नाम: _____ दिनांक: _____ अंक: _____

ज़ीरो ट्रस्ट आर्किटेक्चर और सुरक्षा

निरंतर सत्यापन, नेटवर्क माइक्रो-सेगमेंटेशन, Identity and Access Management, न्यूनतम विशेषाधिकार और पॉश्चर जाँच।

ज़ीरो ट्रस्ट सुरक्षा अध्ययन अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको Zero Trust आर्किटेक्चर और सुरक्षा से परिचित कराता है। आप निरंतर सत्यापन, नेटवर्क माइक्रो-सेगमेंटेशन, आइडेंटिटी एक्सेस मैनेजमेंट (IAM), न्यूनतम विशेषाधिकार और सत्र ऑडिटिंग का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

- ☐ **भाग 1-4: साइबर सुरक्षा और खतरों की रोकथाम में महारत हासिल करें।**
- ☐ **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- ☐ **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- ☐ **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- ☐ **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- ☐ **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/zero-trust-cyber-security/

आपका ज़ीरो ट्रस्ट रणनीति लर्निंग रोडमैप

- निरंतर सत्यापन के मूल सिद्धांत को समझें।
- नेटवर्क माइक्रो-सेगमेंटेशन और न्यूनतम विशेषाधिकार एक्सेस लागू करें।
- डिवाइस पॉश्चर जाँच और सक्रिय सत्र ऑडिटिंग कॉन्फ़िगर करें।

ज़ीरो ट्रस्ट सुरक्षा गाइड निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को Zero Trust आर्किटेक्चर पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

ज़ीरो ट्रस्ट आर्किटेक्चर और सुरक्षा (परिचय)

ज़ीरो ट्रस्ट सुरक्षा पुराने नेटवर्क परिधि मॉडल की जगह सख़्त 'कभी भरोसा न करें, हमेशा सत्यापित करें' नीति लाती है। माइक्रो-सेगमेंटेशन, आइडेंटिटी एंड एक्सेस मैनेजमेंट (IAM), न्यूनतम विशेषाधिकार अधिकार और पोस्चर जाँच लागू करने से पार्श्व खतरों की गति रुकती है।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. ज़ीरो ट्रस्ट सुरक्षा का मूल सिद्धांत क्या है?**

- A. कभी भरोसा न करें, स्रोत चाहे जो हो, हर एक्सेस अनुरोध को हमेशा सत्यापित करें
- B. यह मान लेना कि कॉर्पोरेट फ़ायरवॉल के भीतर सारा ट्रैफ़िक सुरक्षित है
- C. गति बढ़ाने के लिए डेटाबेस फ़ाइलें बिना एन्क्रिप्शन के संग्रहीत करना
- D. केवल SPF रिकॉर्ड से ईमेल प्रमाणीकरण लागू करना

2 **2. नेटवर्क माइक्रो-सेगमेंटेशन क्या है?**

- A. पार्श्व गति को रोकने के लिए नेटवर्क को छोटे, अलग-थलग ज़ोन में बाँटना
- B. डेटा ट्रांज़िट के दौरान नेटवर्क कार्ड को एन्क्रिप्ट करना
- C. सभी स्थानीय सर्वरों को एक ही सार्वजनिक IP पते से जोड़ना
- D. ब्राउज़र सत्रों में उपयोगकर्ता के कीस्ट्रोक की निगरानी करना

3 **3. न्यूनतम विशेषाधिकार का सिद्धांत क्या है?**

- A. उपयोगकर्ता की पहुँच अनुमतियों को केवल उतने तक सीमित करना जितना उनके काम के लिए आवश्यक है
- B. डिफ़ॉल्ट रूप से हर उपयोगकर्ता को सभी सिस्टम विशेषाधिकार देना
- C. कॉर्पोरेट डेटाबेस सर्वर पर गुमनाम लॉगिन की अनुमति देना
- D. बिना पासवर्ड के सार्वजनिक Wi-Fi राउटर कॉन्फ़िगर करना

