ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

พื้นฐานความปลอดภัยไซเบอร์และภัยคุกคามออนไลน์ การป้องกัน

ภัยคุกคามด้านความปลอดภัยไซเบอร์ ไฟร์วอลล์เครือข่าย การยืนยันตัวตนหลายปัจจัย กรอบความปลอดภัย

ภาพรวมการเรียนรู้พื้นฐานความปลอดภัยไซเบอร์

ได้รับการรักษาความปลอดภัย

การเข้ารหัสข้อมูล

มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด

มาตรฐานสากล

กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์

นโยบายการเข้าถึง

การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับหลักการพื้นฐานของความปลอดภัยไซเบอร์เบื้องต้นและการป้องกันภัยคุกคามออนไลน์ คุณจะได้สำรวจภัยคุกคามจากมัลแวร์ การพิสูจน์ตัวตนหลายปัจจัย ไฟร์วอลล์เครือข่าย และกรอบการตอบสนองต่อเหตุการณ์

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/

เส้นทางการเรียนรู้พื้นฐานความปลอดภัยไซเบอร์ของคุณ

- ระบุช่องทางทั่วไปของมัลแวร์ ฟิชชิง และการบุกรุกเครือข่ายองค์กร
- ใช้มาตรการควบคุมความปลอดภัยไซเบอร์มาตรฐาน รวมถึง MFA ไฟร์วอลล์ และการป้องกันปลายทาง
- ประเมินขั้นตอนการตอบสนองต่อเหตุการณ์เพื่อบรรเทาผลกระทบจากข้อมูลรั่วไหล
- วิเคราะห์ปัจจัยเสี่ยงขององค์กรและการจัดแนวความปลอดภัยภายใต้แนวทางของ NIST
- ตั้งค่าแนวปฏิบัติด้านสุขอนามัยความปลอดภัยเพื่อลดการโจมตีแบบ Credential Stuffing อัตโนมัติ

คำแนะนำคู่มือความปลอดภัยไซเบอร์

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การป้องกันภัยคุกคาม ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

พื้นฐานความปลอดภัยไซเบอร์และการป้องกันภัยคุกคาม (บทนำ)

ความปลอดภัยไซเบอร์ปกป้องเครือข่าย ระบบ และข้อมูลจากการโจมตีทางดิจิทัลที่ไม่ได้รับอนุญาต การสร้างนิสัยด้านความปลอดภัยที่แข็งแกร่ง การตั้งค่าไฟร์วอลล์ การกำหนดให้ใช้การยืนยันตัวตนหลายปัจจัย และการฝึกอบรมพนักงานให้รู้จักภัยคุกคาม เป็นองค์ประกอบสำคัญของการป้องกันเครือข่ายองค์กร

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. 1. วัตถุประสงค์หลักของการโจมตีแบบฟิชชิงคืออะไร?
   - A. การขโมยข้อมูลรับรองและข้อมูลที่ละเอียดอ่อนของผู้ใช้
   - B. การเพิ่มการมองเห็นของเว็บไซต์บนเสิร์ชเอนจิน
   - C. เพิ่มแบนด์วิดท์ของเครือข่าย
   - D. การจัดการการทำสำเนาข้อมูลของศูนย์ข้อมูลสำรอง

2. 2. กลไกใดให้การปกป้องบัญชีที่แข็งแกร่งที่สุด?
   - A. การยืนยันตัวตนหลายปัจจัยโดยใช้คีย์ฮาร์ดแวร์
   - B. รหัสผ่านที่ซับซ้อนซึ่งเปลี่ยนทุกสามสิบวัน
   - C. จำกัดการเข้าสู่ระบบบัญชีให้อยู่ในเวลาทำการ
   - D. การซ่อนชื่อผู้ใช้บัญชีจากไดเรกทอรีสาธารณะ

3. 3. อะไรเป็นตัวกำหนดเพย์โหลดของการติดเชื้อแรนซัมแวร์?
   - A. การเข้ารหัสไฟล์ระบบและเรียกร้องค่าไถ่
   - B. การแอบบันทึกการกดแป้นพิมพ์ส่งไปยังเซิร์ฟเวอร์ระยะไกล
   - C. แทรกโฆษณาที่ไม่ได้รับอนุญาตลงในเบราว์เซอร์
   - D. การใช้ทรัพยากร CPU ในเครื่องเพื่อขุดคริปโตเคอร์เรนซี

4. 4. ช่องโหว่ซีโร่เดย์ส่งผลต่อระบบป้องกันความปลอดภัยอย่างไร?
   - A. มุ่งเป้าไปที่ช่องโหว่ที่ยังไม่ได้แพตช์และไม่เป็นที่รู้จัก
   - B. ปิดไฟร์วอลล์ขององค์กรโดยอัตโนมัติ
   - C. บังคับให้ระบบรีบูตแบบฮาร์ด
   - D. ไม่ต้องใช้งบประมาณในการแก้ไข

