วัตถุประสงค์ของการทดสอบประกาศนียบัตรนักวิเคราะห์ความปลอดภัยทางไซเบอร์ (CySA+)

รหัสข้อสอบ: CS0-002

CompTIA

เกี่ยวกับข้อสอบ

ผู้สมัครสอบสามารถใช้เอกสารฉบับนี้เพื่อช่วยเตรียมความพร้อมสำหรับข้อสอบการทดสอบประกาศนียบัตรนักวิเคราะห์ความปลอดภัยทางไซเบอร์ CompTIA (CySA+) CS0-002 ด้วยเป้าหมายสุดท้ายในการปกป้องเชิงรุกและปรับปรุงความปลอดภัยขององค์กรอย่างต่อเนื่อง CySA + จะตรวจสอบว่าผู้สมัครที่ประสบความสำเร็จมีความรู้และทักษะที่จำเป็นในการ:

- ใช้ประโยชน์จากข้อมูลข่าวกรองและเทคนิคการตรวจจับภัยคุกคาม
- วิเคราะห์และตีความข้อมูล
- ระบุและแก้ไขช่องโหว่
- แนะนำมาตรการป้องกัน
- ตอบสนองและกอบกู้จากเหตุการณ์ได้อย่างมีประสิทธิภาพ

ซึ่งเทียบเท่ากับประสบการณ์ 4 ปีในตำแหน่งงานด้านการรักษาความปลอดภัยทางอินเทอร์เน็ตด้านเทคนิค

ตัวอย่างเนื้อหาเหล่านี้ให้ไว้เพื่ออธิบายวัตถุประสงค์เท่านั้น ไม่ใช่รายการหัวข้อเนื้อหาทั้งหมดของข้อสอบชุดนี้

การพัฒนาข้อสอบ

ข้อสอบ CompTIA เป็นผลจากการประชุมเชิงปฏิบัติการของผู้เชี่ยวชาญในหัวข้อเนื้อหาที่สำคัญ และผลสำรวจเกี่ยวกับทักษะและความรู้ที่จำเป็นสำหรับผู้ประกอบวิชาชีพด้าน IT ระดับที่จำเป็นในอุตสาหกรรม

นโยบายการใช้เนื้อหาที่ได้รับอนุญาตของ COMPTIA

CompTIA Certifications, LLC ไม่มีส่วนเกี่ยวข้องกับและไม่ได้อนุญาต สนับสนุน หรือยอมให้มีการใช้เนื้อหาใดที่จัดหาให้โดยเว็บไซต์การฝึกอบรมภายนอกที่ไม่ได้รับอนุญาต (brain dump) ผู้ที่ใช้เนื้อหาดังกล่าวเพื่อเตรียมความพร้อมสำหรับการสอบ CompTIA ใด ๆ จะถูกเพิกถอนประกาศนียบัตรของตนและระงับการทดสอบในอนาคต ตามข้อตกลงผู้สมัครสอบ CompTIA ด้วยความพยายามที่จะสื่อสารนโยบายการสอบว่าด้วยเนื้อหาการเรียนรู้ที่ไม่ได้รับอนุญาตของ CompTIA ให้ชัดเจนยิ่งขึ้น CompTIA จึงแนะนำให้ผู้สมัครสอบประกาศนียบัตรทุกท่านไปที่นโยบายการสอบประกาศนียบัตร CompTIA โปรดทบทวนนโยบายทั้งหมดของ CompTIA ก่อนที่จะเริ่มต้นกระบวนการเรียนรู้สำหรับการสอบ CompTIA ใด ๆ ผู้สมัครสอบจะต้องปฏิบัติตามข้อตกลงผู้สมัครสอบ CompTIA หากผู้สมัครสอบมีคำถามเกี่ยวกับเนื้อหาการเรียนรู้ที่ถือว่าไม่ได้รับอนุญาต (หรือที่เรียกว่า “brain dumps”) ผู้สมัครสอบควรติดต่อ CompTIA ที่ examsecurity@comptia.org เพื่อตรวจสอบยืนยัน

โปรดทราบ

รายการตัวอย่างที่ให้ไว้ในสัญลักษณ์แสดงหัวข้อย่อยเป็นเพียงรายการคร่าว ๆ ตัวอย่างเทคโนโลยี กระบวนการ หรืองานอื่นที่สัมพันธ์กับวัตถุประสงค์แต่ละข้ออาจรวมอยู่ในข้อสอบ แม้ว่าจะไม่ได้อยู่ในรายการหรือถูกกล่าวถึงในเอกสารวัตถุประสงค์ฉบับนี้ก็ตาม CompTIA ได้ทำการทบทวนเนื้อหาข้อสอบและปรับปรุงคำถามในข้อสอบอย่างต่อเนื่อง เพื่อให้ข้อสอบของเราเป็นปัจจุบันและเพื่อรักษาความปลอดภัยในการเก็บรักษาคำถามให้เป็นความลับ ในกรณีที่จำเป็น เราจะจัดทำข้อสอบฉบับปรับปรุงโดยอ้างอิงจากจุดประสงค์ของข้อสอบ โปรดทราบว่าสื่อเตรียมสอบทั้งหมดที่เกี่ยวข้องจะยังคงสามารถใช้ได้อยู่

