نام: _____ تاریخ: _____ نمبر: _____

زیرو ٹرسٹ آرکیٹیکچر اور سیکیورٹی

مسلسل تصدیق، نیٹ ورک مائیکرو سیگمنٹیشن، Identity and Access Management، کم سے کم استحقاق اور ڈیوائس کی حالت کی جانچ۔

زیرو ٹرسٹ سیکیورٹی لرننگ کا جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو Zero Trust آرکیٹیکچر اور سیکیورٹی سے متعارف کراتا ہے۔ آپ مسلسل تصدیق، نیٹ ورک مائیکرو سیگمنٹیشن، شناخت اور رسائی کے انتظام (IAM)، کم از کم استحقاق اور سیشن آڈٹنگ کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- ☐ **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

URL: https://www.vpn.com/cybersecurity/zero-trust-cyber-security/

آپ کی زیرو ٹرسٹ حکمت عملی کا لرننگ روڈ میپ

- مسلسل تصدیق کے بنیادی اصول کو سمجھیں۔
- نیٹ ورک مائیکرو سیگمنٹیشن اور کم سے کم استحقاق کی رسائی نافذ کریں۔
- ڈیوائس کی حالت کی جانچ اور فعال سیشن کی آڈیٹنگ ترتیب دیں۔

زیرو ٹرسٹ سیکیورٹی گائیڈ کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو زیرو ٹرسٹ آرکیٹیکچر پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

زیرو ٹرسٹ آرکیٹیکچر اور سیکیورٹی (تعارف)

Zero Trust سیکیورٹی پرانے نیٹ ورک پیریمیٹر ماڈلز کی جگہ 'کبھی بھروسا نہ کریں، ہمیشہ تصدیق کریں' کی سخت پالیسی لاتی ہے۔ مائیکرو سیگمنٹیشن، شناخت اور رسائی کا نظم (IAM)، کم از کم مراعات کے حقوق، اور پوسچر چیکس نافذ کرنے سے خطرات کی پہلو بہ پہلو نقل و حرکت رک جاتی ہے۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. زیرو ٹرسٹ سیکیورٹی کا بنیادی اصول کیا ہے؟

- A. کبھی بھروسا نہ کریں، ماخذ سے قطع نظر ہر رسائی کی درخواست کی ہمیشہ تصدیق کریں
- B. یہ فرض کرنا کہ کارپوریٹ فائر وال کے اندر تمام ٹریفک محفوظ ہے
- C. رفتار بہتر بنانے کے لیے ڈیٹا بیس فائلیں بغیر خفیہ کاری کے محفوظ کرنا
- D. صرف SPF ریکارڈز کے ذریعے ای میل توثیق نافذ کرنا

2. نیٹ ورک مائیکرو سیگمنٹیشن کیا ہے؟

- A. نیٹ ورکس کو چھوٹے الگ تھلگ زونز میں تقسیم کرنا تاکہ پہلو بہ پہلو پھیلاؤ محدود رہے
- B. ڈیٹا کی ترسیل کے دوران نیٹ ورک کارڈز کو خفیہ کرنا
- C. تمام مقامی سرورز کو ایک ہی عوامی IP ایڈریس سے جوڑنا
- D. براؤزر سیشنز میں صارف کے کی اسٹروکس کی نگرانی کرنا

3. کم سے کم استحقاق کا اصول کیا ہے؟

- A. صارف کی رسائی کی اجازتوں کو صرف ان تک محدود کرنا جو اس کے کام کے لیے ضروری ہیں
- B. ڈیفالٹ طور پر ہر صارف کو تمام سسٹم مراعات دینا
- C. کارپوریٹ ڈیٹا بیس سرورز میں گمنام لاگ اِنز کی اجازت دینا
- D. عوامی Wi-Fi راؤٹرز کو بغیر پاس ورڈ کے ترتیب دینا