5. 5. กรอบงานใดกำกับการควบคุมความปลอดภัยขององค์กร?
   - A. แนวทางของ NIST Cybersecurity Framework
   - B. ข้อกำหนดสคีมาเอกสาร W3C HTML5
   - C. คู่มือการติดตั้งไดรเวอร์เครื่องพิมพ์
   - D. คำนิยามโปรโตคอลการกำหนดเส้นทางของ IETF

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถามจริง/เท็จ 6

6. การโจมตีแบบฟิชชิงมุ่งเป้าเฉพาะบัญชีอีเมลส่วนตัวเท่านั้น

○ จริง ○ เท็จ

7 คำถามจริง/เท็จ 7

7. การยืนยันตัวตนหลายปัจจัยช่วยบล็อกการโจมตีแบบ credential stuffing

○ จริง ○ เท็จ

8 คำถามจริง/เท็จ 8

8. ไฟร์วอลล์ตรวจสอบการรับส่งข้อมูลในเครือข่ายเพื่อบล็อกการเข้าถึงพอร์ตที่ไม่ได้รับอนุญาต

○ จริง ○ เท็จ

9 คำถามจริง/เท็จ 9

9. การแก้ไขการโจมตีซีโร่เดย์ต้องใช้การอัปเดตนิยามแอนตี้ไวรัสมาตรฐาน

○ จริง ○ เท็จ

10 คำถามจริง/เท็จ 10

10. Honeypot คือเซิร์ฟเวอร์ล่อที่ใช้ล่อให้อาชญากรไซเบอร์เข้ามา

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. ผู้ดูแลเครือข่ายติดตั้ง _____ เพื่อกรองทราฟฟิกขาเข้า
2. ผู้โจมตีใช้ _____ แบบซีโรเดย์เพื่อหลบแพตช์ของระบบ
3. ผู้โจมตีส่งอีเมลปลอมเพื่อทำแคมเปญ _____ ต่อพนักงาน
4. แรนซัมแวร์เป็น _____ ชนิดทำลายล้างที่ล็อกข้อมูลของผู้ใช้
5. การสร้าง _____ รหัสผ่านที่แข็งแกร่งลดความเสี่ยงการขโมยข้อมูลประจำตัว
6. เพื่อปกป้องการสื่อสารที่ละเอียดอ่อน ผู้ใช้ใช้โพรโทคอล _____

คลังคำศัพท์

กรอบงาน การเข้ารหัส ช่องโหว่ ฟิชชิง ไฟร์วอลล์ มัลแวร์ สุขอนามัย ฮันนีพอต

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

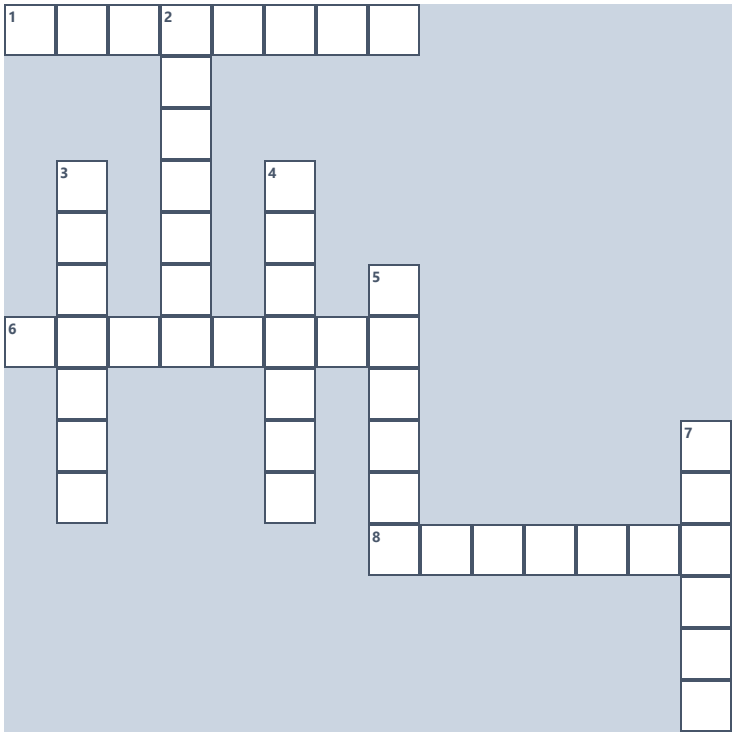
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. ภัยคุกคามแรนซัมแวร์**	**A**	แนวปฏิบัติที่เป็นระบบ เช่น NIST ที่ใช้จัดการความเสี่ยงทางไซเบอร์
☐	**2. การยืนยันตัวตนหลายปัจจัย**	**B**	แผนที่เป็นระบบสำหรับการจัดการและบรรเทาเหตุละเมิดความปลอดภัย
☐	**3. การโจมตีแบบซีโร่เดย์**	**C**	ตัวกั้นเครือข่ายที่กรองการรับส่งข้อมูลตามกฎความปลอดภัย
☐	**4. ฮันนีพอตล่อ**	**D**	มัลแวร์ที่เข้ารหัสข้อมูลและเรียกร้องเงินเพื่อถอดรหัส
☐	**5. ไฟร์วอลล์ป้องกันการบุกรุก**	**E**	การโจมตีช่องโหว่ที่เกิดขึ้นก่อนที่ผู้ผลิตจะปล่อยแพตช์
☐	**6. การรับมือเหตุการณ์**	**F**	แนวปฏิบัติที่ดีที่สุดในการจัดการข้อมูลรับรองและกุญแจยืนยันตัวตน
☐	**7. สุขอนามัยของรหัสผ่าน**	**G**	การตรวจสอบความปลอดภัยที่ต้องใช้ปัจจัยการยืนยันตัวตนตั้งแต่สองปัจจัยขึ้นไป
☐	**8. เฟรมเวิร์กความปลอดภัย**	**H**	ระบบล่อที่ตั้งขึ้นเพื่อล่อและวิเคราะห์ผู้ประสงค์ร้าย