รายละเอียดการทดสอบ

รหัสข้อสอบ	CS0-002
จำนวนคำถาม	ขั้นต่ำ 85 ข้อ
ประเภทคำถาม	ข้อสอบแบบเลือกตอบและแบบประเมินการปฏิบัติงาน
ระยะเวลาการทดสอบ	165 นาที
ประสบการณ์ที่แนะนำ	• ประสบการณ์ 4 ปีในตำแหน่งงานด้านเทคนิคการรักษาความปลอดภัยไซเบอร์ • ความปลอดภัย + และเครือข่าย + หรือความรู้และประสบการณ์เทียบเท่า
คะแนนที่ให้ผ่าน	750

วัตถุประสงค์การสอบ (ขอบเขต)

ตารางด้านล่างแสดงขอบเขตการวัดผลของข้อสอบชุดนี้และสัดส่วนการให้คะแนน

ขอบเขต	อัตราส่วนร้อยของข้อสอบ
1.0 การจัดการภัยคุกคามและช่องโหว่	22%
2.0 ความปลอดภัยของซอฟต์แวร์และระบบ	18%
3.0 การดำเนินการและการตรวจสอบความปลอดภัย	25%
4.0 การตอบสนองต่อเหตุการณ์	22%
5.0 การปฏิบัติตามและการประเมิน	13%
รวม	**100%**

1.0 การจัดการภัยคุกคามและช่องโหว่

1.1 อธิบายความสำคัญของข้อมูลภัยคุกคามและข่าวกรอง

- **แหล่งข่าวกรอง**
  - ข่าวกรองแบบโอเพนซอร์ส
  - ข่าวกรองที่เป็นกรรมสิทธิ์ / ปิดแหล่งที่มา
  - ไทม์ไลน์
  - ความเกี่ยวข้อง
  - ความแม่นยำ
- **ระดับความลับ**
- **การจัดการตัวบ่งชี้**
  - นิพจน์ข้อมูลภัยคุกคามแบบมีโครงสร้าง (STIX)
  - บริการแลกเปลี่ยนข้อมูลสัญญาณบ่งชี้อัตโนมัติที่เชื่อถือได้ (TAXII)
  - OpenIoC
- **การจำแนกภัยคุกคาม**
  - ภัยคุกคามที่เป็นที่รู้จักกับภัยคุกคามที่ไม่รู้จัก
  - ช่องโหว่ของซอฟต์แวร์ที่ผู้พัฒนาซอฟต์แวร์ยังไม่ค้นพบ (zero-day)
  - ภัยคุกคามแบบถาวรขั้นสูง (APT)
- **ตัวภัยคุกคาม**
  - ระดับชาติ
  - แฮกเกอร์นักเคลื่อนไหว
  - ขบวนการอาชญากรรม
  - ภัยคุกคามที่เกิดขึ้นภายในองค์กร
    - จงใจ
    - ไม่จงใจ
- **วงรอบข่าวกรอง**
  - ข้อกำหนด
  - การรวบรวมข้อมูล
  - การวิเคราะห์
  - การเผยแพร่
  - ผลตอบรับ
- **มัลแวร์โจมตีแบบเน้นปริมาณ**
- **การแบ่งปันและวิเคราะห์ข้อมูล**
  - สาธารณสุข
  - สถาบันการเงิน
  - สายการบิน
  - หน่วยงานรัฐบาล
  - โครงสร้างพื้นฐานสำคัญ

1.2 กำหนดสถานการณ์สมมติ ให้ใช้ข่าวกรองทางภัยคุกคามเพื่อสนับสนุนความปลอดภัยขององค์กร

- **แนวทางการโจมตี**
  - MITRE ATT&CK
  - การวิเคราะห์การบุกรุกแบบไดมอนด์โมเดล
  - Kill chain
- **การวิจัยภัยคุกคาม**
  - ด้านชื่อเสียง
  - ด้านพฤติกรรม
  - สัญญาณบ่งชี้การบุกรุก (IoC)
  - ระบบการให้คะแนนช่องโหว่ที่พบได้บ่อย (CVSS)
- **วิธีการสร้างแบบจำลองภัยคุกคาม**
  - ความสามารถของฝ่ายตรงข้าม
  - พื้นผิวการโจมตีทั้งหมด
  - เวกเตอร์โจมตี
  - ผลกระทบ
  - ความเป็นไปได้
- **การแบ่งปันข่าวกรองภัยคุกคามพร้อมฟังก์ชั่นที่รองรับ**
  - การตอบสนองต่อเหตุการณ์
  - การจัดการช่องโหว่
  - การจัดการความเสี่ยง
  - วิศวกรรมความปลอดภัย
  - การตรวจจับและการตรวจสอบ

