نام: _____ تاریخ: _____ نمره: _____

معماری و امنیت اعتماد صفر

راستی‌آزمایی مداوم، ریزتقسیم‌بندی شبکه، مدیریت هویت و دسترسی، کمترین امتیاز و بررسی‌های وضعیت امنیتی.

مرور یادگیری امنیت اعتماد صفر

خوش آمدید! این بستهٔ فعالیت شما را در بررسی معماری و امنیت Zero Trust راهنمایی می‌کند. با راستی‌آزمایی پیوسته، ریزتقسیم‌بندی شبکه، مدیریت هویت و دسترسی (IAM)، حداقل امتیاز و ممیزی نشست آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- [ ] **بخش 1-4: بر امنیت سایبری و پیشگیری از تهدید مسلط شوید.**
- [ ] **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- [ ] **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- [ ] **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- [ ] **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- [ ] **تکمیلی: چالش سریع فکر کن**

ایمن‌شده
رمزگذاری داده
استاندارد AES 256 بیتی

منطبق
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

اعتماد صفر
سیاست دسترسی
احراز هویت چندعاملی

باز کردن راهنمای امنیت سایبری VPN.com

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

نقشهٔ راه یادگیری راهبرد اعتماد صفر شما

- اصل اساسی راستی‌آزمایی پیوسته را درک کنید.
- ریزبخش‌بندی شبکه و دسترسی با حداقل امتیاز را پیاده‌سازی کنید.
- بررسی‌های وضعیت امنیتی دستگاه و ممیزی نشست‌های فعال را پیکربندی کنید.

دستورالعمل راهنمای امنیت اعتماد صفر

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره معماری Zero Trust به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

معماری و امنیت اعتماد صفر (مقدمه)

امنیت اعتماد صفر مدل‌های قدیمی پیرامون شبکه را با سیاست سخت‌گیرانهٔ «هرگز اعتماد نکن، همیشه راستی‌آزمایی کن» جایگزین می‌کند. پیاده‌سازی ریزبخش‌بندی، مدیریت هویت و دسترسی (IAM)، حداقل امتیاز دسترسی و بررسی وضعیت، حرکت جانبی تهدیدها را مسدود می‌کند.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. اصل اساسی امنیت Zero Trust چیست؟

- A. هرگز اعتماد نکن، همیشه هر درخواست دسترسی را بدون توجه به منبع تأیید کن
- B. فرض اینکه همهٔ ترافیک داخل دیوار آتش سازمانی امن است
- C. ذخیرهٔ فایل‌های پایگاه داده بدون رمزگذاری برای افزایش سرعت
- D. اِعمال احراز هویت ایمیل فقط با رکوردهای SPF

2 2. ریزبخش‌بندی شبکه چیست؟

- A. تقسیم شبکه‌ها به منطقه‌های کوچک و ایزوله برای مهار حرکت جانبی
- B. رمزگذاری کارت‌های شبکه هنگام انتقال داده
- C. اتصال همهٔ سرورهای محلی به یک نشانی IP عمومی واحد
- D. پایش کلیدزنی‌های کاربر در نشست‌های مرورگر

3 3. اصل حداقل امتیاز (least privilege) چیست؟

- A. محدود کردن مجوزهای دسترسی کاربر به آنچه برای کارش لازم است
- B. اعطای همهٔ امتیازهای سیستمی به هر کاربر به‌صورت پیش‌فرض
- C. اجازهٔ ورود ناشناس به سرورهای پایگاه داده سازمانی
- D. پیکربندی روترهای Wi-Fi عمومی بدون گذرواژه

4 4. مدیریت هویت و دسترسی (IAM) چیست؟

- A. چارچوب‌هایی که هویت‌های دیجیتال را مدیریت و امتیازهای سیستم را کنترل می‌کنند
- B. ابزارهای آنتی‌ویروس که پوشه‌های فایل محلی را اسکن می‌کنند
- C. سامانهٔ ذخیرهٔ پشتیبان با رسانه‌های جداشده از شبکه (air-gapped)
- D. یک پروتکل دروازهٔ ایمیل که دامنه‌های جعلی را رد می‌کند

5 5. احراز هویت پیوسته به چه معناست؟

- A. تأیید مکرر هویت کاربر و وضعیت امنیتی دستگاه در طول نشست فعال
- B. تغییر گذرواژهٔ اصلی هر 10 دقیقه
- C. درهم‌سازی رکوردهای پایگاه داده با چند الگوریتم
- D. رمزگذاری بسته‌های انتقال شبکه با کلیدهای TLS

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. اعتماد صفر فرض می‌کند که همهٔ ترافیک داخل دیوار آتش سازمانی امن است.