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

1. มัลแวร์ที่เข้ารหัสข้อมูลและเรียกเงินเพื่อถอดรหัส (8)

6. การตรวจสอบความปลอดภัยที่ต้องใช้ปัจจัยยืนยันตัวตนตั้งแต่สองอย่างขึ้นไป (8)

8. แผนที่เป็นระบบสำหรับจัดการและบรรเทาการละเมิดความปลอดภัย (7)

แนวตั้ง

2. แนวทางที่มีโครงสร้าง เช่น NIST ที่ใช้จัดการความเสี่ยงไซเบอร์ (7)

3. แนวปฏิบัติที่ดีที่สุดในการจัดการข้อมูลประจำตัวและคีย์ยืนยันตัวตน (7)

4. เครื่องกั้นเครือข่ายที่กรองทราฟฟิกตามกฎความปลอดภัย (7)

5. ระบบล่อที่ตั้งขึ้นเพื่อล่อและวิเคราะห์ผู้ประสงค์ร้าย (6)

7. การโจมตีจุดอ่อนที่ยังไม่มีแพตช์จากผู้จำหน่าย (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

1 แนวนอน: มัลแวร์ที่เข้ารหัสข้อมูลและเรียกเงินเพื่อถอดรหัส (8 ตัวอักษร):

6 แนวนอน: การตรวจสอบความปลอดภัยที่ต้องใช้ปัจจัยยืนยันตัวตนตั้งแต่สองอย่างขึ้นไป (8 ตัวอักษร):

8 แนวนอน: แผนที่เป็นระบบสำหรับจัดการและบรรเทาการละเมิดความปลอดภัย (7 ตัวอักษร):

แนวตั้ง

2 แนวตั้ง: แนวทางที่มีโครงสร้าง เช่น NIST ที่ใช้จัดการความเสี่ยงไซเบอร์ (7 ตัวอักษร):

3 แนวตั้ง: แนวปฏิบัติที่ดีที่สุดในการจัดการข้อมูลประจำตัวและคีย์ยืนยันตัวตน (7 ตัวอักษร):

4 แนวตั้ง: เครื่องกั้นเครือข่ายที่กรองทราฟฟิกตามกฎความปลอดภัย (7 ตัวอักษร):

5 แนวตั้ง: ระบบล่อที่ตั้งขึ้นเพื่อล่อและวิเคราะห์ผู้ประสงค์ร้าย (6 ตัวอักษร):

7 แนวตั้ง: การโจมตีจุดอ่อนที่ยังไม่มีแพตช์จากผู้จำหน่าย (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า า รี ต ว ย ง ก ค จ น ตี ว ร ตี
ว า ล ล ด า อ ย ต ซ ฟ ก ก ล ม
า ป อ อ ม มี า ล ล อ ป จ า นี กี
พ ต น า ง บ อ ร ก ร บ ง า ซ า
า อ ลี จ ดี เ า น ล ผ ดี ส ซ สุ ก
ล์ พ ด า ต รี า ยื จ า ค ก น ข ดี
ล นี า ซ ว ย ก ด น กี ด ท ผ อ ฟ
อ น ซ มี ม ก อ ต ฟ ยั ร ดี า น ง
ว ฮั ท า ส ค่ ท ข ข า น น ก า า
ร์ ล า ม ร า ช่ มี า ร ช ตั ก มั ด
ฟ ง น ร ต ไ อ สี ย ข มี ดี ว ย ด
ไ ด ว บ ฟ ถ่ ง อ า ร ห ห รี ต น
ผ นี ม ผ ดี ข โ กี ส บ ลี ง ด ร น
ด ค ผ ห ดี ป ห ร กี นี า ต จ ห ดี
ด บ ตี น สี ลี ว่ ว ลี า ค า า ล ห

รายการคำศัพท์

เรียกค่าไถ่ | ยืนยันตัวตน | ช่องโหว่ | ฮันนีพอต | ไฟร์วอลล์ | ตอบสนอง | สุขอนามัย | กรอบงาน