4. شناخت اور رسائی کا انتظام (IAM) کیا ہے؟

- A. فریم ورک جو ڈیجیٹل شناختوں کا انتظام اور سسٹم کے اختیارات کو کنٹرول کرتے ہیں
- B. اینٹی وائرس یوٹیلیٹیز جو مقامی فائل ڈائریکٹریز کو اسکین کرتی ہیں
- C. ایئر گیپڈ میڈیا استعمال کرنے والا بیک اپ اسٹوریج سسٹم
- D. ایک ای میل گیٹ وے پروٹوکول جو جعلی ڈومینز کو مسترد کرتا ہے

5. مسلسل تصدیق کا کیا مطلب ہے؟

- A. فعال سیشن کے دوران صارف کی شناخت اور ڈیوائس کی حالت کی بار بار تصدیق کرنا
- B. ماسٹر پاس ورڈ ہر 10 منٹ بعد تبدیل کرنا
- C. ایک سے زیادہ الگورتھمز استعمال کرتے ہوئے ڈیٹا بیس ریکارڈز کی ہیشنگ کرنا
- D. TLS کیز استعمال کرتے ہوئے نیٹ ورک ترسیلی پیکٹس کو خفیہ کرنا

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. Zero Trust فرض کرتا ہے کہ کارپوریٹ فائر وال کے اندر کا تمام ٹریفک محفوظ ہے۔

○ درست ○ غلط

7 سوال 7

7. مائیکرو سیگمنٹیشن حملہ آوروں کی اندرونی سرورز میں لیٹرل موومنٹ کی صلاحیت کو محدود کرتی ہے۔

○ درست ○ غلط

8 سوال 8

8. کم سے کم استحقاق بطورِ طے شدہ تمام ڈیٹابیس فائلوں تک رسائی دیتا ہے۔

○ درست ○ غلط

9 سوال 9

9. مسلسل تصدیق لاگ اِن سیشن کے دوران ڈیوائس کی صحت اور کریڈینشلز کی توثیق کرتی ہے۔

○ درست ○ غلط

10 سوال 10

10. Zero Trust نافذ کرنے سے متاثرہ کارپوریٹ لاگ اِنز کے اثرات کم ہوتے ہیں۔

○ درست ○ غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. ہر رسائی پوائنٹ پر اسناد مانگنا مسلسل _____ ہے۔
2. کارپوریٹ نیٹ ورک کو چھوٹے زونز میں بانٹنا مائیکرو _____ ہے۔
3. ڈیجیٹل شناخت اور رسائی کنٹرول ترتیب دینے کے لیے _____ سسٹم استعمال ہوتا ہے۔
4. صارف کی اجازتیں محدود کرنے میں کم از کم _____ کا اصول استعمال ہوتا ہے۔
5. جڑے ہوئے آلات کی صحت جانچنے سے ڈیوائس _____ اسکین ہوتی ہے۔
6. فعال سیشنز کو لاگ کرنا اور ان کا جائزہ لینا سیکیورٹی _____ ہے۔

الفاظ کا بینک

استحقاق | آڈٹنگ | آئی اے ایم | پوسچر | تصدیق | راؤٹر | سیگمنٹیشن | فائر وال

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

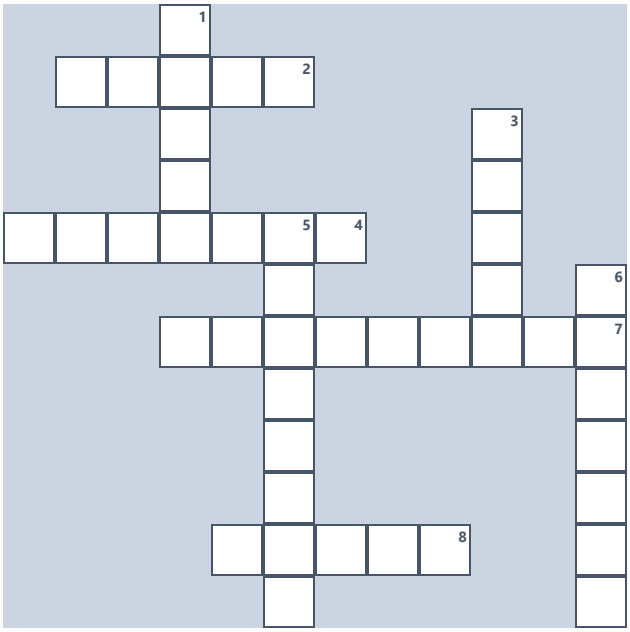
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. تصدیق	A	صارف کی اسناد تک رسائی کا انتظام۔
2. سیگمنٹیشن	B	کم سے کم رسائی کے حقوق کا اصول۔
3. IAM	C	نیٹ ورک پیکٹ ٹریفک کی روٹنگ۔
4. استحقاق	D	بیرونی نیٹ ورک رکاوٹ سے تحفظ۔
5. پوسچر	E	لاگ شدہ رسائی سیشنز کا جائزہ۔
6. آڈٹنگ	F	اندرونی نیٹ ورک زونز کی تقسیم۔
7. فائر وال	G	صارف کی اسناد کی ہمیشہ جانچ کرنا۔
8. راؤٹر	H	ڈیوائس کی صحت کی حالت کا جائزہ۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

