Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Antivirüs Yazılımı ve Uç Nokta Koruma rehberi

İmza algılama, sezgisel yöntemler, davranış izleme, korumalı alan (sandbox), güncellemeler

ANTİVİRÜS YAZILIMI ÖĞRENME ÖZETİ

GÜVENCEDE
VERİ ŞİFRELEME
256 bit AES Standardı

UYUMLU
KÜRESEL STANDARTLAR
GDPR ve CCPA çerçeveleri

SIFIR GÜVEN
ERİŞİM POLİTİKASI
Çok Faktörlü Kimlik Doğrulama

Hoş geldin! Bu etkinlik paketi sana antivirüs yazılımı ve uç nokta koruması konusunda rehberlik eder. İmza veri tabanlarını, buluşsal tarayıcıları, davranış izlemeyi, korumalı alan sanal dosyalarını ve yanlış pozitif azaltmayı keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: Siber güvenlikte ve tehdit önlemede ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com siber güvenlik rehberini aç

URL: https://www.vpn.com/tr/siber-guvenlik/antivirusprogram/

Antivirüs Stratejisi Öğrenme Yol Haritan

- İmza tabanlı ve buluşsal yöntem tabanlı kötü amaçlı yazılım tespitini birbirinden ayır.
- Davranış izleme ve korumalı alan yalıtım protokollerini anla.
- Gerçek zamanlı taramanın sistem performansına ve uç noktalara etkilerini değerlendir.
- Dijital sertifika doğrulamasıyla yanlış pozitif sınıflandırmaları azalt.
- Kurumsal uç noktalarda günlük tanım güncellemesi dağıtımını yönet.

ANTİVİRÜS REHBERİ TALİMATLARI

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: uç nokta antivirüs güvenliği. Hızlı Düşün bonus etkinliğiyle bitir.

ANTİVİRÜS KORUMASI VE İMZA TARAMASI (GİRİŞ)

Antivirüs yazılımı, kötü amaçlı yazılımları tanımlayıp karantinaya alarak ve kaldırarak uç noktaları korur. Modern sistemler, sıfır gün istismarlarını algılamak için imza veritabanlarını (bilinen tehdit özetlerini eşleştirme), sezgisel yöntemleri (dosya yapısını analiz etme) ve davranış izlemeyi birleştirir.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ

Kontrol Noktası 1: Çoktan seçmeli görev

1. İmza tabanlı algılamanın bir sınırlaması nedir?

- A. Bilinmeyen veya değiştirilmiş kötü amaçlı yazılımları tanımlayamaz
- B. Yüksek oranda yanlış pozitif üretir
- C. Yüksek CPU işlem gücü gerektirir
- D. Yalnızca internete bağlıyken çalışır

2. Sezgisel tarayıcılar yeni kötü amaçlı yazılım varyantlarını nasıl tespit eder?

- A. Şüpheli desenleri ve kod yapılarını belirleyerek
- B. Dosya özetlerini bir tehdit veritabanıyla eşleştirerek
- C. İmzalanmamış tüm çalıştırılabilir dosyaları otomatik olarak silerek
- D. Her dosyayı herkese açık bir bulut klasörüne yükleyerek

3. Antivirüs korumalı alanda (sandbox) çalıştırmanın amacı nedir?

- A. Dosyaları güvenli bir sanal kasada yalıtmak ve analiz etmek
- B. Yerel dosya sistemi yedek aktarımını hızlandırmak
- C. Yerel işletim sistemi güvenlik yamalarını güncellemek
- D. Depolama alanından tasarruf etmek için büyük belge dosyalarını sıkıştırmak

4. Hangi algılama yöntemi tehdit davranışını gerçek zamanlı olarak işaretler?

- A. Yazılım eylemlerini izleyen davranış analizi
- B. Gece yapılan geçmiş kayıt incelemesi
- C. Yavaş uygulamaları bildiren manuel kullanıcı müdahalesi
- D. Yüklü programların haftalık manuel incelemeleri

5. Tarayıcılar için düzenli tanım güncellemeleri neden kritiktir?

- A. İmza motorlarının veritabanını tehdit tanımlayıcılarıyla beslemek için
- B. İşlemler sırasında CPU saat hızlarını artırmak
- C. Küresel DNS ad sunucusu önbellekleme sürelerini değiştirmek için
- D. Web tarayıcısı çerez ayarlarını yetkilendirmek için

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru D/Y 6

6. İmza algılama, kriptografik dosya karma değerlerini veritabanı listeleriyle eşleştirir.

