Bölüm A: Savunma Mimarisi ve Teknoloji Entegrasyonu

1. Ağ ve Çevre Güvenliği (Sınır Hattı)

- Firewall ile IDS/IPS'in Rol Ayrımı ve İş Birliği

- Firewall, hangi trafiğin ağa girebileceğini belirler. IDS, Firewall'un izin verdiği trafiğe erken uyarı ve görünürlük sağlarken IPS, bu trafiğin engelleme ve aksiyon tarafına bakar. Böylece ağın güvenliği katmanlı ve dengeli bir savunma yapısında korunur.
  - NDR (Network Detection and Response) Trafik şifreli olsa bile veya Firewall atlatılsa bile, NDR ağ içindeki anormallikleri nasıl yakalar?
- Şifreli trafikte NDR, paketin içeriğini okumadan iletişimin nasıl gerçekleştiğine odaklanır. Böylece alışılmadık iletişim paternlerini analiz ederek, şifre çözülmese bile ağ içindeki olası saldırı faaliyetlerini ortaya çıkarır. Kısaca NDR ağda şifreleme ile görünmez hale gelen saldırılara karşı ağ içindeki iletişimlere bakarak tehdit algılayıcılık sağlar.

2. Uç Nokta Savunması (Son Kale)

- Antivirüs vs EDR: Klasik bir Antivirüs imza tabanlı çalışırken, EDR (Endpoint Detection and Response) davranışsal olarak nasıl fark yaratır? "Dosyasız saldırıları" (Fileless Malware) hangisi yakalar?

- Antivirüs, daha önce tanımlanmış zararlı dosyalar için etkilidir; ancak modern saldırılarda yetersiz kalır. Bu tür durumlarda saldırgan, dosyasız da sistem üzerinde kalıcılık sağlayabildiği için, imza tabanlı tespit mekanizmaları bu durumu anlayamaz. EDR'nin farkı, dosya veya olaydan ziyade davranış zincirini değerlendirmesidir. Böylece dosyasız saldırılar da EDR ile yakalanmış olur.

3. Operasyon Merkezi ve Görünürlük (Beyin Takımı)

- SOC & SIEM: Firewall, EDR ve Sunuculardan gelen binlerce log (kayıt), SIEM üzerinde nasıl anlamlı bir alarma dönüşür? SOC analisti bu ekranda ne görür?

- Önceki aşamalarda üretilen loglar incelendiğinde büyük ve karmaşık veriler taşımaktadır. Burada SIEM'in rolü, farklı aşamalardan gelen büyük ve karmaşık veriyi ana yapıda toplayıp basitleştirerek ve ilişkilendirerek ham veriyi anlamlı bir alarma dönüştürmektir. SOC analistinin ekranda gördüğü şey, karmaşık log satırları değil önceliklendirilmiş olaylar, zaman çizelgeleri ve ilişkilendirilmiş göstergelerdir. SOC Analisti, ekrandan saldırının hangi kaynaktan başladığını, hangi sistemleri etkilediğini, hangi güvenlik kontrollerinin tetiklendiğini ve sürecin devam edip etmediğini izleyebilir.

- SOAR: Tespit edilen bir tehdide insan müdahalesi olmadan otomatik cevap vermek için SOAR nasıl kullanılır?

- SOAR, güvenlik sistemlerinden gelen uyarılara otomatik olarak cevap verilmesini sağlar. Mesela bir phishing maili tespit edildiğinde, SOAR bu maili diğer kullanıcılardan silebilir, IP'yi firewall'da engelleyebilir ve gerekirse kullanıcının bilgisayarını izole edebilir. Böylece olay için insan müdahalesi gerekmez ve saldırı hızlıca durdurulur.

