ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

ซอฟต์แวร์แอนตี้ไวรัสและอุปกรณ์ปลายทาง คู่มือการป้องกัน

การตรวจจับด้วยลายเซ็น ฮิวริสติก การตรวจสอบพฤติกรรม แซนด์บ็อกซ์ การอัปเดต

ภาพรวมการเรียนรู้ซอฟต์แวร์แอนติไวรัส

ได้รับการรักษาความปลอดภัย
การเข้ารหัสข้อมูล
มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด
มาตรฐานสากล
กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์
นโยบายการเข้าถึง
การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับซอฟต์แวร์แอนตี้ไวรัสและการป้องกันเอนด์พอยต์ คุณจะได้สำรวจฐานข้อมูลลายเซ็น ตัวสแกนแบบฮิวริสติก การเฝ้าติดตามพฤติกรรม ไฟล์เสมือนแบบแซนด์บ็อกซ์ และการลดผลบวกลวง

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/antivirus/

เส้นทางการเรียนรู้กลยุทธ์แอนตี้ไวรัสของคุณ

- จำแนกความแตกต่างระหว่างการตรวจจับมัลแวร์แบบอิงลายเซ็นกับแบบฮิวริสติก
- ทำความเข้าใจการตรวจสอบพฤติกรรมและโปรโตคอลการแยกแซนด์บ็อกซ์
- ประเมินผลกระทบของการสแกนแบบเรียลไทม์ต่อประสิทธิภาพของระบบและเอ็นด์พอยต์
- ลดการจัดประเภทผลบวกลวงด้วยการตรวจสอบใบรับรองดิจิทัล
- จัดการการแจกจ่ายการอัปเดตนิยามประจำวันไปยังเอ็นด์พอยต์ขององค์กร

คำแนะนำคู่มือแอนติไวรัส

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ ความปลอดภัยแอนตี้ไวรัสสำหรับอุปกรณ์ปลายทาง ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การป้องกันด้วยแอนติไวรัสและการสแกนลายเซ็น (บทนำ)

ซอฟต์แวร์แอนตี้ไวรัสปกป้องอุปกรณ์ปลายทางด้วยการระบุ กักกัน และกำจัดมัลแวร์ ระบบสมัยใหม่รวมฐานข้อมูลลายเซ็น (จับคู่แฮชของภัยคุกคามที่รู้จัก) กับฮิวริสติก (วิเคราะห์โครงสร้างไฟล์) และการเฝ้าดูพฤติกรรม เพื่อตรวจจับช่องโหว่แบบ zero-day

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. ข้อจำกัดของการตรวจจับตามลายเซ็นคืออะไร?
   - A. ระบุมัลแวร์ที่ไม่รู้จักหรือถูกดัดแปลงไม่ได้
   - B. ทำให้เกิดผลบวกลวงในอัตราสูง
   - C. ต้องใช้พลังประมวลผล CPU สูง
   - D. ทำงานได้เฉพาะเมื่อเชื่อมต่ออินเทอร์เน็ต

2. เครื่องสแกนแบบฮิวริสติกตรวจจับมัลแวร์สายพันธุ์ใหม่ได้อย่างไร?
   - A. ด้วยการระบุรูปแบบและโครงสร้างโค้ดที่น่าสงสัย
   - B. ด้วยการจับคู่แฮชของไฟล์กับฐานข้อมูลภัยคุกคาม
   - C. ด้วยการลบไฟล์ปฏิบัติการที่ไม่ได้ลงนามทั้งหมดโดยอัตโนมัติ
   - D. ด้วยการอัปโหลดทุกไฟล์ไปยังโฟลเดอร์คลาวด์สาธารณะ

3. วัตถุประสงค์ของการรันในแซนด์บ็อกซ์ของแอนติไวรัสคืออะไร?
   - A. การแยกและวิเคราะห์ไฟล์ในห้องนิรภัยเสมือนที่ปลอดภัย
   - B. การเร่งความเร็วการโอนสำรองระบบไฟล์ในเครื่อง
   - C. อัปเดตแพตช์ความปลอดภัยของระบบปฏิบัติการในเครื่อง
   - D. การบีบอัดไฟล์เอกสารขนาดใหญ่เพื่อประหยัดพื้นที่จัดเก็บ

4. วิธีการตรวจจับแบบใดที่ตั้งค่าสถานะพฤติกรรมของภัยคุกคามแบบเรียลไทม์?
   - A. การวิเคราะห์พฤติกรรมที่เฝ้าดูการกระทำของซอฟต์แวร์
   - B. การตรวจสอบล็อกย้อนหลังที่ทำข้ามคืน
   - C. ผู้ใช้ต้องรายงานแอปที่ซ้ำด้วยตนเอง
   - D. การตรวจสอบโปรแกรมที่ติดตั้งด้วยตนเองทุกสัปดาห์

5. เหตุใดการอัปเดตคำจำกัดความเป็นประจำจึงสำคัญสำหรับตัวสแกน?
   - A. เพื่อป้อนตัวระบุภัยคุกคามให้ฐานข้อมูลของเอนจินลายเซ็น
   - B. เพื่อเพิ่มความเร็วสัญญาณนาฬิกา CPU ระหว่างการทำงาน
   - C. เพื่อแก้ไขเวลาแคชเนมเซิร์ฟเวอร์ DNS ทั่วโลก
   - D. เพื่ออนุญาตการตั้งค่าคุกกี้ของเว็บเบราว์เซอร์