1.3 กำหนดสถานการณ์สมมติ ให้ดำเนินกิจกรรมการจัดการช่องโหว่

- **การระบุช่องโหว่**
  - ความสำคัญของสินทรัพย์
  - การสแกนเชิงรุกกับเชิงรับ
  - การทำแผนที่ / การระบุแจกแจง
- **การตรวจสอบความถูกต้อง**
  - True positive
  - False positive
  - True negative
  - False negative
- **การแก้ไข / บรรเทาผลกระทบ**
  - พื้นฐานการกำหนดค่า
  - การใช้แพทช์
  - การทำให้แข็งแกร่ง
  - การควบคุมแบบชดเชย
  - การยอมรับความเสี่ยง
  - การตรวจสอบการบรรเทาลง
- **เกณฑ์และพารามิเตอร์ในการสแกน**
  - ความเสี่ยงที่เกี่ยวข้องกับกิจกรรมการสแกน
  - ฟีดข้อมูลช่องโหว่
  - ขอบเขต
  - มีข้อมูลสิทธิ์เข้าระบบและไม่มีข้อมูลสิทธิ์เข้าระบบ
  - ใช้เซิร์ฟเวอร์เทียบกับเอเจนต์
  - ภายในและภายนอก
  - การพิจารณาเป็นพิเศษ
    - ชนิดของข้อมูล
    - ข้อจำกัดเชิงเทคนิค
    - เวิร์กโฟลว์ (Workflow)
    - ระดับความอ่อนไหว
    - ข้อกำหนดด้านกฎระเบียบ
    - การแบ่งส่วน
    - ระบบป้องกันการบุกรุก (IPS) ระบบตรวจจับการบุกรุก (IDS) และการตั้งค่าไฟร์วอลล์
- **อุปสรรคขัดขวางการแก้ไข**
  - บันทึกความเข้าใจ (MOU)
  - สัญญาระดับการบริการ (SLA)
  - การกำกับดูแลองค์กร
  - การหยุดชะงักของกระบวนการทางธุรกิจ
  - ลดฟังก์ชันการทำงาน
  - ระบบเก่า
  - ระบบเฉพาะ

1.4 กำหนดสถานการณ์สมมติ ให้วิเคราะห์ผลลัพธ์จากเครื่องมือประเมินช่องโหว่แบบทั่วไป

- **ตัวสแกนเว็บแอปพลิเคชัน**
  - OWASP Zed Attack Proxy (ZAP)
  - Burp suite
  - Nikto
  - Arachni
- **เครื่องมือสแกนช่องโหว่โครงสร้างพื้นฐาน**
  - Nessus
  - OpenVAS
  - Qualys
- **เครื่องมือและเทคนิคการประเมินซอฟต์แวร์**
  - การวิเคราะห์โค้ดคงที่
  - การวิเคราะห์โค้ดแบบไดนามิก
  - วิศวกรรมย้อนกลับ
  - Fuzzing
- **การระบุแจงแจง**
  - Nmap
  - hping
  - เชิงรุกกับเชิงรับ
  - ตัวตอบสนอง
- **เครื่องมือการประเมินแบบไร้สาย**
  - Aircrack-ng
  - Reaver
  - oclHashcat
- **เครื่องมือประเมินโครงสร้างพื้นฐานระบบคลาวด์**
  - ScoutSuite
  - Prowler
  - Pacu

1.5 อธิบายถึงภัยคุกคามและช่องโหว่ที่เกี่ยวข้องกับเทคโนโลยีเฉพาะทาง

- **มือถือ**
- **อินเทอร์เน็ตของสรรพสิ่ง (IoT)**
- **แบบฝังตัว**
- **ระบบปฏิบัติการแบบเรียลไทม์ (RTOS)**
- **ระบบบนชิป (SoC)**
- **อุปกรณ์ลอจิกแบบโปรแกรมได้ (FPGA)**
- **การควบคุมการเข้าถึงทางกายภาพ**
- **ระบบควบคุมอาคารอัตโนมัติ**
- **ยานพาหนะและอากาศยานไร้คนขับ**
  - CAN bus
- **เวิร์กโฟลว์และระบบอัตโนมัติของกระบวนการ**
- **ระบบควบคุมอุตสาหกรรม**
- **Supervisory controls and data acquisition (SCADA)**
  - Modbus

1.6 อธิบายถึงภัยคุกคามและช่องโหว่ที่เกี่ยวข้องกับการทำงานบนระบบคลาวด์

- **รูปแบบบริการระบบคลาวด์**
  - การให้บริการซอฟต์แวร์ (SaaS)
  - การให้บริการแพลตฟอร์ม (PaaS)
  - การให้บริการโครงสร้างพื้นฐาน (IaaS)
- **โมเดลการปรับใช้ระบบคลาวด์**
  - สาธารณะ (Public)
  - ส่วนตัว (Private)
  - ชุมชน (Community)
  - ลูกผสม (Hybrid)
- **การให้บริการตามฟังก์ชั่น (FaaS) / สถาปัตยกรรมไร้เซิร์ฟเวอร์**
- **โครงสร้างพื้นฐานเป็นโค้ด (IaC)**
- **ส่วนต่อประสานโปรแกรมประยุกต์ไม่ปลอดภัย (API)**
- **การบริหารจัดการกุญแจไม่เหมาะสม**
- **พื้นที่เก็บข้อมูลที่ไม่ได้รับการป้องกัน**
- **การบันทึกและการตรวจสอบ**
  - การบันทึกและการตรวจสอบไม่เพียงพอ
  - ไม่มีความสามารถเข้าถึงข้อมูลได้

