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

Sıfır Güven Mimarisi ve Güvenliği

Sürekli doğrulama, ağ mikro bölümlendirmesi, Kimlik ve Erişim Yönetimi, en az ayrıcalık ve duruş kontrolleri.

SIFIR GÜVEN GÜVENLİĞİ ÖĞRENME GENEL BAKIŞI

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 Sıfır Güven mimarisi ve güvenlik konusunda rehberlik eder. Sürekli doğrulamayı, ağ mikro segmentasyonunu, kimlik erişim yönetimini (IAM), en az ayrıcalığı ve oturum denetimini 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/sifir-guven-siber-guvenlik/

Sıfır Güven Stratejisi Öğrenme Yol Haritan

- Sürekli doğrulamanın temel ilkesini anla.
- Ağ mikro bölümlendirmesi ve en az ayrıcalıklı erişim uygula.
- Cihaz duruş kontrollerini ve etkin oturum denetimini yapılandır.

SIFIR GÜVEN GÜVENLİĞİ REHBER 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: Sıfır Güven mimarisi. Hızlı Düşün bonus etkinliğiyle bitir.

SIFIR GÜVEN MİMARİSİ VE GÜVENLİĞİ (GİRİŞ)

Sıfır Güven güvenliği, eski ağ çevresi modellerinin yerine katı bir 'asla güvenme, her zaman doğrula' politikası koyar. Mikro segmentasyon, Kimlik ve Erişim Yönetimi (IAM), en az ayrıcalık hakları ve duruş kontrolleri uygulamak yanal tehdit hareketini engeller.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. Zero Trust güvenliğinin temel ilkesi nedir?

- A. Kaynağı ne olursa olsun hiçbir erişim isteğine asla güvenme, her zaman doğrula
- B. Kurumsal güvenlik duvarının içindeki tüm trafiğin güvenli olduğunu varsaymak
- C. Hızı artırmak için veritabanı dosyalarını şifrelemeden saklamak
- D. E-posta kimlik doğrulamasını yalnızca SPF kayıtlarıyla zorunlu kılmak

2. Ağ mikro bölümlendirmesi nedir?

- A. Yanal hareketi sınırlamak için ağları küçük, yalıtılmış bölgelere ayırmak
- B. Veri aktarımı sırasında ağ kartlarını şifrelemek
- C. Tüm yerel sunucuları tek bir genel IP adresine bağlamak
- D. Tarayıcı oturumlarında kullanıcı tuş vuruşlarını izlemek

3. En az ayrıcalık ilkesi nedir?

- A. Kullanıcı erişim izinlerini yalnızca işleri için gerekli olanla sınırlamak
- B. Varsayılan olarak her kullanıcıya tüm sistem ayrıcalıklarını vermek
- C. Kurumsal veritabanı sunucularına anonim girişlere izin vermek
- D. Herkese açık Wi-Fi yönlendiricilerini parolasız yapılandırmak

4. Kimlik ve Erişim Yönetimi (IAM) nedir?

- A. Dijital kimlikleri yöneten ve sistem ayrıcalıklarını denetleyen çerçeveler
- B. Yerel dosya dizinlerini tarayan antivirüs araçları
- C. Hava boşluklu ortam kullanan bir yedek depolama sistemi
- D. Sahte alan adlarını reddeden bir e-posta ağ geçidi protokolü

5. Sürekli kimlik doğrulama ne anlama gelir?

- A. Etkin bir oturum sırasında kullanıcı kimliğini ve cihaz duruşunu tekrar tekrar doğrulamak
- B. Ana parolayı her 10 dakikada bir değiştirmek
- C. Veritabanı kayıtlarını birden fazla algoritmayla karmalamak
- D. Ağ iletim paketlerini TLS anahtarlarıyla şifrelemek

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Sıfır Güven, kurumsal güvenlik duvarının içindeki tüm trafiğin güvenli olduğunu varsayar.

