نام: _____ تاریخ: _____ نمره: _____

نرم‌افزار آنتی‌ویروس و نقطهٔ پایانی راهنمای حفاظت

تشخیص امضا، روش‌های ابتکاری، پایش رفتار، سندباکس، به‌روزرسانی‌ها

مرور آموزشی نرم‌افزار آنتی‌ویروس

خوش آمدید! این بستهٔ فعالیت شما را در بررسی نرم‌افزار آنتی‌ویروس و حفاظت از نقطهٔ پایانی راهنمایی می‌کند. با پایگاه‌های داده امضا، اسکنرهای اکتشافی، پایش رفتاری، فایل‌های مجازی جعبه‌شنی و کاهش موارد مثبت کاذب آشنا می‌شوید.

ایمن‌شده
رمزگذاری داده
استاندارد AES 256 بیتی

منطبق
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

اعتماد صفر
سیاست دسترسی
احراز هویت چندعاملی

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**

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/antivirus/

نقشهٔ راه یادگیری راهبرد آنتی‌ویروس شما

- میان تشخیص بدافزار مبتنی بر امضا و مبتنی بر اکتشاف تمایز قائل شوید.
- پروتکل‌های پایش رفتار و ایزوله‌سازی جعبه‌شنی را درک کنید.
- تأثیر اسکن بلادرنگ بر عملکرد سیستم و نقاط پایانی را ارزیابی کنید.
- کاهش طبقه‌بندی‌های مثبت کاذب با استفاده از راستی‌آزمایی گواهی دیجیتال.
- مدیریت توزیع روزانهٔ به‌روزرسانی تعاریف در نقاط پایانی سازمانی.

دستورالعمل راهنمای آنتی‌ویروس

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 امنیت آنتی‌ویروس نقاط پایانی به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

حفاظت آنتی‌ویروس و اسکن مبتنی بر امضا (مقدمه)

نرم‌افزار آنتی‌ویروس با شناسایی، قرنطینه و حذف بدافزار از نقاط پایانی محافظت می‌کند. سامانه‌های مدرن پایگاه‌های داده امضا (تطبیق هش تهدیدهای شناخته‌شده) را با روش‌های اکتشافی (تحلیل ساختار فایل) و پایش رفتار ترکیب می‌کنند تا اکسپلویت‌های روز صفر را شناسایی کنند.

هر ایستگاه بررسی را با دقت بخوانید و درست‌ترین

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. محدودیت تشخیص مبتنی بر امضا چیست؟

- A. نمی‌تواند بدافزار ناشناخته یا تغییریافته را شناسایی کند
- B. نرخ بالایی از هشدارهای کاذب تولید می‌کند
- C. به توان پردازشی بالای CPU نیاز دارد
- D. فقط هنگام اتصال به اینترنت کار می‌کند

2. اسکنرهای اکتشافی چگونه انواع جدید بدافزار را شناسایی می‌کنند؟

- A. با شناسایی الگوها و ساختارهای کد مشکوک
- B. با تطبیق هش فایل‌ها با پایگاه داده‌ای از تهدیدها
- C. با حذف خودکار همهٔ فایل‌های اجرایی بدون امضا
- D. با بارگذاری هر فایل در یک پوشهٔ ابری عمومی

3. هدف از اجرای سندباکس در آنتی‌ویروس چیست؟

- A. ایزوله کردن و تحلیل فایل‌ها در یک گاوصندوق مجازی امن
- B. سرعت بخشیدن به انتقال پشتیبان‌گیری سیستم فایل محلی
- C. به‌روزرسانی وصله‌های امنیتی سیستم‌عامل محلی
- D. فشرده‌سازی فایل‌های سند بزرگ برای صرفه‌جویی در فضای ذخیره‌سازی

4. کدام روش تشخیص رفتار تهدید را به‌صورت بلادرنگ علامت‌گذاری می‌کند؟

- A. تحلیل رفتاری که اقدامات نرم‌افزار را پایش می‌کند
- B. بازرسی لاگ‌های تاریخی که شبانه انجام می‌شود
- C. مداخلهٔ دستی کاربر برای گزارش برنامه‌های کند
- D. بازبینی دستی هفتگی برنامه‌های نصب‌شده