2. نیٹ ورک پیکٹ ٹریفک کی روٹنگ (5)

4. بیرونی نیٹ ورک کی رکاوٹ سے تحفظ (7)

7. اندرونی نیٹ ورک زونز کی تقسیم (9)

8. صارف کی اسناد کی مسلسل جانچ (5)

عمودی

1. ڈیوائس کی صحت کی حالت کا جائزہ (5)

3. ریکارڈ شدہ رسائی سیشنز کا جائزہ (5)

5. صارف کی اسناد اور رسائی کا انتظام (8)

6. کم ترین رسائی کے حقوق کا اصول (7)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

2 افقی: نیٹ ورک پیکٹ ٹریفک کی روٹنگ (5 حروف):

4 افقی: بیرونی نیٹ ورک کی رکاوٹ سے تحفظ (7 حروف):

7 افقی: اندرونی نیٹ ورک زونز کی تقسیم (9 حروف):

8 افقی: صارف کی اسناد کی مسلسل جانچ (5 حروف):

عمودی

1 عمودی: ڈیوائس کی صحت کی حالت کا جائزہ (5 حروف):

3 عمودی: ریکارڈ شدہ رسائی سیشنز کا جائزہ (5 حروف):

5 عمودی: صارف کی اسناد اور رسائی کا انتظام (8 حروف):

6 عمودی: کم ترین رسائی کے حقوق کا اصول (7 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ج	ن	ک	پ	ہ	ر	چ	ت	ل	ہ	گ	ن	ح	و	م
پ	ص	گ	ی	ے	ٹ	ک	ص	ف	س	ب	ا	ب	پ	ن
ح	ک	ن	ش	ڈ	ش	ح	د	ے	ا	ش	ت	و	گ	س
ت	ر	ٹ	ل	ل	ش	و	ی	ن	چ	ئ	گ	گ	و	ہ
ی	ے	ڈ	ے	چ	س	پ	ق	ی	و	پ	ر	م	د	ی
ق	ب	ا	ئ	ت	ی	ی	ا	ف	ر	ق	و	و	پ	ف
ا	ئ	ج	ش	د	گ	ف	ت	ئ	ل	ٹ	ت	س	ا	و
ق	ح	ن	پ	س	م	ب	ا	ف	ی	ل	و	ت	چ	ل
ح	ش	ا	ت	م	ن	ت	ج	د	ر	ا	ت	ا	ہ	ر
ت	و	گ	ٹ	ر	ٹ	ہ	ف	ی	ج	و	ے	ق	ر	ج
س	ا	ا	و	م	ی	ل	ن	ے	ح	و	ش	ا	ہ	ص
ا	ی	ت	ل	ڈ	ش	ب	ج	ی	ح	ئ	س	ا	ی	ہ
ف	ڈ	ڈ	ک	چ	ن	ر	گ	ہ	س	گ	ک	ے	م	م
د	و	و	د	ف	ا	م	ق	چ	ص	ب	ڈ	ہ	ڈ	ب
د	ک	ف	چ	س	م	ن	ل	ئ	پ	گ	ف	ڈ	چ	ڈ

الفاظ کی فہرست

تصدیق
سیگمنٹیشن
ائیاےایم
استحقاق
پوسچر
اڈٹنگ
فائروال
راوٹر

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. تصدیق
B. سیگمنٹیشن
C. ائیاےایم
D. استحقاق
E. پوسچر
F. اڈٹنگ
G. فائروال
H. راوٹر