○ Doğru ○ Yanlış

7 Soru 7

7. Mikro segmentasyon, saldırganların iç sunucular arasında yanal hareket etme yeteneğini sınırlar.

○ Doğru ○ Yanlış

8 Soru 8

8. En az ayrıcalık ilkesi, varsayılan olarak tüm veritabanı dosyalarına erişim verir.

○ Doğru ○ Yanlış

9 Soru 9

9. Sürekli doğrulama, bir oturum boyunca cihaz sağlığını ve kimlik bilgilerini doğrular.

○ Doğru ○ Yanlış

10 Soru 10

10. Sıfır Güven uygulamak, ele geçirilmiş kurumsal oturum açma bilgilerinin etkisini azaltır.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Her erişim noktasında kimlik bilgisi talep etmek sürekli _____ anlamına gelir.
2. Kurumsal ağı çok küçük bölgelere ayırmaya mikro _____ denir.
3. Dijital kimlikleri ve erişim denetimini yapılandırmak bir _____ sistemi kullanır.
4. Kullanıcı izinlerini kısıtlamak, en az _____ ilkesini kullanır.
5. Bağlı cihazların sağlığını değerlendirmek için _____ taranır.
6. Etkin oturumları kaydetmek ve gözden geçirmek, güvenlik _____ işidir.

KELİME BANKASI

AYRICALIK BÖLÜMLEME CİHAZ DURUŞU DENETİM DOĞRULAMA
GÜVENLİK DUVARI KİMLİK YÖNETİMİ YÖNLENDİRİCİ

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

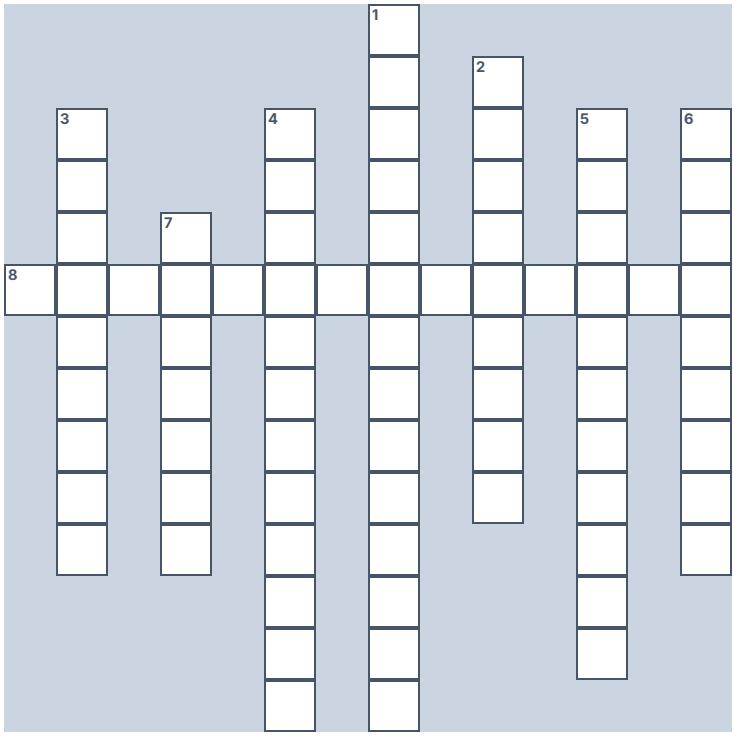
TANIM EŞLEŞTİRME

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

☐	1. DOĞRULAMA	A	Kullanıcı kimlik bilgisi erişimini yönetmek.
☐	2. BÖLÜMLENDİRME	B	En az erişim hakkı ilkesi.
☐	3. IAM	C	Ağ paketi trafiğini yönlendirmek.
☐	4. AYRICALIK	D	Dış ağ sınırı koruması.
☐	5. DURUŞ	E	Kaydedilmiş erişim oturumlarını incelemek.
☐	6. DENETİM YAPMA	F	İç ağ bölgelerini ayırma.
☐	7. GÜVENLİK DUVARI	G	Kullanıcı kimlik bilgilerini her zaman denetlemek.
☐	8. YÖNLENDİRİCİ	H	Cihaz sağlık durumunu değerlendirme.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

