ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

สถาปัตยกรรมและความปลอดภัยแบบซีโร่ทรัสต์

การตรวจสอบอย่างต่อเนื่อง การแบ่งส่วนย่อยของเครือข่าย การจัดการตัวตนและการเข้าถึง สิทธิ์ขั้นต่ำ และการตรวจสอบสถานะความปลอดภัย

ภาพรวมการเรียนรู้ความปลอดภัยแบบซีโร่ทรัสต์

ได้รับการรักษาความปลอดภัย

การเข้ารหัสข้อมูล

มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด

มาตรฐานสากล

กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์

นโยบายการเข้าถึง

การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับสถาปัตยกรรมและความปลอดภัยแบบ Zero Trust คุณจะได้สำรวจการตรวจสอบอย่างต่อเนื่อง การแบ่งส่วนย่อยของเครือข่าย (micro-segmentation) การจัดการข้อมูลระบุตัวตนและการเข้าถึง (IAM) สิทธิ์น้อยที่สุด และการตรวจสอบเซสชัน

จุดตรวจสอบของใบงาน

- ☐ **ส่วนที่ 1-4: เรียนรู้ความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามให้เชี่ยวชาญ**
- ☐ **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- ☐ **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- ☐ **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- ☐ **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- ☐ **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความปลอดภัยไซเบอร์ของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/khwam-plodphai-zero-trust/

เส้นทางการเรียนรู้กลยุทธ์ซีโร่ทรัสต์ของคุณ

- ทำความเข้าใจหลักการสำคัญของการตรวจสอบอย่างต่อเนื่อง
- ใช้การแบ่งส่วนเครือข่ายย่อยและการเข้าถึงด้วยสิทธิ์ขั้นต่ำ
- ตั้งค่าการตรวจสอบสถานะความปลอดภัยของอุปกรณ์และการตรวจสอบเซสชันที่ใช้งานอยู่

คำแนะนำคู่มือความปลอดภัยแบบซีโร่ทรัสต์

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ สถาปัตยกรรม Zero Trust ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

สถาปัตยกรรมและความปลอดภัยแบบซีโร่ทรัสต์ (บทนำ)

ความปลอดภัยแบบซีโร่ทรัสต์มาแทนที่โมเดลขอบเขตเครือข่ายแบบเก่าด้วยนโยบายที่เข้มงวดว่า 'ไม่ไว้วางใจใคร ตรวจสอบเสมอ' การใช้การแบ่งเซกเมนต์ย่อย (micro-segmentation) การจัดการข้อมูลระบุตัวตนและการเข้าถึง (IAM) สิทธิ์ขั้นต่ำที่จำเป็น และการตรวจสอบสถานะอุปกรณ์ ช่วยบล็อกการเคลื่อนที่ด้านข้างของภัยคุกคาม

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **1. หลักการสำคัญของความปลอดภัยแบบ Zero Trust คืออะไร?**
   - A. ไม่ไว้ใจใครเลย ตรวจสอบทุกคำขอเข้าถึงเสมอไม่ว่าจะมาจากแหล่งใด
   - B. การสมมติว่าทราฟฟิกทั้งหมดภายในไฟร์วอลล์ขององค์กรปลอดภัย
   - C. จัดเก็บไฟล์ฐานข้อมูลโดยไม่เข้ารหัสเพื่อเพิ่มความเร็ว
   - D. การบังคับใช้การยืนยันตัวตนอีเมลโดยใช้ระเบียน SPF เท่านั้น

2. **2. การแบ่งส่วนเครือข่ายย่อย (micro-segmentation) คืออะไร?**
   - A. การแบ่งเครือข่ายเป็นโซนเล็กๆ ที่แยกจากกันเพื่อจำกัดการเคลื่อนที่ในแนวขวาง
   - B. การเข้ารหัสการ์ดเครือข่ายระหว่างการส่งข้อมูล
   - C. การเชื่อมต่อเซิร์ฟเวอร์ภายในทั้งหมดเข้ากับที่อยู่ IP สาธารณะเดียว
   - D. การเฝ้าดูการกดแป้นพิมพ์ของผู้ใช้ในเซสชันเบราว์เซอร์

3. **3. หลักการสิทธิ์ขั้นต่ำที่สุด (principle of least privilege) คืออะไร?**
   - A. การจำกัดสิทธิ์การเข้าถึงของผู้ใช้ให้เท่าที่จำเป็นต่อหน้าที่ของตน
   - B. การให้สิทธิ์ระบบทั้งหมดแก่ผู้ใช้ทุกคนโดยค่าเริ่มต้น
   - C. การอนุญาตให้ล็อกอินแบบไม่ระบุตัวตนเข้าสู่เซิร์ฟเวอร์ฐานข้อมูลขององค์กร
   - D. การตั้งค่าเราเตอร์ Wi-Fi สาธารณะโดยไม่มีรหัสผ่าน