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. เรียกค่าไถ่

B. ยืนยันตัวตน

C. ช่องโหว่

D. ฮันนีพอต

E. ไฟร์วอลล์

F. ตอบสนอง

G. สุขอนามัย

H. กรอบงาน

คำนิยามและช่องจับคู่

1. เครื่องกั้นเครือข่ายที่กรองทราฟฟิกตามกฎความปลอดภัย
2. แผนที่เป็นระบบสำหรับจัดการและบรรเทาการละเมิดความปลอดภัย
3. มัลแวร์ที่เข้ารหัสข้อมูลและเรียกเงินเพื่อถอดรหัส
4. การตรวจสอบความปลอดภัยที่ต้องใช้ปัจจัยยืนยันตัวตนตั้งแต่สองอย่างขึ้นไป
5. แนวปฏิบัติที่ดีที่สุดในการจัดการข้อมูลประจำตัวและคีย์ยืนยันตัวตน
6. แนวทางที่มีโครงสร้าง เช่น NIST ที่ใช้จัดการความเสี่ยงไซเบอร์
7. การโจมตีจุดอ่อนที่ยังไม่มีแพตช์จากผู้จำหน่าย
8. ระบบล่อที่ตั้งขึ้นเพื่อล่อและวิเคราะห์ผู้ประสงค์ร้าย

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ไ ก ค่ เ า รี ถ่ ย
2. ว่ ช ง ห โ อ
3. ว ไ อ ส์ ร์ ล ฟ
4. ย ข า น มั สุ อ
5. ต้ ว น น น ย ื ต ย้
6. อ พ ฮั นี ต น
7. ต อ น ง อ ส บ
8. ร บ น ก า ง อ

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	อาชีพในด้านความปลอดภัยไซเบอร์			
2	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
3	สิ่งที่ไฟร์วอลล์บล็อกได้			
4	สัญญาณเตือนในอีเมล			
5	สิ่งที่คุณสำรองข้อมูล			
6	การโจมตีทางไซเบอร์ประเภทที่รู้จักกันดี			
7	สิ่งที่ **honeypot** ล่อให้เข้ามาได้			
8	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
9	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
10	ภาพยนตร์หรือรายการเกี่ยวกับแฮกเกอร์			
11	ชั้นความปลอดภัยที่คุณสร้างได้			
12	สิ่งที่ควรฝึกซ้อมในการซ้อมรับมือด้านความปลอดภัย			
13	เครื่องมือด้านความปลอดภัยที่คุณรู้จัก			
14	บุคคลที่คุณขอความช่วยเหลือด้าน IT ได้			
15	คำที่ขึ้นต้นด้วย "ไซเบอร์"			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: กลยุทธ์กู้คืนจากแรนซัมแวร์



สถานการณ์: เครือข่ายองค์กรติดแรนซัมแวร์ ซึ่งล็อกฐานข้อมูลสำคัญ ผู้โจมตีเรียกร้องค่าไถ่เป็นสกุลเงินดิจิทัล $100,000 บริษัทมีข้อมูลสำรองออฟไลน์จาก 24 ชั่วโมงก่อน

คำถามอภิปราย: วิเคราะห์ความเสี่ยงของการจ่ายเงิน และประเมินกลยุทธ์การกู้คืน

กรณีศึกษาที่ 2: การป้องกัน Credential Stuffing



สถานการณ์: บริการออนไลน์ถูกโจมตีแบบ credential stuffing โดยแฮกเกอร์ทดสอบคู่ชื่อผู้ใช้/รหัสผ่านนับล้านคู่ที่ถูกขโมยจากเว็บไซต์อื่น

คำถามอภิปราย: จงอธิบายกลไกของการโจมตีนี้ และสรุประบบป้องกันสองระบบ

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		35	47	26	26		20	64	39	34		1	49	35

34	54	25	34	48	25	21	48	39	21	25

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: วัตถุประสงค์หลักของความปลอดภัยไซเบอร์คืออะไร?

วัตถุประสงค์หลักคือการปกป้องเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตี และความเสียหายโดยไม่ตั้งใจ

Q2: ฟิชชิงต่างจากสเปียร์ฟิชชิงอย่างไร?

ฟิชชิงเป็นแคมเปญอีเมลวงกว้างที่มุ่งเป้าผู้ใช้แบบสุ่ม ส่วนสเปียร์ฟิชชิงมุ่งเป้าบุคคลเฉพาะโดยใช้ข้อมูลที่ปรับให้เหมาะกับแต่ละคน

Q3: ไฟร์วอลล์เครือข่ายคืออะไร?

ไฟร์วอลล์คือระบบรักษาความปลอดภัยเครือข่ายที่ตรวจสอบและกรองทราฟฟิกขาเข้าและขาออกตามกฎความปลอดภัยที่กำหนดไว้ล่วงหน้า

Q4: ทำไมการยืนยันตัวตนแบบหลายปัจจัย (MFA) จึงจำเป็น?

MFA เพิ่มชั้นการป้องกันที่สำคัญ ช่วยป้องกันการเข้าถึงแม้ผู้โจมตีจะขโมยหรือถอดรหัสผ่านหลักได้

Q5: อะไรเป็นตัวกำหนดว่าเป็นไวรัสคอมพิวเตอร์?