تعریفیں اور ملان کے خانے	
1. بیرونی نیٹ ورک کی رکاوٹ سے تحفظ۔	
2. ریکارڈ شدہ رسائی سیشنز کا جائزہ۔	
3. کم ترین رسائی کے حقوق کا اصول۔	
4. اندرونی نیٹ ورک زونز کی تقسیم۔	
5. نیٹ ورک پیکٹ ٹریفک کی روٹنگ۔	
6. ڈیوائس کی صحت کی حالت کا جائزہ۔	
7. صارف کی اسناد اور رسائی کا انتظام۔	
8. صارف کی اسناد کی مسلسل جانچ۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ی د ت ق ص
2. ا ا م ئ ی ا ے ی
3. س پ ر چ و
4. ل ا و ر ا ف ئ
5. ی ن ی ن ٹ م س ش گ
6. ا ت ق ا ح ق س
7. ن گ ا ٹ ڈ
8. ر ر و ٹ ا

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں		
2	محفوظ عادات جو آپ آج شروع کر سکتے ہیں		
3	ڈیوائس پر جانچی جانے والی چیزیں		
4	وہ چیزیں جو لاگ کی جاتی ہیں		
5	سائبر سیکیورٹی سے متعلق الفاظ		
6	وہ چیزیں جنہیں Zero Trust جانچتا ہے		
7	وہ مقامات جہاں آپ روزمرہ زندگی میں شناخت دکھاتے ہیں		
8	یہ ثابت کرنے کے طریقے کہ واقعی آپ ہی ہیں		
9	ڈیٹا لیک کے بعد کرنے کے کام		
10	کمپیوٹر کے متاثر ہونے کی علامات		
11	سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات		
12	کمپنی میں رسائی کی سطحیں		
13	آپ کے جانے پہچانے سیکیورٹی ٹولز کے نام		
14	نیٹ ورک کو تقسیم کیے جانے والے زونز کے نام		
15	اعتماد سے متعلق کہاوتیں		

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: زیرو ٹرسٹ نیٹ ورک آرکیٹیکچر کی طرف منتقلی



منظرنامہ: ایک بڑا انٹرپرائز اس وقت فلیٹ اندرونی نیٹ ورک استعمال کرتا ہے جس میں لوکل نیٹ ورک پر موجود کوئی بھی ڈیوائس تمام کارپوریٹ سرورز اور ڈیٹا بیسز تک رسائی حاصل کر سکتی ہے۔

بحث کا سوال: لیٹرل موومنٹ کو محدود کرنے کے لیے نیٹ ورک مائیکرو سیگمنٹیشن کی حکمت عملی ڈیزائن کریں۔

کیس اسٹڈی 2: کم سے کم استحقاق پر مبنی رسائی کنٹرول نافذ کرنا



منظرنامہ: آڈٹ لاگز سے ظاہر ہوتا ہے کہ عارضی ڈیٹا بیس صارفین اور نچلی سطح کے ملازمین کے پاس اہم اکاؤنٹنگ ڈیٹا بیسز کی عالمی ریڈ اور رائٹ اجازتیں ہیں۔

بحث کا سوال: کم سے کم استحقاق کے اصول کو نافذ کرنے کے لیے ڈیٹا بیس IAM استحقاقات کا آڈٹ کریں اور انہیں محدود کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

38	18		5	18	14	5		34	14	37	16		35	19	37	31	35

27	37	11	20	4

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: Zero Trust کیا ہے؟

Zero Trust ایک سیکیورٹی فریم ورک ہے جو فرض کرتا ہے کہ خطرات نیٹ ورک کی حد کے باہر اور اندر دونوں موجود ہیں، اور ہر درخواست کی تصدیق ضروری ہے۔ [1]

Q2: Zero Trust کا بنیادی اصول کیا ہے؟

کبھی اعتماد نہ کریں، ہمیشہ تصدیق کریں۔

Q3: مائیکرو سیگمنٹیشن کیا ہے؟

نیٹ ورک کو چھوٹے، محفوظ منطقی حصوں میں تقسیم کرنا تاکہ ٹریفک کنٹرول ہو اور خلاف ورزیاں محدود رہیں۔

