วัตถุประสงค์ของ CompTIA Security+ Certification Exam

รหัสข้อสอบ: SY0-601

CompTIA

เกี่ยวกับข้อสอบ

ผู้สมัครสอบสามารถใช้เอกสารฉบับนี้เพื่อช่วยเตรียมความพร้อมสำหรับข้อสอบ CompTIA Security+ (SY0-601) ข้อสอบ CompTIA Security+ จะรับรองว่าผู้สมัครซึ่งสอบผ่านมีความรู้และทักษะที่จำเป็นในการ:

- **ประเมินสถานะด้านการรักษาความปลอดภัย (security posture) ของสภาพแวดล้อมองค์กร แนะนำและใช้โซลูชันการรักษาความปลอดภัยที่เหมาะสม**
- **เฝ้าติดตามและรักษาความปลอดภัยของสภาพแวดล้อมแบบไฮบริด ซึ่งรวมถึงระบบกลุ่มเมฆ อุปกรณ์เคลื่อนที่ และ IoT**
- **ปฏิบัติงานโดยมีความตระหนักถึงกฎหมายและนโยบายที่บังคับใช้ ซึ่งรวมถึงหลักการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อบังคับ**
- **ระบุ วิเคราะห์ และตอบสนองต่อเหตุการณ์และอุบัติเหตุด้านการรักษาความปลอดภัย**

ข้อสอบนี้เทียบเท่ากับประสบการณ์การทำงานจริงสองปีในบทบาทหน้าที่ผู้ดูแลระบบ/ผู้ดูแลระบบการรักษาความปลอดภัย

ตัวอย่างเนื้อหาเหล่านี้ให้ไว้เพื่ออธิบายวัตถุประสงค์เท่านั้น ไม่ใช่รายการหัวข้อเนื้อหาทั้งหมดของข้อสอบชุดนี้

การพัฒนาข้อสอบ

ข้อสอบ CompTIA เป็นผลจากการประชุมเชิงปฏิบัติการของผู้เชี่ยวชาญในหัวข้อเนื้อหาที่สำคัญ และผลสำรวจเกี่ยวกับทักษะและความรู้ที่จำเป็นสำหรับผู้ประกอบวิชาชีพด้าน IT ในอุตสาหกรรม

นโยบายการใช้เนื้อหาที่ได้รับอนุญาตของ CompTIA

CompTIA Certifications, LLC ไม่มีส่วนเกี่ยวข้องกับและไม่ได้อนุญาต สนับสนุน หรือยอมให้มีการใช้เนื้อหาใดที่จัดหาให้โดยเว็บไซต์การฝึกอบรมภายนอกที่ไม่ได้รับอนุญาต (brain dump) ผู้ที่ใช้เนื้อหาดังกล่าวเพื่อเตรียมความพร้อมสำหรับการสอบ CompTIA ใด ๆ จะถูกเพิกถอนประกาศนียบัตรของตนและระงับการทดสอบในอนาคต ตามข้อตกลงผู้สมัครสอบ CompTIA ด้วยความพยายามที่จะสื่อสารนโยบายการสอบว่าด้วยเนื้อหาการเรียนรู้ที่ไม่ได้รับอนุญาตของ CompTIA ให้ชัดเจนยิ่งขึ้น CompTIA จึงแนะนำให้ผู้สมัครสอบประกาศนียบัตรทุกท่านไปที่**นโยบายการสอบประกาศนียบัตร CompTIA** โปรดทบทวนนโยบายทั้งหมดของ CompTIA ก่อนที่จะเริ่มต้นกระบวนการเรียนรู้สำหรับการสอบ CompTIA ใด ๆ ผู้สมัครสอบจะต้องปฏิบัติตาม**ข้อตกลงผู้สมัครสอบ 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

ข้อสอบที่จำเป็น	SY0-601
จำนวนคำถาม	สูงสุด 90 ข้อ
ประเภทคำถาม	ข้อสอบแบบเลือกตอบและอ้างอิงตามผลการดำเนินงาน
ระยะเวลาการทดสอบ	90 นาที
ประสบการณ์ที่แนะนำ	• ประสบการณ์การทำงานอย่างน้อย 2 ปีในการดูแลระบบไอทีโดยมุ่งเน้นด้านการรักษาความปลอดภัย • ประสบการณ์จริงในการรักษาความปลอดภัยของข้อมูลเทคนิค • มีความรู้กว้างขวางเกี่ยวกับแนวคิดด้านการรักษาความปลอดภัย
คะแนนที่ให้ผ่าน	750 (ในระดับคะแนน 100-900)

วัตถุประสงค์การสอบ (ขอบเขต)

ตารางด้านล่างแสดงขอบเขตการวัดผลของข้อสอบชุดนี้และสัดส่วนการให้คะแนน

ขอบเขต	อัตราส่วนร้อยละของข้อสอบ
1.0 การโจมตี ภัยคุกคาม และช่องโหว่	24%
2.0 สถาปัตยกรรมและการออกแบบ	21%
3.0 การใช้งาน	25%
4.0 การปฏิบัติงานและการตอบสนองต่อเหตุการณ์	16%
5.0 การกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อบังคับ	14%
รวม	**100%**

