A1.Firewall & IDS/IPS: Kapıdaki kilit (Firewall) ile harekete duyarlı alarm (IDS/IPS) arasındaki farkı ve iş birliğini açıklayın. Biri engellerken diğeri neden sadece izler

Cevap:

Firewall dışardan içeriye ya da içerden dışarıya olan trafiği kontrol eder ve yetkisiz olanları engeller (kalenin dışındaki muhafızlar).

IDS ise içeriye giren paketin davranışlarını inceler ve şüpheli bir davranış görürse alarm verir (kaledeki gözcüler).

IPS ise hem alarm hem de engelleme yetkisine sahiptir (kalenin içindeki muhafızlar).

A1.NDR (Network Detection and Response): Trafik şifreli olsa bile veya Firewall atlatılsa bile, NDR ağ içindeki anormallikleri (Örn: Yan ağa sıçrama) nasıl yakalar?

Cevap:

NDR iç ağda bulunur içerdeki cihazların davranışlarına bakarak anormalikleri tespit eder. (Kalenin içinde gezen sivil devriyeler).

A2.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?

Cevap:

Antivirüs önceden belirlenmiş imza tabanlı kayda bakarak tespit eder (Aranıyor broşürleri).

EDR ise çalışma mantığı şudur mesela bir exel tablosunun cmd veya powrshell çalıştırması gibi garip olayları inceleyerek tehdidi algılar (Hazine odasına girmeye çalışan köylü).

Bu nedenle Antivirüslerin veri merkezinde bu dosya önceden yakalanmadıysa o dosyayı yakalayamaz ama EDR davranışlarına bakarak bunları bulabilir.

A3.SOC & SIEM: Firewall, EDR ve Sunuculardan gelen binlerce log (kayıt), SIEM üzerinde nasıl anlamlı bir alarma dönüşür? SOC analisti bu ekranda ne görür?

Cevap:

SIEM firewall, EDR, sunucular gibi yerlerden tonlarca log toplar bu loglar firewall EDR, IDS/IPS gibi sistemlerle tahlikeli olanlar işaretlenir bunlarıda SOC analistlerin ekranına düşer.

A3.SOAR: Tespit edilen bir tehdide (Örn: Phishing maili) insan müdahalesi olmadan otomatik cevap vermek (IP engellemek, kullanıcıyı izole etmek) için SOAR nasıl kullanılır?

Cevap:

SOAR a belirli kurallar yazılır mesela phising olayı olduysa sırayla maili sil ve gönderen ip yi engelle gibi(şehirde suçlu tespit edilirse askerlerin sırayla yapıckları).

A4.XDR (Extended Detection and Response): EDR sadece bilgisayara, NDR sadece ağa bakarken; XDR bu ikisini ve daha fazlasını (E-mail, Cloud) nasıl birleştirir?

Cevap:

EDR, NDR, E-mail, Claoud ayrı ayrı alarmlar üreticek ama XDR bu iki alarmı tek bir saldırının adımı olarak düşünücek bu sayede nokta atışı tespit edilip önlem alınabilcek.

A4.MDR (Managed Detection and Response): Şirketin kendi SOC ekibi yoksa veya yetersizse, MDR hizmeti bu boşluğu insan kaynağı ve uzmanlık olarak nasıl doldurur?

Cevap:

MDR dışardan gelen bir uzman ekiptir (Paralı Asker).

Bu yüzden SOC ekibi yoksa MDR o firmaya SOC ekibi gibi destek sağlar.

B1.Transistör & Bilgisayar: En temelden başlarsak; transistörlerin açılıp kapanması (0-1) ile modern işletim sistemlerinin çalışması arasındaki bağı nasıl kurarsınız?

Cevap:

Transistörlerin açılıp kapanmasıyla oluşan mantık devreleriyle, donanımla ve işletim sisteminin birleşmesiyle modern işletim sistemi oluşur. (Açıksa 1, Kapalıysa 0)

B1.OSI vs TCP/IP: OSI modeli teorik bir referans iken, TCP/IP neden günümüz internetinin pratik temelidir?

Cevap:

OSI modeli daha rahat anlaşılması için oluşturulmuştur ama TCP/IP internetin genel kuralarıdır.

TCP/IP, merkezi kontrol olmadan, hatalara dayanıklı ve ölçeklenebilir şekilde konuşturabildiği için günümüz internetinin pratik temelidir.

B1.Kriptografi: Veriyi şifrelemek neden sadece gizlilik için değil, aynı zamanda veri bütünlüğü (integrity) için de önemlidir?

Cevap:

Veriyi şifrelemek sadece yanlış kişilerin eline düşmesini engellemez bir de veri bütünlüğü sağlar bu sayede karşı tarafa ileti tam olarak gitmesini sağlar. Bunu yaparken dijital imza ve hash değerleri kullanır.

