ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

การปกป้องข้อมูลและที่เก็บข้อมูลองค์กร คู่มือความปลอดภัย

การปกปิดข้อมูล การแปลงเป็นโทเค็น การเข้ารหัสแบบข้อมูลที่จัดเก็บเทียบกับข้อมูลระหว่างส่ง การสำรองข้อมูลออฟไลน์

ภาพรวมการเรียนรู้การปกป้องข้อมูล

ได้รับการรักษาความปลอดภัย
การเข้ารหัสข้อมูล
มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด
มาตรฐานสากล
กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์
นโยบายการเข้าถึง
การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับมาตรฐานและการควบคุมการปกป้องข้อมูล คุณจะได้สำรวจการเข้ารหัสทั้งดิสก์ การควบคุมการเข้าถึงที่ปลอดภัย การสำรองข้อมูลด้วยฮาร์ดแวร์ สถานะความปลอดภัยของคลาวด์ และเทคนิคการปิดบังข้อมูล

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/kan-pongkan-khomun/

เส้นทางการเรียนรู้กลยุทธ์การปกป้องข้อมูลของคุณ

- จำแนกความแตกต่างระหว่างเทคนิคการปกปิดข้อมูลและการแปลงเป็นโทเค็น
- ใช้การเข้ารหัสข้อมูลขณะจัดเก็บสำหรับไดรฟ์จัดเก็บข้อมูล และการเข้ารหัสขณะส่งด้วย TLS
- ออกแบบระบบสำรองข้อมูลออฟไลน์ที่แยกจากเครือข่ายเพื่อป้องกันแรนซัมแวร์

คำแนะนำคู่มือการปกป้องข้อมูล

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การปกป้องข้อมูล ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การปกป้องข้อมูลและความปลอดภัยของระบบจัดเก็บข้อมูลระดับองค์กร (บทนำ)

การปกป้องข้อมูลช่วยรักษาสินทรัพย์ข้อมูลขององค์กรด้วยการปกปิดข้อมูล การแปลงเป็นโทเค็น การเข้ารหัสฐานข้อมูลที่จัดเก็บ และโปรโตคอลส่งข้อมูลที่ปลอดภัย การออกแบบข้อมูลสำรองที่แยกจากเครือข่ายช่วยให้มั่นใจว่าฐานข้อมูลสำคัญจะกู้คืนได้เมื่อเกิดการบุกรุกที่กำลังดำเนินอยู่

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. **1. วัตถุประสงค์หลักของการปกปิดข้อมูล (data masking) คืออะไร?**
   - A. การแทนที่ตัวระบุที่ละเอียดอ่อนด้วยอักขระสมมติแต่สมจริงเพื่อปกป้องความเป็นส่วนตัว
   - B. การบีบอัดไฟล์ฐานข้อมูลขนาดใหญ่เพื่อประหยัดพื้นที่จัดเก็บของเซิร์ฟเวอร์จริง
   - C. การลบอีเมลติดต่อลูกค้าเก่าออกจากระบบสำรองข้อมูลถาวร
   - D. การซ่อน IP สาธารณะของเซิร์ฟเวอร์ฐานข้อมูลจากการสแกนบนอินเทอร์เน็ต

2. **2. กลไกใดที่เข้ารหัสไฟล์ที่เก็บอยู่ในฮาร์ดไดรฟ์ของเซิร์ฟเวอร์ฐานข้อมูล?**
   - A. การเข้ารหัสทั้งดิสก์ขณะจัดเก็บ
   - B. โปรโตคอลแฮนด์เชก TLS session ระหว่างการส่งผ่าน
   - C. กฎการส่งต่อเนมเซิร์ฟเวอร์ DNS แบบไดนามิก
   - D. การยืนยันตัวตนหลายปัจจัยโดยใช้กุญแจฮาร์ดแวร์

3. **3. อะไรแสดงถึงข้อมูลที่กำลังส่งผ่านเครือข่าย?**
   - A. แพ็กเก็ตข้อมูลที่เคลื่อนที่ผ่านเราเตอร์และสวิตช์ของเครือข่าย
   - B. ล็อกธุรกรรมฐานข้อมูลที่เก็บไว้บนไดรฟ์สำรองแบบออฟไลน์
   - C. ไฟล์ผู้ใช้ที่เก็บถาวรไว้ในห้องนิรภัยคลาวด์ที่แยกต่างหาก
   - D. ไฟล์กำหนดค่าระบบแบบสแตติกบนที่เก็บข้อมูลของเดสก์ท็อปภายใน

4. **4. เหตุใดการสำรองข้อมูลแบบออฟไลน์เป็นประจำจึงสำคัญต่อการป้องกันแรนซัมแวร์?**
   - A. ให้สำเนาที่สะอาดแบบออฟไลน์เพื่อกู้คืนไฟล์โดยไม่ต้องจ่ายค่าไถ่
   - B. ป้องกันแฮกเกอร์สแกนการกำหนดค่าพอร์ตที่เปิดอยู่
   - C. เพิ่มความเร็วแบนด์วิดท์การส่งข้อมูลของเครือข่ายภายใน
   - D. ทำให้บันทึกการยินยอมคุกกี้บนเบราว์เซอร์เป็นอัตโนมัติ

