadece IPS kullanırsanız, yanlış bir engelleme durumunda işler durabilir. Sadece IDS kullanırsanız, saldırgan içeri sızdıktan sonra sadece "haberiniz" olur. İkisini birlikte kullanarak hem kapıyı kilitler (IPS), hem de binanın içindeki her hareketi kameralarla izlemiş (IDS) olursunuz.

NDR(network detection and response) ağ trafiğini sürekli izleyen verileri toplayan ve analiz eden bir güvenlik çözümüdür. verilerin toplanmasıyla ağ trafiğindeki normal davranışlar belirlenir. Anormal bir durum (ani trafik artışı, , şüpheli protokeller, gizli bağlantılar)tespit edildiğinde ndr alarm verir ve müdahele edilmesini sağlar maksimum etkinlik için tehdit istihbaratı kaynaklarıyla çalışır. otomatik yanıtlarıyla tehditleri kontrol altına alır.Response: müdahele ilgili cihaz izole edilir bağlantı kesilir şüpheli oturum sonlandırılır firewall a otomatik kural gönderilir. NDR ile veri sızıntıları, yanal hareketler , gizli komuta kontrol bağlantıları , ransomware hazırlığı ve yayılımı , şifreli trafikte saklanan saldırılar, zero-day saldırıları, güvenlik açığı olan cihazların sömürülmesi

SSL/TLS parmak izi şifrelli bağlantılar kurulurken el sıkışma aşamsındaki parametreler analiz edilir. Belirli yazılımların kullandığı özgün şifreleme kütüphaneleri bu şekilde teşhis edilir.Güvenlik duvarları genellikle ağın giriş-çıkışını (Kuzey-Güney trafiği) kontrol eder. NDR ise ağın içindeki trafiği izler.

uç nokta tespit ve müdahele (EDR) ,

şüpheli faaliyetleri sürekli olarak izleyen ve tespit eder .Tehdit bulduğunda zarar meydana gelmeden önce tehditi yok eder.EDR makine öğrenimi ve yapay zekayla olağan dışı durumları tespit eder.Otomatik yanıt verir, virüs bulaşmış yazılımları otomatik izole eder ayrıca bir saldırının neden olduğuna dair derin içgörüler sağlar ve iyileştirme çabalarına yardımcı olur.Adli bilişim araçları ve ağ genelinde analiz imkanıyla daha geniş kapsamlı koruma sunar.

Antivirüs imza tabanlı tespit yöntemi kullanarak bilinen kötü amaçlı yazılımları hedef alır.Zararlı yazılımları kaldırma odaklıdır.Yalnızca dosya bve program bütünlüğü ile sınırlıdır. bilinen tehditlere karşı korur. (virüs,solucan ve truva atları gibi)

Dosyasız saldırıları EDR yakalar, antivirüs sadece dosya ve programlarda çalışır.

Güvenlik Operasyon Merkesi(SOC)

Modern ağlarda çok büyük veri üretilir. bu verilerdeki güvenlik tehditlerini yönetmek zordur. SOC'ta burada devreye girer.SOC, güvenlik duvarları, izinsiz giriş tespit sistemleri, izinsiz giriş önleme sistemleri, SIEM(güvenlik bilgi ve olay yönetimi) sistemleri ve tehdit istihbarat platformları gibi çesşitli kaynaklardan tehdİt verilerini toplayarak aktif bir şekilde izleme ve

uyarı yapar.7/24 bu sistem çalışır. Sürekli proaktif şekilde izleme; sürekli izleme görünürlüğü en üst seviyeye çıkarır. SOC ekibi bunun için ağı sürekli tarayan tehdit oluşturan ve oluşturmayan açık tehditleri ve anormal durumları takip eder.