Doğru Yanlış

7 Soru D/Y 7

7. Sezgisel tarayıcılar güvenli dosyalarda yanlış pozitif uyarılar tetikleyebilir.

Doğru Yanlış

8 Soru D/Y 8

8. Bir korumalı alan, kötü amaçlı yazılımın ağ dosyalarına sınırsız erişmesine izin verir.

Doğru Yanlış

9 Soru D/Y 9

9. Davranışsal tarama, dosyalar kötü amaçlı eylemler sergilediğinde onları engeller.

Doğru Yanlış

10 Soru D/Y 10

10. Standart antivirüs yazılımı tüm sıfırıncı gün saldırılarını tamamen durdurur.

Doğru Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Geleneksel bir tarayıcı, bilinen kötü amaçlı yazılımları belirlemek için _____ eşleştirmesine dayanır.

2. Dosya kod örüntülerini analiz etmeye _____ tarama denir.

3. Antivirüs araçları şüpheli dosyaları bir _____ ortamında izole eder.

4. Gerçek zamanlı izleme, şüpheli etkinlikler için programların şu yönünü izler: _____ .

5. Tarayıcılar, yeni tehditleri tanımak için veritabanlarını her gün indirilen bir _____ ile yeniler.

6. Güvenli programlar kötü amaçlı yazılım olarak işaretlendiğinde _____ uyarısı oluşur.

KELİME BANKASI

ANTİVİRÜS ARACI | DAVRANIŞ | GÜNCELLEME | GÜVENLİK DUVARI | İMZA | KUM KUTUSU | SEZGİSEL | YANLIŞ POZİTİF

Cevaplarını buraya yaz:

1.
2.
3.
4.
5.
6.

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

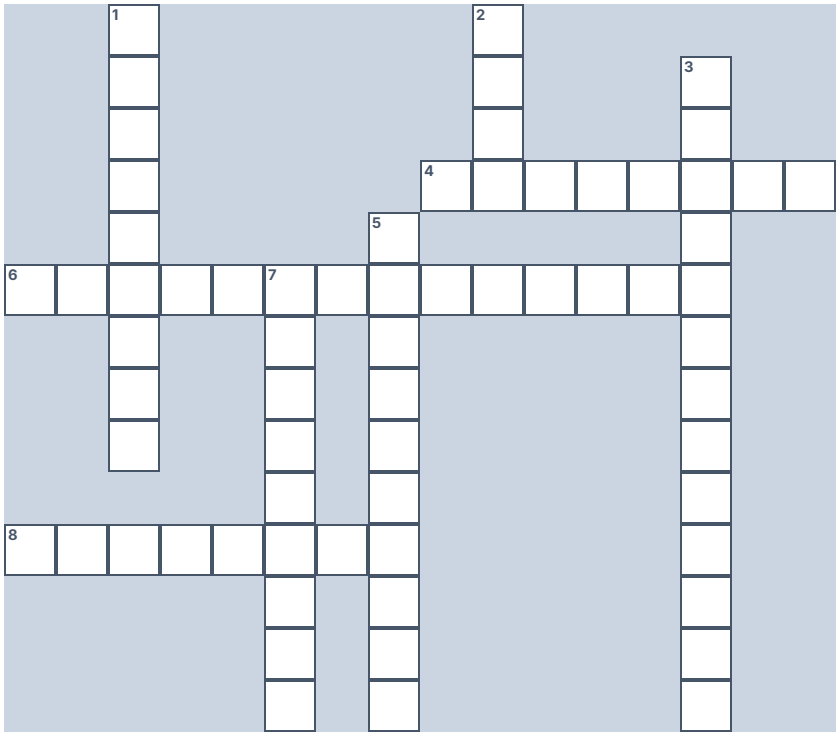
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