4 **4. आइडेंटिटी एंड एक्सेस मैनेजमेंट (IAM) क्या है?**

- A. डिजिटल पहचानों का प्रबंधन करने और सिस्टम विशेषाधिकारों को नियंत्रित करने वाले फ़्रेमवर्क
- B. स्थानीय फ़ाइल डायरेक्टरी स्कैन करने वाली एंटीवायरस यूटिलिटी
- C. एयर-गैप्ड मीडिया का उपयोग करने वाली बैकअप स्टोरेज प्रणाली
- D. स्पूफ़ किए गए डोमेन को अस्वीकार करने वाला ईमेल गेटवे प्रोटोकॉल

5 **5. कंटिन्यूअस ऑथेंटिकेशन का क्या अर्थ है?**

- A. सक्रिय सत्र के दौरान उपयोगकर्ता की पहचान और डिवाइस की स्थिति को बार-बार सत्यापित करना
- B. मास्टर पासवर्ड हर 10 मिनट में बदलना
- C. कई एल्गोरिदम से डेटाबेस रिकॉर्ड्स को हैश करना
- D. TLS कुंजियों से नेटवर्क ट्रांज़िट पैकेट को एन्क्रिप्ट करना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. ज़ीरो ट्रस्ट मानता है कि कॉर्पोरेट फ़ायरवॉल के भीतर का सारा ट्रैफ़िक सुरक्षित है।

○ सही ○ गलत

7 प्रश्न 7

7. माइक्रो-सेगमेंटेशन हमलावरों की आंतरिक सर्वरों में पार्श्व रूप से आगे बढ़ने की क्षमता सीमित करता है।

○ सही ○ गलत

8 प्रश्न 8

8. न्यूनतम विशेषाधिकार डिफ़ॉल्ट रूप से सभी डेटाबेस फ़ाइलों तक पहुँच देता है।

○ सही ○ गलत

9 प्रश्न 9

9. निरंतर सत्यापन पूरे लॉगिन सत्र के दौरान डिवाइस की स्थिति और क्रेडेंशियल की पुष्टि करता है।

○ सही ○ गलत

10 प्रश्न 10

10. Zero Trust लागू करने से समझौता किए गए कॉर्पोरेट लॉगिन का प्रभाव घटता है।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. हर एक्सेस बिंदु पर क्रेडेंशियल माँगना निरंतर _____ है।
2. कॉर्पोरेट नेटवर्क को छोटे ज़ोन में बाँटना माइक्रो _____ है।
3. सिस्टम तक पहुँच देने से पहले हर व्यक्ति की _____ पक्की की जाती है।
4. उपयोगकर्ता अनुमतियाँ सीमित करने में न्यूनतम _____ के सिद्धांत का उपयोग होता है।
5. जुड़े उपकरणों की सेहत का आकलन डिवाइस _____ को स्कैन करता है।
6. सक्रिय सत्रों को लॉग करना और जाँचना सुरक्षा _____ है।

शब्दावली शब्द-बैंक

उपयोगकर्ता पहचान | ऑडिटिंग | पॉश्चर | फ़ायरवॉल | राउटर | विशेषाधिकार | सत्यापन | सेगमेंटेशन

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

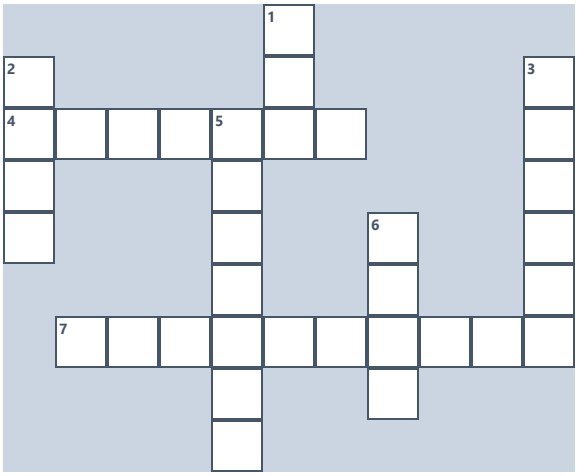
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. सत्यापन**	**A**	उपयोगकर्ता क्रेडेंशियल की पहुँच का प्रबंधन।
☐	**2. सेगमेंटेशन**	**B**	न्यूनतम पहुँच अधिकार का सिद्धांत।
☐	**3. IAM**	**C**	नेटवर्क पैकेट ट्रैफ़िक को रूट करना।
☐	**4. विशेषाधिकार**	**D**	बाहरी नेटवर्क अवरोध सुरक्षा।
☐	**5. पॉश्चर**	**E**	लॉग किए गए एक्सेस सेशन की समीक्षा।
☐	**6. ऑडिटिंग**	**F**	आंतरिक नेटवर्क ज़ोन को विभाजित करना।
☐	**7. फ़ायरवॉल**	**G**	उपयोगकर्ता क्रेडेंशियल की हमेशा जाँच करना।
☐	**8. राउटर**	**H**	डिवाइस की स्वास्थ्य स्थिति का मूल्यांकन।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