5. **5. การโทเคนไนซ์ข้อมูลทำอะไร?**
   - A. แทนที่หมายเลขบัตรที่ละเอียดอ่อนด้วยโทเค็นสุ่มที่ไม่ละเอียดอ่อน
   - B. ส่งทราฟฟิกเว็บผ่านโหนด onion ที่ปลอดภัยหลายโหนด
   - C. สแกนไดเรกทอรีของระบบเพื่อหามัลแวร์ตามลายเซ็น
   - D. ตรวจสอบเวลาเซสชันการเข้าสู่ระบบของผู้ดูแลฐานข้อมูล

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. การปกปิดข้อมูล (data masking) เปลี่ยนระเบียนฐานข้อมูลถาวรบนสภาพแวดล้อมใช้งานจริง

○ จริง ○ เท็จ

7 คำถาม 7

7. ต้องแยกการสำรองข้อมูลนอกสถานที่ออกจากเครือข่ายหลักขององค์กรเพื่อป้องกันแรนซัมแวร์แพร่กระจาย

○ จริง ○ เท็จ

8 คำถาม 8

8. ใบรับรอง SSL/TLS รักษาความปลอดภัยฐานข้อมูลโดยเข้ารหัสข้อมูลที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลจริง

○ จริง ○ เท็จ

9 คำถาม 9

9. Zero-trust network access (ZTNA) ตรวจสอบตัวตนของผู้ใช้ทุกคนก่อนอนุญาตให้เข้าถึงฐานข้อมูล

○ จริง ○ เท็จ

10 คำถาม 10

10. การทำโทเคนไนเซชันแบบใช้ห้องนิรภัย (vault) เก็บค่าบัตรดั้งเดิมไว้ในห้องนิรภัยโทเคนส่วนกลางที่ปลอดภัย

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การแทนชื่อบุคคลด้วยตัวแทนที่สมจริงเรียกว่าการ _____ ข้อมูล
2. การเข้ารหัสระดับบล็อกบนดิสก์จริงปกป้องสินทรัพย์ฐานข้อมูลขณะ _____
3. โพรโทคอล TLS เข้ารหัสแพ็กเก็ตข้อมูลที่ใช้งานอยู่ขณะ _____
4. สิทธิ์ตามบทบาทจำกัดว่าผู้ใช้คนใดจะได้รับ _____ ฐานข้อมูล
5. การกู้คืนไฟล์องค์กรที่สะอาดหลังเกิดการละเมิดต้องมีการ _____ ข้อมูลแบบออฟไลน์ที่ปลอดภัย
6. การตรวจสอบการกำหนดค่าคลาวด์ประเมิน _____ ด้านความปลอดภัยขององค์กร

คลังคำศัพท์

การเข้าถึง | การละเมิด | จัดเก็บ | ปิดบัง | ลดข้อมูล | ส่งผ่าน | สถานะ | สำรอง

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

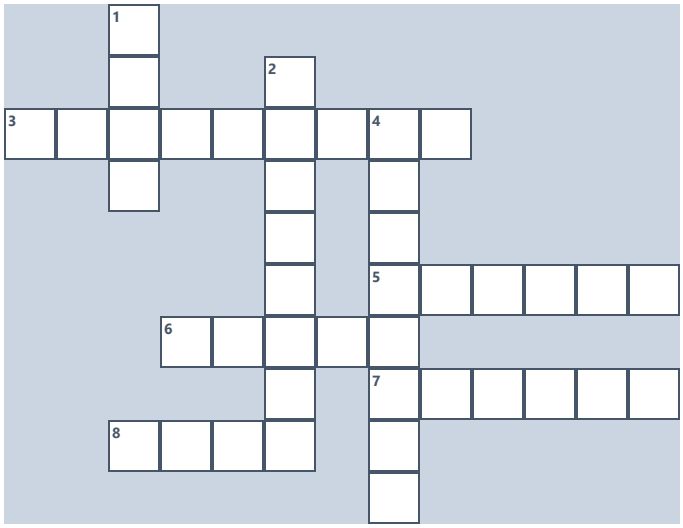
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. การเข้ารหัส**	**A**	การสร้างสำเนาข้อมูลที่ปลอดภัยนอกสถานที่เพื่อกู้คืนในกรณีที่ระบบล้มเหลว
☐	**2. การสำรองข้อมูล**	**B**	การแปลงข้อความธรรมดาให้เป็นข้อความเข้ารหัสที่อ่านไม่ออก เพื่อให้ข้อมูลที่ถูกดักจับยังคงเป็นความลับ
☐	**3. การลดข้อมูลให้น้อยที่สุด**	**C**	สถานะความปลอดภัยโดยรวมและความพร้อมในการป้องกันของคลาวด์ขององค์กร
☐	**4. การเข้าถึง**	**D**	การปฏิบัติตามมาตรฐานด้านกฎระเบียบ เช่น GDPR หรือ CCPA ในการจัดการข้อมูลส่วนตัวของผู้ใช้
☐	**5. สถานะความปลอดภัย**	**E**	เหตุการณ์ด้านความปลอดภัยที่ข้อมูลที่ได้รับการปกป้องถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต
☐	**6. การละเมิดข้อมูล**	**F**	การจำกัดสิทธิ์อ่านและเขียนฐานข้อมูลให้เฉพาะบทบาทผู้ใช้ที่ผ่านการยืนยันตัวตน
☐	**7. การปฏิบัติตามข้อกำหนด**	**G**	การแทนที่อักขระที่ละเอียดอ่อนในฟิลด์ฐานข้อมูลเพื่อปกป้องตัวตนส่วนบุคคล
☐	**8. การปกปิด**	**H**	การจำกัดการเก็บข้อมูลส่วนบุคคลให้เหลือน้อยที่สุดเท่าที่จำเป็นต่อการดำเนินงาน