○ درست ○ نادرست

7 پرسش 7

7. ریزبخش‌بندی (micro-segmentation) توانایی مهاجمان برای حرکت جانبی در سرورهای داخلی را محدود می‌کند.

○ درست ○ نادرست

8 پرسش 8

8. اصل کمترین امتیاز به‌طور پیش‌فرض دسترسی به همهٔ فایل‌های پایگاه داده را می‌دهد.

○ درست ○ نادرست

9 پرسش 9

9. راستی‌آزمایی مداوم، سلامت دستگاه و اعتبارنامه‌ها را در سراسر نشست ورود اعتبارسنجی می‌کند.

○ درست ○ نادرست

10 پرسش 10

10. پیاده‌سازی اعتماد صفر تأثیر ورودهای سازمانی در معرض خطر را کاهش می‌دهد.

○ درست ○ نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. الزام اعتبارنامه در هر نقطهٔ دسترسی، _____ مداوم است.
2. تقسیم شبکهٔ شرکتی به منطقه‌های بسیار کوچک، ریز- _____ است.
3. پیکربندی هویت‌های دیجیتال و کنترل دسترسی از سامانهٔ _____ استفاده می‌کند.
4. محدود کردن مجوزهای کاربر از اصل حداقل _____ پیروی می‌کند.
5. ارزیابی سلامت دستگاه‌های متصل، _____ دستگاه را بررسی می‌کند.
6. ثبت و بازبینی نشست‌های فعال، _____ امنیتی است.

بانک واژگان

امتیاز | بخش‌بندی | تأیید | دیوار آتش | مدیریت هویت | مسیریاب | ممیزی | وضعیت

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

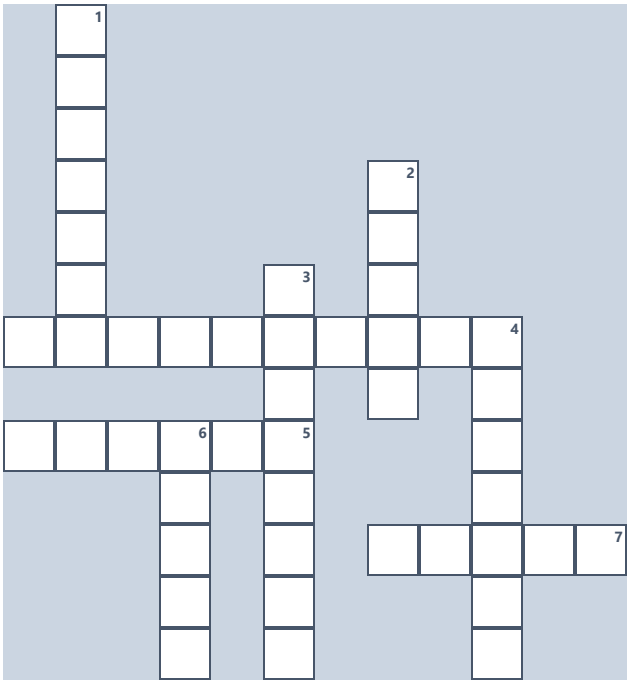
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. راستی‌آزمایی	A	مدیریت دسترسی به اعتبارنامه‌های کاربر.
2. بخش‌بندی	B	اصل کمترین حقوق دسترسی.
3. مدیریت هویت و دسترسی (IAM)	C	مسیریابی ترافیک بستهٔ شبکه.
4. امتیاز دسترسی	D	حفاظت مرزی شبکهٔ خارجی.
5. وضعیت امنیتی	E	بررسی نشست‌های دسترسی ثبت‌شده.
6. ممیزی	F	تقسیم مناطق شبکهٔ داخلی.
7. دیوار آتش	G	همیشه اعتبارنامهٔ کاربر را بررسی می‌کند.
8. روتر	H	ارزیابی وضعیت سلامت دستگاه.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

4. مدیریت دسترسی به اعتبارنامه‌های کاربر. (10)

5. اصل حداقل حقوق دسترسی. (6)