8. Dış ağ bariyeri koruması (14)

YUKARIDAN AŞAĞI

1. Kullanıcı kimlik bilgileri erişimini yönetme (14)

2. Kullanıcı kimlik bilgilerini her zaman kontrol etme (9)

3. İç ağ bölgelerini ayırma (9)

4. Ağ paketi trafiğini yönlendirme (12)

5. Cihaz sağlık durumunu değerlendirme (11)

6. En az erişim hakkı ilkesi (9)

7. Kayıtlı erişim oturumlarını gözden geçirme (7)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

8 soldan sağa: Dış ağ bariyeri koruması (14 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Kullanıcı kimlik bilgileri erişimini yönetme (14 harf):

2 yukarıdan aşağı: Kullanıcı kimlik bilgilerini her zaman kontrol etme (9 harf):

3 yukarıdan aşağı: İç ağ bölgelerini ayırma (9 harf):

4 yukarıdan aşağı: Ağ paketi trafiğini yönlendirme (12 harf):

5 yukarıdan aşağı: Cihaz sağlık durumunu değerlendirme (11 harf):

6 yukarıdan aşağı: En az erişim hakkı ilkesi (9 harf):

7 yukarıdan aşağı: Kayıtlı erişim oturumlarını gözden geçirme (7 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

DOĞRULAMA
BÖLÜMLEME
DENETİM
KİMLİKYÖNETİMİ
GÜVENLİKDUVARI
AYRICALIK
YÖNLENDİRİCİ
CİHAZDURUŞU

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. DOĞRULAMA
B. BÖLÜMLEME
C. KİMLİKYÖNETİMİ
D. AYRICALIK
E. CİHAZDURUŞU
F. DENETİM
G. GÜVENLİKDUVARI
H. YÖNLENDİRİCİ

TANIMLAR VE EŞLEŞTİRME ALANLARI
_____ 1. Dış ağ bariyeri koruması.
_____ 2. Kayıtlı erişim oturumlarını gözden geçirme.
_____ 3. En az erişim hakkı ilkesi.
_____ 4. İç ağ bölgelerini ayırma.
_____ 5. Ağ paketi trafiğini yönlendirme.
_____ 6. Cihaz sağlık durumunu değerlendirme.
_____ 7. Kullanıcı kimlik bilgileri erişimini yönetme.
_____ 8. Kullanıcı kimlik bilgilerini her zaman kontrol etme.

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. **LURODAMAĞ** _____
2. **İİKMYMKİÖİE TNL** _____
3. **CUDRHİŞUZU A** _____
4. **ÜİRUEDLIKAV GVN** _____
5. **EMÖELÜBML** _____
6. **IIYLAACKR** _____
7. **DİTMEEN** _____
8. **İNEİDİYNÖCR L** _____

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Asla paylaşmaman gereken bilgiler			
2	Bugün başlayabileceğin güvenli alışkanlıklar			
3	Bir cihazda kontrol edilen şeyler			
4	Kaydedilen şeyler			
5	Siber güvenlikle ilgili sözcükler			
6	Sıfır Güven'in kontrol ettiği şeyler			
7	Günlük hayatta kimlik gösterdiğin yerler			
8	Gerçekten sen olduğunu kanıtlama yolları			
9	Veri sızıntısından sonra yapılacaklar			
10	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
11	Yazılımı güncelleme nedenleri			
12	Bir şirketteki erişim seviyeleri			
13	Bildiğin güvenlik araçları			
14	Bir ağın bölünebileceği bölgeler			
15	Güven hakkında atasözleri			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: SIFIR GÜVEN AĞ MİMARİSİNE GEÇİŞ

👷

Senaryo: Büyük bir kuruluş şu anda, yerel ağdaki herhangi bir cihazın tüm kurumsal sunuculara ve veritabanlarına erişebildiği düz bir iç ağ kullanıyor.

Tartışma sorusu: Yanal hareketi sınırlamak için bir ağ mikro segmentasyon stratejisi tasarla.