Q4: کم سے کم استحقاق کیا ہے؟

صارفین کو صرف وہ کم سے کم رسائی کے حقوق دینا جو ان کے مخصوص کام انجام دینے کے لیے درکار ہوں۔ [2]

Q5: IAM کا مطلب کیا ہے؟

شناخت اور رسائی کا انتظام۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: ڈیوائس پوسچر چیک کیسے مدد کرتا ہے؟

رسائی دینے سے پہلے یہ تصدیق کرتا ہے کہ ڈیوائس پیچ شدہ ہے، فعال اینٹی وائرس چلا رہی ہے اور محفوظ ہے۔

Q7: لیٹرل موومنٹ کیا ہے؟

وہ عمل جس کے ذریعے حملہ آور ابتدائی طور پر سمجھوتہ شدہ نوڈ سے زیادہ قیمتی سسٹمز تک نیٹ ورک میں آگے بڑھتے ہیں۔

Q8: کیا زیرو ٹرسٹ فائر والز کی جگہ لے لیتا ہے؟

نہیں، یہ شناخت پر مبنی جانچ اور اندرونی سیگمنٹیشن فائر والز شامل کر کے انہیں بہتر بناتا ہے۔

Q9: مسلسل تصدیق کیا ہے؟

فعال لاگ اِن سیشن کے دوران صارف کی شناخت کی مسلسل تصدیق، صرف ابتدائی سائن اِن پر نہیں۔

Q10: فلیٹ نیٹ ورک خطرناک کیوں ہے؟

فلیٹ نیٹ ورکس میں ایک متاثرہ نوڈ حملہ آوروں کو نیٹ ورک پر موجود کسی بھی ڈیٹا بیس تک آسانی سے رسائی دے دیتا ہے۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: Zero Trust پیرامیٹر ماڈل کو کیسے حل کرتا ہے؟

یہ پرانے 'castle-and-moat' ماڈل کی جگہ لیتا ہے، اور دفاع کو حدی نیٹ ورکس سے مخصوص صارف شناختوں اور وسائل پر منتقل کرتا ہے۔

Q2: پالیسی ڈیسیژن پوائنٹ (PDP) کیا ہے؟

سسٹم کا وہ جزو جو سیکیورٹی اصولوں کے مطابق اجازت کی درخواستوں کا جائزہ لیتا ہے تاکہ طے کرے کہ رسائی دی جائے یا نہیں۔

Q3: پالیسی انفورسمنٹ پوائنٹ (PEP) کیا ہے؟

سسٹم نوڈ (جیسے گیٹ وے یا پراکسی) جو PDP کے فیصلے کی بنیاد پر کنکشن درخواستوں کو عملی طور پر اجازت دیتا یا بلاک کرتا ہے۔

Q4: رول بیسڈ ایکسیس کنٹرول (RBAC) زیرو ٹرسٹ کی معاونت کیسے کرتا ہے؟

RBAC اجازتوں کو مخصوص کرداروں میں گروپ کرتا ہے، جس سے صارفین کو حد سے زیادہ انتظامی استحقاق ملنے سے بچنے میں مدد ملتی ہے۔

Q5: سیاق و سباق پر مبنی رسائی کنٹرول کیا ہے؟

خطرے کا اندازہ لگانے کے لیے جغرافیائی مقام، ڈیوائس پوسچر اور لاگ اِن کے وقت جیسے ثانوی اشاروں سے لاگ اِن درخواستوں کا جائزہ۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: مائیکرو سیگمنٹیشن عام VLANs سے کیسے مختلف ہے؟

VLANs نیٹ ورکس کو لیئر 2 پر وسیع منطقی حصوں میں تقسیم کرتے ہیں، جبکہ مائیکرو سیگمنٹیشن انفرادی ورک لوڈز کو الگ کرنے کے لیے سافٹ ویئر پالیسی استعمال کرتی ہے۔