7. بازبینی نشست‌های دسترسی ثبت‌شده. (5)

عمودی

1. تقسیم منطقه‌های داخلی شبکه. (7)

2. ارزیابی سلامت دستگاه. (5)

3. حفاظت مرزی شبکهٔ بیرونی. (8)

4. هدایت ترافیک بسته‌های شبکه میان مسیرها. (7)

6. بررسی همیشگی اعتبارنامه‌های کاربر. (5)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

4 افقی: مدیریت دسترسی به اعتبارنامه‌های کاربر. (10 حرف):

5 افقی: اصل حداقل حقوق دسترسی. (6 حرف):

7 افقی: بازبینی نشست‌های دسترسی ثبت‌شده. (5 حرف):

عمودی

1 عمودی: تقسیم منطقه‌های داخلی شبکه. (7 حرف):

2 عمودی: ارزیابی سلامت دستگاه. (5 حرف):

3 عمودی: حفاظت مرزی شبکهٔ بیرونی. (8 حرف):

4 عمودی: هدایت ترافیک بسته‌های شبکه میان مسیرها. (7 حرف):

6 عمودی: بررسی همیشگی اعتبارنامه‌های کاربر. (5 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ح	ظ	س	ت	غ	ذ	ح	ص	غ	ش	ظ	ن	ع	ض	ت
ک	ف	ت	ق	ج	ژ	ر	پ	م	ا	ت	ب	پ	ط	و
ژ	ز	ی	و	ژ	ن	ک	ز	ث	س	ا	ع	ش	ر	ث
ذ	ص	ع	ز	ژ	ی	ت	م	ا	ص	ی	ژ	ع	ظ	خ
ش	ش	ض	ع	غ	م	ف	ک	ک	خ	ی	ر	پ	ف	ظ
ی	ض	و	د	ف	د	پ	د	م	ی	د	ث	ی	ق	ه
د	گ	ت	ی	م	ی	ح	ز	ی	خ	ز	ی	ث	ا	ص
ن	ث	ع	ن	ظ	ر	پ	گ	ب	و	ا	ی	ی	ض	ب
ب	ث	ژ	ا	ث	ی	ض	ث	چ	خ	ا	ذ	م	ث	غ
ش	ع	ش	ج	ذ	ت	ف	ی	ق	چ	ع	ر	ل	م	چ
خ	ا	ع	ط	ه	ص	ظ	ک	و	ع	ز	ا	غ	ک	
ب	ف	ت	ص	ه	و	پ	ح	ف	ن	م	ر	ا	ت	غ
ی	ه	ژ	ح	ی	ذ	ش	غ	ز	س	س	ق	ط	ش	
خ	ظ	ع	خ	ی	ت	ا	ض	ل	ح	گ	پ	ه	ف	ه
ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی	ه	ح

فهرست واژگان

تأیید
بخشبندی
مدیریتهویت
امتیاز
وضعیت
ممیزی
دیواراتش
مسیریاب

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان	تعاریف و فیلدهای تطبیق
A. تأیید	1. حفاظت مرزی شبکهٔ بیرونی.
B. بخشبندی	2. بازبینی نشست‌های دسترسی ثبت‌شده.
C. مدیریتهویت	3. اصل حداقل حقوق دسترسی.
D. امتیاز	4. تقسیم منطقه‌های داخلی شبکه.
E. وضعیت	5. هدایت ترافیک بسته‌های شبکه میان مسیرها.
F. ممیزی	6. ارزیابی سلامت دستگاه.
G. دیواراتش	7. مدیریت دسترسی به اعتبارنامه‌های کاربر.
H. مسیریاب	8. بررسی همیشگی اعتبارنامه‌های کاربر.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ی ی ت د ا _____
2. ی ر م د ی ت ه و ت ی _____
3. ع و ت ی ض _____
4. ا ت ش ا ر د ی و _____
5. ن ی ب ش ب د خ _____
6. ا ی ا ت ز م _____
7. ز ی م ی م _____
8. س ر ب م ا ی ی _____