ไวรัสคือมัลแวร์ที่ทำสำเนาตัวเองซึ่งแนบตัวกับไฟล์ปกติและแพร่กระจายข้ามระบบเมื่อถูกรัน

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: แรนซัมแวร์ล็อกข้อมูลในเครื่องอย่างไร?

แรนซัมแวร์ใช้อัลกอริทึมการเข้ารหัสเพื่อเข้ารหัสไฟล์ของผู้ใช้ ทำให้อ่านไม่ได้จนกว่าจะใช้คีย์ถอดรหัส

Q7: ช่องโหว่ซีโร่เดย์ (zero-day vulnerability) คืออะไร?

Zero-day คือช่องโหว่ด้านความปลอดภัยในซอฟต์แวร์ที่ผู้จำหน่ายไม่รู้จัก จึงไม่มีเวลาพัฒนาแพตช์ก่อนถูกโจมตี

Q8: กรอบงาน NIST มีบทบาทอะไร?

กรอบการทำงานของ NIST ให้แนวทางและมาตรฐานแบบสมัครใจเพื่อช่วยให้องค์กรจัดการและลดความเสี่ยงด้านความปลอดภัยไซเบอร์

Q9: แผนรับมือเหตุการณ์ด้านความปลอดภัยคืออะไร?

เป็นชุดขั้นตอนที่จัดทำเป็นเอกสารสำหรับตรวจจับ ควบคุม และกู้คืนจากการละเมิดความปลอดภัยและการบุกรุกเครือข่าย

Q10: วิศวกรรมสังคมใช้ประโยชน์จากผู้ใช้อย่างไร?

วิศวกรรมสังคมใช้การบงการทางจิตวิทยาเพื่อหลอกพนักงานให้เปิดเผยรหัสผ่านหรือดาวน์โหลดไฟล์อันตราย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: การโจมตี DDoS ทำให้เว็บเซิร์ฟเวอร์ล้มได้อย่างไร?

การโจมตีแบบ DDoS ประสานอุปกรณ์บอตเน็ตที่ถูกเจาะนับล้านเครื่องให้ส่งทราฟฟิกท่วมเซิร์ฟเวอร์ จนใช้แบนด์วิดท์และขีดจำกัดของ CPU หมด

Q2: การเข้ารหัสแบบสมมาตรกับอสมมาตรต่างกันอย่างไร?

การเข้ารหัสแบบสมมาตรใช้กุญแจเดียวสำหรับการเข้ารหัสและถอดรหัส ส่วนการเข้ารหัสแบบอสมมาตรใช้คู่กุญแจสาธารณะและกุญแจส่วนตัว

Q3: แฮกเกอร์โจมตีด้วย SQL injection ได้อย่างไร?

ผู้โจมตีป้อนคำสั่ง SQL ที่เป็นอันตรายลงในช่องแบบฟอร์ม หลอกให้ฐานข้อมูลส่วนหลังเปิดเผยระเบียนผู้ใช้โดยไม่ได้รับอนุญาต

Q4: การเคลื่อนที่ในแนวขวาง (lateral movement) ในการบุกรุกเครือข่ายคืออะไร?

เป็นเทคนิคที่ผู้โจมตีใช้ประโยชน์จากการเข้าถึงเซิร์ฟเวอร์เบื้องต้นเพื่อบุกรุกระบบอื่นที่เชื่อมต่อกันในเครือข่ายภายใน

Q5: การปลอมแปลง DNS (DNS spoofing) เปลี่ยนเส้นทางทราฟฟิกเว็บได้อย่างไร?

DNS spoofing เปลี่ยนระเบียนแคชของเนมเซิร์ฟเวอร์ ทำให้ผู้ใช้ที่ถูกต้องถูกนำไปยังเว็บไซต์ปลอมที่เลียนแบบแทนโดเมนเป้าหมาย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: โทเค็นความปลอดภัยแบบฮาร์ดแวร์คืออะไร?

เป็นอุปกรณ์จริง (เช่น YubiKey) ที่สร้างหลักฐานยืนยันตัวตนด้วยการเข้ารหัสลับ ให้การป้องกันสูงสุดต่อฟิชชิงระยะไกล

Q7: ทีมรักษาความปลอดภัยใช้ honeypot ล่อ (decoy) อย่างไร?

ทีมติดตั้งเซิร์ฟเวอร์ล่อที่ไม่ใช่โปรดักชันเพื่อตรวจจับการบุกรุกตั้งแต่เนิ่นๆ และวิเคราะห์รูปแบบการโจมตีของผู้ไม่หวังดี

Q8: หลักการสิทธิ์ขั้นต่ำที่จำเป็น (principle of least privilege) คืออะไร?

เป็นมาตรฐานความปลอดภัยที่จำกัดสิทธิ์การเข้าถึงของผู้ใช้ให้เหลือน้อยที่สุดเท่าที่จำเป็นต่อบทบาทหน้าที่

Q9: การโจมตีแบบ Man-in-the-Middle ใช้ประโยชน์จากการเชื่อมต่ออย่างไร?