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 **คำถามจริง/เท็จ 6**

6. การตรวจจับด้วยลายเซ็นจะจับคู่แฮชการเข้ารหัสของไฟล์กับรายการในฐานข้อมูล

○ จริง ○ เท็จ

7 **คำถามจริง/เท็จ 7**

7. เครื่องสแกนแบบฮิวริสติกอาจทำให้เกิดการแจ้งเตือนผลบวกลวงกับไฟล์ที่ปลอดภัยได้

○ จริง ○ เท็จ

8 **คำถามจริง/เท็จ 8**

8. แซนด์บอกซ์อนุญาตให้มัลแวร์เข้าถึงไฟล์เครือข่ายได้โดยไม่มีข้อจำกัด

○ จริง ○ เท็จ

9 **คำถามจริง/เท็จ 9**

9. การสแกนเชิงพฤติกรรมบล็อกไฟล์เมื่อแสดงการกระทำที่เป็นอันตราย

○ จริง ○ เท็จ

10 **คำถามจริง/เท็จ 10**

10. ซอฟต์แวร์แอนตี้ไวรัสมาตรฐานหยุดการโจมตีแบบซีโร่เดย์ได้ทั้งหมด

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. สแกนเนอร์แบบดั้งเดิมอาศัยการจับคู่ _____ เพื่อระบุมัลแวร์ที่รู้จัก
2. การวิเคราะห์รูปแบบโค้ดของไฟล์เรียกว่าการสแกนแบบ _____
3. เครื่องมือแอนติไวรัสแยกไฟล์น่าสงสัยไว้ในสภาพแวดล้อมแบบ _____
4. การเฝ้าระวังแบบเรียลไทม์คอยดู _____ ของโปรแกรมที่น่าสงสัย
5. สแกนเนอร์ดาวน์โหลด _____ ฐานข้อมูลทุกวันเพื่อให้รู้จักภัยคุกคามใหม่
6. โปรแกรมปลอดภัยที่ถูกทำเครื่องหมายเป็นมัลแวร์ทำให้เกิดการแจ้งเตือนเชิงบวก _____

คลังคำศัพท์

กักกัน | การอัปเดต | แซนด์บ็อกซ์ | ที่ผิดพลาด | พฤติกรรม | แรนซัมแวร์ | ลายเซ็น | ฮิวริสติก

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

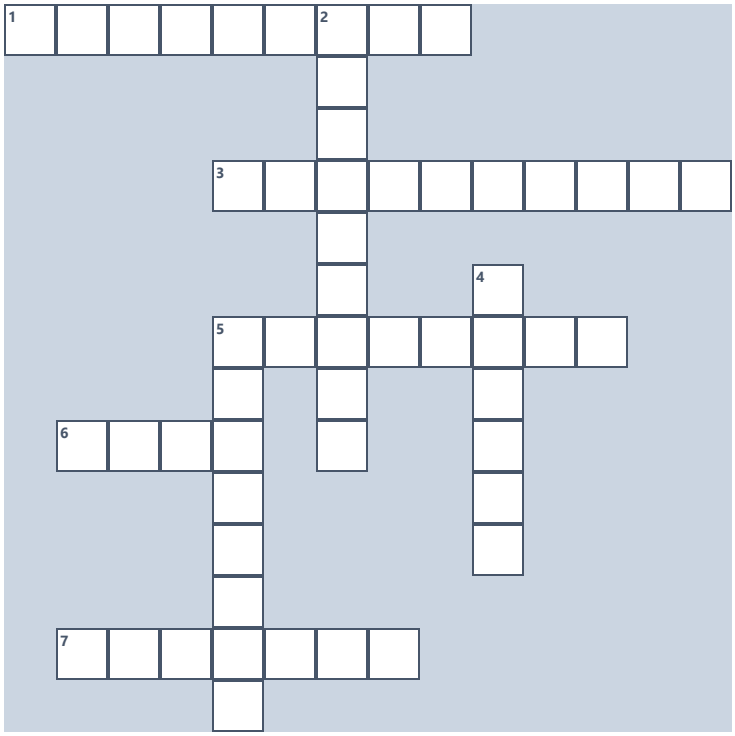
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. ลายเซ็นแฮช**	**A**	การกักไฟล์น่าสงสัยไว้เพื่อป้องกันการเปิดเผยต่อระบบภายใน
☐	**2. ฮิวริสติกของโค้ด**	**B**	ชุดซอฟต์แวร์ที่สแกนและปกป้องอุปกรณ์ปลายทางจากซองโหว่ที่ถูกโจมตี
☐	**3. ไฟล์แซนด์บ็อกซ์**	**C**	การเฝ้าติดตามการทำงานของซอฟต์แวร์ที่กำลังรันเพื่อหารูปแบบการทำงานที่เป็นอันตราย
☐	**4. การสแกนพฤติกรรม**	**D**	ลายนิ้วมือเข้ารหัสเฉพาะของฐานข้อมูลที่ใช้ระบุภัยคุกคามที่รู้จัก
☐	**5. อัปเดตรายวัน**	**E**	สภาพแวดล้อมทดสอบเสมือนที่ปลอดภัยซึ่งรันโค้ดที่ไม่น่าเชื่อถืออย่างปลอดภัย
☐	**6. ผลบวกลวง**	**F**	การดาวน์โหลดนิยามไวรัสเป็นประจำที่ป้อนเข้าฐานข้อมูลภัยคุกคาม
☐	**7. การแยกภัยคุกคาม**	**G**	การวิเคราะห์ตามกฎที่ตั้งธงไฟล์ที่มีโครงสร้างโค้ดน่าสงสัย
☐	**8. เครื่องมือแอนติไวรัส**	**H**	การแจ้งเตือนความปลอดภัยที่จัดซอฟต์แวร์ปลอดภัยเป็นมัลแวร์ผิดพลาด