4. **4. การจัดการตัวตนและการเข้าถึง (IAM) คืออะไร?**
   - A. เฟรมเวิร์กที่จัดการตัวตนดิจิทัลและควบคุมสิทธิ์ของระบบ
   - B. ยูทิลิตีแอนตี้ไวรัสที่สแกนไดเรกทอรีไฟล์ในเครื่อง
   - C. ระบบสำรองข้อมูลที่ใช้สื่อ air-gapped
   - D. โปรโตคอลเกตเวย์อีเมลที่ปฏิเสธโดเมนที่ปลอมแปลง

5. **5. การยืนยันตัวตนอย่างต่อเนื่องหมายความว่าอย่างไร?**
   - A. การตรวจสอบตัวตนผู้ใช้และสถานะอุปกรณ์ซ้ำๆ ระหว่างเซสชันที่ใช้งานอยู่
   - B. การเปลี่ยนรหัสผ่านหลักทุก 10 นาที
   - C. แฮชระเบียนฐานข้อมูลโดยใช้หลายอัลกอริทึม
   - D. การเข้ารหัสแพ็กเก็ตเครือข่ายระหว่างส่งด้วยกุญแจ TLS

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. ซีโร่ทรัสต์ถือว่าทราฟฟิกทั้งหมดภายในไฟร์วอลล์ขององค์กรปลอดภัย

○ จริง ○ เท็จ

7 คำถาม 7

7. Micro-segmentation จำกัดความสามารถของผู้โจมตีในการเคลื่อนที่ในแนวขวางระหว่างเซิร์ฟเวอร์ภายใน

○ จริง ○ เท็จ

8 คำถาม 8

8. หลักการสิทธิ์น้อยที่สุดให้สิทธิ์เข้าถึงไฟล์ฐานข้อมูลทั้งหมดตามค่าเริ่มต้น

○ จริง ○ เท็จ

9 คำถาม 9

9. การตรวจสอบอย่างต่อเนื่องจะตรวจสอบสุขภาพของอุปกรณ์และข้อมูลรับรองตลอดเซสชันการเข้าสู่ระบบ

○ จริง ○ เท็จ

10 คำถาม 10

10. การใช้ Zero Trust ลดผลกระทบจากข้อมูลเข้าสู่ระบบขององค์กรที่ถูกบุกรุก

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การกำหนดให้ใช้ข้อมูลประจำตัวทุกจุดเข้าถึงคือ _____ อย่างต่อเนื่อง
2. การแบ่งเครือข่ายองค์กรออกเป็นโซนเล็ก ๆ คือ _____ ระดับไมโคร
3. การกำหนดค่าตัวตนดิจิทัลและการควบคุมการเข้าถึงใช้ระบบ _____
4. การจำกัดสิทธิ์ของผู้ใช้ใช้หลักการ _____ น้อยที่สุด
5. การประเมินความสมบูรณ์ของอุปกรณ์ที่เชื่อมต่อคือการสแกน _____
6. การบันทึกและทบทวนเซสชันที่ใช้งานอยู่คือ _____ ด้านความปลอดภัย

คลังคำศัพท์

การตรวจสอบ | การแบ่งส่วน | การยืนยัน | ไฟร์วอลล์ไอเอเอ็ม | เราเตอร์ | สถานะอุปกรณ์ | สิทธิ์เข้าถึง