5. چرا به‌روزرسانی منظم تعریف‌ها برای اسکنرها حیاتی است؟

- A. برای تغذیهٔ موتورهای امضا با شناسه‌های تهدید پایگاه داده
- B. افزایش سرعت ساعت CPU در حین عملیات
- C. برای تغییر زمان‌های حافظهٔ پنهان سرور نام DNS جهانی
- D. برای مجاز کردن تنظیمات کوکی مرورگر وب

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش درست/نادرست 6

6. تشخیص مبتنی بر امضا، هش‌های رمزنگاری فایل‌ها را با فهرست‌های پایگاه داده تطبیق می‌دهد.

درست نادرست

7 پرسش درست/نادرست 7

7. اسکنرهای اکتشافی می‌توانند برای فایل‌های ایمن هشدار کاذب ایجاد کنند.

درست نادرست

8 پرسش درست/نادرست 8

8. sandbox به بدافزار اجازه می‌دهد بدون محدودیت به فایل‌های شبکه دسترسی پیدا کند.

درست نادرست

9 پرسش درست/نادرست 9

9. اسکن رفتاری فایل‌ها را زمانی که اقدام‌های مخرب نشان می‌دهند مسدود می‌کند.

درست نادرست

10 پرسش درست/نادرست 10

10. نرم‌افزار آنتی‌ویروس استاندارد تمام حملات روز صفر را کاملاً متوقف می‌کند.

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. یک اسکنر سنتی برای شناسایی بدافزارهای شناخته‌شده به تطبیق _____ متکی است.
2. تحلیل الگوهای کد فایل، اسکن _____ نامیده می‌شود.
3. ابزارهای آنتی‌ویروس فایل‌های مشکوک را در یک محیط _____ جدا می‌کنند.
4. پایش بی‌درنگ، _____ برنامه‌ها را برای فعالیت‌های مشکوک زیر نظر دارد.
5. اسکنرها هر روز برای شناسایی تهدیدهای جدید، _____ پایگاه داده را دانلود می‌کنند.
6. برنامه‌های ایمنی که به‌عنوان بدافزار علامت‌گذاری شوند، باعث هشدار _____ می‌شوند.

بانک واژگان

ابزار آنتی‌ویروس | اکتشافی | امضا | به‌روزرسانی | جعبه شنی | رفتار | قرنطینه | مثبت کاذب