☐	1. Karma İmzası	A	Yerel sistemin açığa çıkmasını önlemek için şüpheli dosyaları sınırlama.
☐	2. Kod Sezgileri	B	Uç noktaları tarayan ve istismarlardan koruyan yazılım paketi.
☐	3. Dosya Korumalı Alanı	C	Çalışan yazılım eylemlerini kötü amaçlı işlem desenleri açısından izlemek.
☐	4. Davranış Taraması	D	Bilinen tehditleri belirlemek için kullanılan benzersiz kriptografik veri tabanı parmak izi.
☐	5. Günlük Güncellemeler	E	Güvenilmeyen kodu güvenle çalıştıran güvenli sanal test ortamı.
☐	6. Yanlış Pozitif	F	Tehdit veritabanını besleyen düzenli tanım indirmeleri.
☐	7. Tehdit Yalıtımı	G	Şüpheli kod düzenlerine sahip dosyaları işaretleyen kural tabanlı analiz.
☐	8. Antivirüs Aracı	H	Güvenli yazılımı yanlışlıkla kötü amaçlı yazılım olarak sınıflandıran güvenlik uyarısı.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

4. Çalışan yazılımın eylemlerini kötü amaçlı çalışma örüntüleri açısından izleme (8)

6. Uç noktaları tarayan ve istismarlara karşı koruyan yazılım paketi (14)

8. Şüpheli kod yapısına sahip dosyaları işaretleyen kural tabanlı analiz (8)

YUKARIDAN AŞAĞI

1. Güvenilmeyen kodu güvenle çalıştıran güvenli sanal test ortamı (9)

2. Bilinen tehditleri tanımlamak için kullanılan benzersiz kriptografik veritabanı izi (4)

3. Güvenli bir yazılımı yanlışlıkla kötü amaçlı yazılım olarak sınıflandıran güvenlik uyarısı (13)

5. Tehdit veritabanını besleyen düzenli tanım dosyası indirmeleri (10)

7. Yerel sistemin risk altına girmesini önlemek için şüpheli dosyaları sınırlandırma (9)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir. SOLDAN SAĞA İPUÇLARI YUKARIDAN AŞAĞIYA İPUÇLARI

SOLDAN SAĞA

4 soldan sağa: Çalışan yazılımın eylemlerini kötü amaçlı çalışma örüntüleri açısından izleme (8 harf):

6 soldan sağa: Uç noktaları tarayan ve istismarlara karşı koruyan yazılım paketi (14 harf):

8 soldan sağa: Şüpheli kod yapısına sahip dosyaları işaretleyen kural tabanlı analiz (8 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Güvenilmeyen kodu güvenle çalıştıran güvenli sanal test ortamı (9 harf):

2 yukarıdan aşağı: Bilinen tehditleri tanımlamak için kullanılan benzersiz kriptografik veritabanı izi (4 harf):

3 yukarıdan aşağı: Güvenli bir yazılımı yanlışlıkla kötü amaçlı yazılım olarak sınıflandıran güvenlik uyarısı (13 harf):

5 yukarıdan aşağı: Tehdit veritabanını besleyen düzenli tanım dosyası indirmeleri (10 harf):

7 yukarıdan aşağı: Yerel sistemin risk altına girmesini önlemek için şüpheli dosyaları sınırlandırma (9 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

F U L Ü E Ü I A P Z Y Y J G H
İ S E L P M İ K K S N Ğ Ö Ö G
T U S Z A N E T F T C Y P Y B
İ T İ Ğ K Z G L I M İ M Z A O
Z U G M Ü C K Z L Y F V N U T
O K Z J T O B M U E S K G T Ç
P M E Y T İ P B Ü Z C V K P Ö
Ş U S V H N D A Ç İ Ö N U Ü Ü
I K J I Ğ Ş Ğ F B E H İ Ü S R
L U P Z Ş I N A R V A D E G Ğ
N A N T İ V İ R Ü S A R A C I
A E R C A J O C Z K İ U P Ş A
Y R İ Z O L A S Y O N Ü I K K
G Ğ L Ğ P F J S J P Ü Ğ B Ş F
Y M Y Ü R Ğ S V A O T M M Z N