VAKA ÇALIŞMASI 2: EN AZ AYRICALIK ERİŞİM KONTROLLERİNİ UYGULAMA

👷

Senaryo: Denetim kayıtları, geçici veritabanı kullanıcılarının ve alt düzey çalışanların kritik muhasebe veritabanlarında genel okuma ve yazma izinlerine sahip olduğunu ortaya koyuyor.

Tartışma sorusu: Veritabanı IAM ayrıcalıklarını denetle ve en az ayrıcalık ilkesini uygulamak için kısıtla.

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

22 11 7 11 21 8 26 27 6 17

16 12 16 1 21 12 22 12 28 15 6 10 6 21 29 1 16 1 17

5 18 9 21 25 15 1

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: Sıfır Güven nedir?

Sıfır Güven, tehditlerin ağ sınırının hem dışında hem içinde bulunduğunu varsayan ve her istek için doğrulama gerektiren bir güvenlik çerçevesidir. [1]

Q2: Sıfır Güven'in temel kuralı nedir?

Asla güvenme, her zaman doğrula.

Q3: Mikro bölümleme nedir?

Trafiği kontrol etmek ve ihlalleri sınırlamak için ağı küçük, güvenli mantıksal bölümlere ayırma.

Q4: En az ayrıcalık nedir?

Kullanıcılara yalnızca belirli iş görevlerini yerine getirmek için gereken en düşük erişim haklarını vermek. [2]

Q5: IAM neyin kısaltmasıdır?

Kimlik ve erişim yönetimi.

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

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Cihaz duruş kontrolü nasıl yardımcı olur?

Erişime izin vermeden önce bir cihazın yamalı olduğunu, etkin antivirüs çalıştırdığını ve güvenli olduğunu doğrular.

Q7: Yanal hareket nedir?

Saldırganların ilk ele geçirilen düğümden daha değerli sistemlere ağ içinde ilerlemek için kullandığı süreç.

Q8: Sıfır Güven güvenlik duvarlarının yerini alır mı?

Hayır, kimlik merkezli kontroller ve iç bölümleme güvenlik duvarları ekleyerek onları geliştirir.

Q9: Sürekli kimlik doğrulama nedir?

Yalnızca ilk girişte değil, etkin oturum boyunca kullanıcı kimliğinin sürekli doğrulanması.

Q10: Düz bir ağ neden tehlikelidir?

Düz ağlarda ele geçirilmiş tek bir düğüm, saldırganların ağdaki herhangi bir veri tabanına kolayca erişmesine olanak tanır.

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: Sıfır Güven, çevre modelini nasıl ele alır?

Eskimiş 'kale ve hendek' modelinin yerini alır; savunmayı sınır ağlardan belirli kullanıcı kimliklerine ve kaynaklara kaydırır.

Q2: İlke karar noktası (PDP) nedir?

Erişimin verilip verilmeyeceğine karar vermek için yetkilendirme isteklerini güvenlik kurallarına göre değerlendiren sistem bileşeni.

Q3: İlke uygulama noktası (PEP) nedir?

PDP kararına göre bağlantı isteklerine fiziksel olarak izin veren veya bunları engelleyen sistem düğümü (ağ geçidi veya proxy gibi).

Q4: Rol Tabanlı Erişim Denetimi (RBAC) Sıfır Güven'i nasıl destekler?

RBAC, izinleri belirli rollerde gruplandırır ve kullanıcıların aşırı yönetici ayrıcalıklarını devralmasını önlemeye yardımcı olur.

Q5: Bağlamsal erişim denetimi nedir?

Riski değerlendirmek için coğrafi konum, cihaz durumu ve oturum açma zamanı gibi ikincil ipuçlarını kullanarak oturum açma isteklerini değerlendirme.

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: Mikro bölümleme standart VLAN'lardan nasıl farklıdır?

VLAN'lar ağları katman 2'de geniş mantıksal bölümlere ayırırken mikro segmentasyon, tek tek iş yüklerini yalıtmak için yazılım ilkesi kullanır.

Q7: Tam zamanında (JIT) erişim nedir?

Yükseltilmiş yönetici izinlerini geçici olarak vermek ve görev bittiğinde otomatik olarak geri almak.