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

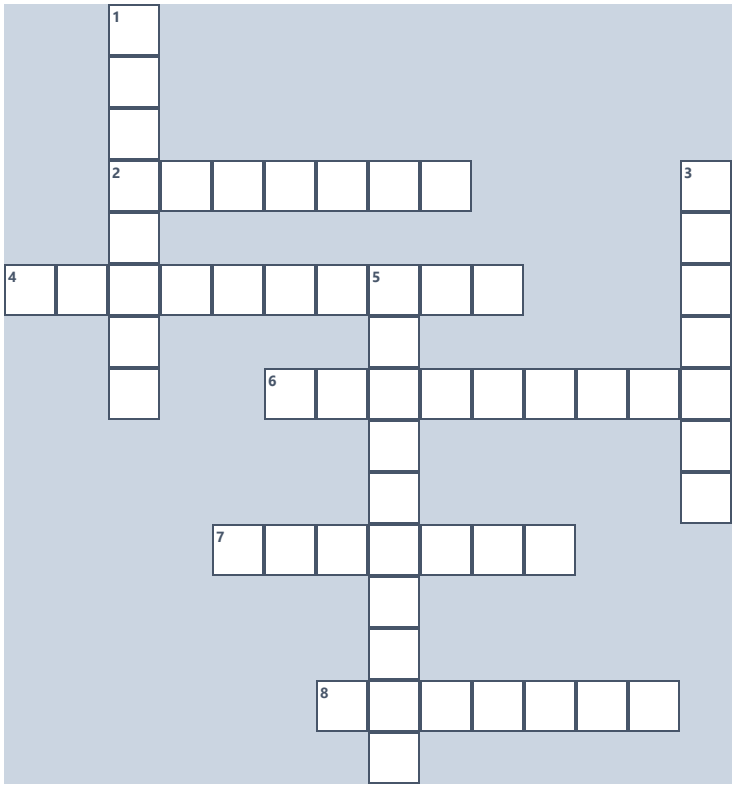
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. การตรวจสอบยืนยัน**	**A**	การจัดการสิทธิ์เข้าถึงข้อมูลประจำตัวของผู้ใช้
☐	**2. การแบ่งเซกเมนต์**	**B**	หลักการสิทธิ์การเข้าถึงน้อยที่สุด
☐	**3. IAM**	**C**	การกำหนดเส้นทางทราฟฟิกแพ็กเก็ตเครือข่าย
☐	**4. สิทธิพิเศษ**	**D**	การป้องกันกำแพงเครือข่ายภายนอก
☐	**5. สถานะความปลอดภัย**	**E**	การตรวจสอบเซสชันการเข้าถึงที่บันทึกไว้
☐	**6. การตรวจสอบ**	**F**	การแบ่งโซนเครือข่ายภายใน
☐	**7. ไฟร์วอลล์**	**G**	ตรวจสอบข้อมูลรับรองผู้ใช้อยู่เสมอ
☐	**8. เราเตอร์**	**H**	การประเมินสถานะสุขภาพของอุปกรณ์

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. การกำหนดเส้นทางทราฟฟิกแพ็กเก็ตเครือข่าย (7)

4. การประเมินสถานะความสมบูรณ์ของอุปกรณ์ (10)

6. การแบ่งโซนเครือข่ายภายใน (9)

7. การป้องกันกำแพงเครือข่ายภายนอก (7)

8. การจัดการสิทธิ์เข้าถึงข้อมูลประจำตัวผู้ใช้ (7)

แนวตั้ง

1. หลักการให้สิทธิ์น้อยที่สุด (8)

3. การตรวจสอบข้อมูลประจำตัวผู้ใช้อยู่เสมอ (7)

5. การทบทวนเซสชันการเข้าถึงที่บันทึกไว้ (10)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: การกำหนดเส้นทางทราฟฟิกแพ็กเก็ตเครือข่าย (7 ตัวอักษร):

4 แนวนอน: การประเมินสถานะความสมบูรณ์ของอุปกรณ์ (10 ตัวอักษร):

6 แนวนอน: การแบ่งโซนเครือข่ายภายใน (9 ตัวอักษร):

7 แนวนอน: การป้องกันกำแพงเครือข่ายภายนอก (7 ตัวอักษร):

8 แนวนอน: การจัดการสิทธิ์เข้าถึงข้อมูลประจำตัวผู้ใช้ (7 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: หลักการให้สิทธิ์น้อยที่สุด (8 ตัวอักษร):

3 แนวตั้ง: การตรวจสอบข้อมูลประจำตัวผู้ใช้อยู่เสมอ (7 ตัวอักษร):

5 แนวตั้ง: การทบทวนเซสชันการเข้าถึงที่บันทึกไว้ (10 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า า รี ต ว ย ง ก ก ค จ น ตี ว ร
ตี ว า ล ล ด า า อ ย ไ ซ ฟ ก ก
บ ร์ ล ม า ป อ ร อ ม อ มี า ล ล
อ อ ป จ า นี กี ยื พ ร เ ง า ซ า
ส ต า ลี จ ส ดี น า น อ ล ผ ก ดี
จ เ ซ ก ด ถ า ยั ต า เ จ า า ค
ว า ก ดี า า ซ น สิ ว อ็ ก ด ร กี
ร ร ด ท ผ น ฟ ซ ท ไ ม มี ม แ อ
ต เ ต ฟ ร ะ ดี า ธิ์ ฟ ท า ส บ่ ท
ร ข ข า น อุ ก า เ ร์ ล า ม ง ร
า มี า ร ซ ป ก ด ข้ ว ง น ร ส่ ต
ก สี ย ข มี ก ดี ด า อ ด ว บ ว ฟ
อ า ร ห ห ร รี น ถี ล ผ นี ม น ผ
ดี ข กี ส บ ณ์ ลี ง ง ล์ ด ร ด ค ผ
ห ดี ป ร กี นี า ต จ ห ดี ด บ ตี น