4. कंप्यूटर, फ़ोन जैसे उपकरणों को ख़तरों से बचाना। (7)

7. यह तय करना कि सिस्टम इस्तेमाल करने वाला व्यक्ति वास्तव में कौन है। (10)

ऊपर से नीचे

1. उपकरण की सेहत की स्थिति का आकलन। (3)

2. लॉग किए गए एक्सेस सत्रों की समीक्षा। (4)

3. आंतरिक नेटवर्क ज़ोन को बाँटना। (6)

5. नेटवर्क की गतिविधियों पर लगातार नज़र रखना। (7)

6. उपयोगकर्ता के क्रेडेंशियल की हमेशा जाँच करना। (4)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

4 बाएँ से दाएँ: कंप्यूटर, फ़ोन जैसे उपकरणों को ख़तरों से बचाना। (7 अक्षर):

7 बाएँ से दाएँ: यह तय करना कि सिस्टम इस्तेमाल करने वाला व्यक्ति वास्तव में कौन है। (10 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: उपकरण की सेहत की स्थिति का आकलन। (3 अक्षर):

2 ऊपर से नीचे: लॉग किए गए एक्सेस सत्रों की समीक्षा। (4 अक्षर):

3 ऊपर से नीचे: आंतरिक नेटवर्क ज़ोन को बाँटना। (6 अक्षर):

5 ऊपर से नीचे: नेटवर्क की गतिविधियों पर लगातार नज़र रखना। (7 अक्षर):

6 ऊपर से नीचे: उपयोगकर्ता के क्रेडेंशियल की हमेशा जाँच करना। (4 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

ड	रे	स	ख	नि	फ	ढ	मा	ना	का	रे	दे	सि	मी	क
पि	ता	ति	ज	श	भ	ऊ	अ	से	ऊ	ए	रि	वि	श	य
वि	व	न	वा	पा	ल	च	से	कि	ग	य	घ	प	के	की
व	सि	प	र	का	धि	षा	शे	वि	री	में	त	की	कि	सि
ना	ने	त्या	पा	ते	उ	ण	ए	ता	सा	मी	टे	न	नी	ऋ
क्षा	ले	स	घ	ति	प	जि	सु	ला	ए	जी	ले	श	ड	ल
र	द	जे	घ	के	यो	च	से	र	दे	री	ए	पी	न	उ
सु	अ	जे	मि	घ	ग	व	आ	च	क्षा	मी	र	च	ट	थ
स	फ	ग	ना	सी	क	का	ज	फ	नी	नि	जी	श्व	ता	ठ
इ	से	लि	ट	आ	र्ता	इ	से	रा	के	री	ग	पा	पॉ	वा
वा	सि	य	नि	पि	प	ने	ख	के	वे	ग	ऊ	रा	ड	नी
डि	दे	दि	भ	आ	ह	नि	जे	वे	टिं	वे	ष	ण	नी	प
कि	से	य	ह	ह	चा	ते	रा	डि	द	सा	सी	थ	जे	इ
मे	ला	ढ	पे	ऋ	न	वे	ऑ	नी	वे	उ	थ	ह	जे	त
य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी	व

शब्दावली शब्द-सूची

सत्यापन, सेगमेंटेशन, उपयोगकर्तापहचान, विशेषाधिकार, पॉश्चर, ऑडिटिंग, सुरक्षानिगरानी, डिवाइससुरक्षा