1.7 กำหนดสถานการณ์สมมติ ให้ดำเนินการควบคุมเพื่อลดการจู่โจมและช่องโหว่ของซอฟต์แวร์

- **ประเภทการโจมตี**
  - การโจมตีภาษามาร์กอัปขยายได้ (XML)
  - การฉีดภาษามาตรฐานในการเข้าถึงฐานข้อมูล (SQL)
  - Overflow attack
    - Buffer
    - Integer
    - Heap
  - โค้ดโจมตีแบบคำสั่งระยะไกล
  - การเข้าถึงผ่านไดเรกทอรี
  - การยกระดับสิทธิ์
  - การโจมตีหลายบัญชีด้วยรหัสผ่านที่คนมักใช้
  - ภัยจากการใช้รหัสผ่านซ้ำ
  - การปลอมตัวเป็นผู้อื่น
  - การที่มีผู้ไม่หวังดีเข้ามาแทรกกลางในการสนทนา (man-in-the-middle)
  - Session hijacking
  - Rootkit
  - Cross-site scripting
    - Reflected
    - Persistent
    - Document object model (DOM)
- **ช่องโหว่**
  - การจัดการข้อความผิดพลาดไม่ดีพอ
  - การดำเนินการทางอ้อม ทำงานกับตัวแปร
  - การอ้างอิงวัตถุที่ไม่ปลอดภัย
  - Race condition
  - ช่องโหว่เกิดขึ้นจากฟังกชั่นระบบการพิสูจน์ตัวตน
  - ช่องโหว่ที่เกิดขึ้นกับข้อมูลเป็นหลัก
  - ส่วนประกอบที่ไม่ปลอดภัย
  - การบันทึกและการตรวจสอบไม่เพียงพอ
  - การตั้งค่าโดยใช้ค่าเริ่มต้นหรือค่าอ่อนแอ
  - การใช้ฟังก์ชันที่ไม่ปลอดภัย
    - ฟังก์ชัน strcpy

2.0 ความปลอดภัยของซอฟต์แวร์และระบบ

2.1 กำหนดสถานการณ์สมมติ ให้ใช้โซลูชันด้านความปลอดภัยสำหรับการจัดการโครงสร้างพื้นฐาน

- **ระบบคลาวด์กับในองค์กร**
- **การจัดการสินทรัพย์**
  - แท็กสินทรัพย์
- **การแบ่งส่วน**
  - กายภาพ
  - แบบเสมือน
  - จั๊มป๊อกซ์
  - การแยกระบบ
    - การเว้นช่องว่าง
- **สถาปัตยกรรมเครือข่าย**
  - กายภาพ
  - ที่กำหนดโดยซอฟต์แวร์
  - คลาวด์เสมือนส่วนตัว (VPC)
  - เครือข่ายเสมือนส่วนตัว (VPN)
  - ไร้เซิร์ฟเวอร์
- **การจัดการการเปลี่ยนแปลง**
- **ระบบเสมือน**
  - โครงสร้างเดสก์ท็อปเสมือน (VDI)
- **การรันในคอนเทนเนอร์**
- **การจัดการข้อมูลประจำตัวและการเข้าถึง**
  - การจัดการระดับสิทธิ์
  - การพิสูจน์ตัวตนแบบหลายปัจจัย
  - ล็อกอินครั้งเดียวเข้าได้ทุกระบบ (SSO)
  - Federation
  - การเข้าถึงตามบทบาทหน้าที่
  - การเข้าถึงตามคุณลักษณะ
  - แบบบังคับ
  - การตรวจสอบด้วยตนเอง
- **ตัวแทนรักษาความปลอดภัยการเข้าถึงระบบคลาวด์ (CASB)**
- **Honeypot**
- **การตรวจสอบและการบันทึก**
- **การเข้ารหัสลับ**
- **การจัดการใบรับรอง**
- **การป้องกันเชิงรุก**

2.2 อธิบายแนวทางปฏิบัติที่ดีที่สุดในการรับประกันซอฟต์แวร์

- **แพลตฟอร์ม**
  - มือถือ
  - แอปพลิเคชันบนเว็บ
  - ไคลเอ็นท์/เซิร์ฟเวอร์
  - แบบฝังตัว
  - ระบบบนชิป (SoC)
  - เฟิร์มแวร์
- **วัฏจักรการพัฒนาซอฟต์แวร์ (SDLC) แบบบูรณาการ**
- **ทีม DevSecOps**
- **วิธีการประเมินซอฟต์แวร์**
  - การทดสอบการยอมรับของผู้ใช้
  - การใช้งานแบบทดสอบความเครียด
  - การทดสอบโปรแกรมที่มีการแก้ไขด้านความปลอดภัย
  - การตรวจสอบโค้ด
- **แนวทางปฏิบัติที่ดีที่สุดในการเข้ารหัสอย่างปลอดภัย**
  - การตรวจสอบอินพุต
  - การเข้ารหัสเอาต์พุต
  - การจัดการเซสชัน
  - การพิสูจน์ตัวตน
  - การป้องกันข้อมูล
  - Parameterized queries
- **การทดสอบการวิเคราะห์โค้ดคงที่**
- **การทดสอบการวิเคราะห์แบบไดนามิก**
- **วิธีการตรวจสอบอย่างเป็นทางการของซอฟต์แวร์ที่สำคัญ**
- **สถาปัตยกรรมที่มุ่งเน้นบริการ**
  - ภาษามาร์คอัปเพื่อยืนยันความปลอดภัย (SAML)
  - Simple Object Access Protocol (SOAP)
  - Representational State Transfer (REST)
  - ไมโครเซอร์วิส