รายการคำศัพท์

การยืนยัน | การแบ่งส่วน | ไอเอเอ็ม | สิทธิ์เข้าถึงเราเตอร์ | สถานะอุปกรณ์ | การตรวจสอบ | ไฟร์วอลล์

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. การยืนยัน

B. การแบ่งส่วน

C. ไอเอเอ็ม

D. สิทธิ์เข้าถึง

E. สถานะอุปกรณ์

F. การตรวจสอบ

G. ไฟร์วอลล์

H. เราเตอร์

คำนิยามและช่องจับคู่

1. การป้องกันกำแพงเครือข่ายภายนอก
2. การทบทวนเซสชันการเข้าถึงที่บันทึกไว้
3. หลักการให้สิทธิ์น้อยที่สุด
4. การแบ่งโซนเครือข่ายภายใน
5. การกำหนดเส้นทางทราฟฟิกแพ็กเก็ตเครือข่าย
6. การประเมินสถานะความสมบูรณ์ของอุปกรณ์
7. การจัดการสิทธิ์เข้าถึงข้อมูลประจำตัวผู้ใช้
8. การตรวจสอบข้อมูลประจำตัวผู้ใช้อยู่เสมอ

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ย ย ั ก น น ร า _____
2. ไ เ ม อ็ เ อ อ _____
3. ส อ ุ ร ป ถ ะ ณ์ น ก า _____
4. ส์ ฟ อ ว ล ไ ร์ _____
5. ส่ ป่ า น ง แ ก ว ร _____
6. ถ ึ ง เ า ส ิ ซ้ ท ธิ์ _____
7. า ต ก จ ว ส อ บ ร ร _____
8. ร เ ร์ เ อ ต า _____

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
2	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
3	สิ่งที่ตรวจสอบบนอุปกรณ์			
4	สิ่งที่ถูกบันทึกเป็นล็อก			
5	คำที่เกี่ยวข้องกับความปลอดภัยไซเบอร์			
6	สิ่งที่ **Zero Trust** ตรวจสอบ			
7	สถานที่ที่คุณแสดงบัตรประจำตัวในชีวิตประจำวัน			
8	วิธีพิสูจน์ว่าเป็นคุณจริง ๆ			
9	สิ่งที่ควรทำหลังข้อมูลรั่วไหล			
10	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
11	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
12	ระดับการเข้าถึงในบริษัท			
13	เครื่องมือด้านความปลอดภัยที่คุณรู้จัก			
14	โซนที่เครือข่ายแบ่งออกได้			
15	คำพูดเกี่ยวกับความไว้วางใจ			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การเปลี่ยนไปใช้สถาปัตยกรรมเครือข่ายแบบ Zero Trust



สถานการณ์: องค์กรขนาดใหญ่ปัจจุบันใช้เครือข่ายภายในแบบแบน ที่อุปกรณ์ใดก็ตามในเครือข่ายภายในเข้าถึงเซิร์ฟเวอร์และฐานข้อมูลขององค์กรทั้งหมดได้

คำถามอภิปราย: จงออกแบบกลยุทธ์การแบ่งส่วนเครือข่ายย่อย (micro-segmentation) เพื่อจำกัดการเคลื่อนที่ในแนวขวาง

กรณีศึกษาที่ 2: การปรับใช้การควบคุมการเข้าถึงตามสิทธิ์ขั้นต่ำ



สถานการณ์: บันทึกการตรวจสอบเผยว่าผู้ใช้ฐานข้อมูลชั่วคราวและพนักงานระดับล่างมีสิทธิ์อ่านและเขียนส่วนกลางต่อฐานข้อมูลบัญชีสำคัญ

คำถามอภิปราย: จงตรวจสอบและจำกัดสิทธิ์ IAM ของฐานข้อมูลเพื่อบังคับใช้หลักการให้สิทธิ์น้อยที่สุด

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ปกป้องทรัพย์สินเครือข่ายจากผู้ก่อภัยคุกคามออนไลน์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ั=48
า=49 ำ=50 ิ=51 ี=52 ึ=53 ื=54 ุ=55 ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ็=62 ่=63 ้=64 ๊=65 ๋=66 ์=67

34	54	25	34	48	25		21	48	39	21	25		57	42	33	45
20	**64**	**39**	**34**		**11**	**52**	**59**	**35**	**63**	**23**	**35**	**48**	**42**	**21**	**67**	

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: Zero Trust คืออะไร?