ผู้โจมตีดักและแก้ไขการสื่อสารระหว่างสองอุปกรณ์บนเครือข่ายที่ไม่ได้เข้ารหัส เพื่อขโมยโทเค็นเซสชันและข้อมูลรับรอง

Q10: ตัวบ่งชี้การถูกบุกรุก (IOC) คืออะไร?

IOC คือเบาะแสข้อมูลนิติวิทยาศาสตร์ เช่น การแก้ไขรีจิสทรีที่ผิดปกติหรือทราฟฟิก IP ที่ไม่ได้รับอนุญาต ซึ่งแสดงว่าระบบถูกบุกรุก

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ผู้โจมตีสแกนหาเซิร์ฟเวอร์ที่มีช่องโหว่บนอินเทอร์เน็ตตลอดเวลา และส่งอีเมลฟิชชิงไปยังกล่องจดหมายของพนักงาน

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ความผิดพลาดของมนุษย์ เช่น การคลิกลิงก์ฟิชชิง เป็นปัจจัยที่พบบ่อยในการละเมิดข้อมูล ซึ่งเป็นเหตุผลที่การอบรมมีความสำคัญ

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ค่าใช้จ่ายจากข้อมูลรั่วไหลรวมถึงค่าปรับทางกฎหมาย การสูญเสียลูกค้า การสืบสวนและแก้ไข และอาจสูงถึงหลายล้านดอลลาร์

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

MFA ที่ทนต่อฟิชชิง เช่น กุญแจความปลอดภัยฮาร์ดแวร์ เป็น MFA ประเภทที่แข็งแกร่งที่สุดและเป็นมาตรฐานที่ CISA เรียกร้อง [2]

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

แรนซัมแวร์ยังคงเป็นภัยคุกคามสำคัญต่อเครือข่ายองค์กร และ CISA แนะนำให้สำรองข้อมูลแบบออฟไลน์และเข้ารหัสเป็นแนวป้องกันหลัก [4]

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

NIST Cybersecurity Framework 2.0 (2024) มีหกฟังก์ชันหลัก ได้แก่ Govern, Identify, Protect, Detect, Respond, Recover [1]

7. ข้อมูลเชิงลึกด้านความปลอดภัย

บอต Credential Stuffing ทดสอบคู่ชื่อผู้ใช้และรหัสผ่านที่รั่วไหลเป็นจำนวนมากกับพอร์ทัลเข้าสู่ระบบของธนาคารและอีคอมเมิร์ซ

8. ข้อมูลเชิงลึกด้านความปลอดภัย

มีตลาดซื้อขายช่องโหว่ซีโร่เดย์อยู่ทั่วโลก ซึ่งช่องโหว่ที่มีความรุนแรงสูงอาจขายได้ในราคาสูงก่อนที่จะถูกแก้ไข

9. ข้อมูลเชิงลึกด้านความปลอดภัย

ระบบล่อ Honeypot รายงานการแจ้งเตือนการบุกรุกทันที เพราะผู้ใช้ที่ถูกต้องไม่มีเหตุผลที่จะเข้าถึง

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

Transport Layer Security (TLS) เข้ารหัสเซสชันเบราว์เซอร์ ป้องกันการดักจับแพ็กเก็ตบนเครือข่าย Wi-Fi สาธารณะ

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] 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

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **การโจมตีแบบฟิชชิง** ฟิชชิง คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

แคมเปญฟิชชิงพยายามขโมยข้อมูลประจำตัวและข้อมูลสำคัญของผู้ใช้โดยใช้อีเมลปลอม อ้างอิง: OWASP Secure Configuration.

2 **การปกป้องบัญชี** คีย์ MFA คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การยืนยันตัวตนหลายปัจจัย (MFA) ที่ใช้โทเคนฮาร์ดแวร์ให้การป้องกันการเข้าถึงบัญชีที่แข็งแกร่งที่สุด อ้างอิง: NIST Digital Identity.

3 **ภัยคุกคามจากแรนซัมแวร์** แรนซัมแวร์ คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

แรนซัมแวร์เข้ารหัสระบบและข้อมูลสำคัญ และเรียกร้องการชำระเงินด้วยสกุลเงินดิจิทัลเพื่อแลกกับคีย์ถอดรหัส แหล่งอ้างอิง: Center for Internet Security (CIS).

4 **ช่องโหว่ซีโร่เดย์** ซีโร่เดย์ คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ภัยคุกคามซีโร่เดย์ใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยที่ยังไม่ได้รับการแก้ไขและไม่เป็นที่รู้จัก ก่อนที่ผู้จำหน่ายจะออกแพตช์ การอ้างอิง: OWASP Secure Configuration.