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द	परिभाषाएँ और मिलान फ़ील्ड
A. सत्यापन	1. नेटवर्क की गतिविधियों पर लगातार नज़र रखना।
B. सेगमेंटेशन	2. लॉग किए गए एक्सेस सत्रों की समीक्षा।
C. उपयोगकर्तापहचान	3. न्यूनतम पहुँच अधिकारों का सिद्धांत।
D. विशेषाधिकार	4. आंतरिक नेटवर्क ज़ोन को बाँटना।
E. पॉश्चर	5. कंप्यूटर, फ़ोन जैसे उपकरणों को ख़तरों से बचाना।
F. ऑडिटिंग	6. उपकरण की सेहत की स्थिति का आकलन।
G. सुरक्षानिगरानी	7. यह तय करना कि सिस्टम इस्तेमाल करने वाला व्यक्ति वास्तव में कौन है।
H. डिवाइससुरक्षा	8. उपयोगकर्ता के क्रेडेंशियल की हमेशा जाँच करना।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर साइबर सुरक्षा की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. **प स न त्या** _____

2. **चा ग उ प क न प ह र्ता यो** _____

3. **र श्च पॉ** _____

4. **नी र ग नि रा सु क्षा** _____

5. **टे में न से श ग** _____

6. **का धि वि षा र शे** _____

7. **टिं ऑ ग डि** _____

8. **वा स क्षा डि र सु इ** _____

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
2	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
3	डिवाइस पर जाँची जाने वाली चीज़ें			
4	ऐसी चीज़ें जिन्हें लॉग किया जाता है			
5	साइबर सुरक्षा से जुड़े शब्द			
6	ऐसी चीज़ें जिनकी Zero Trust जाँच करता है			
7	रोज़मर्रा की ज़िंदगी में पहचान पत्र दिखाने की जगहें			
8	यह साबित करने के तरीके कि यह सचमुच आप ही हैं			
9	डेटा लीक के बाद की जाने वाली चीज़ें			
10	कंप्यूटर के संक्रमित होने के संकेत			
11	सॉफ़्टवेयर अपडेट करने के कारण			
12	कंपनी में एक्सेस के स्तर			
13	आपके जाने-पहचाने सुरक्षा टूल			
14	वे ज़ोन जिनमें नेटवर्क को बाँटा जा सकता है			
15	भरोसे से जुड़ी कहावतें			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: ज़ीरो ट्रस्ट नेटवर्क आर्किटेक्चर की ओर बदलाव



परिदृश्य: एक बड़ा उद्यम फ़िलहाल फ़्लैट आंतरिक नेटवर्क इस्तेमाल करता है जिसमें लोकल नेटवर्क का कोई भी डिवाइस सभी कॉर्पोरेट सर्वर और डेटाबेस तक पहुँच सकता है।

चर्चा प्रश्न: पार्श्व गति सीमित करने के लिए नेटवर्क माइक्रो-सेगमेंटेशन रणनीति डिज़ाइन कीजिए।

केस स्टडी 2: न्यूनतम विशेषाधिकार वाले एक्सेस नियंत्रण लागू करना



परिदृश्य: ऑडिट लॉग दिखाते हैं कि अस्थायी डेटाबेस उपयोगकर्ताओं और निचले स्तर के कर्मचारियों के पास महत्वपूर्ण अकाउंटिंग डेटाबेस के लिए वैश्विक पढ़ने और लिखने की अनुमतियाँ हैं।

चर्चा प्रश्न: न्यूनतम विशेषाधिकार लागू करने के लिए डेटाबेस IAM विशेषाधिकारों का ऑडिट कीजिए और उन्हें सीमित कीजिए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

साइबर सुरक्षा पेशेवर नेटवर्क संपत्तियों को ऑनलाइन ख़तरा पैदा करने वालों से बचाता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

20	60	48	39	54		23	61	39	44	61	23		37	52	57
45	37	52	42	46		44	28	61	38	46	33	32		13	39	52	57

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग A)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q1: Zero Trust क्या है?

ज़ीरो ट्रस्ट एक सुरक्षा फ़्रेमवर्क है जो मानता है कि खतरे नेटवर्क सीमा के बाहर और भीतर दोनों जगह मौजूद हैं, इसलिए हर अनुरोध का सत्यापन ज़रूरी है। [1]

Q2: Zero Trust का मूल नियम क्या है?

कभी भरोसा न करें, हमेशा सत्यापित करें।

Q3: माइक्रो-सेग्मेंटेशन क्या है?