ซีโร่ทรัสต์เป็นกรอบความปลอดภัยที่ถือว่าภัยคุกคามมีอยู่ทั้งภายนอกและภายในขอบเขตเครือข่าย จึงต้องตรวจสอบทุกคำขอ [1]

Q2: กฎหลักของ Zero Trust คืออะไร?

ไม่ไว้วางใจใคร ตรวจสอบทุกครั้ง

Q3: ไมโครเซกเมนเทชัน (micro-segmentation) คืออะไร?

การแบ่งเครือข่ายเป็นส่วนตรรกะเล็กๆ ที่ปลอดภัยเพื่อควบคุมทราฟฟิกและจำกัดความเสียหายจากการบุกรุก

Q4: สิทธิ์ขั้นต่ำที่จำเป็น (least privilege) คืออะไร?

การให้ผู้ใช้มีสิทธิ์การเข้าถึงขั้นต่ำที่จำเป็นต่อการทำงานเฉพาะของตนเท่านั้น [2]

Q5: IAM ย่อมาจากอะไร?

การจัดการตัวตนและการเข้าถึง

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: การตรวจสอบสถานะอุปกรณ์ช่วยได้อย่างไร?

ตรวจสอบว่าอุปกรณ์ได้รับแพตช์ ใช้แอนตี้ไวรัสที่ทำงานอยู่ และปลอดภัย ก่อนอนุญาตให้เข้าถึง

Q7: การเคลื่อนที่ในแนวขวาง (lateral movement) คืออะไร?

กระบวนการที่ผู้โจมตีใช้เคลื่อนที่ผ่านเครือข่ายจากโหนดแรกที่ถูกเจาะไปยังระบบที่มีมูลค่าสูงกว่า

Q8: Zero Trust มาแทนที่ไฟร์วอลล์หรือไม่?

ไม่ แต่ช่วยเสริมด้วยการเพิ่มการตรวจสอบที่เน้นตัวตนและไฟร์วอลล์แบ่งส่วนภายใน

Q9: การพิสูจน์ตัวตนอย่างต่อเนื่อง (continuous authentication) คืออะไร?

การตรวจสอบตัวตนผู้ใช้อย่างต่อเนื่องตลอดเซสชันการเข้าสู่ระบบที่กำลังใช้งาน ไม่ใช่เฉพาะตอนลงชื่อเข้าใช้ครั้งแรก

Q10: ทำไมเครือข่ายแบบแบนราบจึงอันตราย?

ในเครือข่ายแบบแบน โหนดเดียวที่ถูกบุกรุกทำให้ผู้โจมตีเข้าถึงฐานข้อมูลใดๆ ในเครือข่ายได้ง่าย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: Zero Trust จัดการกับโมเดลขอบเขตเครือข่ายอย่างไร?

แทนที่โมเดล 'ปราสาทและคูน้ำ' ที่ล้าสมัย โดยเปลี่ยนการป้องกันจากเครือข่ายขอบเขตไปสู่ตัวตนผู้ใช้และทรัพยากรเฉพาะ

Q2: จุดตัดสินนโยบาย (PDP) คืออะไร?

ส่วนประกอบของระบบที่ประเมินคำขออนุญาตตามกฎความปลอดภัยเพื่อตัดสินว่าควรให้เข้าถึงหรือไม่

Q3: จุดบังคับใช้นโยบาย (PEP) คืออะไร?

โหนดของระบบ (เช่น เกตเวย์หรือพร็อกซี) ที่อนุญาตหรือบล็อกคำขอเชื่อมต่อจริงตามการตัดสินใจของ PDP

Q4: การควบคุมการเข้าถึงตามบทบาท (RBAC) สนับสนุน Zero Trust อย่างไร?

RBAC จัดกลุ่มสิทธิ์เป็นบทบาทเฉพาะ ช่วยป้องกันไม่ให้ผู้ใช้ได้รับสิทธิ์ผู้ดูแลระบบมากเกินไป

Q5: การควบคุมการเข้าถึงตามบริบทคืออะไร?