2.3 อธิบายแนวทางปฏิบัติที่ดีที่สุดในการรับประกันฮาร์ดแวร์

- **เพิ่มระบบรักษาความปลอดภัยที่ระดับของฮาร์ดแวร์**
  - โมดูลแพลตฟอร์มที่เชื่อถือได้ (TPM)
  - โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM)
- **eFuse**
- **ส่วนต่อประสานเฟิร์มแวร์ Unified ที่ขยายได้ (UEFI)**
- **โปรแกรมซัพพลายเออร์ที่น่าเชื่อถือ**
- **การประมวลผลที่ปลอดภัย**
  - การดำเนินการที่เชื่อถือได้
  - Secure enclave
  - ส่วนขยายความปลอดภัยของโปรเซสเซอร์
  - การดำเนินการแบบอะตอมมิค
- **ป้องกันการงัดแงะ**
- **ไดรฟ์เข้ารหัสตัวเอง**
- **อัปเดตเฟิร์มแวร์ที่เชื่อถือได้**
- **การบูตและการพิสูจน์ที่วัดได้**
- **การเข้ารหัสบัส**

3.0 การดำเนินการและการตรวจสอบความปลอดภัย

3.1 กำหนดสถานการณ์สมมติ ให้วิเคราะห์ข้อมูลเป็นส่วนหนึ่งของกิจกรรมการตรวจสอบความปลอดภัย

- **ฮิวริสติก**
- **การวิเคราะห์แนวโน้ม**
- **Endpoint**
  - มัลแวร์
    - วิศวกรรมย้อนกลับ
  - หน่วยความจำ
  - พฤติกรรมการใช้งานแอปพลิเคชันและระบบ
    - พฤติกรรมที่เป็นที่รู้จักดี
    - พฤติกรรมผิดปกติ
    - Exploit techniques
  - ระบบไฟล์
  - การวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี (UEBA)
- **เครือข่าย**
  - Uniform Resource Locator และการวิเคราะห์ระบบชื่อโดเมน (DNS)
    - อัลกอริทึมการสร้างโดเมน
  - วิเคราะห์กระแสงาน
  - การวิเคราะห์แพ็คเก็ตและโปรโตคอล
    - มัลแวร์
- **ตรวจสอบบันทึก**
  - บันทึกตามเหตุการณ์
  - Syslog
  - บันทึกไฟร์วอล์
  - ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน
  - พรอกซี
  - ระบบตรวจจับการบุกรุก / ระบบป้องกันการบุกรุก
- **การวิเคราะห์ผลกระทบ**
  - ผลกระทบต่อองค์กรกับผลกระทบตามท้องถิ่น
  - ทันทีกับทั้งหมด
- **การตรวจสอบข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (SIEM)**
  - การเขียนกฎ
  - โปรโตคอลอินเตอร์เน็ตมีชื่อเสียงไม่ดี (IP)
  - แดชบอร์ด
- **Query string**
  - การค้นหาในสตริง
  - สคริป
  - Piping
- **การวิเคราะห์อีเมล**
  - การกระทำที่เป็นอันตราย
  - การเพิ่มลายเซ็นดิจิทัลที่ส่วนหัวของอีเมล
  - วิธีการตรวจสอบสิทธิ์อีเมลมาตรฐาน (DMARC)
  - วิธีการตรวจสอบอีเมลจากผู้ส่งจริง (SPF)
  - ฟิชชิง
  - การส่งต่อ
  - ลายเซ็นดิจิทัล
  - รูปแบบการตั้งค่าลายเซ็น
  - ลิงก์แบบฝังตัว
  - การปลอมตัวเป็นผู้อื่น
  - ส่วนหัว

3.2 กำหนดสถานการณ์สมมติ ให้ใช้การเปลี่ยนแปลงการกำหนดค่ากับการควบคุมที่มีอยู่เพื่อปรับปรุงความปลอดภัย

- **สิทธิ์การเข้าถึง**
- **อนุญาตพิเศษ**
- **การขึ้นบัญชีดำ**
- **ไฟร์วอลล์**
- **กฎของระบบป้องกันการบุกรุก (IPS)**
- **การป้องกันการสูญหายของข้อมูล (DLP)**
- **การตรวจจับและตอบสนองปลายทาง (EDR)**
- **การควบคุมการเข้าถึงเครือข่าย (NAC)**
- **Sinkholing**
- **ลายเซ็นมัลแวร์**
  - การพัฒนา / การเขียนกฎ
- **Sandboxing**
- **การรักษาความปลอดภัยพอร์ต**