5 **กรอบงานด้านความปลอดภัย** เฟรมเวิร์ก คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

กรอบงานอย่าง NIST ให้แนวทางที่เป็นระบบเพื่อช่วยให้องค์กรจัดการและลดความเสี่ยงทางไซเบอร์ การอ้างอิง: NIST Digital Identity.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **ฟิชชิงแบบเจาะจงเป้าหมาย** ฟิชชิง — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

การโจมตีแบบฟิชชิงมุ่งเป้าทั้งเครือข่ายองค์กรและบัญชีส่วนตัวเพื่อขยายช่องทางการโจมตี อ้างอิง: OWASP Secure Configuration.

7 **คำถาม 7** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

MFA ต้องใช้ปัจจัยที่สอง ดังนั้นรหัสผ่านที่ถูกขโมยเพียงอย่างเดียวมักไม่เพียงพอต่อการเข้าสู่ระบบ

8 **ไฟร์วอลล์ทราฟฟิก** ไฟร์วอลล์ — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

ไฟร์วอลล์ตรวจสอบและบล็อกการรับส่งข้อมูลบนพอร์ตเครือข่ายที่กำหนดเพื่อกรองการเชื่อมต่อที่ไม่ได้รับอนุญาต การอ้างอิง: Center for Internet Security (CIS).

9 **การตอบสนองต่อซีโร่เดย์** ซีโร่เดย์ — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

การแก้ไขช่องโหว่ซีโร่เดย์ต้องใช้แพตช์โค้ดและการกรองด้วย WAF เนื่องจากยังไม่มีลายเซ็น การอ้างอิง: OWASP Secure Configuration.

10 **ฮันนีพอตล่อเป้า** ฮันนีพอต — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

ฮันนีพอตคือเซิร์ฟเวอร์ล่อที่ทีมรักษาความปลอดภัยใช้ล่อ แจ้งเตือน และศึกษาผู้ประสงค์ร้าย การอ้างอิง: Center for Internet Security (CIS).

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

D 1. ภัยคุกคามแรนซัมแวร์	G 2. การยืนยันตัวตนหลายปัจจัย	E 3. การโจมตีแบบซีโร่เดย์	H 4. ฮันนีพอตล่อ
C 5. ไฟร์วอลล์ป้องกันการบุกรุก	B 6. การรับมือเหตุการณ์	F 7. สุขอนามัยของรหัสผ่าน	A 8. เฟรมเวิร์กความปลอดภัย

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ไฟร์วอลล์	2 ช่องโหว่	3 ฟิชชิง	4 มัลแวร์
5 สุขอนามัย	6 การเข้ารหัส		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 E – ไฟร์วอลล์	2 F – ตอบสนอง	3 A – เรียกค่าไถ่	4 B – ยืนยันตัวตน
5 G – สุขอนามัย	6 H – กรอบงาน	7 C – ช่องโหว่	8 D – ฮันนีพอต

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย *ภัยคุกคามแรนซัมแวร์* *การยืนยันตัวตนหลายปัจจัย* และ *การโจมตีแบบซีโร่เดย์* ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

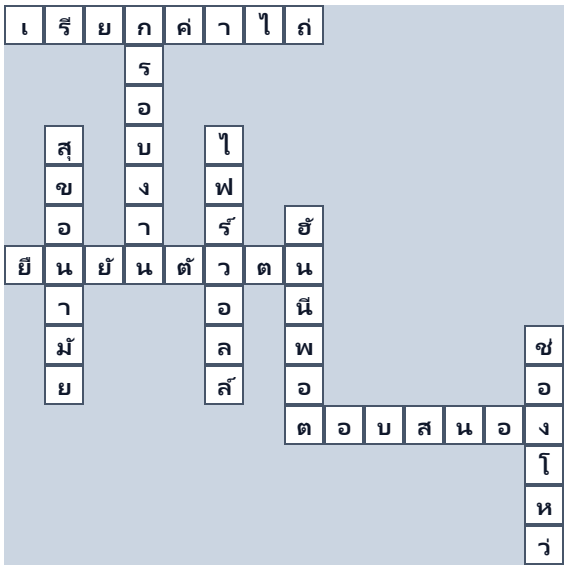
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	า	รี	ต	ว	ย	ง	ก	ค	จ	น	ตี	ว	ร	ตี
ว	า	ล	ล	ด	า	อ	ย	ต	ช	ฟ	ก	ก	ล	ม
า	ป	อ	อ	ม	มี	า	ล	ล	อ	ป	จ	า	นี	กี
พ	ต	น	า	ง	บ	อ	ร	ก	ร	บ	ง	า	ช	า
า	อ	ลี	จ	ดี	เ	า	น	ล	ผ	ดี	ส	ช	สุ	ก
ล์	พ	ด	า	ต	รี	า	ยื	จ	า	ค	ก	น	ข	ดี
ล	นี	า	ช	ว	ย	ก	ด	น	กี	ด	ท	ผ	อ	ฟ
อ	น	ช	มี	ม	ก	อ	ต	ฟ	ยั	ร	ดี	า	น	ง
ว	ฮั	ท	า	ส	ค่	ท	ข	ข	า	น	น	ก	า	า
ร์	ล	า	ม	ร	า	ช่	มี	า	ร	ช	ตั	ก	มั	ด
ฟ	ง	น	ร	ต	ไ	อ	สี	ย	ข	มี	ดี	ว	ย	ด
ไ	ด	ว	บ	ฟ	ถ่	ง	อ	า	ร	ห	ห	รี	ต	น
ผ	นี	ม	ผ	ดี	ข	โ	กี	ส	บ	ลี	ง	ด	ร	น
ด	ค	ผ	ห	ดี	ป	ห	ร	กี	นี	า	ต	จ	ห	ดี
ด	บ	ตี	น	สี	ลี	ว่	ว	ลี	า	ค	า	า	ล	ห