KELİME LİSTESİ

İMZA SEZGİSEL KUMKUTUSU DAVRANIŞ GÜNCELLEME YANLIŞPOZİTİF İZOLASYON ANTİVİRÜSARACI

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. İMZA**
- **B. SEZGİSEL**
- **C. KUMKUTUSU**
- **D. DAVRANIŞ**
- **E. GÜNCELLEME**
- **F. YANLIŞPOZİTİF**
- **G. İZOLASYON**
- **H. ANTİVİRÜSARACI**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Çalışan yazılımın eylemlerini kötü amaçlı çalışma örüntüleri açısından izleme.
2. Uç noktaları tarayan ve istismarlara karşı koruyan yazılım paketi.
3. Tehdit veritabanını besleyen düzenli tanım dosyası indirmeleri.
4. Şüpheli kod yapısına sahip dosyaları işaretleyen kural tabanlı analiz.
5. Yerel sistemin risk altına girmesini önlemek için şüpheli dosyaları sınırlandırma.
6. Bilinen tehditleri tanımlamak için kullanılan benzersiz kriptografik veritabanı izi.
7. Güvenilmeyen kodu güvenle çalıştıran güvenli sanal test ortamı.
8. Güvenli bir yazılımı yanlışlıkla kötü amaçlı yazılım olarak sınıflandıran güvenlik uyarısı.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel siber güvenlik kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. **ZİAM** _____

2. **UKSKUTUUM** _____

3. **GLMLÜEECEN** _____

4. **ANOLYSİZO** _____

5. **İSELGSEZ** _____

6. **IŞRNDAAV** _____

7. **İTOŞYAZIFİNPL** _____

8. **İÜAİSANIARTCRV** _____

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Yazılımı güncelleme nedenleri			
2	BT yardımı için sorabileceğin kişiler			
3	Antivirüs bir şey bulduğunda yapılacaklar			
4	Bilgisayar virüsü işaretleri			
5	Karantinaya alınan şeyler			
6	Virüslerin saklandığı yerler			
7	Asla paylaşmaman gereken bilgiler			
8	Kötü amaçlı yazılım türleri			
9	Bildiğin güvenlik araçları			
10	Bir antivirüsün taradığı şeyler			
11	Yedeklediğin şeyler			
12	Hacklenebilecek cihazlar			
13	Bildiğin antivirüs programları			
14	Yanlış alarm nedenleri			
15	Bugün başlayabileceğin güvenli alışkanlıklar			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: İMZA VE SEZGİSEL TARAMA KARŞILAŞTIRMASI

👷

Senaryo: Bir çalışan, başka bir ekibin şirket içinde geliştirdiği özel bir yardımcı programı indiriyor. İmza tarayıcısı programı onaylıyor, ancak sezgisel tarayıcı şüpheli olarak işaretliyor.

Tartışma sorusu: Bunun neden olduğunu açıkla ve dosyanın güvenli olup olmadığını nasıl doğrulayacağını anlat.

VAKA ÇALIŞMASI 2: YANLIŞ POZİTİFLERİ YÖNETME

👷

Senaryo: Bir yazılım geliştiricisi uygulamasını derliyor. Sistemin antivirüsü yeni çalıştırılabilir dosyayı kötü amaçlı yazılım olarak işaretliyor ve karantinaya alıyor.

Tartışma sorusu: İstisna listesine (whitelist) eklemenin risklerini özetle ve doğru çözüm yolunu anlat.

Kontrol Noktası 9: Şifreyi Çöz

Bir siber güvenlik uzmanı, ağ varlıklarını çevrimiçi tehdit aktörlerine karşı korur. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10

I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20

R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

28	6	17	12		14	19	24	26		28	1	29	11	15	11	16	11
22	6	29	8	12	22	6	15		1	17	1	15	12	29	15	6	
				24	6	22	20	12	24		6	24					

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm A)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q1: Virüsten koruma yazılımı kötü amaçlı yazılımı nasıl tanımlar?