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
2	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
3	چیزهایی که روی یک دستگاه بررسی می‌شوند		
4	چیزهایی که ثبت (log) می‌شوند		
5	واژه‌های مرتبط با امنیت سایبری		
6	چیزهایی که Zero Trust بررسی می‌کند		
7	جاهایی که در زندگی روزمره مدرک شناسایی نشان می‌دهید		
8	روش‌های اثبات اینکه واقعاً خودتان هستید		
9	کارهایی که پس از نشت داده باید انجام داد		
10	نشانه‌های آلوده بودن رایانه		
11	دلایل به‌روزرسانی نرم‌افزار		
12	سطوح دسترسی در یک شرکت		
13	ابزارهای امنیتی که می‌شناسید		
14	منطقه‌هایی که یک شبکه می‌تواند به آن‌ها تقسیم شود		
15	ضرب‌المثل‌هایی دربارهٔ اعتماد		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: گذار به معماری شبکهٔ اعتماد صفر



سناریو: یک سازمان بزرگ اکنون از یک شبکهٔ داخلی مسطح استفاده می‌کند که در آن هر دستگاه در شبکهٔ محلی می‌تواند به همهٔ سرورها و پایگاه‌های داده شرکت دسترسی داشته باشد.

پرسش برای بحث: یک راهبرد ریزبخش‌بندی (micro-segmentation) شبکه برای محدود کردن حرکت جانبی طراحی کنید.

مطالعهٔ موردی 2: استقرار کنترل‌های دسترسی با کمترین امتیاز



سناریو: گزارش‌های ممیزی نشان می‌دهند کاربران موقت پایگاه داده و کارکنان رده‌پایین مجوزهای خواندن و نوشتن سراسری روی پایگاه‌های داده حسابداری حیاتی دارند.

پرسش برای بحث: امتیازهای IAM پایگاه داده را ممیزی و محدود کنید تا کمترین امتیاز (least privilege) اعمال شود.

ایستگاه بررسی 9: رمزگشایی

متخصص امنیت سایبری از دارایی‌های شبکه در برابر عوامل تهدید آنلاین محافظت می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

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

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

32	12	1	28	21	28		12	10		32	28	32	1	10		10	32	32	1	4

12	23	17		10	1	28	4	21	1

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش A)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q1: اعتماد صفر چیست؟

اعتماد صفر چارچوبی امنیتی است که فرض می‌کند تهدیدها هم بیرون و هم درون مرز شبکه وجود دارند و برای هر درخواست راستی‌آزمایی لازم است. [1]

Q2: قاعدهٔ اصلی اعتماد صفر چیست؟

هرگز اعتماد نکن، همیشه راستی‌آزمایی کن.

Q3: ریزبخش‌بندی چیست؟

تقسیم شبکه به بخش‌های منطقی کوچک و امن برای کنترل ترافیک و مهار نقض‌ها.

Q4: کمترین امتیاز دسترسی چیست؟

دادن حداقل حقوق دسترسی لازم به کاربران فقط برای انجام وظایف کاری خاص آنها. [2]

Q5: IAM مخفف چیست؟

مدیریت هویت و دسترسی.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش B)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q6: بررسی وضعیت دستگاه چه کمکی می‌کند؟

راستی‌آزمایی می‌کند که دستگاه وصله شده، آنتی‌ویروس فعال دارد و پیش از اجازهٔ دسترسی ایمن است.

Q7: حرکت جانبی چیست؟

فرایندی که مهاجمان برای حرکت در شبکه از یک گرهٔ نفوذشدهٔ اولیه به سامانه‌های باارزش‌تر به کار می‌برند.

Q8: آیا اعتماد صفر جایگزین دیوارهای آتش می‌شود؟

خیر، با افزودن بررسی‌های هویت‌محور و دیوارهای آتش بخش‌بندی داخلی، آن‌ها را تقویت می‌کند.

Q9: احراز هویت پیوسته چیست؟

راستی‌آزمایی مداوم هویت کاربر در طول نشست ورود فعال، نه فقط در ورود اولیه.

Q10: چرا شبکهٔ تخت خطرناک است؟

در شبکه‌های تخت، یک گره در معرض خطر به مهاجمان اجازه می‌دهد به‌راحتی به هر پایگاه‌داده در شبکه دسترسی پیدا کنند.

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q1: اعتماد صفر چگونه به مدل پیرامونی می‌پردازد؟

مدل منسوخ «قلعه و خندق» را جایگزین می‌کند و دفاع را از شبکه‌های مرزی به هویت‌ها و منابع مشخص کاربر منتقل می‌کند.