B2.Sosyal Mühendislik & Phishing: Bir sistemi hacklemek yerine insanı hacklemek (Social Engineering) neden daha kolaydır? Phishing ve E-mail Spoofing arasındaki teknik fark nedir?

Cevap:

İnsanları kandırıp rahatlıkla bilgisayar şifrelerini alabilirsiniz ama bilgisayarı hacklemek için bir ton aşamdan geçmeniz gerekir.

Phishing kullanıcıyı sahte içeriklerle kandırarak hassas bilgilerini ele geçirmeyi amaçlayar, E-mail Spoofing ise gönderen kişiyi önemli birinden gelmiş gibi yaparak kandırır.

B2.Malware Dünyası: Genel bir terim olan Malware ile özel bir tehdit olan Ransomware (Fidye Yazılımı) arasındaki fark nedir?

Cevap:

Malware zararlı yazılımların genel adıdır. Ransomware ise dosyaları şifreleyerek fidye isteyen bir yazılımdır.

B2.Zero-Day (Sıfır Gün): Bir zafiyetin "Zero-Day" olarak adlandırılması, savunma tarafı için neden bir kabustur?

Cevap:

Zero-Day bulunamayan açıklardır bu yüzden saldırının nerden geleceği belli olmaz bu yüzden tam bir kabustur.

B3.Yama (Patch) Yönetimi: Güvenlik güncellemelerini (Patch) zamanında yapmamak ile Güvenlik Açığı (Vulnerability) oluşması arasında nasıl bir ilişki vardır?

Cevap:

Patchlerin zamanında yapılmaması güvenlik açıkların kapanmamasına neden olur o yüzden tehlikelidir.

B3.Kimlik ve Erişim: Parola neden yetmez? İki Faktörlü Kimlik Doğrulama (2FA) güvenliği matematiksel olarak nasıl artırır?

Cevap:

Parolanın kırılma ihtimali: 1 / 1.000 olsun

OTP kodunun tahmin edilme ihtimali: 1 / 1.000.000 olsun

1 / 1.000 × 1 / 1.000.000 = 1 / 1.000.000.000 olur. Daha düşük bir ihtimale sahip olur.

B3.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?

Cevap:

VPN sadece tünel(IP gizler, trafiği şifreler) oluşturur ve nereye baktığını gizler.

SSL/TLS ise uygulama seviyesinde yapar. (kullanıcı→vpn→ssl/tls)

B4.Zafiyet Taraması: Ağ zafiyet taraması yapmak ile Sızma Testi (Pentest) yapmak arasındaki temel fark nedir? (Biri otomatik, biri manuel mi?)

Cevap:

Zafiyet Taraması otamatiktir genellikle araçlarla yapılır. (Nesus,OpenVas vb.)

Pentest ise manuel dir çünkü insan + araç kullanır. Araçlar açıkları bulur insan oraya sızmayı dener.

B4.Regülasyonlar: ISO 27001, NIST veya GDPR gibi standartlar teknik birer araç mıdır, yoksa bir yönetim anlayışı mıdır? Bir mühendis neden bunları bilmelidir?

Cevap:

Bir yönetim anlayışıdır ve izlenmesi gereken kurallar bütünüdür bir mühendis bunları güvenlik süreçlerin tam olarak uygulanması için bilmelidir.

C1.Kimlik Tespiti: Bu IP adresi hangi ülkeye ve hangi organizasyona (ISP/ASN) aittir?
Cevap:
İlgili ip (45.128.232.67) incelendiğinde hollandaya ait olduğu ve Anton Levin (AS 50053) adlı kişiye ait olduğu tespit edilmiştir.

C1.Sicil Kaydı: Bu IP daha önce hangi saldırı türleriyle (Brute Force, Phishing, Port Scan vb.) veya hangi zararlı yazılım aileleriyle (Malware Families) ilişkilendirilmiş?
Cevap:
İlgili ip (45.128.232.67) incelendiğinde çok sayıda ssh brute force denendiği görülmüştür.

C1.Zaman Çizelgesi: Bu IP ile ilgili raporlamalar yeni mi (son 24 saat), yoksa eski bir tehdit mi?
Cevap:
İlgili ip (45.128.232.67) incelendiğinde 2 sene öncesine ait olduğu tespit edilmiştir.