Kötü amaçlı yazılımı veri tabanı imza eşleştirmesi, sezgisel kod düzeni analizi ve gerçek zamanlı davranış izleme ile tanımlar.

Q2: İmza tabanlı tespit nedir?

Kriptografik dosya özetlerini bilinen kötü amaçlı yazılım tehditlerinin veri tabanı listeleriyle eşleştiren bir tarama yöntemidir.

Q3: Sezgisel tarayıcı nedir?

Sezgisel yöntemler bir dosyanın yapısını ve kod talimatlarını analiz eder, kötü amaçlı yazılım varyantlarında yaygın olan şüpheli kalıpları işaretler.

Q4: Bir dosyanın karantinaya alınması ne anlama gelir?

Virüsten koruma, dosyayı güvenli, yalıtılmış bir klasöre taşıyarak işletim sistemini korumak için çalıştırılmasını engeller.

Q5: Antivirüs yanlış pozitifi nedir?

Meşru, güvenli bir yazılımın tarama algoritmaları tarafından yanlışlıkla kötü amaçlı yazılım olarak işaretlendiği bir hatadır.

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm B)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Davranış izleme sistemleri nasıl korur?

Çalışan yazılımı gerçek zamanlı izler ve kod enjekte etmek gibi şüpheli değişiklikler yapmaya çalışan süreçleri engeller.

Q7: Korumalı alan testi neden önemlidir?

Korumalı alan, güvenilmeyen dosyaları yalıtılmış bir sanal makinede çalıştırır ve eylemleri sistemi riske atmadan güvenle gözlemler.

Q8: Antivirüs tanımları ne sıklıkla güncellenmelidir?

Tarayıcılar, yeni keşfedilen kötü amaçlı yazılım türlerini tanımak için tanımları günlük veya saatlik olarak güncellemelidir.

Q9: Antivirüs ile EDR arasındaki fark nedir?

Antivirüs dosya taramaya odaklanırken, Uç Nokta Algılama ve Yanıt (EDR) ağ genelinde tehdit takibi ve sınırlandırma sağlar.

Q10: İki virüsten koruma programını birlikte çalıştırabilir miyim?

Hayır. İki etkin tarayıcı çalıştırmak sistem çakışmalarına yol açar, performansı yavaşlatır ve birbirinin işlemlerini engelleyebilir.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q1: Buluşsal kurallar tehdit atlatmayı nasıl en aza indirir?

Sezgisel yöntemler belirli imzalar yerine genel tehdit kalıplarını analiz eder ve bilinen kötü amaçlı yazılım ailelerinin değiştirilmiş varyantlarını yakalar.

Q2: Polimorfik virüs nedir?

Her çalıştırmada dosya düzenini ve şifre çözme rutinini değiştiren, böylece imza taramalarını etkisiz kılan kötü amaçlı yazılımdır.

Q3: Korumalı alanlar (sandbox) sanal makineden kaçınmayı nasıl tespit eder?

Modern korumalı alanlar (sandbox), fare tıklamalarını ve sistem çalışma süresini taklit ederek sanal makinelerde çalışırken saklanmak üzere tasarlanmış kötü amaçlı yazılımları kandırır.

Q4: İmza güncellemesi indirme biçimleri nelerdir?

Güncellemeler genellikle hafif artımlı ikili fark dosyalarıdır ve istemcinin ağ bant genişliği tüketimini en aza indirir.

Q5: Uç nokta ajanları yerel taramaları nasıl yönetir?

Aracılar hafif arka plan kontrolleri yapar ve derin kriptografik karma aramalarını bulut tehdit veritabanlarına devreder.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q6: Rootkit tespit taraması nedir?

Rootkit'lerin etkin iş parçacıklarını gizlemek için kancaladığı işletim sistemi API'lerini atlayarak çekirdek düzeyindeki bellek tablolarını tarar.

Q7: Davranış taraması fidye yazılımını nasıl engeller?

Otomatik toplu dosya şifreleme döngülerini algılar ve sistem veri tabanları kilitlenmeden önce ana bilgisayar sürecini sonlandırır.

Q8: Kod imzalama sertifikası doğrulaması nedir?