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

1. รอยพิมพ์เข้ารหัสเฉพาะตัวในฐานข้อมูลที่ใช้ระบุภัยคุกคามที่รู้จักแล้ว (9)

3. การดาวน์โหลดนิยามเป็นประจำเพื่อป้อนให้ฐานข้อมูลภัยคุกคาม (10)

5. ชุดซอฟต์แวร์ที่สแกนและปกป้องอุปกรณ์ปลายทางจากช่องโหว่ที่ถูกโจมตี (8)

6. การกักไฟล์น่าสงสัยไว้เพื่อป้องกันไม่ให้ระบบในเครื่องได้รับผลกระทบ (4)

7. การเฝ้าดูการทำงานของซอฟต์แวร์ที่กำลังรันเพื่อหารูปแบบการทำงานที่เป็นอันตราย (7)

แนวตั้ง

2. การแจ้งเตือนด้านความปลอดภัยที่จัดซอฟต์แวร์ปลอดภัยเป็นมัลแวร์อย่างผิดพลาด (9)

4. การวิเคราะห์ตามกฎที่ทำเครื่องหมายไฟล์ซึ่งมีโครงสร้างโค้ดน่าสงสัย (6)

5. สภาพแวดล้อมจำลองทดสอบที่ปลอดภัยสำหรับรันโค้ดที่ไม่น่าเชื่อถืออย่างปลอดภัย (8)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง เบาะแสแนวนอน เบาะแสแนวตั้ง

แนวนอน

1 แนวนอน: รอยพิมพ์เข้ารหัสเฉพาะตัวในฐานข้อมูลที่ใช้ระบุภัยคุกคามที่รู้จักแล้ว (9 ตัวอักษร):

3 แนวนอน: การดาวน์โหลดนิยามเป็นประจำเพื่อป้อนให้ฐานข้อมูลภัยคุกคาม (10 ตัวอักษร):

5 แนวนอน: ชุดซอฟต์แวร์ที่สแกนและปกป้องอุปกรณ์ปลายทางจากช่องโหว่ที่ถูกโจมตี (8 ตัวอักษร):

6 แนวนอน: การกักไฟล์น่าสงสัยไว้เพื่อป้องกันไม่ให้ระบบในเครื่องได้รับผลกระทบ (4 ตัวอักษร):

7 แนวนอน: การเฝ้าดูการทำงานของซอฟต์แวร์ที่กำลังรันเพื่อหารูปแบบการทำงานที่เป็นอันตราย (7 ตัวอักษร):

แนวตั้ง

2 แนวตั้ง: การแจ้งเตือนด้านความปลอดภัยที่จัดซอฟต์แวร์ปลอดภัยเป็นมัลแวร์อย่างผิดพลาด (9 ตัวอักษร):

4 แนวตั้ง: การวิเคราะห์ตามกฎที่ทำเครื่องหมายไฟล์ซึ่งมีโครงสร้างโค้ดน่าสงสัย (6 ตัวอักษร):

5 แนวตั้ง: สภาพแวดล้อมจำลองทดสอบที่ปลอดภัยสำหรับรันโค้ดที่ไม่น่าเชื่อถืออย่างปลอดภัย (8 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

า นี ก า น นี ส แ ช มี ฟ บ า า ห
นี า ติ ม กี จ า อ า รี พ ต ว ย ง
ก ค ส จ น ตี ว น ร ตี ฤ ว า ล ล
ช ด ริ า อ ย ซ ติ ฟ ก ติ ก ล ม า
ฮ ป ว อ อ อ้ ม ไ มี า ก ล ล แ ป
แ จ ฮิ า นี ป กี ว พ ร ร ง า จ้ ซ
น า า ลี จ เ ดี ร้ แ า ร น ล ง ผ
ซ็ ดี ช ก ด ด า ส ช ต ม า จ เ า
เ ค ก ดี า ต ซ ว น ก ด กี ด ตื ท
ย ผ ฟ ช มี ร ม อ ด์ ต ฟ ร ดี อ า
า ท า ส ท า ข ข ป็ า น น ก น า
ล ล า ม ร ย มี า อ กั ร ช ก ผิ ด
ง น ร ต สี วั ย ข ก มี ดี ด ด ด ว
บ ฟ อ า ร น ห กั ช์ ห รี น ผ นี ม
ผ ดี ข กี ส บ ลี ง ด ร ด ค ผ ห ดี