Q7: جسٹ ان ٹائم (JIT) رسائی کیا ہے؟

بلند انتظامی اجازتیں عارضی طور پر دینا اور کام مکمل ہونے پر انہیں خود بخود واپس لے لینا۔

Q8: آپ زیرو ٹرسٹ فریم ورک میں APIs کو کیسے محفوظ بناتے ہیں؟

کرپٹوگرافک طور پر دستخط شدہ OAuth ٹوکنز کا تقاضا کر کے اور ہر API گیٹ وے پر درخواست کے دستخطوں کا آڈٹ کر کے۔

Q9: زیرو ٹرسٹ نیٹ ورک ایکسیس (ZTNA) کلائنٹ کیا ہے؟

سافٹ ویئر ایجنٹ جو خام نیٹ ورک سب نیٹس کے بجائے مخصوص ایپلیکیشنز تک محفوظ، خفیہ کردہ باہر جانے والے کنکشنز قائم کرتا ہے۔

Q10: لاگ آڈیٹنگ Zero Trust میں کیسے مدد کرتی ہے؟

مسلسل لاگنگ خودکار سیکیورٹی تجزیاتی ٹولز کو بے قاعدگیاں پکڑنے اور مشکوک لاگ اِنز کو فوراً معطل کرنے کے قابل بناتی ہے۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

Zero Trust آرکیٹیکچرز روایتی قلعہ اور خندق والے ماڈل کی جگہ شناخت پر مبنی تصدیقی اصولوں کو دیتے ہیں۔

2. سیکیورٹی بصیرت

نیٹ ورک مائیکرو سیگمنٹیشن ورک لوڈز کو چھوٹے محفوظ زونز میں الگ کر کے میل ویئر کی پہنچ کا دائرہ کم کرتی ہے۔

3. سیکیورٹی بصیرت

Zero Trust کی توجہ نیٹ ورک سیگمنٹس کے بجائے اثاثوں، سروسز اور اکاؤنٹس جیسے وسائل کے تحفظ پر ہے۔ [1]

4. سیکیورٹی بصیرت

کم سے کم استحقاق کی رسائی کی پالیسیاں بنیادی ڈیٹابیس سے اندرونی خطرے کے تحت ڈیٹا کے اخراج کا خطرہ کم کرتی ہیں۔

5. سیکیورٹی بصیرت

ڈیوائس پوسچر کی توثیق آپریٹنگ سسٹم پیچ کی سطح اور فعال اینٹی وائرس کی حالت کو حقیقی وقت میں جانچتی ہے۔

6. سیکیورٹی بصیرت

Zero Trust Network Access (ZTNA) بروکرز صارف کی رسائی کا دائرہ محدود کرنے کے لیے کارپوریٹ VPNs کی جگہ لے سکتے ہیں یا ان کی تکمیل کر سکتے ہیں۔

7. سیکیورٹی کی بصیرت

Just-in-Time (JIT) انتظامی استحقاق کی سپردگی ڈومین کنٹرولرز پر اسناد کی چوری کا خطرہ کم کرتی ہے۔

8. سیکیورٹی کی بصیرت

مسلسل توثیق سیشن کے رویے کو لاگ اور آڈٹ کرتی ہے، اور غیر معمولی اسکرپٹ عمل درآمد کے نمونے دکھانے والے صارفین کو معطل کر دیتی ہے۔

9. سیکیورٹی کی بصیرت

روایتی پیرامیٹر دفاعی اقدامات انتظامی اسناد لیک ہونے کے بعد پہلو بہ پہلو حملوں کو روکنے میں ناکام رہتے ہیں۔

10. سیکیورٹی بصیرت

NIST Special Publication 800-207 (2020) تعیناتی کے ماڈلز کے ساتھ Zero Trust آرکیٹیکچر کی ایک تجریدی تعریف پیش کرتی ہے۔ [1]

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: A

تدریسی نوٹ

زیرو ٹرسٹ سیکیورٹی کا بنیادی اصول کیا ہے؟ → کبھی بھروسا نہ کریں، ماخذ سے قطع نظر ہر رسائی کی درخواست کی ہمیشہ تصدیق کریں