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

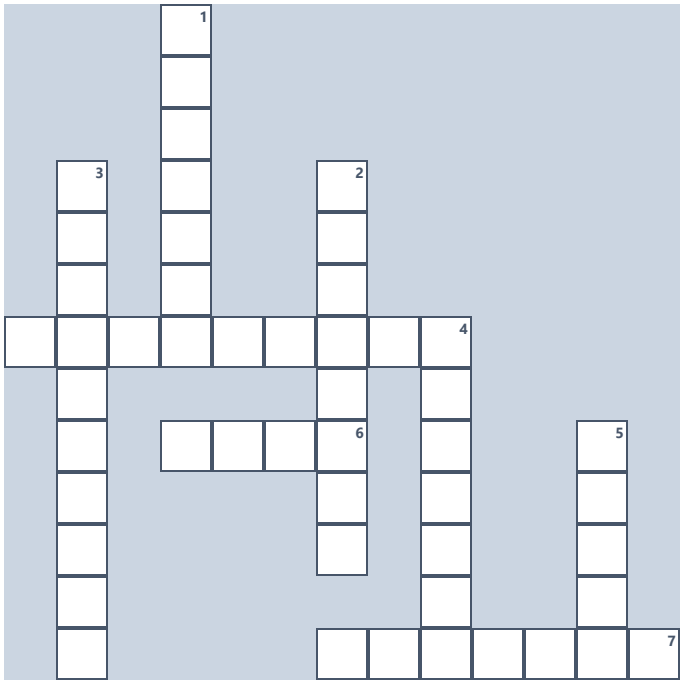
تطبیق تعاریف

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. امضای درهم‌ساز	A	محدود کردن فایل‌های مشکوک برای جلوگیری از در معرض قرار گرفتن سیستم محلی.
2. اکتشافی کد	B	مجموعه نرم‌افزاری که نقاط پایانی را اسکن می‌کند و در برابر اکسپلویت‌ها محافظت می‌کند.
3. جعبه‌شنی فایل	C	پایش اقدامات نرم‌افزار در حال اجرا برای یافتن الگوهای عملیات مخرب.
4. اسکن رفتار	D	ردپای رمزنگاری منحصربه‌فرد پایگاه داده که برای شناسایی تهدیدهای شناخته‌شده به کار می‌رود.
5. به‌روزرسانی‌های روزانه	E	محیط آزمایشی مجازی امن که کد غیرقابل‌اعتماد را با ایمنی اجرا می‌کند.
6. مثبت کاذب	F	دانلودهای منظم تعریف‌ها که پایگاه داده تهدید را تغذیه می‌کنند.
7. ایزوله‌سازی تهدید	G	تحلیل مبتنی بر قاعده که فایل‌هایی با ساختار کد مشکوک را علامت می‌زند.
8. ابزار آنتی‌ویروس	H	هشدار امنیتی که نرم‌افزار ایمن را به‌اشتباه بدافزار تشخیص می‌دهد.

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. مجموعه‌ای نرم‌افزاری که نقاط پایانی را اسکن می‌کند و در برابر بهره‌برداری‌ها محافظت می‌کند (9)

6. اثر انگشت رمزنگاری‌شدهٔ منحصربه‌فرد در پایگاه داده که برای شناسایی تهدیدهای شناخته‌شده به کار می‌رود (4)

7. محدود کردن فایل‌های مشکوک برای جلوگیری از آسیب‌پذیری سامانهٔ محلی (7)

عمودی

1. محیط آزمایش مجازی و امن که کد نامعتبر را با ایمنی اجرا می‌کند (7)

2. هشدار امنیتی که نرم‌افزار ایمن را به‌اشتباه بدافزار طبقه‌بندی می‌کند (8)

3. دانلودهای منظم تعاریف که پایگاه دادهٔ تهدیدها را تغذیه می‌کنند (10)

4. تحلیل قاعده‌محور که فایل‌هایی با ساختار کد مشکوک را علامت‌گذاری می‌کند (7)

5. پایش اقدامات نرم‌افزارهای در حال اجرا برای یافتن الگوهای عملکرد مخرب (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.
سرنخ‌های افقی سرنخ‌های عمودی

افقی

4 افقی: مجموعه‌ای نرم‌افزاری که نقاط پایانی را اسکن می‌کند و در برابر بهره‌برداری‌ها محافظت می‌کند (9 حرف):

6 افقی: اثر انگشت رمزنگاری‌شدهٔ منحصربه‌فرد در پایگاه داده که برای شناسایی تهدیدهای شناخته‌شده به کار می‌رود (4 حرف):

7 افقی: محدود کردن فایل‌های مشکوک برای جلوگیری از آسیب‌پذیری سامانهٔ محلی (7 حرف):

عمودی

1 عمودی: محیط آزمایش مجازی و امن که کد نامعتبر را با ایمنی اجرا می‌کند (7 حرف):

2 عمودی: هشدار امنیتی که نرم‌افزار ایمن را به‌اشتباه بدافزار طبقه‌بندی می‌کند (8 حرف):

3 عمودی: دانلودهای منظم تعاریف که پایگاه دادهٔ تهدیدها را تغذیه می‌کنند (10 حرف):

4 عمودی: تحلیل قاعده‌محور که فایل‌هایی با ساختار کد مشکوک را علامت‌گذاری می‌کند (7 حرف):

5 عمودی: پایش اقدامات نرم‌افزارهای در حال اجرا برای یافتن الگوهای عملکرد مخرب (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.