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

3. การปฏิบัติตามมาตรฐานทางกฎระเบียบ เช่น GDPR หรือ CCPA ในการจัดการข้อมูลส่วนตัวของผู้ใช้ (9)

5. การจำกัดการเก็บข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นต่อการดำเนินงาน (6)

6. สถานะความปลอดภัยโดยรวมและความพร้อมในการป้องกันของคลาวด์ขององค์กร (5)

7. การแปลงข้อความธรรมดาเป็นข้อความเข้ารหัสที่อ่านไม่ได้ เพื่อให้ข้อมูลที่ถูกดักไว้ยังเป็นส่วนตัว (6)

8. การสร้างสำเนาข้อมูลนอกสถานที่อย่างปลอดภัยเพื่อกู้คืนเมื่อระบบล้มเหลว (4)

แนวตั้ง

1. การแทนที่อักขระที่ละเอียดอ่อนในช่องฐานข้อมูลเพื่อปกป้องตัวตนของบุคคล (4)

2. การจำกัดสิทธิ์อ่านและเขียนฐานข้อมูลให้เฉพาะบทบาทผู้ใช้ที่ผ่านการยืนยันตัวตน (8)

4. เหตุการณ์ความปลอดภัยที่มีการเข้าถึงหรือเปิดเผยข้อมูลที่ได้รับการปกป้องโดยไม่ได้รับอนุญาต (8)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

3 แนวนอน: การปฏิบัติตามมาตรฐานทางกฎระเบียบ เช่น GDPR หรือ CCPA ในการจัดการข้อมูลส่วนตัวของผู้ใช้ (9 ตัวอักษร):

5 แนวนอน: การจำกัดการเก็บข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นต่อการดำเนินงาน (6 ตัวอักษร):

6 แนวนอน: สถานะความปลอดภัยโดยรวมและความพร้อมในการป้องกันของคลาวด์ขององค์กร (5 ตัวอักษร):

7 แนวนอน: การแปลงข้อความธรรมดาเป็นข้อความเข้ารหัสที่อ่านไม่ได้ เพื่อให้ข้อมูลที่ถูกดักไว้ยังเป็นส่วนตัว (6 ตัวอักษร):

8 แนวนอน: การสร้างสำเนาข้อมูลนอกสถานที่อย่างปลอดภัยเพื่อกู้คืนเมื่อระบบล้มเหลว (4 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: การแทนที่อักขระที่ละเอียดอ่อนในช่องฐานข้อมูลเพื่อปกป้องตัวตนของบุคคล (4 ตัวอักษร):

2 แนวตั้ง: การจำกัดสิทธิ์อ่านและเขียนฐานข้อมูลให้เฉพาะบทบาทผู้ใช้ที่ผ่านการยืนยันตัวตน (8 ตัวอักษร):

4 แนวตั้ง: เหตุการณ์ความปลอดภัยที่มีการเข้าถึงหรือเปิดเผยข้อมูลที่ได้รับการปกป้องโดยไม่ได้รับอนุญาต (8 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า นี า น นี ส ช มี ฟ บ า า ห นี า
ม ก จ า า รี ต ว เ ย ส ง ก ค จ
น ต ง ว ร ต ว า ล ข้ ถ ล ด า อ
ย ช อ ล มู อ ข้ ด ล ฟ า ก ก ล ม
ด า ร ป อ ป อ ม มี า น ร ล ล ป
มิ จ สำ า นี ฏิ ก ี ก พ ร ะ ง ห้ า ช
เ า า ลี จ บั ด ี า า น ล ผ ด ี ส ช
ะ ก ด า ต ติ า จ า ร ค ก ด ี า ช
ล ว ก ด ก ี ต ด ท ผ ฟ เ ช มี ม อ
ร ต ฟ ร ด ี า า ท า ส ท ข้ ข ข า
า น ก า ล ม า ม ร มี ง า า ร ช
ก ก ด ง น ก ร ต ส ี บั ย ข มี ถ ึ ด ี
ด ด ว บ ฟ ฏ อ า ด ร ห ห ร ี น ง
ผ นี ม ผ ด ี ข ก ี ป ี ส บ ล ี ง ด ร ด
ค ผ ห ด ี ป ร ก ี นี า ต จ ห ด ี ด บ