ट्रैफ़िक नियंत्रित करने और उल्लंघनों को सीमित रखने के लिए नेटवर्क को छोटे, सुरक्षित तार्किक खंडों में बाँटना।

Q4: लीस्ट प्रिविलेज क्या है?

उपयोगकर्ताओं को उनके विशिष्ट कार्य करने के लिए ज़रूरी न्यूनतम एक्सेस अधिकार ही देना। [2]

Q5: IAM का पूरा नाम क्या है?

पहचान और एक्सेस प्रबंधन।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q6: डिवाइस पोस्चर चेक कैसे मदद करता है?

यह एक्सेस देने से पहले जाँचता है कि डिवाइस पैच किया हुआ है, सक्रिय एंटीवायरस चला रहा है और सुरक्षित है।

Q7: लेटरल मूवमेंट क्या है?

वह प्रक्रिया जिससे हमलावर किसी शुरुआती समझौता किए गए नोड से नेटवर्क में आगे बढ़कर अधिक मूल्यवान सिस्टमों तक पहुँचते हैं।

Q8: क्या Zero Trust फ़ायरवॉल की जगह लेता है?

नहीं, यह पहचान-केंद्रित जाँच और आंतरिक सेगमेंटेशन फ़ायरवॉल जोड़कर उन्हें बेहतर बनाता है।

Q9: कंटीन्युअस ऑथेंटिकेशन क्या है?

केवल शुरुआती साइन-इन पर नहीं, बल्कि सक्रिय लॉगिन सत्र के दौरान उपयोगकर्ता की पहचान का निरंतर सत्यापन।

Q10: फ़्लैट नेटवर्क खतरनाक क्यों है?

फ़्लैट नेटवर्क में एक समझौता किया गया नोड हमलावरों को नेटवर्क के किसी भी डेटाबेस तक आसानी से पहुँचने देता है।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q1: Zero Trust परिधि मॉडल को कैसे संबोधित करता है?

यह पुराने 'castle-and-moat' मॉडल की जगह लेता है, जिससे सुरक्षा सीमा वाले नेटवर्क से हटकर विशिष्ट उपयोगकर्ता पहचान और संसाधनों पर केंद्रित हो जाती है।

Q2: पॉलिसी डिसीज़न पॉइंट (PDP) क्या है?

सिस्टम का वह घटक जो सुरक्षा नियमों के आधार पर प्राधिकरण अनुरोधों का मूल्यांकन करके तय करता है कि एक्सेस दिया जाए या नहीं।

Q3: पॉलिसी एन्फ़ोर्समेंट पॉइंट (PEP) क्या है?

सिस्टम नोड (जैसे गेटवे या प्रॉक्सी) जो PDP के निर्णय के आधार पर कनेक्शन अनुरोधों को भौतिक रूप से अनुमति देता या रोकता है।

Q4: रोल-बेस्ड एक्सेस कंट्रोल (RBAC) Zero Trust को कैसे सपोर्ट करता है?

RBAC अनुमतियों को विशिष्ट भूमिकाओं में समूहित करता है, जिससे उपयोगकर्ताओं को अत्यधिक प्रशासनिक विशेषाधिकार विरासत में मिलने से रोकने में मदद मिलती है।

Q5: कॉन्टेक्स्चुअल एक्सेस कंट्रोल क्या है?

जोखिम आँकने के लिए भौगोलिक स्थान, डिवाइस पोस्चर और लॉगिन समय जैसे द्वितीयक संकेतों से लॉगिन अनुरोधों का मूल्यांकन।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q6: माइक्रो-सेग्मेंटेशन सामान्य VLAN से कैसे अलग है?

VLAN लेयर 2 पर नेटवर्क को बड़े तार्किक खंडों में बाँटते हैं, जबकि माइक्रो-सेगमेंटेशन अलग-अलग वर्कलोड को अलग करने के लिए सॉफ़्टवेयर नीति का उपयोग करता है।

Q7: जस्ट-इन-टाइम (JIT) एक्सेस क्या है?

अस्थायी रूप से उच्च प्रशासनिक अनुमतियाँ देना और कार्य पूरा होते ही उन्हें अपने-आप वापस ले लेना।

Q8: Zero Trust फ़्रेमवर्क में आप API को कैसे सुरक्षित करते हैं?