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

فهرست واژگان

امضا | اکتشافی | جعبهشنی | رفتار | بهروزرسانی | مثبتکاذب | قرنطینه | انتیویروس

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
A. امضا
B. اکتشافی
C. جعبه‌شنی
D. رفتار
E. بهروزرسانی
F. مثبت‌کاذب
G. قرنطینه
H. انتیویروس

	تعاریف و فیلدهای تطبیق
	1. پایش اقدامات نرم‌افزارهای در حال اجرا برای یافتن الگوهای عملکرد مخرب.
	2. مجموعه‌ای نرم‌افزاری که نقاط پایانی را اسکن می‌کند و در برابر بهره‌برداری‌ها محافظت می‌کند.
	3. دانلودهای منظم تعاریف که پایگاه دادهٔ تهدیدها را تغذیه می‌کنند.
	4. تحلیل قاعده‌محور که فایل‌هایی با ساختار کد مشکوک را علامت‌گذاری می‌کند.
	5. محدود کردن فایل‌های مشکوک برای جلوگیری از آسیب‌پذیری سامانهٔ محلی.
	6. اثر انگشت رمزنگاری‌شدهٔ منحصربه‌فرد در پایگاه داده که برای شناسایی تهدیدهای شناخته‌شده به کار می‌رود.
	7. محیط آزمایش مجازی و امن که کد نامعتبر را با ایمنی اجرا می‌کند.
	8. هشدار امنیتی که نرم‌افزار ایمن را به‌اشتباه بدافزار طبقه‌بندی می‌کند.

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. ض ا ا م _____

2. ج ب ی ن ش ه ع _____

3. ب ر ن س ه ز ی و ا ر _____

4. ه ر ی ط ن ق ن _____

5. ا ی ش ت ا ف ک _____

6. ا ر ت ر ف _____

7. م ب ک ا ذ ث ت ب _____

8. س و و ا ی ن ی ر ت _____

فعالیت تکمیلی: سریع فکر کن

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

1	دلایل به‌روزرسانی نرم‌افزار		
2	افرادی که می‌توانید برای کمک فناوری اطلاعات از آن‌ها بپرسید		
3	کارهایی که وقتی آنتی‌ویروس چیزی پیدا می‌کند باید انجام داد		
4	نشانه‌های ویروسی شدن رایانه		
5	چیزهایی که قرنطینه می‌شوند		
6	جاهایی که ویروس‌ها پنهان می‌شوند		
7	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
8	انواع نرم‌افزارهای مخرب		
9	ابزارهای امنیتی که می‌شناسید		
10	چیزهایی که یک آنتی‌ویروس اسکن می‌کند		
11	چیزهایی که پشتیبان می‌گیرید		
12	دستگاه‌هایی که می‌توانند هک شوند		
13	برنامه‌های آنتی‌ویروس که می‌شناسید		
14	دلایل هشدارهای اشتباه		
15	عادت‌های ایمن که می‌توانید از امروز شروع کنید		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

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

مطالعهٔ موردی 1: اسکن مبتنی بر امضا در برابر اکتشافی



سناریو: یک کارمند ابزار سفارشی‌ای را دانلود می‌کند که تیم دیگری به‌صورت داخلی ساخته است. اسکنر مبتنی بر امضا آن را تأیید می‌کند، اما اسکنر ابتکاری (heuristic) آن را مشکوک علامت‌گذاری می‌کند.

پرسش برای بحث: توضیح دهید چرا این اتفاق افتاد و چگونه می‌توان ایمن بودن فایل را تأیید کرد.

مطالعهٔ موردی 2: مدیریت هشدارهای کاذب



سناریو: یک توسعه‌دهندهٔ نرم‌افزار برنامهٔ خود را کامپایل می‌کند. آنتی‌ویروس سیستم فایل اجرایی جدید را بدافزار علامت‌گذاری و قرنطینه می‌کند.

پرسش برای بحث: خطرهای افزودن به فهرست مجاز (whitelisting) را شرح دهید و مسیر درست رفع مشکل را توضیح دهید.

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	23	1	16	4	25	1		27	32	27	8	4		1	2

10	32	2	1	32	2		30	29		12	1	13	23	1	10	2

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: نرم‌افزار آنتی‌ویروس چگونه بدافزار را شناسایی می‌کند؟

بدافزار را با تطبیق امضا در پایگاه‌داده، تحلیل چیدمان کد به روش اکتشافی و پایش رفتاری بی‌درنگ شناسایی می‌کند.

Q2: تشخیص مبتنی بر امضا چیست؟

روش اسکنی است که هش‌های رمزنگاری‌شدهٔ فایل را با فهرست‌های پایگاه‌داده از تهدیدهای شناخته‌شدهٔ بدافزار تطبیق می‌دهد.