Tarayıcılar, kodun dijital imzalarını güvenilir kök sertifika yetkililerine karşı kontrol ederek yazılım geliştiricisinin kimliğini doğrular.

Q9: Paketleyiciler (packers) tarama motorlarını nasıl etkiler?

Paketleyiciler kötü amaçlı yazılım yüklerini sıkıştırır veya şifreler. Tarayıcılar imza eşleşmeleri çalışmadan önce dosyayı bellekte açmalıdır.

Q10: EDR araçları yalıtımı nasıl otomatikleştirir?

EDR aracıları, ele geçirilmiş uç noktaları ağ düzeyinde karantinaya alır, yanal hareketi engellerken analist erişimine izin verir.

Bölüm 11: Siber güvenlikle ilgili 10 gerçek dünya gerçeği ve içgörüsü

Güvenlik ihlalleri, savunma mekanizmaları ve uyumluluk standartlarıyla ilgili gerçek dünya bilgilerini incele.

1. GÜVENLİK İPUCU

İmza veritabanları bilinen kötü amaçlı yazılımların karma değerlerini saklar; bu nedenle yepyeni veya değiştirilmiş dosyalar, tanımlar güncellenene kadar gözden kaçar.

2. GÜVENLİK İPUCU

Sezgisel motorlar, imzalar henüz yokken bazı yeni kötü amaçlı yazılım varyantlarını işaretleyebilir; bunun bedeli daha fazla yanlış pozitiftir.

3. GÜVENLİK İPUCU

Yanlış pozitif uyarılar, BT ekiplerinin yanlışlıkla karantinaya alınan dosyaları doğrulayıp geri yüklemek için harcadığı zamana mal olur.

4. GÜVENLİK İPUCU

Polimorfik kötü amaçlı yazılım her kopyada kodunu değiştirir; bu yüzden savunmacılar imzaları buluşsal ve davranış denetimleriyle birlikte kullanır.

6. GÜVENLİK İPUCU

Kötü amaçlı yazılım yazarları, sanal korumalı alan ortamlarını kontrol etmek için özel kodlar yazar ve zamanlayıcıları atlatmak için çalıştırmayı geciktirir.

5. GÜVENLİK İPUCU

Bulut tabanlı antivirüs motorları, şüpheli dosya karmalarını büyük çevrimiçi tehdit veritabanlarıyla neredeyse gerçek zamanlı karşılaştırır.

7. GÜVENLİK İÇGÖRÜSÜ

Satıcılar, tarayıcıların yeni doğrulanmış tehditleri tanıyabilmesi için uç noktalara düzenli olarak tanım güncellemeleri gönderir.

8. GÜVENLİK İÇGÖRÜSÜ

Fidye yazılımı davranış izleyicileri, dosya şifreleme ve gölge kopya silme ile ilişkili belirli Win32 API çağrılarını hedefler.

9. GÜVENLİK İÇGÖRÜSÜ

Geçerli kod imzaları yanlış pozitif riskini azaltabilir, ancak imzalı dosyalar da taranır; çünkü kötü amaçlı yazılımlar da imzalanabilir.

10. GÜVENLİK İPUCU

Rootkit'ler sistem çekirdeği yapılarını değiştirir; bunları algılamak ve temizlemek için önyükleme sırasında çalışan özel tarayıcılar gerekir.

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir. AKADEMİK VE SEKTÖREL KAYNAKLAR

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

https://csrc.nist.gov/pubs/sp/800/61/r3/final

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** İMZALAR **Doğru cevap: A**

ÖĞRETMEN NOTU

İmza taraması bilinen veritabanı karmalarına dayanır; bu yüzden bilinmeyen veya değiştirilmiş kötü amaçlı yazılımları tespit edemez. Kaynak: OWASP Güvenli Yapılandırma.

2 **Soru 2** SEZGİSEL YÖNTEMLER **Doğru cevap: A**

ÖĞRETMEN NOTU

Sezgisel yöntemler, yeni tehdit varyantlarının şüpheli özelliklerini belirlemek için kod düzenini ve komutları analiz eder. Kaynak: Center for Internet Security (CIS).