การประเมินคำขอล็อกอินโดยใช้เบาะแสรองอย่างตำแหน่งทางภูมิศาสตร์ สถานะอุปกรณ์ และเวลาล็อกอินเพื่อประเมินความเสี่ยง

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: ไมโครเซกเมนเทชันต่างจาก VLAN มาตรฐานอย่างไร?

VLAN แบ่งเครือข่ายเป็นส่วนตรรกะกว้างๆ ที่เลเยอร์ 2 ในขณะที่ micro-segmentation ใช้นโยบายซอฟต์แวร์แยกเวิร์กโหลดแต่ละรายการ

Q7: การเข้าถึงแบบทันเวลา (just-in-time หรือ JIT) คืออะไร?

การให้สิทธิ์ผู้ดูแลระบบระดับสูงชั่วคราวและเพิกถอนโดยอัตโนมัติเมื่อทำงานเสร็จ

Q8: คุณรักษาความปลอดภัย API ในกรอบงาน Zero Trust ได้อย่างไร?

ด้วยการกำหนดให้ใช้โทเคน OAuth ที่ลงนามด้วยการเข้ารหัสและตรวจสอบลายเซ็นของคำขอที่ทุกเกตเวย์ API

Q9: ไคลเอนต์ zero-trust network access (ZTNA) คืออะไร?

ตัวแทนซอฟต์แวร์ที่สร้างการเชื่อมต่อขาออกที่ปลอดภัยและเข้ารหัสไปยังแอปพลิเคชันเฉพาะ แทนที่จะเป็นซับเน็ตเครือข่ายดิบ

Q10: การตรวจสอบบันทึกช่วย Zero Trust ได้อย่างไร?

การบันทึกอย่างต่อเนื่องช่วยให้เครื่องมือวิเคราะห์ความปลอดภัยอัตโนมัติตรวจจับความผิดปกติและระงับการเข้าสู่ระบบที่ผิดปกติได้ทันที

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

สถาปัตยกรรมซีโร่ทรัสต์มาแทนที่โมเดลปราสาทและคูน้ำแบบเดิมด้วยกฎการตรวจสอบที่ยึดตัวตนเป็นศูนย์กลาง

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

Network micro-segmentation ลดพื้นที่ที่มัลแวร์เข้าถึงได้ด้วยการแยกเวิร์กโหลดออกเป็นโซนป้องกันขนาดเล็ก

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ซีโร่ทรัสต์เน้นปกป้องทรัพยากร เช่น สินทรัพย์ บริการ และบัญชี มากกว่าส่วนย่อยของเครือข่าย [1]

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

นโยบายการเข้าถึงด้วยสิทธิ์น้อยที่สุดช่วยลดความเสี่ยงที่ภัยคุกคามจากภายในจะนำข้อมูลออกจากฐานข้อมูลหลัก

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การตรวจสอบสถานะอุปกรณ์ตรวจสอบระดับแพตช์ของระบบปฏิบัติการและสถานะแอนติไวรัสที่ใช้งานอยู่แบบเรียลไทม์

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ตัวกลาง Zero Trust Network Access (ZTNA) สามารถแทนที่หรือเสริม VPN ขององค์กรเพื่อจำกัดขอบเขตการเข้าถึงของผู้ใช้

7. ข้อมูลเชิงลึกด้านความปลอดภัย

การมอบสิทธิ์ผู้ดูแลระบบแบบ Just-in-Time (JIT) ลดความเสี่ยงการขโมยข้อมูลเข้าสู่ระบบบนโดเมนคอนโทรลเลอร์

8. ข้อมูลเชิงลึกด้านความปลอดภัย

บันทึกการตรวจสอบความถูกต้องอย่างต่อเนื่องและตรวจสอบพฤติกรรมเซสชัน โดยระงับผู้ใช้ที่แสดงรูปแบบการรันสคริปต์ผิดปกติ

9. ข้อมูลเชิงลึกด้านความปลอดภัย

การป้องกันแบบเส้นรอบวงแบบดั้งเดิมไม่สามารถบล็อกการโจมตีแนวขวางได้เมื่อข้อมูลรับรองผู้ดูแลระบบรั่วไหล

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

NIST Special Publication 800-207 (2020) ให้คำนิยามเชิงนามธรรมของสถาปัตยกรรม Zero Trust พร้อมรูปแบบการนำไปใช้ [1]

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

หลักการสำคัญของความปลอดภัยแบบ Zero Trust คืออะไร? → ไม่ไว้ใจใครเลย ตรวจสอบทุกคำขอเข้าถึงเสมอไม่ว่าจะมาจากแหล่งใด