SIEM nedir? (security information and event management): Yüksek doğrulukta uyarılar oluşturan araçlardır.Temelde çok çeşitli kaynaklardan veri çeken bir araçtır.Verileri bir araya getirir ve tehditleri belirlemek için sınıflandırır.SIEM, birçok kruluşun bilgisayar korsanlarına karşı kullandığı temel tehdit koruma tekmnolojisidir.SIEM sistemine loglar, tehdit istihbaratı , güvenlik açığı verileri , ağ algılama ve müdahele verileri ile uç nokta ve müdahele araçlarınızdan gelen verileri girebilirsiniz

SIEM sistemi AI,ML ve analitik ile donatılmıştır ve buradaki tüm farklı verileri gerçek zamanlı olarak(güvenlik tehditleri ortaya çıkar çıkmaz tamamlanabileceği ve yanıtlanabileceği anlamına gelebilir.)İlişkilendirerek yÜksek doğrulukta uyarılar üretecek ve bu uyarılar önem derecesine göre önceliklendirilecektir. bu uyarıları analistlerin sürekli olarak izlemesi gerekir.

SOAR(security orchestration , automation and response) nedir?:Bir şirketin veya kurumun güvenlik olaylarının yanıtlaması, tehditler ekarşı otomatik müdahelede bulunması ve önlemlerin alınmasını sağlayan çözümlerdir. bu sistemde yapay zeka ön plandadır . siem üzerinden gelen verileri otomatik olarak yönetir. herhangi bir saldırı durumunda daha hızlı bir çözümdür. soar farklı güvenlik araçlarını entegre ederek olay yönetimi sürecini 3 ana katmanda yer alır.

1. orchestration (orkestrasyon): e posta sunucusu, siem, threat intelligence, firewall /edr araçları tek bir merkezden yönetilir. farklı sistemlerr arasındaki veri ve olay akışı senkronize edilir.

2. automation(otomasyon): tekrarlayan ve rutin görevle otomatik hale getirilir. örneğin şüpheli e posta tespit edildiğinde otomatik sandbox analizi, hash kontrolü, ve url taraması yapılır. önceden tanımlanmış playbook(iş akışının) aracılığıyla makine hızında müdahele eder.

3. response(yanıt): olaylaraa anında yanıt verilir. proaktif savunma sağlnır manuel müdahele ihtiyacı en aza indirilir. saldırganın ıp sini engeller. , virüslü bilagisayar ın ağ bağlantısını keser ve şüpheli hesapları askıya alır. ayrıca bu süreci raporlar.

Genişletilmiş ve yönetilen hizmetler (büyük resim) : Yönetilen hizmetler hizmet sağlayıcı tarafından , hizmet alan işletmenin sistemlerinin uygulamalarının , network ve güvenliğinin 7/24 izlenmesini sağllar.

XDR(genişletilmiş tespit ve müdahele): gelişmiş yapay zeka ve makine öğrenimi teknolojilerinden yararlanır. farklı güvenlik katmanlarından(e posta,ağ, bulut sşstemleri, sunucular) gelen verileri gerçek zamanlı olarak toplar ve analiz eder.Otomatik ve bilinçli, risk yanıtları oluşturulur. Yanıt önlemlerini öncelik sırasına göre belirler.EDR uç noktalara odaklanırken XDR derin analiz ve otomasyon kullanarak daha çok tehditleri daha hızlı tespit etmek için bir dizi güvenlik kontrol noktasına odaklanır.

MDR: 7/24 hizmet veren siber güvenlik çözümüdür.SOC ekibi için sürekli uyarı ve sürekli çalışma yorucu bir konu olmaktadır. MDR sistemi etkinlik önceliklendirme, tehdit avcılarıyla anormal faaliyetleri ve potansiyel veri ihlali ile karşılaştıklarında sergilenen davranış türlerini tespit eder.Bu şekilde olağan dışı durumda düzeltilme yapılmasını sağlar.Tehditleri çok iyi analiz eder ve davranışları kaydederek tehdit durumlarını hızlıca tespit eder.Ayrıca sistemi iyileştirmeye çalışır.Bir tehdit oluştuğunda sistemleri, uygulamaları ve verileri saldırı gerçekleşmeden önceki haline çevirmeye çalışır.MDR saldır olduğunda reçete sunar ve eğer yetki verilirse müdahale eder.