3.3 อธิบายความสำคัญของการไล่ล่าจากภัยคุมคามเชิงรุก

- สร้างสมมติฐาน
- รวบรวมรายละเอียดรายชื่อผู้กระทำและกิจกรรมการคุกคาม
- กลวิธีไล่ล่าภัยคุกคาม
  - การวิเคราะห์กระบวนการปฏิบัติการ
- ลดพื้นที่ผิวการโจมตี
- การรวมสินทรัพย์ที่สำคัญ
- เวกเตอร์โจมตี
- ปัญญาบูรณาการ
- การปรับปรุงความสามารถในการตรวจจับ

3.4 เปรียบเทียบและหาข้อแตกต่างระหว่างแนวคิดและเทคโนโลยีระบบอัตโนมัติ

- การจัดระเบียบเวิร์กโฟลว์
  - การทำงานของระบบความปลอดภัยให้ราบรื่น ทำงานแบบอัตโนมัติ เพิ่มความเร็วในการตอบสนองต่อเหตุการณ์ภัยไซเบอร์ (SOAR)
- การทำสคริปต์
- การบูรณาการส่วนต่อประสานโปรแกรมประยุกต์ (API)
- การสร้างลายเซ็นมัลแวร์อัตโนมัติ
- การเพิ่มคุณค่าข้อมูล
- หน้าฟีดภัยคุกคามโดยรวม
- แมชชีนเลิร์นนิ่ง
- การใช้โปรโตคอลอัตโนมัติและมาตรฐาน
  - Security Content Automation Protocol (SCAP)
- การบูรณาการแบบต่อเนื่อง
- การปรับใช้งาน / ส่งมอบแบบต่อเนื่อง

4.0 การตอบสนองต่อเหตุการณ์

4.1 อธิบายความสำคัญของกระบวนการตอบสนองต่อเหตุการณ์

- **แผนการสื่อสาร**
  - การจำกัดการสื่อสารกับฝ่ายที่เชื่อถือได้
  - การเปิดเผยข้อมูลตามกฎข้อบังคับ / ข้อกำหนดทางกฎหมาย
  - ป้องกันการเผยแพร่ข้อมูลโดยไม่ตั้งใจ
  - ใช้วิธีการที่ปลอดภัยในการสื่อสาร
  - ข้อกำหนดการรายงาน
- **การประสานงานการตอบรับกับหน่วยงานที่เกี่ยวข้อง**
  - ฝ่ายกฎหมาย
  - ฝ่ายทรัพยากรมนุษย์
  - ฝ่ายประชาสัมพันธ์
  - ภายในและภายนอก
  - การบังคับใช้ทางกฎหมาย
  - ผู้นำระดับสูง
  - หน่วยงานกำกับดูแล
- **ปัจจัยที่เอื้อต่อความสำคัญของข้อมูล**
  - ข้อมูลที่ระบุตัวบุคคลได้ (PII)
  - ข้อมูลสุขภาพส่วนบุคคล (PHI)
  - ข้อมูลส่วนตัวที่ละเอียดอ่อน (SPI)
  - ทรัพย์สินมูลค่าสูง
  - ข้อมูลการเงิน
  - ทรัพย์สินทางปัญญา
  - ข้อมูลขององค์กร

4.2 กำหนดสถานการณ์สมมติให้ใช้ขั้นตอนการตอบสนองต่อเหตุการณ์ที่เหมาะสม

- **การเตรียมการ**
  - การอบรม
  - การทดสอบ
  - ขั้นตอนเอกสาร
- **การตรวจจับและการวิเคราะห์**
  - ลักษณะที่เอื้อต่อการจำแนกระดับความรุนแรง
  - ระยะเวลาหยุดชะงัก
  - เวลาการกู้คืน
  - ความสมบูรณ์ของข้อมูล
  - สภาพเศรษฐกิจ
  - ความสำคัญของกระบวนการของระบบ
  - วิศวกรรมย้อนกลับ
  - ความสัมพันธ์ของข้อมูล
- **การควบคุม**
  - การแบ่งส่วน
  - การแยก
- **การกำจัดและการกู้คืน**
  - การลดบรรเทาช่องโหว่
  - การทำลายข้อมูล
  - การจัดโครงสร้าง/การรีอิมเมจ
  - การกำจัดอย่างปลอดภัย
  - การใช้แพทช์
  - การกู้คืนสิทธิ์
  - การรื้อฟื้นทรัพยากร
  - การฟื้นฟูความสามารถและบริการ
  - การตรวจสอบการบันทึก / การสื่อสารไปยังการตรวจสอบความปลอดภัย
- **กิจกรรมหลังเกิดเหตุการณ์**
  - การเก็บรักษาหลักฐาน
  - รายงานบทเรียนที่เรียนรู้
  - เปลี่ยนแปลงกระบวนการควบคุม
  - อัปเดตแผนการตอบสนองต่อเหตุการณ์
  - รายงานสรุปเหตุการณ์
  - การสร้าง IoC
  - การตรวจสอบ