4. Genişletilmiş ve Yönetilen Hizmetler (Büyük Resim)

    - XDR (Extended Detection and Response): EDR sadece bilgisayara, NDR sadece ağa bakarken; XDR bu ikisini ve daha fazlasını (E-mail, Cloud) nasıl birleştirir?
- XDR, çeşitli güvenlik araçlarının tek tek gördüğü olayları toplayarak büyük resmi görmeyi sağlar. EDR uç noktadaki hareketleri, NDR ağ trafiğini izlerken XDR bunları E-mail ve Cloud ortamlarından gelen verilerle birleştirir. Böylece tek başına masum görünen olaylar değerlendirildiğinde bir saldırı zinciri olarak anlaşılır ve tehdit daha erken fark edilir.

<u>Bölüm B: Teknik Sözlük ve Kavram Av</u>

1. Temel Yapıtaşları ve Ağ

    - Transistör & Bilgisayar: Transistörlerin açılıp kapanması (0-1) ile modern işletim sistemlerinin çalışması arasındaki bağ
- Transistörlerin açılıp kapanmasıyla oluşan 0 ve 1'ler, bilgisayarların temelini oluşturur. Modern iletişim sistemleri bu basit sinyalleri kullanarak bellek yönetimi, işlemci zamanlaması ve donanım–yazılım iletişimi gibi süreçleri yönetir.

    - OSI vs TCP/IP: OSI modeli teorik bir referans iken, TCP/IP neden günümüz internetinin pratik temelidir?
- OSI modeli, ağın nasıl çalıştığı mantığını anlamak için kullanılan teorik referanstır ancak TCP/IP gerçek ağ trafiğinde kullanılan protokolleri içerdiği için bugünün internetinin temelidir.

    - Kriptografi: Veriyi şifrelemek neden sadece gizlilik için değil, aynı zamanda veri bütünlüğü (integrity) için de önemlidir?
- Kriptografi, veriyi şifreleyerek başkası tarafından okunmasını engellemek için vardır. Aynı zamanda verinin aktarımı sırasında değiştirilip değiştirilmediğini anlamamıza yardımcı olduğundan dolayı veri bütünlüğünü için önemlidir.

2. Saldırı Vektörleri (Offensive Terminology)

- Sosyal Mühendislik & Phishing: Bir sistemi hacklemek yerine insanı hacklemek (Social Engineering) neden daha kolaydır? Phishing ve E-mail Spoofing arasındaki teknik fark nedir?

- Sosyal mühendislik, karmaşık güvenlik önlemlerini aşmak yerine insanların güvenini kazanıp hacklediği için genelde daha kolaydır. Phishing, kullanıcıyı sahte link veya içerikle kandırmaya çalışırken E-mail spoofing, e-postanın gönderici adresini taklit ederek mesajın güvenilir görünmesini sağlar.

- Malware Dünyası: Genel bir terim olan Malware ile özel bir tehdit olan Ransomware (Fidye Yazılımı) arasındaki fark nedir?

- Malware, bilgisayara zarar vermek veya izinsiz işlem yapmak amacıyla kullanılan tüm zararlı yazılımlar için genel bir terimdir. Ransomware ise bu zararlı yazılımların dosyaları şifreleyerek fidye talep eden özel bir türüdür

- Zero-Day (Sıfır Gün): Bir zafiyetin "Zero-Day" olarak adlandırılması, savunma tarafı için neden bir kabustur?

- Bir zafiyetin zero-day olarak adlandırılması, henüz üretici tarafından bilinmediği anlamına gelir. Bu yüzden savunma tarafı neyi engellemesi gerektiğini tam olarak bilmediği için saldırıları önlemek zorlaşır.

3. Savunma Mekanizmaları (Defensive Terminology)

- Yama (Patch) Yönetimi: Güvenlik güncellemelerini (Patch) zamanında yapmamak ile Güvenlik Açığı (Vulnerability) oluşması arasında nasıl bir ilişki vardır?

- Güvenlik yamaları, sistemlerdeki açıkları kapatmak için yayınlanır. Bu güncellemeler zamanında yapılmadığında bilinen açıklar sistemde kalır ve saldırganlar tarafından istismar edilebilir.