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

1 แนวนอน: เรียกค่าไถ่ มัลแวร์ที่เข้ารหัสข้อมูลและเรียกเงินเพื่อถอดรหัส (8 ตัวอักษร)

6 แนวนอน: ยืนยันตัวตน การตรวจสอบความปลอดภัยที่ต้องใช้ปัจจัยยืนยันตัวตนตั้งแต่สองอย่างขึ้นไป (8 ตัวอักษร)

8 แนวนอน: ตอบสนอง แผนที่เป็นระบบสำหรับจัดการและบรรเทาการละเมิดความปลอดภัย (7 ตัวอักษร)

แนวตั้ง

2 แนวตั้ง: กรอบงาน แนวทางที่มีโครงสร้าง เช่น NIST ที่ใช้จัดการความเสี่ยงไซเบอร์ (7 ตัวอักษร)

3 แนวตั้ง: สุขอนามัย แนวปฏิบัติที่ดีที่สุดในการจัดการข้อมูลประจำตัวและคีย์ยืนยันตัวตน (7 ตัวอักษร)

4 แนวตั้ง: ไฟร์วอลล์ เครื่องกั้นเครือข่ายที่กรองทราฟฟิกตามกฎความปลอดภัย (7 ตัวอักษร)

5 แนวตั้ง: ฮันนีพอต ระบบล่อที่ตั้งขึ้นเพื่อล่อและวิเคราะห์ผู้ประสงค์ร้าย (6 ตัวอักษร)

7 แนวตั้ง: ช่องโหว่ การโจมตีจุดอ่อนที่ยังไม่มีแพตช์จากผู้จำหน่าย (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ไกค่เารีถ่ย → **เรียกค่าไถ่**
2. ว่ช่งหโอ → **ช่องโหว่**
3. ว์ไอส์ร์ลฟ → **ไฟร์วอลล์**
4. ยขานมัสุอ → **สุขอนามัย**
5. ต้วนนนยืตยั → **ยืนยันตัวตน**
6. อพฮันีตน → **ฮันนีพอต**
7. ตอนงอสบ → **ตอบสนอง**
8. รบนกางอ → **กรอบงาน**

เฉลยภารกิจรหัสลับ

"ปกป้อง ระบบ ด้วย การ ยืนยันตัวตน"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: กลยุทธ์กู้คืนจากแรนซัมแวร์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: เครือข่ายองค์กรติดแรนซัมแวร์ ล็อกฐานข้อมูลสำคัญ ผู้โจมตีเรียกค่าไถ่เป็นคริปโตมูลค่า 100,000 ดอลลาร์ บริษัทมีข้อมูลสำรองออฟไลน์จากเมื่อ 24 ชั่วโมงก่อน
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ความเสี่ยงของการจ่าย: การจ่ายไม่รับประกันว่าไฟล์จะถูกถอดรหัส ทำให้บริษัทถูกมองเป็นเป้าหมายที่ยอมจ่าย และเป็นการสนับสนุนเงินทุนแก่กิจกรรมอาชญากรรม กลยุทธ์การกู้คืน: ทีมควรแยกโฮสต์ที่ติดเชื้อ ล้างเซิร์ฟเวอร์ที่ถูกบุกรุก และกู้คืนข้อมูลจากข้อมูลสำรองออฟไลน์ ต้องแพตช์ช่องทางเข้าถึงแรกเริ่ม (ฟิชชิงหรือการเจาะช่องโหว่) เพื่อป้องกันการติดเชื้อซ้ำทันที

B กรณีศึกษาที่ 2: การป้องกัน Credential Stuffing

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บริการออนไลน์ถูกโจมตีแบบ credential stuffing โดยแฮกเกอร์ทดสอบคู่ชื่อผู้ใช้/รหัสผ่านนับล้านที่ขโมยมาจากเว็บไซต์อื่น
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: กลไก: ผู้โจมตีใช้ประโยชน์จากการใช้รหัสผ่านซ้ำข้ามเว็บไซต์ โดยใช้บอตอัตโนมัติล็อกอินเข้าบัญชีผู้ใช้ การป้องกัน: 1. การยืนยันตัวตนหลายปัจจัย (MFA) บล็อกความพยายามล็อกอินแม้รหัสผ่านจะถูกต้อง 2. การจำกัดอัตราและ CAPTCHA บล็อกทราฟฟิกบอตอัตโนมัติที่ยิงถล่มจุดล็อกอิน