รายการคำศัพท์

เข้ารหัส | สำรอง | ลดข้อมูล | การเข้าถึง | สถานะ | การละเมิด | ปฏิบัติตามกฎ | ปิดบัง

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. เข้ารหัส

B. สำรอง

C. ลดข้อมูล

D. การเข้าถึง

E. สถานะ

F. การละเมิด

G. ปฏิบัติตามกฎ

H. ปิดบัง

คำนิยามและช่องจับคู่

1. เหตุการณ์ความปลอดภัยที่มีการเข้าถึงหรือเปิดเผยข้อมูลที่ได้รับการปกป้องโดยไม่ได้รับอนุญาต

2. การแทนที่อักขระที่ละเอียดอ่อนในช่องฐานข้อมูลเพื่อปกป้องตัวตนของบุคคล

3. การจำกัดสิทธิ์อ่านและเขียนฐานข้อมูลให้เฉพาะบทบาทผู้ใช้ที่ผ่านการยืนยันตัวตน

4. สถานะความปลอดภัยโดยรวมและความพร้อมในการป้องกันของคลาวด์ขององค์กร

5. การปฏิบัติตามมาตรฐานทางกฎระเบียบ เช่น GDPR หรือ CCPA ในการจัดการข้อมูลส่วนตัวของผู้ใช้

6. การจำกัดการเก็บข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นต่อการดำเนินงาน

7. การแปลงข้อความธรรมดาเป็นข้อความเข้ารหัสที่อ่านไม่ได้ เพื่อให้ข้อมูลที่ถูกดักไว้ยังเป็นส่วนตัว

8. การสร้างสำเนาข้อมูลนอกสถานที่อย่างปลอดภัยเพื่อกู้คืนเมื่อระบบล้มเหลว

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. า เ ร ห ั ส ข้
2. ล ล ข้ ม ู อ ด
3. า ส ะ น ถ
4. ต ฎ ก ต ิ ม า ป ฏ ิ บ ั
5. ง ส ำ อ ร
6. ถ ึ ง เ า ก ข้ า ร
7. ก ด ะ เ ม ิ า ล ร
8. ป ิ ง บ ั ด

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สิ่งที่คุณสำรองข้อมูล			
2	คำที่เกี่ยวข้องกับความปลอดภัยไซเบอร์			
3	บุคคลที่ได้รับอนุญาตให้เห็นข้อมูลที่ละเอียดอ่อน			
4	วิธีลบข้อมูลอย่างปลอดภัย			
5	สถานที่ที่จัดเก็บข้อมูล			
6	สิ่งที่ควรเข้ารหัส			
7	ข้อมูลที่โรงพยาบาลต้องปกป้อง			
8	ประเภทของการสำรองข้อมูล			
9	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
10	สัญญาณเตือนในอีเมล			
11	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
12	บุคคลที่คุณขอความช่วยเหลือด้าน IT ได้			
13	อุปกรณ์ที่ถูกแฮกได้			
14	วิธีปกป้องข้อมูล			
15	สิ่งที่ทำลายข้อมูลได้			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การอัปเกรดการเข้ารหัสฐานข้อมูลองค์กรขณะจัดเก็บ



สถานการณ์: ร้านค้าปลีกออนไลน์จัดเก็บฐานข้อมูลธุรกรรมบนที่เก็บข้อมูลคลาวด์โดยไม่มีการเข้ารหัสดิสก์ทั้งหมด การตรวจสอบการปฏิบัติตามข้อกำหนดล่าสุดระบุว่านี่เป็นความเสี่ยงด้านความปลอดภัยของข้อมูลตาม CCPA ที่ร้ายแรง จงออกแบบสถาปัตยกรรมการกู้คืน

คำถามอภิปราย: จงวิเคราะห์ความเสี่ยงด้านการปฏิบัติตาม CCPA และเสนอกลยุทธ์การเข้ารหัสข้อมูลที่จัดเก็บอยู่ (at-rest)

กรณีศึกษาที่ 2: การจำกัดแรนซัมแวร์และการกู้คืนข้อมูล



สถานการณ์: การโจมตีด้วยแรนซัมแวร์ที่กำลังดำเนินอยู่กำลังเข้ารหัสไดรฟ์เครือข่ายบนเครือข่ายภายในขององค์กร ผู้ดูแลระบบตรวจพบการติดเชื้อตั้งแต่เนิ่น ๆ จงวางแผนขั้นตอนการจำกัดวงและการกู้คืน

คำถามอภิปราย: จงอธิบายการดำเนินการจำกัดวงทันทีโดยละเอียด และวางแผนกระบวนการกู้คืนอย่างปลอดภัย

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

27	1	27	64	45	7		2	64	45	33	56	37		42	63	39	25	21	48	39

20	64	39	34		1	49	35		4	39	26	4	55	33

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: การคุ้มครองข้อมูลคืออะไร?