- Kimlik ve Erişim: Parola neden yetmez?İki Faktörlü Kimlik Doğrulama (2FA) güvenliği matematiksel olarak nasıl artırır?

- Parola tek başına yeterli değildir çünkü çalınabilir, tahmin edilebilir veya başka sistemlerden sızdırılmış olabilir. İki faktörlü kimlik doğrulama (2FA), parolaya ek ikinci bir doğrulama gerektirdiği için saldırganın şifreyi kırma ihtimalini ciddi şekilde düşürür.

- Tünelleme ve Gizlilik: VPN (Sanal Özel Ağ) kullanmak bizi internette tamamen görünmez yapar mı, yoksa sadece tünel mi oluşturur? SSL/TLS protokolü bu tünelin neresindedir?

Tabii ki VPN kullanmak bizi internette tamamen görünmez yapmaz, sadece internet trafiğimizi şifreli şekilde geçirir. SSL/TLS ise verinin uçtan uca güvenli şekilde şifrelenmesini sağlayan protokoldür

4. Standartlar ve Süreçler

- Zafiyet Taraması: Ağ zafiyet taraması yapmak ile Sızma Testi (Pentest) yapmak arasındaki temel fark nedir?

- Ağ zafiyet taraması, sistemde bilinen güvenlik açıklarını otomatik araçlarla tespit etmeye odaklanır. Sızma testi (pentest) ise açıkların gerçekten istismar edilip edilemeyeceğini manuel şekilde tespit etmeyi amaçlar.

- Regülasyonlar: ISO 27001, NIST veya GDPR gibi standartlar teknik birer araç mıdır, yoksa bir yönetim anlayışı mıdır? Bir mühendis neden bunları bilmelidir?

- ISO 27001, NIST ve GDPR gibi standartlar tamamen teknik araçlar değil, kurumların güvenliği nasıl yöneteceğini belirleyen birer yönetim çerçevesidir. Bir mühendis bu standartları bilirse, yaptığı teknik işlerin şirket politikaları ve risk yönetimiyle uyumlu olmasını sağlar.

<u>Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi</u>

1. Adım: Pasif İstihbarat Toplama (CTI)

SOC ekibindeki nöbetim sırasında, sorumluluğumdaki kritik bir sunucunun 45.128.232.67 IP adresi ile şüpheli bir trafik oluşturduğunu tespit ettim.

AbuseIPDB kullanarak aşağıda yer alan kimlik tespiti verilerini elde ettim.

SP	ndividual Entrepreneur Anton Levin
Usage Type	Data Center/Web Hosting/Transit
ASN	AS50053
Domain Name	nterlir.com
Country	NL Netherlands
City	Amsterdam, North Holland

Sicil Kaydı:

Bu IP AbuseIPDB raporlarında daha önce SSH brute-force saldırılarında kullanılmış.

Zaman Çizelgesi:

Bu IP ile ilgili AbuseIPDB'de en son raporlama 2025-07-24 00:06:09 tarihinde gerçekleşmiş bu yüzden aktifliği azalıyor olabilir.

2. Adım: Terminoloji ve Yapılandırma (Applied Concepts)

Bu senaryoda IOC, kritik sunucunun geçmişte SSH brute-force saldırılarıyla ilişkilendirilmiş olan 45.128.232.67 IP adresiyle şüpheli bir iletişim kurmasıdır.

- CTI (Cyber Threat Intelligence):

- 45.128.232.67 IP adresi, geçmişte SSH brute-force saldırılarıyla ilişkilendirilmiş ve bir veri merkezi altyapısında barındırılan bir adres olarak öne çıkmaktadır. Bu tür altyapılar saldırganlar tarafından sıklıkla geçici saldırı kaynakları veya komuta altyapıları olarak kullanılabilmektedir.
- Bu IP'nin şirket bünyesindeki kritik bir sunucuyla şüpheli bir iletişim kurmuş olması, bu trafiğin meşru bir iş akışından ziyade olası bir yetkisiz erişim denemesi veya saldırı öncesi keşif faaliyeti olabileceğini düşündürmektedir. Bu bağlamda IP, şirket için operasyonel ve güvenlik riski oluşturmaktadır.