รายการคำศัพท์

ลายเซ็นแฮช ฮิวริสติก แซนด์บ็อกซ์ พฤติกรรมแอนตี้ไวรัส อัปเดตรายวัน แจ้งเตือนผิด กักกัน

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ลายเซ็นแฮช
B. ฮิวริสติก
C. แซนด์บ็อกซ์
D. พฤติกรรม
E. อัปเดตรายวัน
F. แจ้งเตือนผิด
G. กักกัน
H. แอนติไวรัส

คำนิยามและช่องจับคู่	
	1. การเฝ้าดูการทำงานของซอฟต์แวร์ที่กำลังรันเพื่อหารูปแบบการทำงานที่เป็นอันตราย
	2. ชุดซอฟต์แวร์ที่สแกนและปกป้องอุปกรณ์ปลายทางจากช่องโหว่ที่ถูกโจมตี
	3. การดาวน์โหลดนิยามเป็นประจำเพื่อป้อนให้ฐานข้อมูลภัยคุกคาม
	4. การวิเคราะห์ตามกฎที่ทำเครื่องหมายไฟล์ซึ่งมีโครงสร้างโค้ดน่าสงสัย
	5. การกักไฟล์น่าสงสัยไว้เพื่อป้องกันไม่ให้ระบบในเครื่องได้รับผลกระทบ
	6. รอยพิมพ์เข้ารหัสเฉพาะตัวในฐานข้อมูลที่ใช้ระบุภัยคุกคามที่รู้จักแล้ว
	7. สภาพแวดล้อมจำลองทดสอบที่ปลอดภัยสำหรับรันโค้ดที่ไม่น่าเชื่อถืออย่างปลอดภัย
	8. การแจ้งเตือนด้านความปลอดภัยที่จัดซอฟต์แวร์ปลอดภัยเป็นมัลแวร์อย่างผิดพลาด

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. น ซ็ เ า ล แ ฮ ช ย
2. ด์ แ ซ์ ซ ก อ บ็ น
3. อั ร ว้ า ป ต น ด ย เ
4. น กั กั ก
5. ส ริ ก ฮิ ติ ว
6. ร ติ ร พ ก ม ฤ
7. อ แ ผิ ด น เ จ้ ตึ ง
8. ติ อ ไ ส แ ร้ ว น

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
2	บุคคลที่คุณขอความช่วยเหลือด้าน IT ได้			
3	สิ่งที่ควรทำเมื่อแอนติไวรัสพบบางอย่าง			
4	สัญญาณของไวรัสคอมพิวเตอร์			
5	สิ่งที่ถูกกักกัน			
6	สถานที่ที่ไวรัสซ่อนอยู่			
7	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
8	ประเภทของซอฟต์แวร์ที่เป็นอันตราย			
9	เครื่องมือด้านความปลอดภัยที่คุณรู้จัก			
10	สิ่งที่แอนติไวรัสสแกน			
11	สิ่งที่คุณสำรองข้อมูล			
12	อุปกรณ์ที่ถูกแฮกได้			
13	โปรแกรมแอนติไวรัสที่คุณรู้จัก			
14	เหตุผลที่เกิดการแจ้งเตือนผิดพลาด			
15	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การสแกนตามลายเซ็นเทียบกับฮิวริสติก



สถานการณ์: พนักงานคนหนึ่งดาวน์โหลดยูทิลิตีแบบกำหนดเองที่ทีมอื่นสร้างขึ้นภายใน ตัวสแกนแบบซิกเนเจอร์ปล่อยผ่าน แต่ตัวสแกนแบบฮิวริสติกแจ้งว่าไฟล์น่าสงสัย

คำถามอภิปราย: จงอธิบายว่าเหตุใดจึงเกิดเหตุการณ์นี้ และจะตรวจสอบได้อย่างไรว่าไฟล์ปลอดภัยหรือไม่

กรณีศึกษาที่ 2: การจัดการผลบวกลวง



สถานการณ์: นักพัฒนาซอฟต์แวร์คอมไพล์แอปพลิเคชันของตน แอนติไวรัสของระบบแจ้งว่าไฟล์ปฏิบัติการใหม่เป็นมัลแวร์และกักกันไว้

คำถามอภิปราย: จงสรุปความเสี่ยงของการอนุญาตข้อยกเว้น (whitelisting) และอธิบายแนวทางแก้ไขที่ถูกต้อง

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

21	35	39	8	8	48	26		33	48	37	58	39	35	67		60	43	33	63			
			20	64	39	34		46	51	39	35	51	42	21	51	1						

ข้อความที่ถอดรหัสแล้ว:

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

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: ซอฟต์แวร์แอนติไวรัสระบุมัลแวร์ได้อย่างไร?

ระบุมัลแวร์โดยใช้การจับคู่ลายเซ็นในฐานข้อมูล การวิเคราะห์โครงสร้างโค้ดแบบฮิวริสติก และการเฝ้าติดตามพฤติกรรมแบบเรียลไทม์

Q2: การตรวจจับด้วยลายเซ็นคืออะไร?