2 سوال 2 — درست جواب: A

تدریسی نوٹ

نیٹ ورک مائیکرو سیگمنٹیشن کیا ہے؟ → نیٹ ورکس کو چھوٹے الگ تھلگ زونز میں تقسیم کرنا تاکہ پہلو بہ پہلو پھیلاؤ محدود رہے

3 سوال 3 — درست جواب: A

تدریسی نوٹ

کم سے کم استحقاق کا اصول کیا ہے؟ → صارف کی رسائی کی اجازتوں کو صرف ان تک محدود کرنا جو اس کے کام کے لیے ضروری ہیں

4 سوال 4 — درست جواب: A

تدریسی نوٹ

شناخت اور رسائی کا انتظام (IAM) کیا ہے؟ → فریم ورک جو ڈیجیٹل شناختوں کا انتظام اور سسٹم کے اختیارات کو کنٹرول کرتے ہیں

5 سوال 5 — درست جواب: A

تدریسی نوٹ

مسلسل تصدیق کا کیا مطلب ہے؟ → فعال سیشن کے دوران صارف کی شناخت اور ڈیوائس کی حالت کی بار بار تصدیق کرنا

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

غلط: Zero Trust نیٹ ورک کی لوکیشن کی بنیاد پر، اندر یا باہر، کوئی ضمنی اعتماد نہیں دیتا۔

7 سوال 7

درست جواب: درست

تدریسی نوٹ

درست: چھوٹے الگ تھلگ زونز اس بات کو محدود کرتے ہیں کہ دراندازی کرنے والا سرورز کے درمیان کتنا آگے جا سکتا ہے۔

8 سوال 8

درست جواب: غلط

تدریسی نوٹ

غلط: کم از کم استحقاق ہر کردار کو صرف اس کے لیے درکار کم از کم رسائی دیتا ہے۔

9 سوال 9

درست جواب: درست

تدریسی نوٹ

مسلسل تصدیق لاگ اِن سیشن کے دوران ڈیوائس کی صحت اور کریڈینشلز کی توثیق کرتی ہے۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

Zero Trust نافذ کرنے سے متاثرہ کارپوریٹ لاگ اِنز کے اثرات کم ہوتے ہیں۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

G 1. تصدیق	F 2. سیگمنٹیشن	A 3. IAM	B 4. استحقاق
H 5. پوسچر	E 6. آڈٹنگ	D 7. فائر وال	C 8. راؤٹر

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 تصدیق	2 سیگمنٹیشن	3 آئی اے ایم	4 استحقاق
5 پوسچر	6 آڈٹنگ		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 G – فائروال	2 F – اڈٹنگ	3 D – استحقاق	4 B – سیگمنٹیشن
5 H – راوٹر	6 E – پوسچر	7 C – ائیاےایم	8 A – تصدیق

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ تصدیق، سیگمنٹیشن اور IAM کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

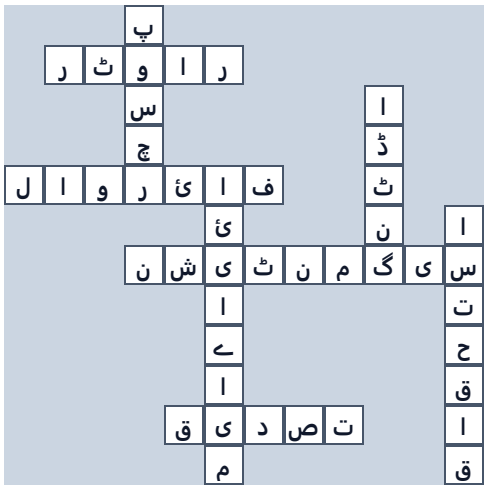
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