Q8: Sıfır Güven çerçevesinde API'leri nasıl güvene alırsın?

Kriptografik olarak imzalanmış OAuth belirteçleri isteyerek ve her API ağ geçidinde istek imzalarını denetleyerek.

Q9: Sıfır güven ağ erişimi (ZTNA) istemcisi nedir?

Ham ağ alt ağları yerine belirli uygulamalara güvenli, şifreli giden bağlantılar kuran yazılım aracısı.

Q10: Kayıt denetimi Sıfır Güven'e nasıl yardımcı olur?

Sürekli günlük kaydı, otomatik güvenlik analizi araçlarının anormallikleri tespit etmesine ve sahte girişleri hemen askıya almasına olanak tanır.

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

Sıfır Güven mimarileri eski kale-hendek modelinin yerine kimlik merkezli doğrulama kurallarını koyar.

2. GÜVENLİK İPUCU

Ağ mikro bölümlemesi, iş yüklerini küçük korumalı bölgelere ayırarak kötü amaçlı yazılımın ulaşabileceği alanı daraltır.

3. GÜVENLİK İPUCU

Sıfır Güven, ağ segmentleri yerine varlıklar, hizmetler ve hesaplar gibi kaynakları korumaya odaklanır. [1]

4. GÜVENLİK İPUCU

En az ayrıcalık erişim politikaları, çekirdek veritabanlarından içeriden kaynaklanan veri sızdırma tehdidinin riskini azaltır.

5. GÜVENLİK İPUCU

Cihaz durumu doğrulaması, işletim sistemi yama düzeylerini ve etkin antivirüs durumunu gerçek zamanlı olarak denetler.

6. GÜVENLİK İPUCU

Sıfır Güvenli Ağ Erişimi (ZTNA) aracıları, kullanıcı erişim kapsamını kısıtlamak için kurumsal VPN'lerin yerini alabilir veya onları tamamlayabilir.

7. GÜVENLİK İÇGÖRÜSÜ

Tam zamanında (JIT) yönetici ayrıcalığı devri, etki alanı denetleyicilerinde kimlik bilgisi hırsızlığı riskini azaltır.

8. GÜVENLİK İÇGÖRÜSÜ

Sürekli doğrulama, oturum davranışını günlüğe kaydeder ve denetler; anormal komut dosyası yürütme kalıpları gösteren kullanıcıları askıya alır.

9. GÜVENLİK İÇGÖRÜSÜ

Geleneksel çevre savunmaları, bir yönetici kimlik bilgisi sızdığında yanal saldırıları engelleyemez.

10. GÜVENLİK İPUCU

NIST Özel Yayını 800-207 (2020), dağıtım modelleriyle birlikte Sıfır Güven mimarisinin soyut bir tanımını verir. [1]

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Zero Trust güvenliğinin temel ilkesi nedir? → Kaynağı ne olursa olsun hiçbir erişim isteğine asla güvenme, her zaman doğrula

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Ağ mikro bölümlendirmesi nedir? → Yanal hareketi sınırlamak için ağları küçük, yalıtılmış bölgelere ayırmak

3 **Soru 3** — **Doğru cevap: A**

ÖĞRETMEN NOTU

En az ayrıcalık ilkesi nedir? → Kullanıcı erişim izinlerini yalnızca işleri için gerekli olanla sınırlamak

4 **Soru 4** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kimlik ve Erişim Yönetimi (IAM) nedir? → Dijital kimlikleri yöneten ve sistem ayrıcalıklarını denetleyen çerçeveler

5 **Soru 5** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Sürekli kimlik doğrulama ne anlama gelir? → Etkin bir oturum sırasında kullanıcı kimliğini ve cihaz duruşunu tekrar tekrar doğrulamak

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: Zero Trust, ağın içinde veya dışında olmasına bakılmaksızın ağ konumuna dayalı hiçbir örtük güven tanımaz.

7 **Soru 7** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Doğru: küçük, yalıtılmış bölgeler bir izinsiz girenin sunucular arasında ne kadar ilerleyebileceğini sınırlar.