क्रिप्टोग्राफ़िक रूप से हस्ताक्षरित OAuth टोकन अनिवार्य करके और हर API गेटवे पर अनुरोध हस्ताक्षरों का ऑडिट करके।

Q9: ज़ीरो-ट्रस्ट नेटवर्क एक्सेस (ZTNA) क्लाइंट क्या है?

सॉफ़्टवेयर एजेंट जो कच्चे नेटवर्क सबनेट के बजाय विशिष्ट एप्लिकेशन से सुरक्षित, एन्क्रिप्टेड आउटबाउंड कनेक्शन बनाता है।

Q10: लॉग ऑडिटिंग Zero Trust में कैसे मदद करती है?

निरंतर लॉगिंग स्वचालित सुरक्षा विश्लेषण टूल को विसंगतियाँ पहचानने और संदिग्ध लॉगिन को तुरंत निलंबित करने देती है।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

सुरक्षा उल्लंघनों, बचाव तंत्रों और अनुपालन मानकों से जुड़े वास्तविक तथ्य देखें।

1. सुरक्षा इनसाइट

ज़ीरो ट्रस्ट आर्किटेक्चर पुराने किले-और-खाई मॉडल की जगह पहचान-केंद्रित सत्यापन नियम लाते हैं।

2. सुरक्षा इनसाइट

नेटवर्क माइक्रो-सेगमेंटेशन वर्कलोड को छोटे सुरक्षित क्षेत्रों में अलग करके मैलवेयर की पहुँच का दायरा घटा देता है।

3. सुरक्षा इनसाइट

ज़ीरो ट्रस्ट नेटवर्क सेगमेंट के बजाय संपत्तियों, सेवाओं और खातों जैसे संसाधनों की सुरक्षा पर केंद्रित है। [1]

4. सुरक्षा इनसाइट

न्यूनतम विशेषाधिकार वाली पहुँच नीतियाँ कोर डेटाबेस से अंदरूनी खतरे द्वारा डेटा बाहर ले जाने का जोखिम कम करती हैं।

5. सुरक्षा इनसाइट

डिवाइस पोस्चर सत्यापन ऑपरेटिंग सिस्टम पैच स्तर और सक्रिय एंटीवायरस की स्थिति को रियल टाइम में जाँचता है।

6. सुरक्षा इनसाइट

Zero Trust Network Access (ZTNA) ब्रोकर उपयोगकर्ता की पहुँच का दायरा सीमित करने के लिए कॉर्पोरेट VPN की जगह ले सकते हैं या उनके पूरक बन सकते हैं।

7. सिक्योरिटी इनसाइट

Just-in-Time (JIT) प्रशासनिक विशेषाधिकार प्रत्यायोजन डोमेन कंट्रोलर पर क्रेडेंशियल चोरी का जोखिम घटाता है।

8. सिक्योरिटी इनसाइट

निरंतर सत्यापन लॉग और सत्र व्यवहार का ऑडिट करता है, और असामान्य स्क्रिप्ट निष्पादन पैटर्न दिखाने वाले उपयोगकर्ताओं को निलंबित करता है।

9. सिक्योरिटी इनसाइट

किसी प्रशासनिक क्रेडेंशियल के लीक होने पर पारंपरिक परिधि-आधारित सुरक्षा पार्श्व (लेटरल) हमलों को रोकने में विफल रहती है।

10. सुरक्षा इनसाइट

NIST Special Publication 800-207 (2020) Zero Trust आर्किटेक्चर की एक अमूर्त परिभाषा देता है, जिसमें डिप्लॉयमेंट मॉडल भी शामिल हैं। [1]

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक NIST, OWASP और डेटा गोपनीयता अनुपालन मानकों से तैयार की गई हैं।

शैक्षणिक और उद्योग संदर्भ

[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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 प्रश्न 1 सही उत्तर: A

शिक्षण नोट

ज़ीरो ट्रस्ट सुरक्षा का मूल सिद्धांत क्या है? → कभी भरोसा न करें, स्रोत चाहे जो हो, हर एक्सेस अनुरोध को हमेशा सत्यापित करें

2 प्रश्न 2 सही उत्तर: A

शिक्षण नोट

नेटवर्क माइक्रो-सेगमेंटेशन क्या है? → पार्श्व गति को रोकने के लिए नेटवर्क को छोटे, अलग-थलग ज़ोन में बाँटना