เป็นวิธีสแกนที่จับคู่แฮชไฟล์เข้ารหัสลับกับรายการฐานข้อมูลของภัยคุกคามมัลแวร์ที่รู้จัก

Q3: ตัวสแกนแบบฮิวริสติก (heuristic scanner) คืออะไร?

ฮิวริสติกวิเคราะห์โครงสร้างของไฟล์และคำสั่งโค้ด แล้วตั้งสถานะรูปแบบที่น่าสงสัยซึ่งพบได้ทั่วไปในมัลแวร์สายพันธุ์ต่างๆ

Q4: เมื่อไฟล์ถูกกักกัน (quarantine) หมายความว่าอย่างไร?

โปรแกรมป้องกันไวรัสย้ายไฟล์ไปยังโฟลเดอร์ที่ปลอดภัยและแยกส่วน และบล็อกการเรียกใช้งานเพื่อปกป้องระบบปฏิบัติการ

Q5: ผลบวกลวง (false positive) ของโปรแกรมป้องกันไวรัสคืออะไร?

เป็นข้อผิดพลาดที่ซอฟต์แวร์ที่ถูกต้องและปลอดภัยถูกอัลกอริทึมสแกนตั้งสถานะผิดว่าเป็นมัลแวร์

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: การเฝ้าติดตามพฤติกรรมปกป้องระบบอย่างไร?

เฝ้าติดตามซอฟต์แวร์ที่ทำงานอยู่แบบเรียลไทม์ บล็อกโปรเซสที่พยายามเปลี่ยนแปลงอย่างน่าสงสัย เช่น การแทรกโค้ด

Q7: ทำไมการทดสอบในแซนด์บ็อกซ์จึงสำคัญ?

แซนด์บ็อกซ์รันไฟล์ที่ไม่น่าเชื่อถือในเครื่องเสมือนที่แยกอิสระ สังเกตการกระทำได้อย่างปลอดภัยโดยไม่กระทบระบบ

Q8: ควรอัปเดตฐานข้อมูลลายเซ็นของโปรแกรมป้องกันไวรัสบ่อยแค่ไหน?

ตัวสแกนควรอัปเดตนิยามทุกวันหรือทุกชั่วโมงเพื่อจดจำมัลแวร์สายพันธุ์ใหม่ที่ค้นพบ

Q9: โปรแกรมป้องกันไวรัสและ EDR ต่างกันอย่างไร?

แอนตี้ไวรัสเน้นการสแกนไฟล์ ส่วน Endpoint Detection and Response (EDR) ติดตามและควบคุมภัยคุกคามทั่วทั้งเครือข่าย

Q10: ฉันรันโปรแกรมแอนติไวรัสสองตัวพร้อมกันได้หรือไม่?

ไม่ การเปิดตัวสแกนที่ทำงานอยู่สองตัวทำให้ระบบขัดแย้งกัน ประสิทธิภาพช้าลง และอาจบล็อกการทำงานของกันและกัน

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: กฎฮิวริสติกลดการหลบภัยคุกคามได้อย่างไร?

ฮิวริสติกวิเคราะห์รูปแบบภัยคุกคามทั่วไปแทนที่จะใช้ลายเซ็นเฉพาะ จึงจับมัลแวร์สายพันธุ์ที่ถูกดัดแปลงของตระกูลมัลแวร์ที่รู้จักได้

Q2: ไวรัสโพลีมอร์ฟิกคืออะไร?

เป็นมัลแวร์ที่เปลี่ยนโครงสร้างไฟล์และกระบวนการถอดรหัสทุกครั้งที่ทำงาน ทำให้การสแกนลายเซ็นไม่ได้ผล

Q3: แซนด์บ็อกซ์ตรวจจับการหลบเลี่ยง VM ได้อย่างไร?

แซนด์บ็อกซ์สมัยใหม่จำลองการคลิกเมาส์และเวลาทำงานของระบบ หลอกมัลแวร์ที่ออกแบบมาให้ซ่อนตัวเมื่อทำงานบนเครื่องเสมือน

Q4: รูปแบบการดาวน์โหลดอัปเดตลายเซ็น (signature) มีอะไรบ้าง?

การอัปเดตมักเป็นไฟล์ผลต่างไบนารีแบบส่วนเพิ่มขนาดเล็ก เพื่อลดการใช้แบนด์วิดท์เครือข่ายของไคลเอนต์

Q5: เอเจนต์บนอุปกรณ์ปลายทางจัดการการสแกนในเครื่องอย่างไร?

เอเจนต์ทำการตรวจสอบเบื้องหลังแบบเบา โดยโอนการค้นหาแฮชเข้ารหัสเชิงลึกไปยังฐานข้อมูลภัยคุกคามบนคลาวด์

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การสแกนตรวจจับรูทคิต (rootkit) คืออะไร?

สแกนตารางหน่วยความจำระดับเคอร์เนล ข้าม API ของระบบปฏิบัติการที่รูทคิตดักไว้เพื่อซ่อนเธรดที่ทำงานอยู่

Q7: การสแกนพฤติกรรมบล็อกแรนซัมแวร์ได้อย่างไร?

ตรวจจับลูปการเข้ารหัสไฟล์จำนวนมากแบบอัตโนมัติ และยุติโปรเซสของโฮสต์ก่อนที่ฐานข้อมูลระบบจะถูกล็อก

Q8: การตรวจสอบใบรับรองการลงนามโค้ด (code-signing certificate) คืออะไร?