Q2: نقطهٔ تصمیم سیاست (PDP) چیست؟

مؤلفهٔ سیستمی که درخواست‌های مجوز را با قواعد امنیتی ارزیابی می‌کند تا تصمیم بگیرد دسترسی داده شود یا نه.

Q3: نقطهٔ اجرای سیاست (PEP) چیست؟

گره سیستمی (مانند دروازه یا پروکسی) که بر اساس تصمیم PDP درخواست‌های اتصال را از نظر فیزیکی مجاز یا مسدود می‌کند.

Q4: کنترل دسترسی مبتنی بر نقش (RBAC) چگونه از اعتماد صفر پشتیبانی می‌کند؟

RBAC مجوزها را در نقش‌های مشخص گروه‌بندی می‌کند و به جلوگیری از ارث‌بری امتیازهای مدیریتی بیش‌ازحد توسط کاربران کمک می‌کند.

Q5: کنترل دسترسی مبتنی بر زمینه چیست؟

ارزیابی درخواست‌های ورود با استفاده از سرنخ‌های ثانویه مانند موقعیت جغرافیایی، وضعیت دستگاه و زمان ورود برای سنجش ریسک.

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q6: ریزبخش‌بندی با VLANهای استاندارد چه تفاوتی دارد؟

VLANها شبکه‌ها را در لایهٔ 2 به بخش‌های منطقی گسترده تقسیم می‌کنند، در حالی که ریزتقسیم‌بندی با سیاست نرم‌افزاری بارهای کاری منفرد را ایزوله می‌کند.

Q7: دسترسی به‌موقع (JIT) چیست؟

اعطای موقت مجوزهای مدیریتی ارتقایافته و لغو خودکار آنها پس از پایان کار.

Q8: در چارچوب اعتماد صفر چگونه APIها را ایمن می‌کنید؟

با الزام به توکن‌های OAuth امضاشدهٔ رمزنگاری و ممیزی امضای درخواست‌ها در هر دروازهٔ API.

Q9: کلاینت دسترسی شبکهٔ اعتماد صفر (ZTNA) چیست؟

عامل نرم‌افزاری که اتصال‌های خروجی امن و رمزگذاری‌شده را به برنامه‌های مشخص برقرار می‌کند، نه به زیرشبکه‌های خام شبکه.

Q10: ممیزی لاگ چگونه به اعتماد صفر کمک می‌کند؟

ثبت لاگ مداوم به ابزارهای تحلیل امنیتی خودکار اجازه می‌دهد ناهنجاری‌ها را شناسایی و ورودهای مخرب را فوراً معلق کنند.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ امنیت سایبری

واقعیت‌های دنیای واقعی دربارهٔ نقض‌های امنیتی، سازوکارهای دفاعی و استانداردهای انطباق را مرور کنید.

1. بینش امنیت

معماری‌های اعتماد صفر مدل قدیمی قلعه و خندق را با قواعد راستی‌آزمایی هویت‌محور جایگزین می‌کنند.

2. بینش امنیت

ریزبخش‌بندی شبکه با جداسازی بارهای کاری در ناحیه‌های کوچک محافظت‌شده، محدوده‌ای را که بدافزار می‌تواند به آن برسد کوچک می‌کند.

3. بینش امنیت

اعتماد صفر بر حفاظت از منابعی مانند دارایی‌ها، سرویس‌ها و حساب‌ها تمرکز دارد، نه بخش‌های شبکه. [1]

4. بینش امنیت

سیاست‌های دسترسی با کمترین امتیاز، خطر خروج داده از پایگاه‌های داده اصلی توسط تهدید داخلی را کاهش می‌دهند.

5. بینش امنیت

اعتبارسنجی وضعیت دستگاه، سطوح وصله‌های سیستم‌عامل و وضعیت فعال آنتی‌ویروس را به‌صورت بلادرنگ بررسی می‌کند.

6. بینش امنیت

کارگزارهای دسترسی شبکهٔ اعتماد صفر (ZTNA) می‌توانند جایگزین VPNهای سازمانی شوند یا مکمل آن‌ها باشند تا دامنهٔ دسترسی کاربران را محدود کنند.

7. بینش امنیت

تفویض امتیاز مدیریتی Just-In-Time (JIT) خطر سرقت اطلاعات ورود را روی کنترلرهای دامنه کاهش می‌دهد.