3 प्रश्न 3 सही उत्तर: A

शिक्षण नोट

न्यूनतम विशेषाधिकार का सिद्धांत क्या है? → उपयोगकर्ता की पहुँच अनुमतियों को केवल उतने तक सीमित करना जितना उनके काम के लिए आवश्यक है

4 प्रश्न 4 सही उत्तर: A

शिक्षण नोट

आइडेंटिटी एंड एक्सेस मैनेजमेंट (IAM) क्या है? → डिजिटल पहचानों का प्रबंधन करने और सिस्टम विशेषाधिकारों को नियंत्रित करने वाले फ़्रेमवर्क

5 प्रश्न 5 सही उत्तर: A

शिक्षण नोट

कंटिन्यूअस ऑथेंटिकेशन का क्या अर्थ है? → सक्रिय सत्र के दौरान उपयोगकर्ता की पहचान और डिवाइस की स्थिति को बार-बार सत्यापित करना

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** **सही उत्तर: गलत**

शिक्षण नोट

गलत: Zero Trust नेटवर्क लोकेशन के आधार पर, अंदर या बाहर, कोई अंतर्निहित भरोसा नहीं देता।

7 **प्रश्न 7** **सही उत्तर: सही**

शिक्षण नोट

सही: छोटे अलग-थलग ज़ोन सीमित करते हैं कि घुसपैठिया सर्वरों के बीच कितनी दूर जा सकता है।

8 **प्रश्न 8** **सही उत्तर: गलत**

शिक्षण नोट

गलत: न्यूनतम विशेषाधिकार हर भूमिका को केवल उसके लिए ज़रूरी न्यूनतम एक्सेस देता है।

9 **प्रश्न 9** **सही उत्तर: सही**

शिक्षण नोट

निरंतर सत्यापन पूरे लॉगिन सत्र के दौरान डिवाइस की स्थिति और क्रेडेंशियल की पुष्टि करता है।

10 **प्रश्न 10** **सही उत्तर: सही**

शिक्षण नोट

Zero Trust लागू करने से समझौता किए गए कॉर्पोरेट लॉगिन का प्रभाव घटता है।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

G 1. सत्यापन	F 2. सेगमेंटेशन	A 3. IAM	B 4. विशेषाधिकार
H 5. पॉश्चर	E 6. ऑडिटिंग	D 7. फ़ायरवॉल	C 8. राउटर

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 सत्यापन	2 सेगमेंटेशन	3 उपयोगकर्ता पहचान	4 विशेषाधिकार
5 पॉश्चर	6 ऑडिटिंग		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 G – सुरक्षानिगरानी	2 F – ऑडिटिंग	3 D – विशेषाधिकार	4 B – सेगमेंटेशन
5 H – डिवाइससुरक्षा	6 E – पॉश्चर	7 C – उपयोगकर्तापहचान	8 A – सत्यापन

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी सत्यापन, सेगमेंटेशन और IAM को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

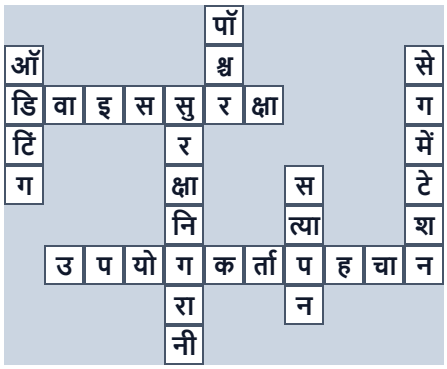
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ड	रे	स	ख	नि	फ	ढ	मा	ना	का	रे	दे	सि	मी	क
पि	ता	ति	ज	श	भ	ऊ	अ	से	ऊ	ए	रि	वि	श	य
वि	व	न	वा	पा	ल	च	से	कि	ग	य	घ	प	के	की
व	सि	प	र	का	धि	षा	शे	वि	री	में	त	की	कि	सि
ना	ने	त्या	पा	ते	उ	ण	ए	ता	सा	मी	टे	न	नी	ऋ
क्षा	ले	स	घ	ति	प	जि	सु	ला	ए	जी	ले	श	ड	ल
र	द	जे	घ	के	यो	च	से	र	दे	री	ए	पी	न	उ
सु	अ	जे	मि	घ	ग	व	आ	च	क्षा	मी	र	च	ट	थ
स	फ	ग	ना	सी	क	का	ज	फ	नी	नि	जी	श्व	ता	ठ
इ	से	लि	ट	आ	र्ता	इ	से	रा	के	री	ग	पा	पॉ	वा
वा	सि	य	नि	पि	प	ने	ख	के	वे	ग	ऊ	रा	ड	नी
डि	दे	दि	भ	आ	ह	नि	जे	वे	टिं	वे	ष	ण	नी	प
कि	से	य	ह	ह	चा	ते	रा	डि	द	सा	सी	थ	जे	इ
मे	ला	ढ	पे	ऋ	न	वे	ऑ	नी	वे	उ	थ	ह	जे	त
य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी	व

