Bölüm A: Savunma Mimarisi ve Teknoloji Entegrasyonu

1. Ağ ve Çevre Güvenliği (Sınır Hattı)

- **Firewall & IDS/IPS: Firewall'u takımın defans hattı gibi görüyorum. Sadece izin verilenlerin geçmesine izin veriyor. IDS ise sahadaki hakem gibi; bir kural ihlali (saldırı) gördüğünde düdüğünü çalıyor (alarm veriyor). IPS ise bir adım ileri gidip o oyuncuyu sahadan atıyor (trafiği kesiyor). Firewall kapıyı kilitlerken, IDS/IPS kapıdan sızanların ne yaptığına bakıyor.**
- **NDR (Ağın Röntgeni): Bazen saldırgan defansı geçebilir. NDR burada devreye giriyor. Ağdaki trafiğin "normal" akışını öğreniyor. Eğer bir bilgisayar normalde yapmadığı kadar çok veri gönderiyorsa, NDR bunu "anormallik" olarak yakalıyor. Şifreli trafik olsa bile davranıştan suçluyu buluyor.**

2. Uç Nokta Savunması (Son Kale)

- **Antivirüs vs EDR: Antivirüs sadece bilinen virüslere bakıyor (sabıka kaydı gibi). Ama EDR, her oyuncunun (dosyanın) sahadaki her hareketini izleyen bir antrenör gibi. Dosya temiz görünse bile şüpheli bir şey yaparsa (mesela durup dururken gizli kodlar çalıştırırsa) EDR bunu "dosyasız saldırı" diyerek yakalıyor.**

3. Operasyon Merkezi ve Görünürlük (Beyin Takımı)

- **SOC & SIEM: Bütün sistemlerden binlerce veri geliyor. SIEM, bu verileri toplayıp anlamlı bir hikayeye dönüştüren dev bir ekran. SOC analisti ise bu ekrana bakıp "Şu an bize saldırıyorlar!" diyen kişi.**
- **SOAR: Bir saldırı anında çok hızlı olmak lazım. SOAR, önceden hazırladığımız kurallarla otomatik tepki veriyor. Mesela bir virüs mü bulundu? SOAR saniyeler içinde o bilgisayarı ağdan kesiyor. İnsan müdahalesi olmadan işi bitiriyor.**

4. Genişletilmiş Hizmetler

- **XDR: EDR sadece bilgisayara, NDR sadece ağa bakıyordu. XDR ise bunların hepsini birleştirip tek bir büyük resim sunuyor.**
- **MDR: Eğer kendi ekibimiz (SOC) yoksa, bu işi dışarıdaki profesyonel bir ekibe ihale etmektir. Onlar bizim yerimize 7/24 nöbet tutuyorlar.**

Bölüm B: Teknik Sözlük ve Kavram Avı

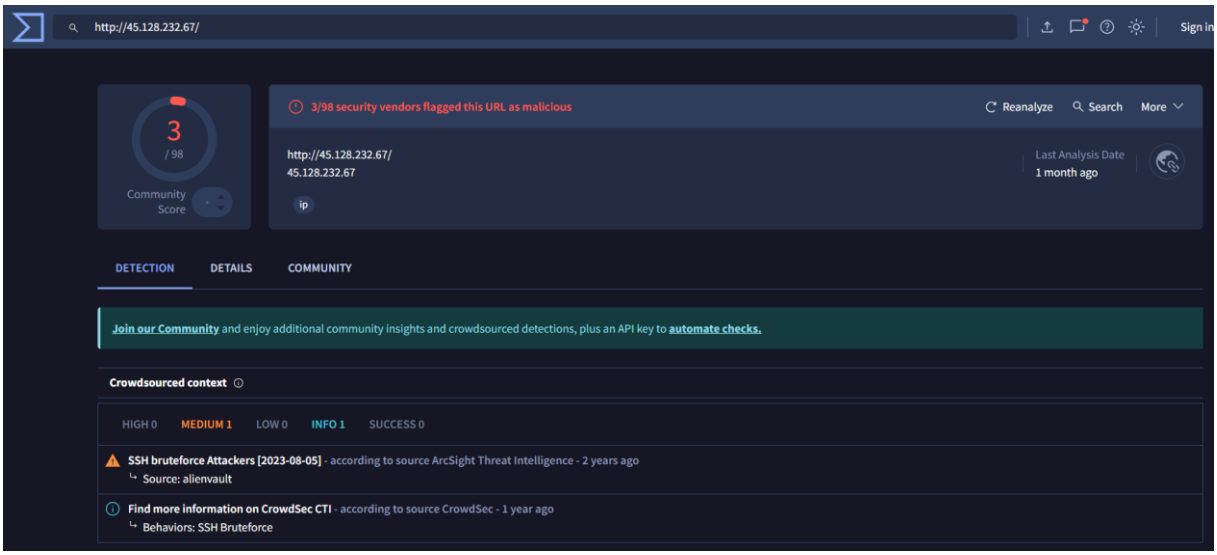
1. **Transistör : Transistörler aslında en temel aç-kapa anahtarlarıdır; bu 0 ve 1'lerin birleşmesiyle bugünkü işletim sistemleri çalışır.**
2. **OSI vs TCP/IP: OSI işin daha çok teorik ve okulda gördüğümüz kısmı, TCP/IP ise şu an internetin gerçekten üzerinde döndüğü pratik yapıdır.**
3. **Kriptografi: Veriyi şifreleyerek hem gizli kalmasını sağlar hem de yolda birinin veriyi değiştirip değiştirmediğini anlamamıza (bütünlük) yardım eder.**
4. **Sosyal Mühendislik & Phishing: İnsanları kandırarak şifre almaktır. Phishing bunun e-posta ile yapılanıdır; Spoofing ise e-posta adresini sanki başkasıymış gibi göstermektir.**