คือกระบวนการปกป้องข้อมูลส่วนบุคคลและธุรกิจจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือความเสียหายผ่านมาตรการควบคุมทางเทคนิค

Q2: เหตุใดการเข้ารหัสทั้งดิสก์จึงสำคัญ?

รักษาความปลอดภัยบล็อกข้อมูลที่จัดเก็บบนไดรฟ์จริง ป้องกันไม่ให้ใครอ่านข้อมูลได้หากขโมยฮาร์ดไดรฟ์ไป

Q3: การเข้ารหัสข้อมูลที่จัดเก็บ (at rest) และข้อมูลที่กำลังส่ง (in transit) ต่างกันอย่างไร?

การเข้ารหัสข้อมูลที่จัดเก็บปกป้องไฟล์ที่เก็บในไดรฟ์ ส่วนการเข้ารหัสข้อมูลระหว่างส่งปกป้องแพ็กเก็ตเครือข่ายที่กำลังเคลื่อนที่ผ่านเราเตอร์

Q4: การปกปิดข้อมูล (data masking) คืออะไร?

แทนที่รายละเอียดที่ละเอียดอ่อน (เช่น เลขบัตรเครดิต) ด้วยข้อมูลสมมติที่สมจริงเพื่อใช้ทดสอบโดยไม่เปิดเผยบันทึกจริง

Q5: ทำไมการสำรองข้อมูลแบบออฟไลน์จึงสำคัญ?

เก็บสำเนาไฟล์ที่สะอาดไว้แยกจากเครือข่าย ซึ่งช่วยปกป้องข้อมูลสำรองของคุณไม่ให้ถูกแรนซัมแวร์เข้ารหัส

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: ห้องนิรภัยโทเค็นข้อมูล (data tokenization vault) คืออะไร?

ฐานข้อมูลที่ปลอดภัยและแยกต่างหากซึ่งแมปโทเค็นสุ่มกับค่าที่ละเอียดอ่อนดั้งเดิม (เช่น หมายเลขบัตรเครดิตหลัก)

Q7: การเข้าถึงฐานข้อมูลแบบ zero-trust หมายความว่าอะไร?

หมายถึงการตรวจสอบตัวตนของผู้ใช้ทุกคนและสถานะอุปกรณ์ทุกครั้งที่เข้าสู่ระบบ แทนการไว้วางใจผู้ใดภายในเครือข่าย

Q8: TLS ปกป้องข้อมูลขณะส่งผ่านอย่างไร?

TLS เข้ารหัสเพย์โหลดของเซสชัน TCP ป้องกันผู้ไม่หวังดีบนเครือข่ายสาธารณะจากการดักฟังหรือแก้ไขแพ็กเก็ตที่ส่งผ่าน

Q9: การตรวจสอบการเข้าถึงฐานข้อมูลคืออะไร?

การบันทึกการสืบค้นฐานข้อมูลและการเข้าสู่ระบบอย่างต่อเนื่อง เพื่อตรวจจับรูปแบบการเข้าถึงโดยไม่ได้รับอนุญาตหรือความผิดปกติด้านความปลอดภัย

Q10: การตรวจสอบสถานะความปลอดภัยของคลาวด์คืออะไร?

กระบวนการวิเคราะห์การกำหนดค่าบนคลาวด์เพื่อระบุพอร์ตที่เปิดอยู่ กฎการเข้าถึงที่ตั้งค่าผิด และช่องว่างด้านการปฏิบัติตามข้อกำหนดด้านความปลอดภัย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: envelope encryption ทำงานอย่างไร?

เข้ารหัสข้อมูลด้วยคีย์ข้อมูล แล้วเข้ารหัสคีย์ข้อมูลนั้นด้วยมาสเตอร์คีย์ ทำให้การจัดเก็บและการหมุนเวียนคีย์ง่ายขึ้น

Q2: homomorphic encryption คืออะไร?

วิธีการเข้ารหัสขั้นสูงที่ช่วยให้ดำเนินการกับข้อมูลที่เข้ารหัสได้โดยตรงโดยไม่ต้องถอดรหัสก่อน

Q3: เหตุใดจึงมีการเข้ารหัสระดับคอลัมน์ของฐานข้อมูล?

เข้ารหัสคอลัมน์ที่ละเอียดอ่อนบางคอลัมน์ (เช่น เลขบัตรประชาชน) แยกกัน เพื่อปกป้องแม้ผู้ดูแลระบบได้สิทธิ์อ่านตารางทั่วไป

Q4: การป้องกันข้อมูลสูญหาย (DLP) คืออะไร?

ซอฟต์แวร์ที่ตรวจสอบจุดออกของเครือข่ายเพื่อตรวจจับและบล็อกการถ่ายโอนไฟล์ที่ละเอียดอ่อนออกไปโดยไม่ได้รับอนุญาต

Q5: การสำรองข้อมูลแบบเขียนครั้งเดียวอ่านได้หลายครั้ง (WORM) ป้องกันแรนซัมแวร์ได้อย่างไร?