ตัวสแกนตรวจสอบลายเซ็นดิจิทัลของโค้ดกับผู้ออกใบรับรองรากที่เชื่อถือได้ เพื่อยืนยันตัวตนของผู้พัฒนาซอฟต์แวร์

Q9: packer ส่งผลต่อเอนจินสแกนอย่างไร?

แพ็กเกอร์บีบอัดหรือเข้ารหัสเพย์โหลดของมัลแวร์ เครื่องสแกนต้องแตกไฟล์ในหน่วยความจำก่อนจึงจะจับคู่ลายเซ็นได้

Q10: เครื่องมือ EDR แยกอุปกรณ์ที่ติดเชื้อโดยอัตโนมัติได้อย่างไร?

ตัวแทน EDR กักกันเอ็นด์พอยต์ที่ถูกบุกรุกในระดับเครือข่าย ป้องกันการเคลื่อนที่ด้านข้างขณะที่ยังให้นักวิเคราะห์เข้าถึงได้

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ฐานข้อมูลลายเซ็นเก็บแฮชของมัลแวร์ที่รู้จัก ดังนั้นไฟล์ใหม่ล่าสุดหรือที่ถูกแก้ไขจะตรวจไม่พบจนกว่าจะอัปเดตข้อมูลนิยาม

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

กลไกฮิวริสติกสามารถตั้งสถานะมัลแวร์สายพันธุ์ใหม่บางตัวได้ก่อนที่จะมีลายเซ็น แต่แลกกับผลบวกลวงที่มากขึ้น

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การแจ้งเตือนที่เป็นผลบวกลวงทำให้ทีมไอทีเสียเวลาตรวจสอบและกู้คืนไฟล์ที่ถูกกักกันโดยผิดพลาด

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

มัลแวร์โพลีมอร์ฟิกเปลี่ยนโค้ดของตัวเองในแต่ละสำเนา ผู้ป้องกันจึงใช้ลายเซ็นควบคู่กับการตรวจสอบแบบฮิวริสติกและพฤติกรรม

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ผู้เขียนมัลแวร์เขียนโค้ดแบบกำหนดเองเพื่อตรวจสอบสภาพแวดล้อมแซนด์บ็อกซ์ และหน่วงการทำงานเพื่อหลบตัวจับเวลา

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

เอนจินแอนติไวรัสบนคลาวด์ตรวจสอบแฮชของไฟล์ที่น่าสงสัยกับฐานข้อมูลภัยคุกคามออนไลน์ขนาดใหญ่แบบเกือบเรียลไทม์

7. ข้อมูลเชิงลึกด้านความปลอดภัย

ผู้จำหน่ายส่งอัปเดตนิยามไปยังอุปกรณ์ปลายทางเป็นประจำ เพื่อให้เครื่องสแกนจดจำภัยคุกคามที่เพิ่งยืนยันใหม่ได้

8. ข้อมูลเชิงลึกด้านความปลอดภัย

ตัวเฝ้าติดตามพฤติกรรมแรนซัมแวร์มุ่งเป้าไปที่การเรียก Win32 API เฉพาะที่เกี่ยวข้องกับการเข้ารหัสไฟล์และการลบ shadow copy

9. ข้อมูลเชิงลึกด้านความปลอดภัย

ลายเซ็นโค้ดที่ถูกต้องอาจลดความเสี่ยงของผลบวกลวง แต่ไฟล์ที่ลงนามยังคงถูกสแกน เพราะมัลแวร์ก็ลงนามได้

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

รูทคิตแก้ไขโครงสร้างเคอร์เนลของระบบ ต้องใช้ตัวสแกนขณะบูตเฉพาะทางเพื่อตรวจจับและกำจัด

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล แหล่งอ้างอิงทางวิชาการและอุตสาหกรรม

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
https://csrc.nist.gov/pubs/sp/800/83/r1/final

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

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

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

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **คำถาม 1** ลายเซ็น **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

การสแกนตามลายเซ็นอาศัยแฮชในฐานข้อมูลที่ทราบแล้ว จึงตรวจไม่พบมัลแวร์ที่ไม่รู้จักหรือถูกดัดแปลง แหล่งอ้างอิง: OWASP Secure Configuration.

2 **คำถาม 2** ฮิวริสติก **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

ฮิวริสติกวิเคราะห์โครงสร้างโค้ดและคำสั่งเพื่อระบุลักษณะน่าสงสัยของภัยคุกคามรูปแบบใหม่ แหล่งอ้างอิง: Center for Internet Security (CIS).

3 **คำถาม 3** การรันในแซนด์บ็อกซ์ **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

แซนด์บ็อกซ์รันไฟล์ที่น่าสงสัยในเครื่องเสมือนที่แยกต่างหากเพื่อสังเกตพฤติกรรมการทำงานอย่างปลอดภัย แหล่งอ้างอิง: NIST Digital Identity.

4 **คำถาม 4** เชิงพฤติกรรม **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

การสแกนพฤติกรรมเฝ้าติดตามโปรแกรมที่กำลังทำงานแบบเรียลไทม์เพื่อบล็อกการเปลี่ยนแปลงระบบที่ไม่ได้รับอนุญาต แหล่งอ้างอิง: Center for Internet Security (CIS).