3 **Soru 3** KORUMALI ALAN KULLANIMI **Doğru cevap: A**

ÖĞRETMEN NOTU

Kum havuzu, yürütme davranışını güvenle gözlemlemek için şüpheli dosyaları yalıtılmış bir sanal makinede çalıştırır. Kaynak: NIST Dijital Kimlik.

4 **Soru 4** DAVRANIŞSAL **Doğru cevap: A**

ÖĞRETMEN NOTU

Davranış taraması, yetkisiz sistem değişikliklerini engellemek için çalışan programları gerçek zamanlı izler. Kaynak: Center for Internet Security (CIS).

5 **Soru 5** GÜNCELLEMELER **Doğru cevap: A**

ÖĞRETMEN NOTU

Tarayıcılar, tehdit ortamıyla eşzamanlı kalmak için günlük artımlı tanım güncellemeleri indirir. Kaynak: OWASP Güvenli Yapılandırma.

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** İMZALAR **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

İmza araçları şifreleme karmaları hesaplar ve bunları bilinen tehdit karmalarından oluşan bir veritabanıyla eşleştirir. Kaynak: OWASP Güvenli Yapılandırma.

7 **Soru 7** SEZGİSEL YÖNTEMLER **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Sezgisel motorlar, meşru ve güvenli dosyaları da şüpheli olarak işaretleyebilen kural tabanlı düzenler çalıştırır. Kaynak: Center for Internet Security (CIS).

8 **Soru 8** KORUMALI ALAN KULLANIMI **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Kum havuzu, kodu sanal bir konteynerde çalıştırır ve ağ paylaşımlarına erişimi kesin biçimde engeller. Kaynak: NIST Dijital Kimlik.

9 **Soru 9** DAVRANIŞSAL **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Gerçek zamanlı izleme, yasa dışı yazma veya dosya kilitleme girişiminde bulunan çalışan süreçleri işaretler. Kaynak: Center for Internet Security (CIS).

10 **Soru 10** **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Hiçbir antivirüs her sıfırıncı gün (zero-day) saldırısını durdurmaz; bilinmeyen tehditler imzalardan ve sezgisel yöntemlerden kaçabilir.

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

D 1. Karma İmzası	G 2. Kod Sezgileri	E 3. Dosya Korumalı Alanı	C 4. Davranış Taraması
F 5. Günlük Güncellemeler	H 6. Yanlış Pozitif	A 7. Tehdit Yalıtımı	B 8. Antivirüs Aracı

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 İMZA	2 SEZGİSEL	3 KUM KUTUSU	4 DAVRANIŞ
5 GÜNCELLEME	6 YANLIŞ POZİTİF		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 D – DAVRANIŞ	2 H – ANTİVİRÜSARACI	3 E – GÜNCELLEME	4 B – SEZGİSEL
5 G – İZOLASYON	6 A – İMZA	7 C – KUMKUTUSU	8 F – YANLIŞPOZİTİF

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin Karma İmzası, Kod Sezgileri ve Dosya Korumalı Alanı terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

F	U	L	Ü	E	Ü	I	A	P	Z	Y	Y	J	G	H
İ	S	E	L	P	M	İ	K	K	S	N	Ğ	Ö	Ö	G
T	U	S	Z	A	N	E	T	F	T	C	Y	P	Y	B
İ	T	İ	Ğ	K	Z	G	L	I	M	İ	M	Z	A	O
Z	U	G	M	Ü	C	K	Z	L	Y	F	V	N	U	T
O	K	Z	J	T	O	B	M	U	E	S	K	G	T	Ç
P	M	E	Y	T	İ	P	B	Ü	Z	C	V	K	P	Ö
Ş	U	S	V	H	N	D	A	Ç	İ	Ö	N	U	Ü	Ü
I	K	J	I	Ğ	Ş	Ğ	F	B	E	H	İ	Ü	S	R
L	U	P	Z	Ş	I	N	A	R	V	A	D	E	G	Ğ
N	A	N	T	İ	V	İ	R	Ü	S	A	R	A	C	I
A	E	R	C	A	J	O	C	Z	K	İ	U	P	Ş	A
Y	R	İ	Z	O	L	A	S	Y	O	N	Ü	I	K	K
G	Ğ	L	Ğ	P	F	J	S	J	P	Ü	Ğ	B	Ş	F
Y	M	Y	Ü	R	Ğ	S	V	A	O	T	M	M	Z	N