การสำรองข้อมูลแบบ WORM ป้องกันไม่ให้ไฟล์ถูกลบหรือแก้ไขตลอดระยะเวลาที่กำหนด ซึ่งช่วยหยุดแรนซัมแวร์ไม่ให้เข้ารหัสข้อมูลสำรองที่มีอยู่

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การใช้คีย์ซ้ำมีความเสี่ยงอะไร?

การใช้คีย์เข้ารหัสเดียวกันซ้ำข้ามฐานข้อมูลต่างๆ หมายความว่าหากคีย์ถูกบุกรุกเพียงครั้งเดียว ฐานข้อมูลทั้งหมดจะถูกเปิดเผย

Q7: การทำโทเค็นข้อมูลฐานข้อมูล (database tokenization) ช่วยการปฏิบัติตาม CCPA ได้อย่างไร?

โทเค็นช่วยแทนชื่อจริงด้วยนามแฝงในระเบียนบนระบบที่ไม่ใช่ระบบใช้งานจริง และจำกัดความเสี่ยงเมื่อข้อมูลรั่วไหล แต่ข้อมูลที่ผ่านการโทเค็นอาจยังเป็นข้อมูลส่วนบุคคล

Q8: ทำไมการจัดประเภทข้อมูลจึงสำคัญยิ่ง?

จัดหมวดหมู่ไฟล์ตามระดับความอ่อนไหว ช่วยให้องค์กรใช้การเข้ารหัสและการควบคุมการเข้าถึงที่เข้มงวดที่สุดกับข้อมูลความเสี่ยงสูง

Q9: การหมุนเวียนคีย์ (key rotation) มีบทบาทอะไร?

การอัปเดตคีย์เข้ารหัสสม่ำเสมอจำกัดปริมาณข้อมูลในอดีตที่ถูกเปิดเผยหากคีย์ใดคีย์หนึ่งถูกถอดรหัสได้ในภายหลัง

Q10: secure enclave ปกป้องคิวรีฐานข้อมูลในหน่วยความจำได้อย่างไร?

Secure enclave แยกการทำงานของคำค้นไว้ในบล็อกหน่วยความจำที่ CPU ปกป้อง ป้องกันไม่ให้ผู้ดูแลโฮสต์เห็นข้อความที่ไม่ได้เข้ารหัสใน RAM

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

กฎระเบียบ GDPR มีผลบังคับใช้ในเดือนพฤษภาคม 2018 ซึ่งเปลี่ยนวิธีที่เว็บไซต์ทั่วโลกจัดการความยินยอมเรื่องคุกกี้และทะเบียนข้อมูลส่วนบุคคล

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ค่าปรับจากการละเมิด GDPR อาจสูงถึง 20 ล้านยูโรหรือ 4% ของรายได้ทั่วโลก ซึ่งเป็นความเสี่ยงทางกฎหมายที่มาก [4]

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

CCPA มีผลบังคับใช้ในเดือนมกราคม 2020 สร้างสิทธิของผู้บริโภคด้านความเป็นส่วนตัวทางดิจิทัลที่เป็นต้นแบบในสหรัฐอเมริกา

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การใช้ข้อมูลให้น้อยที่สุดช่วยลดพื้นที่จัดเก็บฐานข้อมูล ลดต้นทุนการดำเนินงานของเซิร์ฟเวอร์ และลดผลกระทบเมื่อเกิดข้อมูลรั่วไหล

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การทำลายข้อมูลด้วยการเข้ารหัสแก้ปัญหาการลบข้อมูลสำรองโดยล้างกุญแจแทนการแก้ไขไฟล์เทปสำรองในอดีต

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ปัจจุบันประเทศส่วนใหญ่ทั่วโลกประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อปกป้องสิทธิความเป็นส่วนตัวของผู้บริโภค

7. ข้อมูลเชิงลึกด้านความปลอดภัย

แบบฟอร์มขอความยินยอมแบบเลือกเข้าร่วมที่ติ๊กช่องไว้ล่วงหน้าถูกห้ามอย่างชัดเจนตามนิยามของข้อบังคับความเป็นส่วนตัวของข้อมูลในยุโรป

8. ข้อมูลเชิงลึกด้านความปลอดภัย

GDPR กำหนดให้รายงานการละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานกำกับดูแลภายใน 72 ชั่วโมงนับจากที่ทราบเหตุ หากสามารถทำได้ [3]

9. ข้อมูลเชิงลึกด้านความปลอดภัย

การแฮชรหัสผ่านด้วยอัลกอริทึมที่ช้าอย่าง bcrypt หรือ Argon2 ทำให้การแคร็กแฮชที่ถูกขโมยแบบออฟไลน์ยากขึ้นมาก [6]

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ข้อมูลที่จัดเก็บ (data at rest) คือไฟล์ฐานข้อมูลที่บันทึกไว้ ส่วนข้อมูลระหว่างส่ง (data in transit) คือแพ็กเก็ตที่กำลังเคลื่อนที่ผ่านเราเตอร์ในเครือข่าย