4.3 พิจารณาเหตุการณ์สมมติ ให้วิเคราะห์ตัวบ่งชี้ที่เป็นไปได้ของการบุกรุก

- **เกี่ยวข้องกับเครือข่าย**
  - การใช้แบนด์วิดท์
  - สัญญาณเตือน
  - การสื่อสารแบบเพียร์ทูเพียร์ที่ผิดปกติ
  - อุปกรณ์แปลกปลอมบนเครือข่าย
  - สแกน /sweep
  - ปริมาณการจราจรที่เพิ่มขึ้นอย่างผิดปกติ
  - โปรโตคอลทั่วไปมีมากกว่าพอร์ตที่ไม่ได้มาตรฐาน
- **เกี่ยวกับโฮสต์**
  - การใช้ทรัพยากรโปรเซสเซอร์
  - การใช้ทรัพยากรหน่วยความจำ
  - การใช้ทรัพยากรความจุของไดรฟ์
  - ซอฟต์แวร์ที่ไม่ได้รับอนุญาต
  - กระบวนการที่เป็นอันตราย
  - การเปลี่ยนแปลงที่ไม่ได้รับอนุญาต
  - การขอสิทธิ์ที่ไม่ได้รับอนุญาต
  - การแอบดึงข้อมูล
  - ลักษณะการทำงานของกระบวนการใน OS ที่ผิดปกติ
  - ระบบไฟล์มีการเปลี่ยนแปลงหรือผิดปกติ
  - การเปลี่ยนแปลงหรือความผิดปกติในรีจิสทรี
  - กำหนดตั้งเวลาทำงานที่ไม่ได้รับอนุญาต
- **เกี่ยวกับแอปพลิเคชั่น**
  - กิจกรรมที่ผิดปกติ
  - การเริ่มต้นบัญชีใหม่
  - ผลลัพธ์ที่ไม่คาดคิด
  - การติดต่อสื่อสารกับขาออกแบบไม่คาดคิด
  - บริการขัดข้อง
  - บันทึกแอปพลิเคชัน

4.4 กำหนดสถานการณ์สมมติใช้เทคนิคพื้นฐานทางนิติวิทยาศาสตร์ดิจิทัล

- **เครือข่าย**
  - Wireshark
  - tcpdump
- **Endpoint**
  - ดิสก์
  - หน่วยความจำ
- **มือถือ**
- **คลาวด์**
- **ระบบเสมือน**
- **การระงับทางกฎหมาย**
- **ขั้นตอน**
- **การแฮช**
  - การเปลี่ยนแปลงไบนารี
- **การแกะและแจกแจงข้อมูล**
- **การรวบรวมข้อมูล**

5.0 การปฏิบัติตามและการประเมิน

5.1 เข้าใจถึงความสำคัญของความเป็นส่วนตัวและการปกป้องข้อมูล

- **ความเป็นส่วนตัวกับความปลอดภัย**
- **การควบคุมที่ไม่ใช่ทางเทคนิค**
  - การจัดประเภท
  - ความเป็นเจ้าของ
  - การเก็บรักษา
  - ชนิดข้อมูล
  - มาตรฐานการเก็บรักษา
  - การเก็บรักษาความลับ
  - ข้อกำหนดทางกฎหมาย
  - อธิปไตยด้านข้อมูล
  - การจัดเก็บข้อมูลเฉพาะที่จำเป็น
  - ข้อจำกัดเชิงวัตถุประสงค์
  - ข้อตกลงไม่เปิดเผย (NDA)
- **การควบคุมเชิงเทคนิค**
  - การเข้ารหัสลับ
  - การป้องกันการสูญหายของข้อมูล (DLP)
  - การปกปิดข้อมูล
  - การยกเลิกการระบุตัวตน
  - การทำโทเค็น
  - การจัดการสิทธิ์ดิจิทัล (DRM)
    - ลายน้ำดิจิทัล
  - ข้อกำหนดการเข้าถึงทางภูมิศาสตร์
  - การควบคุมการเข้าถึง

5.2 กำหนดสถานการณ์สมมติ ใช้แนวคิดด้านความปลอดภัยเพื่อสนับสนุนการลดความเสี่ยงขององค์กร

- **การวิเคราะห์ผลกระทบทางธุรกิจ**
- **กระบวนการระบุความเสี่ยง**
- **การคำนวณความเสี่ยง**
  - ความน่าจะเป็นไปได้
  - มิติ
- **การสื่อสารปัจจัยเสี่ยง**
- **การจัดลำดับความเสี่ยง**
  - การควบคุมความปลอดภัย
  - จุดสมดุลเชิงวิศวกรรม
- **การประเมินระบบ**
- **การควบคุมที่มาทดแทนเอกสาร**
- **การฝึกอบรมและการฝึกซ้อม**
  - Red team
  - Blue team
  - White team
  - การฝึกซ้อมแผนบนโต๊ะ
- **การประเมินระบบห่วงโซ่อุปทาน**
  - การสอบทานธุรกิจกับผู้ขาย
  - การยืนยันตัวตนของฮาร์ดแวร์ต้นฉบับ