5 **คำถาม 5** การอัปเดต **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

ตัวสแกนดาวน์โหลดการอัปเดตนิยามแบบเพิ่มทีละส่วนทุกวันเพื่อให้ทันกับสถานการณ์ภัยคุกคาม แหล่งอ้างอิง: OWASP Secure Configuration.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** ลายเซ็น **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

เครื่องมือแบบลายเซ็นคำนวณแฮชเข้ารหัสและจับคู่กับฐานข้อมูลแฮชภัยคุกคามที่ทราบแล้ว แหล่งอ้างอิง: OWASP Secure Configuration.

7 **คำถาม 7** ฮิวริสติก **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

เอนจินฮิวริสติกใช้รูปแบบตามกฎ ซึ่งอาจทำเครื่องหมายไฟล์ที่ถูกต้องและปลอดภัยว่าน่าสงสัยได้ แหล่งอ้างอิง: Center for Internet Security (CIS).

8 **คำถาม 8** การรันในแซนด์บ็อกซ์ **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

แซนด์บ็อกซ์รันโค้ดในคอนเทนเนอร์เสมือน และบล็อกการเข้าถึงเครือข่ายที่แชร์อย่างเข้มงวด แหล่งอ้างอิง: NIST Digital Identity.

9 **คำถาม 9** เชิงพฤติกรรม **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

การเฝ้าติดตามแบบเรียลไทม์ทำเครื่องหมายกระบวนการที่กำลังทำงานซึ่งพยายามเขียนข้อมูลที่ผิดกฎหมายหรือล็อกไฟล์ แหล่งอ้างอิง: Center for Internet Security (CIS).

10 **คำถาม 10** **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

ไม่มีแอนติไวรัสใดหยุดการโจมตีแบบ zero-day ได้ทุกครั้ง ภัยคุกคามที่ไม่รู้จักสามารถหลบซิกเนเจอร์และฮิวริสติกได้

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

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

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

D 1. ลายเซ็นแฮช	G 2. ฮิวริสติกของโค้ด	E 3. ไฟล์แซนด์บ็อกซ์	C 4. การสแกนพฤติกรรม
F 5. อัปเดตรายวัน	H 6. ผลบวกลวง	A 7. การแยกภัยคุกคาม	B 8. เครื่องมือแอนตี้ไวรัส

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ลายเซ็น	2 ฮิวริสติก	3 แซนด์บ็อกซ์	4 พฤติกรรม
5 การอัปเดต	6 ที่ผิดพลาด		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 D – พฤติกรรม	2 H – แอนตี้ไวรัส	3 E – อัปเดตรายวัน	4 B – ฮิวริสติก
5 G – กักกัน	6 A – ลายเซ็นแฮช	7 C – แซนด์บ็อกซ์	8 F – แจ้งเตือนผิด

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย ลายเซ็นแฮช ฮิวริสติกของโค้ด และ ไฟล์แซนด์บ็อกซ์ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

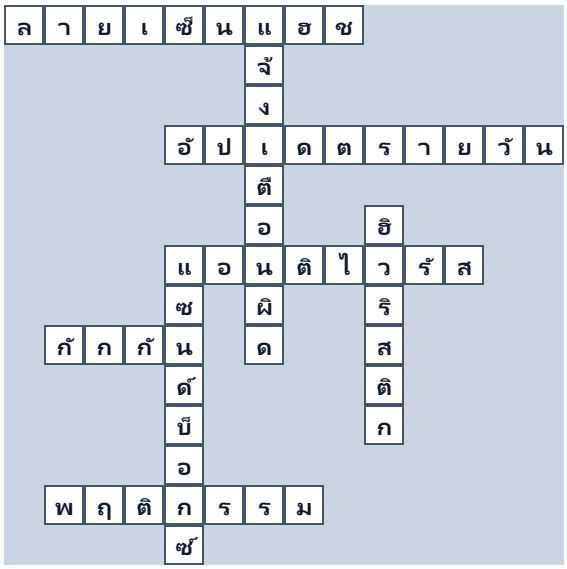
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

า	นี	ก	า	น	นี	ส	แ	ช	มี	ฟ	บ	า	า	ห
นี	า	ติ	ม	กี	จ	า	อ	า	รี	พ	ต	ว	ย	ง
ก	ค	ส	จ	น	ตี	ว	น	ร	ดี	ฤ	ว	า	ล	ล
ช	ด	ริ	า	อ	ย	ช	ดิ	ฟ	ก	ติ	ก	ล	ม	า
ฮ	ป	ว	อ	อ	อ้	ม	ไ	มี	า	ก	ล	ล	แ	ป
แ	จ	ฮิ	า	นี	ป	กี	ว	พ	ร	ร	ง	า	จ้	ช
น	า	า	ลี	จ	เ	ดี	ร้	แ	า	ร	น	ล	ง	ผ
ชิ	ดี	ช	ก	ด	ด	า	ส	ช	ต	ม	า	จ	เ	า
เ	ค	ก	ดี	า	ต	ช	ว	น	ก	ด	กี	ด	ตื	ท
ย	ผ	ฟ	ช	มี	ร	ม	อ	ด์	ต	ฟ	ร	ดี	อ	า
า	ท	า	ส	ท	า	ข	ข	บ็	า	น	น	ก	น	า
ล	ล	า	ม	ร	ย	มี	า	อ	ก้	ร	ช	ก	ผิ	ด
ง	น	ร	ต	สี	ว้	ย	ข	ก	มี	ดี	ด	ด	ด	ว
บ	ฟ	อ	า	ร	น	ห	ก้	ช์	ห	รี	น	ผ	นี	ม
ผ	ดี	ข	กี	ส	บ	ลี	ง	ด	ร	ด	ค	ผ	ห	ดี