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

วัตถุประสงค์หลักของการปกปิดข้อมูล (data masking) คืออะไร? → การแทนที่ตัวระบุที่ละเอียดอ่อนด้วยอักขระสมมติแต่สมจริงเพื่อปกป้องความเป็นส่วนตัว

2 คำถาม 2 คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

กลไกใดที่เข้ารหัสไฟล์ที่เก็บอยู่ในฮาร์ดไดรฟ์ของเซิร์ฟเวอร์ฐานข้อมูล? → การเข้ารหัสทั้งดิสก์ขณะจัดเก็บ

3 คำถาม 3 คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

อะไรแสดงถึงข้อมูลที่กำลังส่งผ่านเครือข่าย? → แพ็กเก็ตข้อมูลที่เคลื่อนที่ผ่านเราเตอร์และสวิตช์ของเครือข่าย

4 คำถาม 4 คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

เหตุใดการสำรองข้อมูลแบบออฟไลน์เป็นประจำจึงสำคัญต่อการป้องกันแรนซัมแวร์? → ให้สำเนาที่สะอาดแบบออฟไลน์เพื่อกู้คืนไฟล์โดยไม่ต้องจ่ายค่าไถ่

5 คำถาม 5 คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การโทเคนไนซ์ข้อมูลทำอะไร? → แทนที่หมายเลขบัตรที่ละเอียดอ่อนด้วยโทเค็นสุ่มที่ไม่ละเอียดอ่อน

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

การปิดบังข้อมูล (masking) เปลี่ยนแปลงสำเนาทดสอบหรือซ่อนค่าขณะสืบค้น ส่วนระเบียนจริงในระบบใช้งานจะไม่เปลี่ยนแปลง

7 **คำถาม 7** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

ต้องแยกการสำรองข้อมูลนอกสถานที่ออกจากเครือข่ายหลักขององค์กรเพื่อป้องกันแรนซัมแวร์แพร่กระจาย

8 **คำถาม 8** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

ใบรับรอง TLS ปกป้องข้อมูลระหว่างการส่ง ส่วนข้อมูลที่จัดเก็บอยู่ต้องใช้การเข้ารหัสดิสก์ ไฟล์ หรือฐานข้อมูล

9 **คำถาม 9** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

Zero-trust network access (ZTNA) ตรวจสอบตัวตนของผู้ใช้ทุกคนก่อนอนุญาตให้เข้าถึงฐานข้อมูล

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การทำโทเคนไนเซชันแบบใช้ห้องนิรภัยเก็บค่าดั้งเดิมไว้ในห้องนิรภัยโทเคนที่ปลอดภัย ซึ่งจับคู่แต่ละโทเคนกลับไปยังข้อมูลของมัน

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

B 1. การเข้ารหัส	A 2. การสำรองข้อมูล	H 3. การลดข้อมูลให้น้อยที่สุด	F 4. การเข้าถึง
C 5. สถานะความปลอดภัย	E 6. การละเมิดข้อมูล	D 7. การปฏิบัติตามข้อกำหนด	G 8. การปกปิด

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ปิดบัง	2 จัดเก็บ	3 ส่งผ่าน	4 การเข้าถึง
5 สำรอง	6 สถานะ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 F – การละเมิด	2 H – ปิดบัง	3 D – การเข้าถึง	4 E – สถานะ
5 G – ปฏิบัติตามกฎ	6 C – ลดข้อมูล	7 A – เข้ารหัส	8 B – สำรอง

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย การเข้ารหัส การสำรองข้อมูล และ การลดข้อมูลให้น้อยที่สุด ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	นี	า	น	นี	ส	ช	มี	ฟ	บ	า	า	ห	นี	า
ม	กี	จ	า	า	รี	ต	ว	เ	ย	ส	ง	ก	ค	จ
น	ตี	ง	ว	ร	ตี	ว	า	ล	ข้	ถ	ล	ด	า	อ
ย	ช	อ	ล	มู	อ	ข้	ด	ล	ฟ	า	ก	ก	ล	ม
ด	า	ร	ป	อ	ป	อ	ม	มี	า	น	ร	ล	ล	ป
มิ	จ	สำ	า	นี	ฏิ	กี	ก	พ	ร	ะ	ง	ห้	า	ช
เ	า	า	ลี	จ	บั	ตี	า	า	น	ล	ผ	ดี	ส	ช
ะ	ก	ด	า	ต	ติ	า	จ	า	ร	ค	ก	ดี	า	ช
ล	ว	ก	ด	กี	ต	ด	ท	ผ	ฟ	เ	ช	มี	ม	อ
ร	ต	ฟ	ร	ดี	า	า	ท	า	ส	ท	ข้	ข	ข	า
า	น	ก	า	ล	ม	า	ม	ร	มี	ง	า	า	ร	ช
ก	ก	ด	ง	น	ก	ร	ต	สี	บั	ย	ข	มี	ถี	ดี
ด	ด	ว	บ	ฟ	ฎ	อ	า	ด	ร	ห	ห	รี	น	ง
ผ	นี	ม	ผ	ดี	ข	กี	ปิ	ส	บ	ลี	ง	ด	ร	ด
ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด	บ