2 คำถาม 2 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การแบ่งส่วนเครือข่ายย่อย (micro-segmentation) คืออะไร? → การแบ่งเครือข่ายเป็นโซนเล็กๆ ที่แยกจากกันเพื่อจำกัดการเคลื่อนที่ในแนวขวาง

3 คำถาม 3 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

หลักการสิทธิ์ขั้นต่ำที่สุด (principle of least privilege) คืออะไร? → การจำกัดสิทธิ์การเข้าถึงของผู้ใช้ให้เท่าที่จำเป็นต่อหน้าที่ของตน

4 คำถาม 4 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การจัดการตัวตนและการเข้าถึง (IAM) คืออะไร? → เฟรมเวิร์กที่จัดการตัวตนดิจิทัลและควบคุมสิทธิ์ของระบบ

5 คำถาม 5 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การยืนยันตัวตนอย่างต่อเนื่องหมายความว่าอย่างไร? → การตรวจสอบตัวตนผู้ใช้และสถานะอุปกรณ์ซ้ำๆ ระหว่างเซสชันที่ใช้งานอยู่

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: Zero Trust ไม่ให้ความไว้วางใจโดยปริยายตามตำแหน่งของเครือข่าย ทั้งภายในและภายนอก

7 **คำถาม 7** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: โซนที่แยกออกจากกันขนาดเล็กจำกัดระยะที่ผู้บุกรุกเคลื่อนที่ระหว่างเซิร์ฟเวอร์ได้

8 **คำถาม 8** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: หลักการให้สิทธิ์น้อยที่สุด (least privilege) ให้การเข้าถึงขั้นต่ำที่แต่ละบทบาทต้องการเท่านั้น

9 **คำถาม 9** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การตรวจสอบอย่างต่อเนื่องจะตรวจสอบสุขภาพของอุปกรณ์และข้อมูลรับรองตลอดเซสชันการเข้าสู่ระบบ

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การใช้ Zero Trust ลดผลกระทบจากข้อมูลเข้าสู่ระบบขององค์กรที่ถูกบุกรุก

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

G 1. การตรวจสอบยืนยัน	F 2. การแบ่งเซกเมนต์	A 3. IAM	B 4. สิทธิพิเศษ
H 5. สถานะความปลอดภัย	E 6. การตรวจสอบ	D 7. ไฟร์วอลล์	C 8. เราเตอร์

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 การยืนยัน	2 การแบ่งส่วน	3 ไอเอเอ็ม	4 สิทธิ์เข้าถึง
5 สถานะอุปกรณ์	6 การตรวจสอบ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 G – ไฟร์วอลล์	2 F – การตรวจสอบ	3 D – สิทธิ์เข้าถึง	4 B – การแบ่งส่วน
5 H – เราเตอร์	6 E – สถานะอุปกรณ์	7 C – ไอเอเอ็ม	8 A – การยืนยัน

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย การตรวจสอบยืนยัน การแบ่งเซกเมนต์ และ IAM ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

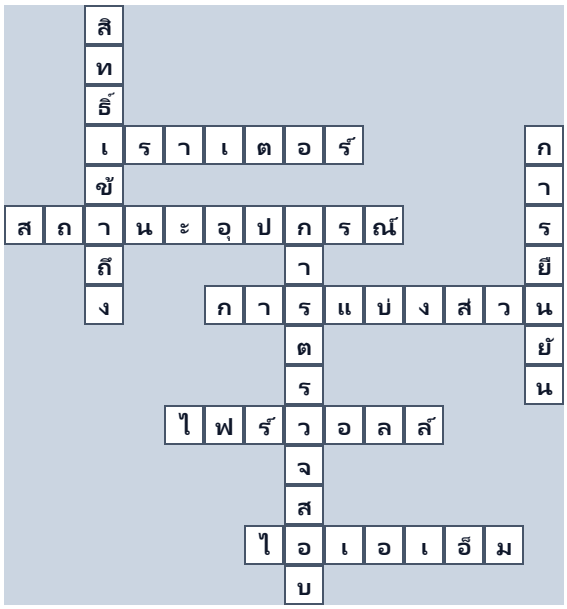
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	า	รี	ต	ว	ย	ง	ก	ก	ค	จ	น	ตี	ว	ร
ตี	ว	า	ล	ล	ด	า	า	อ	ย	ไ	ซ	ฟ	ก	ก
บ	ร์	ล	ม	า	ป	อ	ร	อ	ม	อ	มี	า	ล	ล
อ	อ	ป	จ	า	นี	กี	ยื	พ	ร	เ	ง	า	ช	า
ส	ต	า	ลี	จ	ส	ดี	น	า	น	อ	ล	ผ	ก	ดี
จ	เ	ช	ก	ด	ถ	า	ย้	ต	า	เ	จ	า	า	ค
ว	า	ก	ดี	า	า	ช	น	สิ	ว	อ็	ก	ด	ร	กี
ร	ร	ด	ท	ผ	น	ฟ	ช	ท	ไ	ม	มี	ม	แ	อ
ต	เ	ต	ฟ	ร	ะ	ดี	า	ธิ์	ฟ	ท	า	ส	บ่	ท
ร	ข	ข	า	น	อุ	ก	า	เ	ร์	ล	า	ม	ง	ร
า	มี	า	ร	ช	ป	ก	ด	ข้	ว	ง	น	ร	ส่	ต
ก	สี	ย	ข	มี	ก	ดี	ด	า	อ	ด	ว	บ	ว	ฟ
อ	า	ร	ห	ห	ร	รี	น	ถึ	ล	ผ	นี	ม	น	ผ
ดี	ข	กี	ส	บ	ณ์	ลี	ง	ง	ล์	ด	ร	ด	ค	ผ
ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ	ตี	น