เฉลยปริศนาอักษรไขว้



แนวนอน

1 แนวนอน: ลายเซ็นแฮช รอยพิมพ์เข้ารหัสเฉพาะตัวในฐานข้อมูลที่ใช้ระบุภัยคุกคามที่รู้จักแล้ว (9 ตัวอักษร)

3 แนวนอน: อัปเดตรายวัน การดาวน์โหลดนิยามเป็นประจำเพื่อป้อนให้ฐานข้อมูลภัยคุกคาม (10 ตัวอักษร)

5 แนวนอน: แอนตี้ไวรัส ชุดซอฟต์แวร์ที่สแกนและปกป้องอุปกรณ์ปลายทางจากช่องโหว่ที่ถูกโจมตี (8 ตัวอักษร)

6 แนวนอน: กักกัน การกักไฟล์น่าสงสัยไว้เพื่อป้องกันไม่ให้ระบบในเครื่องได้รับผลกระทบ (4 ตัวอักษร)

7 แนวนอน: พฤติกรรม การเฝ้าดูการทำงานของซอฟต์แวร์ที่กำลังรันเพื่อหารูปแบบการทำงานที่เป็นอันตราย (7 ตัวอักษร)

แนวตั้ง

2 แนวตั้ง: แจ้งเตือนผิด การแจ้งเตือนด้านความปลอดภัยที่จัดซอฟต์แวร์ปลอดภัยเป็นมัลแวร์อย่างผิดพลาด (9 ตัวอักษร)

4 แนวตั้ง: ฮิวริสติก การวิเคราะห์ตามกฎที่ทำเครื่องหมายไฟล์ซึ่งมีโครงสร้างโค้ดน่าสงสัย (6 ตัวอักษร)

5 แนวตั้ง: แซนด์บ็อกซ์ สภาพแวดล้อมจำลองทดสอบที่ปลอดภัยสำหรับรันโค้ดที่ไม่น่าเชื่อถืออย่างปลอดภัย (8 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. นซ็เาลแฮซย → ลายเซ็นแฮช
2. ด์แซ์ซกอบ็น → แซนด์บ็อกซ์
3. อัรว้าปตนดยเ → อัปเดตรายวัน
4. นกักัก → กักกัน
5. สริกฮิติว → ฮิวริสติก
6. รติรพกมฤ → พฤติกรรม
7. อแผิดนเจ้ตึง → แจ้งเตือนผิด
8. ติอไสแร้วน → แอนติไวรัส

เฉลยภารกิจรหัสลับ

"ตรวจจับ มัลแวร์ ใหม่ ด้วย ฮิวริสติก"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การสแกนตามลายเซ็นเทียบกับฮิวริสติก

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: พนักงานดาวน์โหลดยูทิลิตีแบบกำหนดเองที่ทีมอื่นสร้างขึ้นภายใน ตัวสแกนลายเซ็นให้ผ่าน แต่ตัวสแกนฮิวริสติกตั้งธงว่าน่าสงสัย
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ทำไมจึงเกิดขึ้น: การสแกนลายเซ็นตรวจสอบแฮชของไฟล์ เนื่องจากเป็นไฟล์ที่สร้างเอง จึงไม่อยู่ในฐานข้อมูลภัยคุกคาม ฮิวริสติกวิเคราะห์โครงสร้างและตั้งธงการกระทำที่น่าสงสัย (เช่น การเขียนรีจิสทรี) การตรวจสอบ: รันไฟล์ในแซนด์บ็อกซ์เพื่อสังเกตการกระทำ ตรวจสอบลายเซ็นดิจิทัล และส่งแฮชไปยังพอร์ทัลข่าวกรองภัยคุกคาม

B กรณีศึกษาที่ 2: การจัดการผลบวกลวง

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: นักพัฒนาซอฟต์แวร์คอมไพล์แอปพลิเคชันของตน แอนตี้ไวรัสของระบบตั้งธงไฟล์ปฏิบัติการใหม่ว่าเป็นมัลแวร์และกักกันไว้
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ความเสี่ยงของการ whitelist: การข้ามตัวสแกนอาจทำให้โค้ดติดเชื้อจริงรันได้ แนวทางแก้ไข: ส่งไฟล์ให้ผู้ให้บริการแอนตี้ไวรัสวิเคราะห์ ลงนามดิจิทัลในโค้ดโดยใช้ผู้ออกใบรับรอง และกำหนดข้อยกเว้นเฉพาะโฟลเดอร์ชั่วคราวแทนการปิดแอนตี้ไวรัส