8 **Soru 8** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: en az ayrıcalık ilkesi her role yalnızca ihtiyaç duyduğu minimum erişimi verir.

9 **Soru 9** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Sürekli doğrulama, bir oturum boyunca cihaz sağlığını ve kimlik bilgilerini doğrular.

10 **Soru 10** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Sıfır Güven uygulamak, ele geçirilmiş kurumsal oturum açma bilgilerinin etkisini azaltır.

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

G 1. DOĞRULAMA	F 2. BÖLÜMLENDİRME	A 3. IAM	B 4. AYRICALIK
H 5. DURUŞ	E 6. DENETİM YAPMA	D 7. GÜVENLİK DUVARI	C 8. YÖNLENDİRİCİ

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 DOĞRULAMA	2 BÖLÜMLEME	3 KİMLİK YÖNETİMİ	4 AYRICALIK
5 CİHAZ DURUŞU	6 DENETİM		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 G – GÜVENLİKDUVARI	2 F – DENETİM	3 D – AYRICALIK	4 B – BÖLÜMLEME
5 H – YÖNLENDİRİCİ	6 E – CİHAZDURUŞU	7 C – KİMLİKYÖNETİMİ	8 A – DOĞRULAMA

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin DOĞRULAMA, BÖLÜMLENDİRME ve IAM 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

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

BULMACA ÇÖZÜMÜ

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

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

8 soldan sağa: GÜVENLİKDUVARI Dış ağ bariyeri koruması (14 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: KİMLİKYÖNETİMİ Kullanıcı kimlik bilgileri erişimini yönetme (14 harf)

2 yukarıdan aşağı: DOĞRULAMA Kullanıcı kimlik bilgilerini her zaman kontrol etme (9 harf)

3 yukarıdan aşağı: BÖLÜMLEME İç ağ bölgelerini ayırma (9 harf)

4 yukarıdan aşağı: YÖNLENDİRİCİ Ağ paketi trafiğini yönlendirme (12 harf)

5 yukarıdan aşağı: CİHAZDURUŞU Cihaz sağlık durumunu değerlendirme (11 harf)

6 yukarıdan aşağı: AYRICALIK En az erişim hakkı ilkesi (9 harf)

7 yukarıdan aşağı: DENETİM Kayıtlı erişim oturumlarını gözden geçirme (7 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	LURODAMAĞ	DOĞRULAMA	5.	EMÖELÜBML	BÖLÜMLEME
2.	İİKMYMKİÖİETNL	KİMLİKYÖNETİMİ	6.	IIYLAACKR	AYRICALIK
3.	CUDRHİŞUZUA	CİHAZDURUŞU	7.	DİTMEEN	DENETİM
4.	ÜİRUEDLIKAVGVN	GÜVENLİKDUVARI	8.	İNEİDİYNÖCRL	YÖNLENDİRİCİ

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SIFIR GÜVEN MİMARİSİYLE HER ZAMAN DOĞRULA"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Sıfır Güven Ağ Mimarisine Geçiş

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Büyük bir işletme şu anda, yerel ağdaki herhangi bir cihazın tüm kurumsal sunuculara ve veritabanlarına erişebildiği düz bir dahili ağ kullanıyor.
- Önerilen Strateji ve Çözüm: Düz ağı yalıtılmış departman bölgelerine ayır. Bölgeler arası trafiği denetlemek için dahili güvenlik duvarları kur ve tüm erişimlerde bağlantı belirteci doğrulamasını zorunlu kıl.

B Vaka Çalışması 2: En Az Ayrıcalık Erişim Kontrollerini Uygulama

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Denetim kayıtları, geçici veritabanı kullanıcılarının ve alt düzey çalışanların kritik muhasebe veritabanlarında genel okuma ve yazma izinlerine sahip olduğunu ortaya koyuyor.
- Önerilen Strateji ve Çözüm: Tüm genel yönetici ayrıcalıklarını iptal et. Tam iş rollerine uyması için Rol Tabanlı Erişim Denetimi (RBAC) uygula ve haftalık otomatik izin incelemeleri oluştur.