BÖLÜM B: TEKNİK SÖZLÜK VE KAVRAM AVI

Temel Yapıtaşları ve Ağ

Transistör ve bilgisayar: Transistörler elektrik sinyallerini yükseltmek, anahtarlama yapmak ve amplifikasyon sağlamak için kullanılan bilgisayardaki çok sayıda hesaplamayı kısa sürede yapmayı sağlayan küçük elektronik cihazdır..transistörlerin basit anahatarlama işlemi bilgisyarın karmaşık işler yapabilmesini sağlar. "0-1" (mantık kapıları oluşturur) ikili dururm arasında geçiş yapar bu bilgisayarın dilidir. transistorlar bilgisayar çipinde ayrı ayrı durmazlar birbirlerine entegre bir sistem üzerine kuruludurlar. bu sayede bilgisayar kısa süre içerisinde çok karmaşık işlemeler yapabilir.

OSI vs TCP/IP: OSI modeli, ISO tarafından oluşturulan standartlaşmış bir ağ oluşturmak için 7 katmandan oluşan internet protokolü referans modelidir. TCP/IP modeli 4 katmandan oluşan bilgisayarların birbirleriyle iletişim kurmasını sağlayan internet protokolleridir. TCP/IP modelinin OSI modelinde çok daha az katman içermesi daha hızlı ve az maliyetli bir çözüm sunmuştur.TCP/IP modeli protokollere göre tasarlanan bir modelken OSI modelinde ise tam tersi durum söz konusudur. BU yüzden pratikk kullanımda TCP/IP modeli geçerlidir.

Kriptografi: Veriyi şifrelerken sadece gizli kılmaz veriye "hash" (parmak izi) ekleyerek bütünlüğünü de korur. Bütünlüğün korunması, veri gizli olsa bile üzerinde matematiksel işlemler yapılarak değiştirilmeye çalışıldığında bunu engeller böylece yanlış veri çıkışını engeller. Veri içerisinde herhangi bir değişiklikte hash değeri farklı bir değer alır.

2.Saldırı Vektörleri

Sosyal Mühendislik ve Phishing: Sosyal mühendislik, kötü amaçlı kişilerin insanları psikolojik manipülasyonlar uygulayarak bilgisayarına sızmaya çalışması, bilgi sızdırması gibi faaliyetlere hizmet etmesidir. Phishing yani oltalama ise sosyal mühendislerin sıkça kullandığı hedeflerine e-posta, sms veya sosyal medya yoluyla inandırıcı mesajlar yollayarak kandırıp istedikleri web sitesine yönlendirerek şifrelerinizi çalmaları veya cihazınıza zararlı yazılımlar yüklemesidir. Sistemler algoritmalar ve çok fazla güvenliği sağlayan araç kullanılır bu yüzden çok fazla aşılması gereken faktör vardır insanlar ise sadece psikolojik manipülasyonla hacklenebilir. Phishing bir saldırı yöntemiyken e-mail spoofing , phishing yönteminde kullanılan bir tekniktir. E-mail spoofing , e-mail de gönderen kısmında sahte isim konulmasıdır örneğin bir banka ismi.

Malware dünyası:Malware bilgisayar sistemi aksaması, veri hırsızlığı, uzaktan kontrol, virüs yüklemek gibi amaçalara hizmet eden zararlı yazılımlara denir. Ransomware ise genellikle dijital varlıklarınızın erişimini kısıtlayan ve karşılığında para teklifinde bulunan malware çeşididir.