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

4 बाएँ से दाएँ: डिवाइससुरक्षा कंप्यूटर, फ़ोन जैसे उपकरणों को ख़तरों से बचाना। (7 अक्षर)

7 बाएँ से दाएँ: उपयोगकर्तापहचान यह तय करना कि सिस्टम इस्तेमाल करने वाला व्यक्ति वास्तव में कौन है। (10 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: पॉश्चर उपकरण की सेहत की स्थिति का आकलन। (3 अक्षर)

2 ऊपर से नीचे: ऑडिटिंग लॉग किए गए एक्सेस सत्रों की समीक्षा। (4 अक्षर)

3 ऊपर से नीचे: सेगमेंटेशन आंतरिक नेटवर्क ज़ोन को बाँटना। (6 अक्षर)

5 ऊपर से नीचे: सुरक्षानिगरानी नेटवर्क की गतिविधियों पर लगातार नज़र रखना। (7 अक्षर)

6 ऊपर से नीचे: सत्यापन उपयोगकर्ता के क्रेडेंशियल की हमेशा जाँच करना। (4 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. पसनत्या — **सत्यापन**
2. चागउपकनपहर्तायो — **उपयोगकर्तापहचान**
3. रश्वपॉ — **पॉश्चर**
4. नीरगनिरासुक्षा — **सुरक्षानिगरानी**
5. टेमेंनसेशग — **सेगमेंटेशन**
6. काधिविषारशे — **विशेषाधिकार**
7. टिऑगडि — **ऑडिटिंग**
8. वासक्षाडिरसुइ — **डिवाइससुरक्षा**

गुप्त कूट चुनौती कुंजी

"ज़ीरो ट्रस्ट में हमेशा सत्यापन करें"

केस स्टडी के उत्तर

A केस स्टडी 1: ज़ीरो ट्रस्ट नेटवर्क आर्किटेक्चर की ओर बदलाव

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक बड़ा एंटरप्राइज़ अभी फ़्लैट आंतरिक नेटवर्क इस्तेमाल करता है, जहाँ लोकल नेटवर्क का कोई भी डिवाइस सभी कॉर्पोरेट सर्वरों और डेटाबेस तक पहुँच सकता है।
- अनुशंसित रणनीति और समाधान: फ़्लैट नेटवर्क को अलग-अलग विभागीय ज़ोन में बाँटें। ज़ोन के बीच ट्रैफ़िक नियंत्रित करने के लिए आंतरिक फ़ायरवॉल लगाएँ, और हर पहुँच के लिए कनेक्शन टोकन का सत्यापन अनिवार्य करें।

B केस स्टडी 2: न्यूनतम विशेषाधिकार वाले एक्सेस नियंत्रण लागू करना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: ऑडिट लॉग से पता चलता है कि अस्थायी डेटाबेस उपयोगकर्ताओं और निचले स्तर के कर्मचारियों के पास महत्वपूर्ण अकाउंटिंग डेटाबेस की वैश्विक रीड और राइट अनुमतियाँ हैं।
- अनुशंसित रणनीति और समाधान: सभी वैश्विक प्रशासनिक विशेषाधिकार रद्द करें। सटीक कार्य-भूमिकाओं के अनुरूप Role-Based Access Control (RBAC) लागू करें, और साप्ताहिक स्वचालित अनुमति समीक्षा शुरू करें।