چ	ن	ک	پ	ہ	ر	چ	ت	ل	ہ	گ	ن	ح	و	م
پ	ں	گ	ی	ے	ٹ	ک	ں	ف	س	ب	ا	پ	ب	ن
ح	ک	ن	ش	ڈ	ش	ح	د	ے	ا	ش	ت	و	گ	س
ت	ر	ٹ	ل	ل	ش	و	ی	ن	ج	ئ	گ	گ	و	ہ
ی	ے	ڈ	ے	ج	س	پ	ق	ی	و	پ	ر	م	د	ی
ق	ب	ا	ئ	ت	ی	ی	ا	ف	ر	ق	و	و	پ	ف
ا	ئ	ج	ش	د	گ	ف	ت	ئ	ل	ٹ	ت	س	ا	و
ق	ح	ن	پ	ں	م	ب	ا	ف	ی	ل	و	ت	چ	ل
ح	ش	ا	ت	م	ن	ت	چ	د	ر	ا	ت	ا	ہ	ر
ت	و	گ	ٹ	ر	ٹ	ہ	ف	ی	ج	و	ے	ق	ر	چ
س	ا	ا	و	م	ی	ل	ح	ن	ے	ش	ا	ہ	ں	ص
ا	ی	ت	ل	ڈ	ش	ب	ج	ی	ح	ئ	س	ا	ی	ہ
ف	ڈ	ڈ	ک	چ	ن	ر	گ	ہ	س	گ	ک	ے	م	م
د	و	و	د	ف	ا	م	ق	ج	ں	ب	ڈ	ہ	ڈ	ب
د	ک	ف	چ	س	م	ں	ل	ئ	پ	گ	ف	ڈ	چ	ڈ

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

2 افقی: راوٹر نیٹ ورک پیکٹ ٹریفک کی روٹنگ (5 حروف)

4 افقی: فائروال بیرونی نیٹ ورک کی رکاوٹ سے تحفظ (7 حروف)

7 افقی: سیگمنٹیشن اندرونی نیٹ ورک زونز کی تقسیم (9 حروف)

8 افقی: تصدیق صارف کی اسناد کی مسلسل جانچ (5 حروف)

عمودی

1 عمودی: پوسچر ڈیوائس کی صحت کی حالت کا جائزہ (5 حروف)

3 عمودی: اڈٹنگ ریکارڈ شدہ رسائی سیشنز کا جائزہ (5 حروف)

5 عمودی: ائیاےایم صارف کی اسناد اور رسائی کا انتظام (8 حروف)

6 عمودی: استحقاق کم ترین رسائی کے حقوق کا اصول (7 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. یدتقص → تصدیق
2. اامئیاےی → ائیاےایم
3. سپرچو → پوسچر
4. لاورافئ → فائروال
5. ینینٹمسشگ → سیگمنٹیشن
6. اتقاحقس → استحقاق
7. نگاٹڈ → اڈٹنگ
8. رروٹا → راوٹر

خفیہ سائفر چیلنج کی کلید

"ہمیشہ زیرو ٹرسٹ سے تصدیق"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: زیرو ٹرسٹ نیٹ ورک آرکیٹیکچر کی طرف منتقلی

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک بڑا انٹرپرائز فی الحال فلیٹ اندرونی نیٹ ورک استعمال کرتا ہے جہاں مقامی نیٹ ورک پر موجود کوئی بھی ڈیوائس تمام کارپوریٹ سرورز اور ڈیٹا بیسز تک رسائی حاصل کر سکتی ہے۔
- تجویز کردہ حکمت عملی اور حل: فلیٹ نیٹ ورک کو الگ تھلگ محکمانہ زونز میں تقسیم کریں۔ زونز کے درمیان ٹریفک کنٹرول کرنے کے لیے اندرونی فائر والز لگائیں، اور ہر رسائی کے لیے کنکشن ٹوکن کی توثیق لازمی کریں۔

B کیس اسٹڈی 2: کم سے کم استحقاق پر مبنی رسائی کنٹرول نافذ کرنا

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: آڈٹ لاگز سے ظاہر ہوتا ہے کہ عارضی ڈیٹا بیس صارفین اور نچلے درجے کے ملازمین کے پاس اہم اکاؤنٹنگ ڈیٹا بیسز کی عالمی ریڈ اور رائٹ اجازتیں ہیں۔
- تجویز کردہ حکمت عملی اور حل: تمام عالمی انتظامی مراعات منسوخ کریں۔ ملازمت کے عین کرداروں کے مطابق رول بیسڈ ایکسیس کنٹرول (RBAC) نافذ کریں، اور ہفتہ وار خودکار اجازتوں کے جائزے قائم کریں۔