8. بینش امنیت

اعتبارسنجی مداوم، نشست‌ها را ثبت و ممیزی می‌کند و کاربرانی را که الگوهای اجرای اسکریپت غیرعادی نشان می‌دهند معلق می‌کند.

9. بینش امنیت

دفاع‌های محیطی سنتی پس از افشای یک اعتبارنامهٔ مدیریتی نمی‌توانند حملات جانبی را مسدود کنند.

10. بینش امنیت

انتشارات ویژهٔ NIST 800-207 (2020) تعریفی انتزاعی از معماری اعتماد صفر همراه با مدل‌های استقرار ارائه می‌دهد. [1]

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردهای جهانی NIST، OWASP و انطباق با حریم خصوصی داده گردآوری شده‌اند.

منابع علمی و صنعتی

[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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1

پاسخ درست: **A**

نکتهٔ آموزشی

اصل اساسی امنیت Zero Trust چیست؟ → هرگز اعتماد نکن، همیشه هر درخواست دسترسی را بدون توجه به منبع تأیید کن

2 پرسش 2

پاسخ درست: **A**

نکتهٔ آموزشی

ریزبخش‌بندی شبکه چیست؟ → تقسیم شبکه‌ها به منطقه‌های کوچک و ایزوله برای مهار حرکت جانبی

3 پرسش 3

پاسخ درست: **A**

نکتهٔ آموزشی

اصل حداقل امتیاز (least privilege) چیست؟ → محدود کردن مجوزهای دسترسی کاربر به آنچه برای کارش لازم است

4 پرسش 4

پاسخ درست: **A**

نکتهٔ آموزشی

مدیریت هویت و دسترسی (IAM) چیست؟ → چارچوب‌هایی که هویت‌های دیجیتال را مدیریت و امتیازهای سیستم را کنترل می‌کنند

5 پرسش 5

پاسخ درست: **A**

نکتهٔ آموزشی

احراز هویت پیوسته به چه معناست؟ → تأیید مکرر هویت کاربر و وضعیت امنیتی دستگاه در طول نشست فعال

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: Zero Trust هیچ اعتماد ضمنی بر اساس موقعیت شبکه، چه درون و چه بیرون، اعطا نمی‌کند.

7 پرسش 7

پاسخ درست: درست

نکتهٔ آموزشی

درست: مناطق کوچک و جداشده محدود می‌کنند نفوذگر چقدر می‌تواند میان سرورها حرکت کند.

8 پرسش 8

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: کمترین امتیاز (least privilege) فقط حداقل دسترسی مورد نیاز هر نقش را می‌دهد.

9 پرسش 9

پاسخ درست: درست

نکتهٔ آموزشی

راستی‌آزمایی مداوم، سلامت دستگاه و اعتبارنامه‌ها را در سراسر نشست ورود اعتبارسنجی می‌کند.

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

پیاده‌سازی اعتماد صفر تأثیر ورودهای سازمانی در معرض خطر را کاهش می‌دهد.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

G 1. راستی‌آزمایی	F 2. بخش‌بندی	A 3. مدیریت هویت و دسترسی (IAM)	B 4. امتیاز دسترسی
H 5. وضعیت امنیتی	E 6. ممیزی	D 7. دیوار آتش	C 8. روتر

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 تأیید	2 بخش‌بندی	3 مدیریت هویت	4 امتیاز
5 وضعیت	6 ممیزی		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 G – دیواراتش	2 F – ممیزی	3 D – امتیاز	4 B – بخشبندی
5 H – مسیریاب	6 E – وضعیت	7 C – مدیریتهویت	8 A – تأیید

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند راستی‌آزمایی، بخش‌بندی و مدیریت هویت و دسترسی (IAM) را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