Q3: اسکنر اکتشافی چیست؟

روش‌های اکتشافی ساختار فایل و دستورهای کد را تحلیل می‌کنند و الگوهای مشکوکِ رایج در انواع بدافزار را علامت‌گذاری می‌کنند.

Q4: وقتی فایلی قرنطینه می‌شود به چه معناست؟

آنتی‌ویروس فایل را به پوشه‌ای امن و ایزوله منتقل می‌کند و اجرای آن را مسدود می‌کند تا از سیستم‌عامل محافظت کند.

Q5: مثبت کاذب آنتی‌ویروس چیست؟

خطایی است که در آن نرم‌افزار مشروع و ایمن به اشتباه توسط الگوریتم‌های اسکن به‌عنوان بدافزار علامت‌گذاری می‌شود.

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

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

Q6: پایش رفتار چگونه از سیستم‌ها محافظت می‌کند؟

نرم‌افزارهای در حال اجرا را به‌صورت بی‌درنگ پایش می‌کند و فرایندهایی را که سعی در تغییرات مشکوک مانند تزریق کد دارند مسدود می‌کند.

Q7: چرا آزمایش سندباکس مهم است؟

سندباکس فایل‌های نامطمئن را در یک ماشین مجازی ایزوله اجرا می‌کند و رفتار آن‌ها را بدون در معرض خطر قرار دادن سیستم، با ایمنی مشاهده می‌کند.

Q8: تعریف‌های آنتی‌ویروس هر چند وقت یک‌بار باید به‌روز شوند؟

اسکنرها باید تعریف‌ها را روزانه یا ساعتی به‌روز کنند تا سویه‌های بدافزار تازه‌کشف‌شده را شناسایی کنند.

Q9: تفاوت آنتی‌ویروس و EDR چیست؟

آنتی‌ویروس بر اسکن فایل‌ها تمرکز دارد، در حالی که تشخیص و پاسخ در نقطهٔ پایانی (EDR) ردیابی و مهار تهدیدها را در سطح کل شبکه فراهم می‌کند.

Q10: آیا می‌توانم دو برنامهٔ آنتی‌ویروس را با هم اجرا کنم؟

خیر. اجرای دو پویشگر فعال باعث تداخل سیستم می‌شود، عملکرد را کند می‌کند و می‌تواند عملیات یکدیگر را مسدود کند.

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

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

Q1: قوانین ابتکاری چگونه دور زدن تهدید را به حداقل می‌رسانند؟

روش‌های اکتشافی به‌جای امضاهای خاص، الگوهای کلی تهدید را تحلیل می‌کنند و انواع تغییریافتهٔ خانواده‌های شناخته‌شدهٔ بدافزار را شناسایی می‌کنند.

Q2: ویروس چندریخت چیست؟

بدافزاری است که با هر اجرا چیدمان فایل و رویهٔ رمزگشایی خود را تغییر می‌دهد و اسکن امضا را بی‌اثر می‌کند.

Q3: سندباکس‌ها چگونه گریز از ماشین مجازی را تشخیص می‌دهند؟

جعبه‌ماسه‌های نوین کلیک ماوس و زمان روشن بودن سیستم را شبیه‌سازی می‌کنند و بدافزارهایی را فریب می‌دهند که برای پنهان شدن هنگام اجرا در ماشین‌های مجازی طراحی شده‌اند.

Q4: قالب‌های دانلود به‌روزرسانی امضا کدامند؟

به‌روزرسانی‌ها معمولاً فایل‌های دودویی تفاضلی افزایشی سبک هستند که مصرف پهنای باند شبکهٔ کلاینت را به حداقل می‌رسانند.

Q5: عامل‌های نقطهٔ پایانی اسکن‌های محلی را چگونه مدیریت می‌کنند؟

عامل‌ها بررسی‌های سبک پس‌زمینه انجام می‌دهند و جستجوی عمیق درهم‌سازهای رمزنگاری را به پایگاه‌های داده تهدید ابری واگذار می‌کنند.

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

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

Q6: اسکن تشخیص روت‌کیت چیست؟

جدول‌های حافظهٔ سطح هسته را اسکن می‌کند و APIهای سیستم‌عامل را که روت‌کیت‌ها برای پنهان کردن رشته‌های فعال خود هوک می‌کنند دور می‌زند.