5.3 อธิบายความสำคัญของกรอบนโยบาย ขั้นตอนและการควบคุม

- **กรอบการทำงาน**
  - ขึ้นอยู่กับความเสี่ยง
  - มีสิทธิ์เป็นเจ้าของตามกฎหมาย
- **นโยบายและขั้นตอน**
  - จรรยาบรรณ/จริยธรรม
  - นโยบายการใช้งานที่ยอมรับได้ (AUP)
  - นโยบายรหัสผ่าน
  - ความเป็นเจ้าของข้อมูล
  - การเก็บรักษาข้อมูล
  - การจัดการบัญชี
  - การตรวจสอบอย่างต่อเนื่อง
  - การเก็บรักษาชิ้นงาน
- **ประเภทการควบคุม**
  - ระดับการจัดการ
  - ระดับดำเนินการ
  - ระดับทางเทคนิค
  - ระดับป้องกัน
  - ระดับตรวจจับ
  - ระดับตอบสนอง
  - ระดับแก้ไข
- **การตรวจสอบและการประเมิน**
  - ตามข้อกำหนด
  - การปฏิบัติตาม

รายการคำย่อของนักวิเคราะห์ความปลอดภัยทางไซเบอร์ CompTIA (CySA+)

รายการต่อไปนี้คืออักษรย่อที่ปรากฏในข้อสอบ CompTIA CySA+ ผู้สมัครสอบควรทบทวนรายการทั้งหมดและศึกษาหาความรู้ในการปฏิบัติงานเกี่ยวกับอักษรย่อทั้งหมดเพื่อการเตรียมความพร้อมสำหรับการสอบที่ครอบคลุม

คำย่อ	คำเต็ม
3DES	Triple Data Encryption Algorithm
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
BEC	Business Email Compromise
BYOD	Bring Your Own Device
CA	Certificate Authority
CAN	Controller Area Network
CASB	Cloud Access Security Broker
CI/CD	Continuous Integration/Continuous Delivery
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPU	Central Processing Unit
CRM	Customer Relations Management
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DGA	Domain Generation Algorithm
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOM	Document Object Model
DRM	Digital Rights Management
EDR	Endpoint Detection and Response

คำย่อ	คำเต็ม
ELK	Elasticsearch, Logstash, Kibana
ERP	Enterprise Resource Planning
FaaS	Function as a Service
FPGA	Field-programmable Gate Array
FTK	Forensic Toolkit
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MaaS	Monitoring as a Service
MAC	Mandatory Access Control
MD5	Message Digest 5
MDM	Mobile Device Management
MFA	Multifactor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRTG	Multi Router Traffic Grapher
NAC	Network Access Control
NAS	Network-attached Storage

คำย่อ	คำเต็ม
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OSSIM	Open Source Security Information Management
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Pluggable Authentication Module
PCAP	Packet Capture
PCI	Payment Card Industry
PHI	Personal Health Information
PID	Process Identification Number
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-in User Service
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RTOS	Real-time Operating System
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDLC	Software Development Life Cycle
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMB	Server Message Block
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SoC	System on Chip
SPF	Sender Policy Framework
SPI	Sensitive Personal Information
SQL	Structured Query Language
SSH	Secure Shell
SSHD	Solid-state Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
TACACS+	Terminal Access Controller Access Control System Plus
TAXII	Trusted Automated eXchange of Intelligence Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-site Scripting
ZAP	Zed Attack Proxy

รายการฮาร์ดแวร์และซอฟต์แวร์ที่มีการเสนอสำหรับข้อสอบ CySA+

CompTIA แนบตัวอย่างรายการฮาร์ดแวร์และซอฟต์แวร์มาในที่นี้เพื่อช่วยเหลือผู้สมัครสอบในการเตรียมตัวสอบ CySA+ รายการนี้อาจมีประโยชน์ต่อบริษัทฝึกอบรมที่ต้องการสร้างองค์ประกอบห้องปฏิบัติการสำหรับจัดการฝึกอบรม รายการย่อยในแต่ละหัวข้อเป็นเพียงตัวอย่างโดยคร่าวเท่านั้นและไม่ครบสมบูรณ์

ฮาร์ดแวร์ต้านไอที

- เวิร์กสเตชัน (หรือแล็ปท็อป) ด้วยความสามารถในการเรียกใช้ VM
- สวิตช์ประเภท managed
- ไฟร์วอลล์
- อุปกรณ์เคลื่อนที่
- โทรศัพท์ระบบ VoIP
- WAP
- ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก
- อุปกรณ์ IoT
- เซิร์ฟเวอร์

ซอฟต์แวร์

- อิมเมจ VM สำหรับเป้าหมายการโจมตี
- วินโดว์เซิร์ฟเวอร์
- วินโดว์ไคลเอนต์
  - Commando VM
- Linux
  - Kali
  - ParrotOS
  - Security Onion
- Chrome OS
- อุปกรณ์ UTM
- pfSense
- เมทาสปลอยต์
- เข้าถึงอินสแตนซ์ระบบคลาวด์
  - Azure
  - AWS
  - GCP
- SIEM
  - Graylog
  - ELK
  - Splunk
- เครื่องสแกนช่องโหว่
  - OpenVAS
  - Nessus

พิมพ์ในสหรัฐอเมริกา 06692-มิถุนายน2562