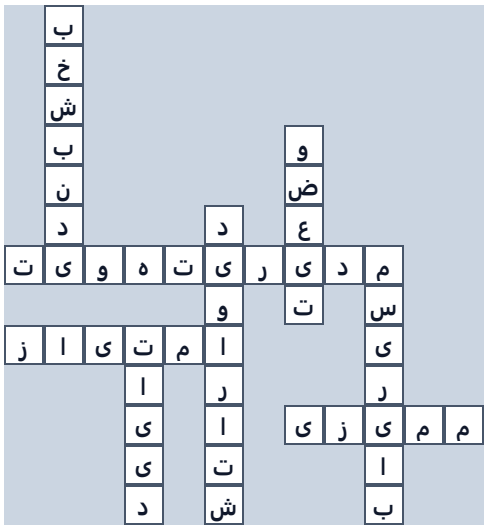
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ح	ظ	س	ت	غ	ذ	ح	ص	غ	ش	ظ	ن	ع	ض	ت
ک	ف	ت	ق	چ	ژ	ر	پ	م	ا	ت	ب	پ	ط	و
ژ	ز	ی	و	ژ	ن	ک	ز	ث	س	ا	ع	ش	ر	ث
ذ	ص	ع	ز	ا	ی	ت	م	ا	ص	ی	ژ	ع	ظ	خ
ش	ش	ض	ع	غ	م	ف	ک	ک	خ	ی	ر	پ	ف	ظ
ی	ض	و	د	ف	د	پ	د	م	ی	د	ث	ی	ق	ه
د	گ	ت	ی	م	ی	ح	ی	ز	خ	ز	ی	ا	ص	ص
ن	ث	ع	ن	ظ	ر	پ	گ	ب	و	ا	ی	ی	ض	ب
ب	ث	ژ	ا	ث	ی	ض	ث	چ	خ	ا	ذ	م	ث	غ
ش	ع	ش	چ	ذ	ت	ف	ی	ق	چ	ع	ر	ل	م	چ
خ	ا	ع	ط	ه	ظ	ص	ع	و	ک	ز	ا	غ	ک	
ب	ف	ت	ص	ه	و	پ	ح	ف	ن	م	ر	ا	ت	غ
ی	ه	ه	ژ	ح	ی	ذ	ش	غ	ز	س	س	ق	ط	ش
خ	ظ	ع	خ	ی	ت	ا	ض	ل	ح	گ	پ	ه	ف	ه
ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی	ه	ح

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

4 افقی: مدیریتهویت مدیریت دسترسی به اعتبارنامه‌های کاربر. (10 حرف)

5 افقی: امتیاز اصل حداقل حقوق دسترسی. (6 حرف)

7 افقی: ممیزی بازبینی نشست‌های دسترسی ثبت‌شده. (5 حرف)

عمودی

1 عمودی: بخشبندی تقسیم منطقه‌های داخلی شبکه. (7 حرف)

2 عمودی: وضعیت ارزیابی سلامت دستگاه. (5 حرف)

3 عمودی: دیواراتش حفاظت مرزی شبکهٔ بیرونی. (8 حرف)

4 عمودی: مسیریاب هدایت ترافیک بسته‌های شبکه میان مسیرها. (7 حرف)

6 عمودی: تأیید بررسی همیشگی اعتبارنامه‌های کاربر. (5 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. یتدا — تأیید
2. یرمدیتهوتی — مدیریتهویت
3. عوتیض — وضعیت
4. اتشاردیو — دیواراتش
5. نیبشبدخ — بخشبندی
6. ایاتزم — امتیاز
7. زیمیم — ممیزی
8. سربمایی — مسیریاب

کلید چالش رمز مخفی

"تأیید دائمی در معماری اعتماد صفر"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: گذار به معماری شبکهٔ اعتماد صفر

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک شرکت بزرگ اکنون از شبکهٔ داخلی مسطحی استفاده می‌کند که در آن هر دستگاه در شبکهٔ محلی می‌تواند به همهٔ سرورها و پایگاه‌های داده سازمانی دسترسی داشته باشد.
- راهبرد و راه‌حل پیشنهادی: شبکهٔ مسطح را به مناطق ایزولهٔ ادارات تقسیم کنید. دیوار آتش داخلی نصب کنید تا ترافیک بین مناطق کنترل شود و اعتبارسنجی توکن اتصال را برای همهٔ دسترسی‌ها الزامی کنید.

B مطالعهٔ موردی 2: استقرار کنترل‌های دسترسی با کمترین امتیاز

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: گزارش‌های ممیزی نشان می‌دهند کاربران موقت پایگاه داده و کارمندان رده‌پایین مجوزهای سراسری خواندن و نوشتن روی پایگاه‌های داده حسابداری حیاتی دارند.
- راهبرد و راه‌حل پیشنهادی: همهٔ امتیازهای مدیریتی سراسری را لغو کنید. کنترل دسترسی مبتنی بر نقش (RBAC) را مطابق نقش‌های شغلی دقیق پیاده کنید و بازبینی‌های خودکار هفتگی مجوزها را برقرار کنید.