Q7: اسکن رفتاری چگونه باج‌افزار را مسدود می‌کند؟

حلقه‌های خودکار رمزگذاری انبوه فایل را شناسایی می‌کند و پیش از قفل شدن پایگاه‌های داده سیستم، فرایند میزبان را خاتمه می‌دهد.

Q8: راستی‌آزمایی گواهی امضای کد چیست؟

اسکنرها امضاهای دیجیتال کد را با مراجع صدور گواهی ریشهٔ معتبر تطبیق می‌دهند و هویت توسعه‌دهندهٔ نرم‌افزار را اعتبارسنجی می‌کنند.

Q9: بسته‌بندهای فشرده‌ساز (packers) چه تأثیری بر موتورهای اسکن دارند؟

بسته‌سازها محموله‌های بدافزار را فشرده یا رمزگذاری می‌کنند. اسکنرها باید پیش از تطبیق امضا، فایل را در حافظه از حالت بسته خارج کنند.

Q10: ابزارهای EDR چگونه جداسازی را خودکار می‌کنند؟

عامل‌های EDR نقاط پایانی در معرض خطر را در سطح شبکه قرنطینه می‌کنند و ضمن اجازهٔ دسترسی به تحلیلگر، حرکت جانبی را مسدود می‌کنند.

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

پایگاه‌های داده امضا هش‌های بدافزارهای شناخته‌شده را ذخیره می‌کنند، بنابراین فایل‌های کاملاً جدید یا تغییریافته تا به‌روزرسانی تعاریف شناسایی نمی‌شوند.

2. بینش امنیت

موتورهای اکتشافی می‌توانند برخی انواع جدید بدافزار را پیش از وجود امضا شناسایی کنند، به بهای هشدارهای کاذب بیشتر.

3. بینش امنیت

هشدارهای مثبت کاذب برای تیم‌های فناوری اطلاعات هزینهٔ زمان صرف‌شده برای تأیید و بازیابی فایل‌هایی را دارند که به‌اشتباه قرنطینه شده‌اند.

4. بینش امنیت

بدافزار چندریخت با هر نسخه کد خود را تغییر می‌دهد، بنابراین مدافعان امضاها را با بررسی‌های ابتکاری و رفتاری ترکیب می‌کنند.

5. بینش امنیت

موتورهای آنتی‌ویروس ابری هش فایل‌های مشکوک را تقریباً در لحظه با پایگاه‌های داده بزرگ تهدیدهای آنلاین مقایسه می‌کنند.

6. بینش امنیت

سازندگان بدافزار کدهای سفارشی می‌نویسند که محیط‌های جعبه‌ماسه را بررسی می‌کنند و اجرا را به تأخیر می‌اندازند تا زمان‌سنج‌ها را دور بزنند.

7. بینش امنیت

فروشندگان به‌طور منظم به‌روزرسانی‌های تعریف را به نقاط پایانی می‌فرستند تا اسکنرها بتوانند تهدیدهای تازه تأییدشده را بشناسند.

8. بینش امنیت

پایشگرهای رفتاری باجافزار فراخوانی‌های مشخص Win32 API مرتبط با رمزگذاری فایل و حذف نسخه‌های سایه را هدف می‌گیرند.

9. بینش امنیت

امضای معتبر کد می‌تواند خطر هشدار کاذب را کاهش دهد، اما فایل‌های امضاشده هم همچنان اسکن می‌شوند، چون بدافزار هم می‌تواند امضا شود.

10. بینش امنیت

روت‌کیت‌ها ساختارهای هستهٔ سیستم را تغییر می‌دهند و برای شناسایی و پاک‌سازی به اسکنرهای تخصصی زمان بوت نیاز است.

منابع و مراجع فنی

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

منابع علمی و صنعتی

[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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1 — امضاها — پاسخ درست: A

نکتهٔ آموزشی

اسکن مبتنی بر امضا به هش‌های شناخته‌شدهٔ پایگاه داده متکی است و بدافزارهای ناشناخته یا تغییریافته را تشخیص نمی‌دهد. منبع: OWASP Secure Configuration.