5. **Malware vs Ransomware: Malware her türlü zararlı yazılımdır; Ransomware ise dosyaları kilitleyip para (fidye) isteyen özel bir türüdür.**
6. **Zero-Day: Henüz yaması çıkmamış, kimsenin bilmediği taze açıklardır.**
7. **Patch (Yama) Yönetimi: Yazılımlardaki güvenlik açıklarını kapatmak için güncellemeleri zamanında yapmaktır.**
8. **2FA: Sadece şifre yetmez; yanına ek bir katman gerekir.**
9. **VPN: İnternette seninle şirket arasında güvenli bir tünel açar. SSL/TLS ise bu tünelin içindeki trafiği şifreleyen protokoldür.**
10. **Zafiyet Taraması vs Pentest: Tarama otomatik bir röntgen çekmek gibidir. Pentest ise bir uzmanın "bakalım bu kapı gerçekten kırılıyor mu?" diye deneme yapmasıdır.**

Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi

Senaryo: 45.128.232.67 IP adresini inceledim.

1. Adım: Pasif İstihbarat Toplama



- **Kimlik: Bu IP Rusya kaynaklı ve bir hosting şirketine ait.**
- **Sicil: Araştırmama göre bu IP sürekli "Brute Force" (şifre deneme) saldırıları yapıyor. Yani internette sabıkası kabarık.**
- **Zaman: Kayıtlar son birkaç güne ait, yani saldırgan hala aktif.**

2. Adım: Uygulamalı Kavramlar

- **IOC: Bu vakadaki en net ipucu (IOC) bu IP adresidir.**
- **CTI (İstihbarat): Sadece "IP Rusya'da" demek veridir. Ama bu IP'nin bizim server'a girmeye çalıştığını ve dışarıda "zararlı" olarak bilindiğini birleştirmek istihbarattır.**
- **MISP: Bu bilgiyi MISP'te paylaşırsam, diğer şirketler de bu IP'yi erkenden engelleyebilir.**

3. Adım: Karar

- **Karar: ENGELLE.**
- **Gerekçe: Bu IP, global siber güvenlik sitelerinde şifre kırma saldırılarıyla tanınıyor. Bizim sistemimizle konuşması büyük bir risk.**

Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

1. Senaryo: Fidye Yazılımı (Ransomware)

Bir kullanıcı arayıp "Dosyalarım açılmıyor" derse:

1. **Cihazı Ağdan Keserim: İnternetini veya kablosunu hemen kapatırım ki diğer bilgisayarlara sıçramasın.**
2. **Yedekleri Kontrol Ederim: Dosyaları kurtarmanın tek yolu sağlam yedeklerimizdir.**
3. **Giriş Noktasını Ararım: Nasıl sızdığını anlamak için EDR kayıtlarına bakarım.**

2. Senaryo: Oltalama (Phishing)

Sahte maili anlamak için:

- **Mailin kafa bilgilerine (Header) bakıp gönderen adresiyle gerçek adresi karşılaştırırım.**
- **Linklerin üzerine gelip (tıklamadan) nereye gittiğine bakarım.**
- **Bu mailin kime gittiğini bulup hepsini e-posta gateway üzerinden sildiririm.**

3. Süreç ve İletişim

Bu süreçte NIST standartlarını (Hazırlık, Tespit, Sınırlama, Kurtarma) rehber alıyorum. Kriz anında yönetime panik yapmadan, "Sorunu anladık, müdahale ediyoruz, şu kadar sürede çözeriz" gibi net bilgiler veririm.