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: เราเตอร์ การกำหนดเส้นทางทราฟฟิกแพ็กเก็ตเครือข่าย (7 ตัวอักษร)

4 แนวนอน: สถานะอุปกรณ์ การประเมินสถานะความสมบูรณ์ของอุปกรณ์ (10 ตัวอักษร)

6 แนวนอน: การแบ่งส่วน การแบ่งโซนเครือข่ายภายใน (9 ตัวอักษร)

7 แนวนอน: ไฟร์วอลล์ การป้องกันกำแพงเครือข่ายภายนอก (7 ตัวอักษร)

8 แนวนอน: ไอเอเอ็ม การจัดการสิทธิ์เข้าถึงข้อมูลประจำตัวผู้ใช้ (7 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: สิทธิ์เข้าถึง หลักการให้สิทธิ์น้อยที่สุด (8 ตัวอักษร)

3 แนวตั้ง: การยืนยัน การตรวจสอบข้อมูลประจำตัวผู้ใช้อยู่เสมอ (7 ตัวอักษร)

5 แนวตั้ง: การตรวจสอบ การทบทวนเซสชันการเข้าถึงที่บันทึกไว้ (10 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ยียักนนรา — การยืนยัน
2. ไมอีเออ — ไอเอเอ็ม
3. สอุรปถะณ์นกา — สถานะอุปกรณ์
4. ส์ฟอวลไร์ — ไฟร์วอลล์
5. ส่ปานงแกวร — การแบ่งส่วน
6. ถึงเาสิข้ทธิ์ — สิทธิ์เข้าถึง
7. าตกจวสอบรร — การตรวจสอบ
8. รเร์เอตา — เราเตอร์

เฉลยภารกิจรหัสลับ

"ยืนยัน ตัวตน เสมอ ด้วย ซีโร่ทรัสต์"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การเปลี่ยนไปใช้สถาปัตยกรรมเครือข่ายแบบ Zero Trust

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: องค์กรขนาดใหญ่ปัจจุบันใช้เครือข่ายภายในแบบแบนราบ ซึ่งอุปกรณ์ใดก็ตามในเครือข่ายท้องถิ่นเข้าถึงเซิร์ฟเวอร์และฐานข้อมูลขององค์กรทั้งหมดได้
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: แบ่งเครือข่ายแบบแบนราบออกเป็นโซนแผนกที่แยกจากกัน ติดตั้งไฟร์วอลล์ภายในเพื่อควบคุมทราฟฟิกระหว่างโซน และกำหนดให้ตรวจสอบโทเค็นการเชื่อมต่อสำหรับการเข้าถึงทั้งหมด

B กรณีศึกษาที่ 2: การปรับใช้การควบคุมการเข้าถึงตามสิทธิ์ขั้นต่ำ

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บันทึกการตรวจสอบเผยว่าผู้ใช้ฐานข้อมูลชั่วคราวและพนักงานระดับล่างมีสิทธิ์อ่านและเขียนแบบเต็มต่อฐานข้อมูลบัญชีที่สำคัญ
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เพิกถอนสิทธิ์ผู้ดูแลระบบระดับโกลบอลทั้งหมด ใช้การควบคุมการเข้าถึงตามบทบาท (RBAC) ให้ตรงกับหน้าที่งานจริง และจัดให้มีการตรวจสอบสิทธิ์อัตโนมัติทุกสัปดาห์