2 پرسش 2 — روش‌های اکتشافی — پاسخ درست: A

نکتهٔ آموزشی

روش اکتشافی چیدمان کد و دستورها را تحلیل می‌کند تا ویژگی‌های مشکوک انواع جدید تهدید را شناسایی کند. منبع: Center for Internet Security (CIS).

3 پرسش 3 — سندباکس‌سازی — پاسخ درست: A

نکتهٔ آموزشی

جعبه‌شنی فایل‌های مشکوک را در یک ماشین مجازی ایزوله اجرا می‌کند تا رفتار اجرا را به‌طور ایمن مشاهده کند. منبع: NIST Digital Identity.

4 پرسش 4 — رفتاری — پاسخ درست: A

نکتهٔ آموزشی

اسکن رفتاری برنامه‌های در حال اجرا را در لحظه پایش می‌کند تا تغییرات غیرمجاز سیستم را مسدود کند. منبع: Center for Internet Security (CIS).

5 پرسش 5 — به‌روزرسانی‌ها — پاسخ درست: A

نکتهٔ آموزشی

اسکنرها به‌روزرسانی‌های افزایشی روزانهٔ تعریف‌ها را دانلود می‌کنند تا با چشم‌انداز تهدیدها همگام بمانند. منبع: OWASP Secure Configuration.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **پرسش 6** — امضاها — پاسخ درست: درست

نکتهٔ آموزشی

پاسخ درست: درست ابزارهای امضایی هش‌های رمزنگاری را محاسبه می‌کنند و آن‌ها را با پایگاه داده‌ای از هش‌های تهدیدهای شناخته‌شده تطبیق می‌دهند. منبع: OWASP Secure Configuration.

7 **پرسش 7** — روش‌های اکتشافی — پاسخ درست: درست

نکتهٔ آموزشی

پاسخ درست: درست موتورهای اکتشافی چیدمان‌های مبتنی بر قاعده اجرا می‌کنند که می‌توانند فایل‌های قانونی و ایمن را مشکوک علامت‌گذاری کنند. منبع: Center for Internet Security (CIS).

8 **پرسش 8** — سندباکس‌سازی — پاسخ درست: نادرست

نکتهٔ آموزشی

پاسخ درست: نادرست جعبه‌شنی کد را در یک کانتینر مجازی اجرا می‌کند و دسترسی به اشتراک‌های شبکه را به‌طور کامل مسدود می‌کند. منبع: NIST Digital Identity.

9 **پرسش 9** — رفتاری — پاسخ درست: درست

نکتهٔ آموزشی

پاسخ درست: درست پایش لحظه‌ای، فرایندهای در حال اجرا را که تلاش به نوشتن غیرقانونی یا قفل کردن فایل دارند علامت‌گذاری می‌کند. منبع: Center for Internet Security (CIS).

10 **پرسش 10** — پاسخ درست: نادرست

نکتهٔ آموزشی

پاسخ درست: نادرست. هیچ آنتی‌ویروسی جلوی هر حملهٔ روز صفر (zero-day) را نمی‌گیرد؛ تهدیدهای ناشناخته می‌توانند از امضاها و روش‌های ابتکاری (heuristics) عبور کنند.

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

D 1. امضای درهم‌ساز	G 2. اکتشافی کد	E 3. جعبه‌شنی فایل	C 4. اسکن رفتار
F 5. به‌روزرسانی‌های روزانه	H 6. مثبت کاذب	A 7. ایزوله‌سازی تهدید	B 8. ابزار آنتی‌ویروس

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 امضا	2 اکتشافی	3 جعبه شنی	4 رفتار
5 به‌روزرسانی	6 مثبت کاذب		

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

1 D – رفتار	2 H – انتیویروس	3 E – بهروزرسانی	4 B – اکتشافی
5 G – قرنطینه	6 A – امضا	7 C – جعبهشنی	8 F – مثبتکاذب

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند امضای درهم‌ساز، اکتشافی کد و جعبه‌شنی فایل 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.