BULMACA ÇÖZÜMÜ

		K					İ							
		U					M				Y			
		M					Z				A			
		K				D	A	V	R	A	N	I	Ş	
		U			G						L			
A	N	T	İ	V	İ	R	Ü	S	A	R	A	C	I	
		U		Z		N							Ş	
		S		O		C							P	
		U		L		E							O	
				A		L							Z	
S	E	Z	G	İ	S	E	L						İ	
					Y		E						T	
					O		M						İ	
					N		E						F	

SOLDAN SAĞA

4 soldan sağa: DAVRANIŞ Çalışan yazılımın eylemlerini kötü amaçlı çalışma örüntüleri açısından izleme (8 harf)

6 soldan sağa: ANTİVİRÜSARACI Uç noktaları tarayan ve istismarlara karşı koruyan yazılım paketi (14 harf)

8 soldan sağa: SEZGİSEL Şüpheli kod yapısına sahip dosyaları işaretleyen kural tabanlı analiz (8 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: KUMKUTUSU Güvenilmeyen kodu güvenle çalıştıran güvenli sanal test ortamı (9 harf)

2 yukarıdan aşağı: İMZA Bilinen tehditleri tanımlamak için kullanılan benzersiz kriptografik veritabanı izi (4 harf)

3 yukarıdan aşağı: YANLIŞPOZİTİF Güvenli bir yazılımı yanlışlıkla kötü amaçlı yazılım olarak sınıflandıran güvenlik uyarısı (13 harf)

5 yukarıdan aşağı: GÜNCELLEME Tehdit veritabanını besleyen düzenli tanım dosyası indirmeleri (10 harf)

7 yukarıdan aşağı: İZOLASYON Yerel sistemin risk altına girmesini önlemek için şüpheli dosyaları sınırlandırma (9 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. ZİAM	İMZA	5. İSELGSEZ	SEZGİSEL
2. UKSKUTUUM	KUMKUTUSU	6. IŞRNDAAV	DAVRANIŞ
3. GLMLÜEECEN	GÜNCELLEME	7. İTOŞYAZIFİNPL	YANLIŞPOZİTİF
4. ANOLYSİZO	İZOLASYON	8. İÜAİSANIARTCRV	ANTİVİRÜSARACI

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"YENİ KÖTÜ YAZILIMI SEZGİSEL ANALİZLE TESPİT ET"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: İmza ve Sezgisel Tarama Karşılaştırması

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir çalışan, başka bir ekip tarafından dahili olarak geliştirilen özel bir yardımcı program indirir. İmza tarayıcısı onu geçirir, ancak sezgisel tarayıcı şüpheli olarak işaretler.
- Önerilen Strateji ve Çözüm: Neden Oldu: İmza taraması dosya karmalarını kontrol eder; dosya özel olduğu için tehdit veritabanında yoktur. Sezgisel yöntemler yapıyı analiz eder ve şüpheli eylemleri (ör. kayıt defteri yazmaları) işaretler. Doğrulama: Eylemleri gözlemlemek için dosyayı bir korumalı alanda çalıştır, dijital imzaları kontrol et ve karmayı tehdit istihbaratı portallarına gönder.

B Vaka Çalışması 2: Yanlış Pozitifleri Yönetme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir yazılım geliştirici uygulamasını derler. Sistem antivirüsü yeni yürütülebilir dosyayı kötü amaçlı yazılım olarak işaretler ve karantinaya alır.
- Önerilen Strateji ve Çözüm: Beyaz Listeye Almanın Riskleri: Tarayıcıları atlamak, gerçek ve enfekte kodun çalışmasına izin verebilir. Çözüm Yolu: Dosyayı analiz için antivirüs sağlayıcısına gönder, kodu sertifika yetkilileri aracılığıyla dijital olarak imzala ve antivirüsü kapatmak yerine geçici olarak belirli klasör istisnaları yapılandır.