- MISP (Malware Information Sharing Platform):

- Bu IP'nin yeni bir Fidye Yazılımı (Ransomware) yaydığını tespit edilmesi durumunda, bu bilginin MISP gibi platformlarda yayınlanması diğer kurumların aynı IP'yi kendi güvenlik sistemlerinde erken aşamada tespit edip engellemesine olanak sağlar.

3. Adım: Karar ve Aksiyon (Actionable Intelligence)

Karar: Engelle

Gerekçe:

Bu IP'nin şirket bünyesindeki kritik bir sunucuyla şüpheli bir iletişim kurmuş olması, trafiğin meşru bir iş ihtiyacından ziyade olası bir yetkisiz erişim denemesi veya saldırı öncesi keşif faaliyeti olabileceğini düşündürmektedir. Kritik varlıklar için risk toleransının düşük olması gerektiği göz önünde bulundurularak, potansiyel tehditlerin önlenmesi amacıyla IP adresinin ağ seviyesinde engellenmesi uygun görülmüştür.

Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

1. Senaryo: Fidye Yazılımı (Ransomware) Kıyameti:

Ben olsaydım, kullanıcıdan fidye yazılımı belirtisi geldiğinde önce bilgisayarı kapatmadan ağ bağlantısını keserdim, böylece virüsün başka bilgisayarlara yayılmasını önlerdim. Daha sonra bunun sadece bu bilgisayarda mı yoksa başka sistemlerde de mi olduğunu anlamak için hızlıca kontrol yapardım. Son olarak zararlının nasıl bulaştığını anlayabilmek için e-posta kayıtlarına, bilgisayarda hangi programların çalıştırıldığına ve uzak bağlantı (VPN/RDP) loglarına bakarak inceleme başlatırdım.

2. Senaryo: Oltalama (Phishing) Dedektifliği:

Ben olsaydım, CEO'dan gelmiş gibi görünen e-postanın sahte olup olmadığını anlamak için önce e-posta header bilgilerine bakar, mailin gerçekten şirket adına bir sunucudan gelip gelmediğini kontrol ederdim. Ardından e-postadaki linkleri tıklamadan URL adresini inceler, garip bir alan adı olup olmadığına bakardım. E-postanın oltalama olduğu anlaşılırsa, diğer çalışanlara da gitmemesi için Email Gateway üzerinde gönderici adresi veya linki engelleyen bir kural yazarak önlem alırdım.

3. Süreç ve İletişim:

Ben olsaydım, olay müdahale sürecini NIST Olay Müdahale Yaşam Döngüsüne göre yürütürdüm; yani önce hazırlık yapar, olayı tespit eder, yayılmasını sınırlar, sistemi temizler ve en son güvenli şekilde tekrar çalışır hale getirirdim. Saldırı sırasında ortam gergin olduğunda ise ekip içinde paniği önlemek için herkesin ne yaptığını netleştirir, yönetimi de teknik detaya boğmadan, kısa ve düzenli aralıklarla "ne oldu, ne yapıyoruz, risk nedir" şeklinde açık ve sakin bir dille bilgilendirirdim.

4. Vizyon: Güncel Kalma Sanatı

Siber güvenlik alanında güncel kalmak için ağırlıklı olarak r/blueteamsec kanalını takip ediyorum. Bunun yanında, sistem yönetimi ve gerçek vaka paylaşımları açısından r/sysadmin kanalındaki gönderiler de ilgimi çekiyor. Ayrıca farklı konularda bakış açısı kazanmak için çeşitli siber güvenlik bloglarını düzenli olarak okumaya çalışıyorum; ancak şu an için belirli tek bir bloga bağlı kaldığımı söyleyemem.