เฉลยปริศนาอักษรไขว้

		ปิ												
		ด			ก									
ป	ฏิ	บั	ติ	ต	า	ม	ก	ฎ						
		ง			ร		า							
					เ		ร							
					ข้		ล	ด	ข้	อ	มู	ล		
			ส	ถ	า	น	ะ							
					ถี		เ	ข้	า	ร	ห้	ส		
		สำ	ร	อ	ง		มิ							
							ด							

คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

3 แนวนอน: ปฏิบัติตามกฎ การปฏิบัติตามมาตรฐานทางกฎระเบียบ เช่น GDPR หรือ CCPA ในการจัดการข้อมูลส่วนตัวของผู้ใช้ (9 ตัวอักษร)

5 แนวนอน: ลดข้อมูล การจำกัดการเก็บข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นต่อการดำเนินงาน (6 ตัวอักษร)

6 แนวนอน: สถานะ สถานะความปลอดภัยโดยรวมและความพร้อมในการป้องกันของคลาวด์ขององค์กร (5 ตัวอักษร)

7 แนวนอน: เข้ารหัส การแปลงข้อความธรรมดาเป็นข้อความเข้ารหัสที่อ่านไม่ได้ เพื่อให้ข้อมูลที่ถูกดักไว้ยังเป็นส่วนตัว (6 ตัวอักษร)

8 แนวนอน: สำรอง การสร้างสำเนาข้อมูลนอกสถานที่อย่างปลอดภัยเพื่อกู้คืนเมื่อระบบล้มเหลว (4 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: ปิดบัง การแทนที่อักขระที่ละเอียดอ่อนในช่องฐานข้อมูลเพื่อปกป้องตัวตนของบุคคล (4 ตัวอักษร)

2 แนวตั้ง: การเข้าถึง การจำกัดสิทธิ์อ่านและเขียนฐานข้อมูลให้เฉพาะบทบาทผู้ใช้ที่ผ่านการยืนยันตัวตน (8 ตัวอักษร)

4 แนวตั้ง: การละเมิด เหตุการณ์ความปลอดภัยที่มีการเข้าถึงหรือเปิดเผยข้อมูลที่ได้รับการปกป้องโดยไม่ได้รับอนุญาต (8 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. าเรหัสข้ — เข้ารหัส
2. ลลข้มูอด — ลดข้อมูล
3. าสะนถ — สถานะ
4. ตฎกติมาปฏิบั — ปฏิบัติตามกฎ
5. งสำอร — สำรอง
6. ถึงเากข้าร — การเข้าถึง
7. กดะเมิาลร — การละเมิด
8. ปิงบัด — ปิดบัง

เฉลยภารกิจรหัสลับ

"ปกป้อง ข้อมูล ส่วนตัว ด้วย การ ควบคุม"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การอัปเกรดการเข้ารหัสฐานข้อมูลองค์กรขณะจัดเก็บ

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ร้านค้าปลีกออนไลน์เก็บฐานข้อมูลธุรกรรมบนที่เก็บข้อมูลคลาวด์โดยไม่มีการเข้ารหัสทั้งดิสก์ การตรวจสอบการปฏิบัติตามข้อกำหนดล่าสุดระบุว่านี่เป็นความเสี่ยงด้านความปลอดภัยของข้อมูลตาม CCPA ที่ร้ายแรง จงออกแบบสถาปัตยกรรมการกู้คืน
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ใช้การเข้ารหัสดิสก์ทั้งหมดแบบ AES-256 ขณะจัดเก็บบนระบบไฟล์ทั้งหมด ใช้บริการจัดการคีย์ (KMS) แบบรวมศูนย์ที่หมุนเวียนคีย์อัตโนมัติ และบังคับใช้นโยบาย IAM อย่างเข้มงวดเพื่อควบคุมสิทธิ์การถอดรหัส

B กรณีศึกษาที่ 2: การจำกัดแรนซัมแวร์และการกู้คืนข้อมูล

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: การโจมตีด้วยแรนซัมแวร์ที่กำลังเกิดขึ้นเข้ารหัสไดรฟ์เครือข่ายบนเครือข่ายท้องถิ่นขององค์กร ผู้ดูแลระบบตรวจพบการติดเชื้อตั้งแต่เนิ่นๆ จงวางแผนขั้นตอนการจำกัดวงความเสียหายและการกู้คืน
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: แยกเซกเมนต์ที่ถูกบุกรุกออกทันที ฟอร์แมตอุปกรณ์ปลายทางที่ได้รับผลกระทบและกู้คืนจากข้อมูลสำรองออฟไลน์แบบเขียนครั้งเดียวอ่านได้หลายครั้ง (WORM) ล่าสุด ตรวจสอบความสมบูรณ์ของข้อมูลสำรองก่อนเชื่อมต่อระบบกลับ