Zero-Day: Sıfırıncı -Gün saldırısı daha önce hiç karşılaşılmamış veya düzeltilememiş güvenlik açıklarını hedef alan bir siber saldırı türüdür. Kuruluşlar bu saldırıya hazırlıksız yakalandıkları ve geleneksel savunma mekanizmalarının çalışmadığı bir saldırı olduğundan yüksek riskli bir saldırıdır.

3.Savunma Mekanizmaları(defensive terminiology)

Yama(Patch) yönetimi: Yazılım geliştiriciler tarafından yayımlanan güncelleme paketlerin tespit edilmesi elde edilmesi, test edilmesi ve dağıtım süreçlerini kontrol eden teknik bir süreçtir. Veri ihlalerinin büyük bir kısmı uygulanmamış yamalar üzerinden gerçekleştirilir bu yüzden yamalrın uygulanmaması büyük bir güvenlik açığı oluşturur.

Kimlik ve Erişim: Kullanıcıların sisteme girdiklerinde kimliklerini doğrulaması ve siteme erişimini kapsar. Parola güvenlik içinne genelde pek yeterli olmaz çünkü insanlar genelde unutmamak için kolay şifreler belirler ayrıca 2 aşamalı kimlik doğrulama parolanın yanında bildiğiniz bir şey veya sahip olduğunuz bir şey veya sizinle kimliğinizle ilgili bir şey belirleyerek erişimi çok daha güvenli kılar.

Tünelleme ve Gizlilik: Tünelleme bir veri paketinin başka bir protokol paketine kapsüllenerek güvenli bir şekilde taşınmasıdır. VPN, gerçek IP adresinizi ve veri içeriğinizi tünelin bir ucunda paketlenir ve şifrelenir güvenli bir şekilde istenen adrese akatarılması SSL/TLS

sayesinde gerçekleşir, ISS sadece VPN sunucusuna yoğun veri akışı olduğunu görür. VPN den çıktıktan sonra veri trafiğiniz "açık internet"e dökülür.

Web siteleri çerezlerden veya oturumunuzdan sizi tanıyabilir.

4.Standartlar ve Süreçler

Zafiyet Taraması: Zafiyet taraması birtakım araçlar(Nessus, OpenVAS,..) kullanarak güvenlik açıklarını otomatik olarak tespit eden ve yöneticilere sunan güvenlik taramasıdır. Sızma testi ise bir siber güvenlik uzmanının zafiyet taramasındaki verileri de göz önünde bulundurarak sistemi manuel yöntemlerle ele geçirmeye çalışmasıdır.Sızma testi hem otomatik hem manuel olarak işlemlerini gerçekleştirir.

Regülasyonlar:Regülasyon, bir alanın işleyişi için gerekli olan kural, yasa ve denetimlerin bütünüdür. ISO27001, NIST veya GDPR gibi standartlar teknik birer araç değil, birer yönetim anlayışıdır. GDR , Avrupa Birliği'nin kişisel verilerri koruma regülasyonudr. ISO27001 , organizasyonların, kurumların bilgi güvenliği yönetim sistemini oluşturullmasını sağlayan uluslararası bir regülasyondur. NIST, siber güvenliği 5 ana fonksiyonla yöneten bir regülasyondur. Mühendislerin bu standartları bilmesi, sistemleri en baştan güvenli, yasalara uyumlu ve finansal cezaların önünü alarak projeler geliştirmesini sağlar.

BÖLÜM C:CTI ve İstihbarat odaklı Vaka Analizi(45.128.232.67 IP adresi şüpheli bir trafik oluşturuyor.)

1.Adım:Pasif İstihbarat Toplama(CTI):

Kimlik Tespiti: IP adresinin Hollanda kaynaklı olduğunu ve Anton Levin adlı organizasyona ait olduğunu gördüm.

Sicil Kaydı: 93 güvenlik sağlayıcısından 4 ü bu IP adresini malware olarak işaretlemiş. 2 tanesi şüpheli olduğunu bildirmiş. Phishing saldırı türünü kullanmış.