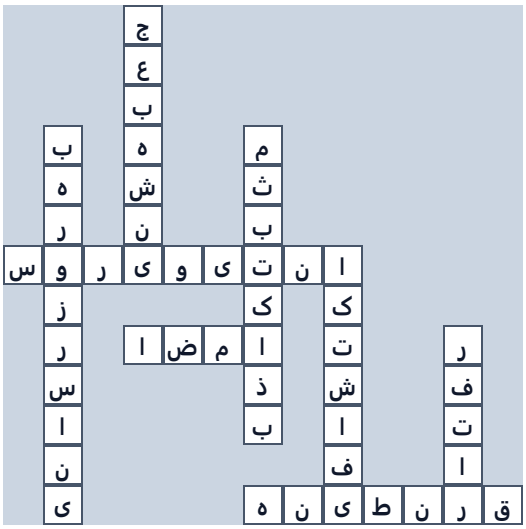
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



افقی

4 افقی: انتیویروس مجموعه‌ای نرم‌افزاری که نقاط پایانی را اسکن می‌کند و در برابر بهره‌برداری‌ها محافظت می‌کند (9 حرف)

6 افقی: امضا اثر انگشت رمزنگاری‌شدهٔ منحصربه‌فرد در پایگاه داده که برای شناسایی تهدیدهای شناخته‌شده به کار می‌رود (4 حرف)

7 افقی: قرنطینه محدود کردن فایل‌های مشکوک برای جلوگیری از آسیب‌پذیری سامانهٔ محلی (7 حرف)

عمودی

1 عمودی: جعبهشنی محیط آزمایش مجازی و امن که کد نامعتبر را با ایمنی اجرا می‌کند (7 حرف)

2 عمودی: مثبتکاذب هشدار امنیتی که نرم‌افزار ایمن را به‌اشتباه بدافزار طبقه‌بندی می‌کند (8 حرف)

3 عمودی: بهروزرسانی دانلودهای منظم تعاریف که پایگاه دادهٔ تهدیدها را تغذیه می‌کنند (10 حرف)

4 عمودی: اکتشافی تحلیل قاعده‌محور که فایل‌هایی با ساختار کد مشکوک را علامت‌گذاری می‌کند (7 حرف)

5 عمودی: رفتار پایش اقدامات نرم‌افزارهای در حال اجرا برای یافتن الگوهای عملکرد مخرب (5 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. ضاام — امضا
2. جبینشهع — جعبهشنی
3. برنسهزیوار — بهروزرسانی
4. هریطنقن — قرنطینه
5. ایشتافک — اکتشافی
6. ارترف — رفتار
7. مبکاذتب — مثبتکاذب
8. سوواینیرت — انتیویروس

کلید چالش رمز مخفی

"با تحلیل اکتشافی بدافزار نو بیابید"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: اسکن مبتنی بر امضا در برابر اکتشافی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک کارمند ابزاری سفارشی را دانلود می‌کند که تیم دیگری به‌صورت داخلی ساخته است. اسکنر امضا آن را می‌پذیرد، اما اسکنر اکتشافی آن را مشکوک علامت می‌زند.
- راهبرد و راه‌حل پیشنهادی: چرا رخ داد: اسکن امضا هش فایل‌ها را بررسی می‌کند؛ چون فایل سفارشی است، در پایگاه داده تهدید وجود ندارد. روش‌های اکتشافی ساختار را تحلیل کردند و اقدام‌های مشکوک (مانند نوشتن در رجیستری) را علامت زدند. راستی‌آزمایی: فایل را در یک سندباکس اجرا کنید تا اقدام‌ها مشاهده شود، امضاهای دیجیتال را بررسی کنید و هش را به پورتال‌های اطلاعات تهدید ارسال کنید.

B مطالعهٔ موردی 2: مدیریت هشدارهای کاذب

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک توسعه‌دهندهٔ نرم‌افزار برنامهٔ خود را کامپایل می‌کند. آنتی‌ویروس سیستم فایل اجرایی جدید را بدافزار علامت‌گذاری و قرنطینه می‌کند.
- راهبرد و راه‌حل پیشنهادی: خطرهای فهرست مجاز: دور زدن اسکنرها می‌تواند به اجرای کد واقعاً آلوده اجازه دهد. مسیر حل: فایل را برای تحلیل به فروشندهٔ آنتی‌ویروس ارسال کنید، کد را با مراجع صدور گواهی امضای دیجیتال کنید و به‌جای خاموش کردن آنتی‌ویروس، موقتاً استثناهای پوشهٔ مشخص تعریف کنید.