IOC (Indicator of Compromise): Bu senaryodaki "IOC" tam olarak nedir? Sadece IP adresi midir, yoksa URL veya dosya hash'i de olabilir mi? Bu vakadaki IOC verisini teknik bir formatta yazın.
Cevap:
Bu senaryodaki IOC ip adresi ve davranışıdır (brute force).
IOC_TYPE: ip adresi
IOC_VALUE: 45.128.232.67
DESCRIPTION: ip adresinden brute force denemesi
PORT: 22
PROTOCOL: TCP
ASN: AS50003
COUNTRY: NL
ATTACK_TYPE: SSH brute force
MITRE_TECHNIQUE: T1110

CTI (Cyber Threat Intelligence): Sadece "IP adresi Rusya'da" demek bir **Veri (Data)**'dir. Bunu **İstihbarat (Intelligence)**'a dönüştüren şey nedir. Bu IP'nin şirketiniz için neden tehdit oluşturduğunu "Bağlam" (Context) katarak açıklayın.
Cevap:
İstihbarata dönüştüren şey tüm bilgilerin toplanmasıyla oluşur.
İlgili ip (45.128.232.67) incelendiğinde hollandaya ait olduğu ve Anton Levin (AS 50053) adlı kişiye ait olduğu tespit edilmiştir. Bu ip adresi firmaya çok sayıda ssh brute force denemesi yapmıştır.

C2.MISP (Malware Information Sharing Platform): Diyelim ki bu IP'nin yeni bir Fidye Yazılımı (Ransomware) yaydığını keşfettiniz. Bu bilgiyi MISP gibi bir platformda paylaşmak, diğer kurumların savunmasına (Mavi Takım) nasıl yardımcı olur?
Cevap:
Bu ip adresi diğer MISP platformunda paylaşılırsa diğer firmalar bu ip adresini direk engelliyerek bir tehdidi daha başlamadan imha etmiş olurlar.

C3.Gerekçe: "VirusTotal skoru X olduğu için..." gibi basit değil, "Bu IP, Cobalt Strike C2 sunucusu olarak bilindiği ve sunucumuzla iletişim kurmaya çalıştığı için..." şeklinde teknik bir gerekçe sunun.
Cevap:
İlgili ip adresi firmaya çok sayıda başarısız ssh brute force denemesi yaptığı için kesinlikle engellenmelidir.

D1.Acil Müdahale: Panik yapmadan atacağınız **ilk 3 teknik adım** nedir? (İpucu: Fişi çekmek veri kaybına yol açabilir mi? Ağı izole etmek daha mı mantıklı?)
Cevap:
İlk adım bence ağı izole etmek bu sayede diğer cihazlarada ransomware sıçramasını engelleriz.
İkinci adım suçlu hakkında toplanabildiğimiz kadar veri toplamak.
Üçüncü adım yedekleri kontrol etmek eğer yedekler duruyorsa herhangi bir fidye ödemeye gerek yoktur. Ama yedeklerde şifrelenmişse verinin ne kadar değerli olup olmadığına karar verip fidye ödenebilir.

D1.Analiz: Bu zararlının sisteme nasıl girdiğini bulmak için hangi loglara bakarsınız?
Cevap:
Bence o cihazın hangi sitelere girdiğini, gelen e-postalara ve uygulamaların herhangi bir açığından yararlanıldımı bunlara bakılmalı.

D2.Teknik İnceleme: E-postanın sahte olduğunu kanıtlamak için hangi teknik parametrelere (Header analizi, Gönderici IP, URL yapısı vb.) bakarsınız?

Cevap:
İlk adım bence şüpeli bir e-posta varsa direk ceo ya sorulabilir.
ceo dan geri dönüş yoksa şunlara bakılmalıdır: eğer link varsa güvenli bir ortamda link tıklanıp neler olduğu gözlenebilir, dosya uzantısına, IP adresine

ve header analizi(e-postanın nereden geldiğini ve size nasıl ulaştığını gösterir) yapılmalı.

D2.Önlem: Bu saldırının diğer çalışanlara ulaşmasını engellemek için hangi güvenlik cihazında (Email Gateway, Firewall vb.) kural yazarsınız?
Cevap:
Email Gateway üzerinden gönderen maili, ip engellenir. Ayriyetten başka cihazlarada mail geldiyse silinmesini isterim. Firewall üzerindende gönderilen linki engellerim.

D3.Standartlar: Olay müdahale sürecinizi (Hazırlık -> Tespit -> Sınırlama -> Temizleme -> Kurtarma) hangi uluslararası standarda (Örn: NIST veya ISO 27001) dayandırırsınız?
Cevap:
NIST SP 800-61 dayandırılır.

D3.Kriz İletişimi: Saldırı devam ederken yönetim sizden sürekli bilgi istiyor ve ortam çok gergin. Ekip içindeki paniği önlemek ve yönetimi doğru bilgilendirmek için nasıl bir iletişim stratejisi izlersiniz?
Cevap:
Öncelikle tek bir lider belirlenir ve bütün bilgiler ve yönetim o kişi üzerinden geçer,
Sadece kesin bilgiler üzerinden iş yapılır düşüncelere yer verilmez. Yönetimi bir kenara atarım “olay bitince bilgilendirileceksiniz” derim çünkü yönetimin orada bulunması sadece stres yaratır.

D4. Kendinizi güncel tutmak için takip ettiğiniz 3 somut kaynak (Web sitesi, Twitter hesabı, CVE veritabanı vb.) nedir?
Cevap:
1.Youtube-Can Deger