Zaman Çİzelgesi: Bu veriler son 1 ayın kayıtlarıdır.

2.Adım : Termonoloji ve Yapılandırma(APPLİED Concepts)

IOC (Indicator of Compromise): Bir cihaza yapılan saldırı ya da tehdit göstergesine IOC denir, buradaki IOC'lar phishing veya malware yazılım olarak işaretlenmiş 45.128.232.67 bu

IP adresi bir IOC'tur ancak IOC sadece IP adresi değildir bu IP adresi üzerinden ulaşılan URL veya indirilen bir dosya (hash) IOC olabilir.

IP: 45.128.232.67

ASN: AS50053

Country: NL (Netherlands)

Threat Category: Phishing, Malware,C2

CTI(Cyber Threat Intelligence): IP adresinin sicil kaydığına baktığınızda 4 güvenlik sağlayıcısı malware veya phishing yöntemleriyle bu IP adresi tarafından saldırya uğramıştır. Bu veriler de IP adresine şüpheyle yaklaşmamız gerektiğini gösterir.

MISP(Malware Information Sharing Platform): IP adresinde Ransomware keşfettim ve bunu MISP platformunda paylaştım. Çünkü bu şekilde zararlı bir IP adresini duyurarak cihazların bu adrese karşı önlem almasını ve bir ihtimal çok farklı yöntemleri olan bir hacker olduğunu varsayalım mavi takım gibi kuruluşların bu tehditi inceleyerek önlem almalarını ve savunmalarını geliştirmelerini sağlayabiliriz.

3.Adım: Karar ve Aksiyon

Karar: Bu adresi engelle kararı verilir.

Gerekçe: Bu IP adresi araştırıldığında Cobalt Strike (C2) sunucusu olarak bilinen kurgusal karakter olan Anton Levin'e aittir , bu yöntem saldırganlar tarafından sıkça tercih edilir çünkü bulletproof hosting kategorisindedir yani saldırganı korur. Aynı zamanda IP adresinin phishing veya malware saldırıda bulunduğu da bilinmektedir.

BÖLÜM D: Kriz Yönetimi ve Olay Müdahale Refleksleri

1.Senaryo: Fidye Yazılımı (Ransomware) Kıyameti

Acil Müdahale: İnternet bağlantısını keserek fideye yazılımın yayılmasını engellerim. Cihazda virüs taraması yaparak tehditleri görürüm. Kötü amaçlı dosyaları silerim. Yedeklemelerimi geri yüklerim.

Analiz: Sisteme nasıl girdiğini anlamak için e-postaları, RDP (uzak masaüstü protokolü) , ziyaret edilen web siteleri kontrol ederim.

2.Senaryo: Oltalama(Phishing) Dedektifliği

Teknik İnceleme: E- postanın IP adresine bakarak (SPF) gönderme yetkisi olup olmadığını kontrol ederim. DKIM , göndericinin dijital imzasının değiştirilip değiştirilmediğini gösterir bunu kontrol ederim. URL yapısına bakarak taklit mi yoksa gerçek mi olduğunu teyit ederim.

Önlem: Göndericiyi E-mail Gateway ile "Blacklist"e eklerim. E- posta içindeki URL'ye URL filtreleme kuralıyla kurum içinde erişilemez hale getiririm.

3.Süreç ve İletişim:

Standartlar :NIST uluslararası standartına dayanarak ; hazırlık, tespit, sınırlama, temizleme ve kurtarma adımlarını takip ederiz.

Kriz İletişimi: Görev paylaşımı yaparak sürecin daha düzenli ilerlemesini ve belirli aralıklarla ya da yeni gelişmelerle durum bildirimi yapılmasını sağlarım.

4.Vizyon

Sürekli değişen gelişmeleri takip etmek için medium, tryhackme, cyberwire daily takip edilebilecek kaynaklardandır.