1.0 การโจมตี ภัยคุกคาม และช่องโหว่

1.1 เปรียบเทียบข้อเหมือนและต่างของเทคนิควิศวกรรมสังคมประเภทต่าง ๆ

- ฟิชชิง **(phishing)**
- สมิชชิง **(smishing)**
- วิชชิง **(vishing)**
- สแปม **(spam)**
- สแปมผ่านข้อความโต้ตอบแบบทันที **(SPIM)**
- สเปียร์ฟิชชิง **(spear phishing)**
- การค้นข้อมูลจากถังขยะ **(dumpster diving)**
- การแอบดูข้อมูลโดยยืนข้างหลังมองข้ามไหล่ **(shoulder surfing)**
- ฟาร์มมิ่ง **(pharming)**
- การลักลอบเข้าพื้นที่โดยไม่ได้รับอนุญาต **(tailgating)**
- การขอข้อมูล **(eliciting information)**
- เวลลิง **(whaling)**
- การแนบสคริปต์ไว้ด้านหน้า **(prepending)**
- การฉ้อโกงข้อมูลเอกลักษณ์บุคคล **(identity fraud)**
- การหลอกลวงใบแจ้งหนี้ **(invoice scam)**
- การรวบรวมข้อมูลประจำตัว **(credential harvesting)**
- การลาดตระเวน **(reconnaissance)**
- ข่าวไวรัสหลอกลวง **(hoax)**
- การปลอมตัวเป็นผู้อื่น **(impersonation)**
- การโจมตีหลุมรดน้ำ **(watering-hole attack)**
- การจดชื่อโดเมนทีมีการสะกดคล้ายคลึงกับชื่อเว็บเป้าหมาย **(typosquatting)**
- การแอบอ้างตนเป็นผู้มีความน่าเชื่อถือ **(pretexting)**
- แคมเปญอิทธิพล **(influence campaign)**
  - สงครามลูกผสม (hybrid warfare)
  - สื่อสังคม
- หลักการ **(เหตุผลเพื่อประสิทธิผล)**
  - อำนาจหน้าที่
  - การข่มขู่
  - ความเห็นพ้องต้องกัน
  - ความขาดแคลน
  - ความคุ้นเคย
  - ความเชื่อมั่น
  - ความเร่งด่วน

1.2 วิเคราะห์สัญญาณบ่งชี้ที่เป็นไปได้เพื่อระบุประเภทการโจมตีตามสถานการณ์สมมติ

- มัลแวร์
  - ไวรัสเรียกค่าไถ่ (ransomware)
  - โทรจัน
  - เวิร์ม
  - โปรแกรมที่อาจไม่จำเป็นบนเครื่อง (PUP)
  - ไวรัสแบบไร้ไฟล์
  - บัญชาการและควบคุม
  - บอท
  - คริปโตมัลแวร์
  - ระเบิดตรรกะ (logic bomb)
  - สปายแวร์
  - ตัวบันทึกการพิมพ์ (keylogger)
  - โทรจันการเข้าถึงระยะไกล (RAT)
  - รูทคิท
  - ประตูหลัง
- การโจมตีรหัสผ่าน
  - การโจมตีหลายบัญชีด้วยรหัสผ่านที่คนมักใช้ (spraying)
  - พจนานุกรม
  - การสุ่มรหัสผ่าน
    - ออฟไลน์
    - ออนไลน์
  - Rainbow table
  - ข้อความธรรมดา/ไม่เข้ารหัส
- การโจมตีทางกายภาพ
  - สายเคเบิล Universal Serial Bus (USB) ที่ประสงค์ร้าย
  - แฟลชไดรฟ์ที่ประสงค์ร้าย
  - การโคลนการ์ด (card cloning)
  - การสกิม (skimming)
- ปัญญาประดิษฐ์ **(AI)** ที่เป็นปรปักษ์
  - ข้อมูลการฝึกอบรมที่มีมลทินเพื่อการเรียนรู้ของเครื่อง (ML)
  - ความปลอดภัยของอัลกอริทึมการเรียนรู้ของเครื่อง
- การโจมตีห่วงโซ่อุปทาน
- การโจมตีบนระบบกลุ่มเมฆเทียบกับระบบที่ตั้งอยู่ในบริษัท
- การโจมตีเข้ารหัสลับ
  - วันเกิด
  - การชน
  - การดาวน์เกรด

1.3 วิเคราะห์สัญญาณบ่งชี้ที่เกี่ยวข้องกับการโจมตีแอปพลิเคชันตามสถานการณ์สมมติ

- การยกระดับสิทธิ์ **(privilege escalation)**
- การส่งสคริปต์ข้ามเว็บไซต์ **(cross-site scripting)**
- การฉีด **(injection)**
  - Structured query language (SQL)
  - Dynamic-link library (DLL)
  - Lightweight Directory Access Protocol (LDAP)
  - Extensible Markup Language (XML)
- ตัวชี้/การคล้อยตามของวัตถุ **(object deference)**
- การเข้าถึงผ่านไดเรกทอรี **(directory traversal)**
- การอ้างอิงข้อมูลเกินขอบเขตที่กำหนด **(buffer overflow)**
- สภาวะการแข่งขัน **(race condition)**
  - เวลาการตรวจสอบ/เวลาที่ใช้
- การจัดการข้อผิดพลาด
- การจัดการข้อมูลนำเข้าไม่เหมาะสม
- การโจมตีแบบทำซ้ำ **(replay attack)**
  - การทำซ้ำเซสชัน (Session replay)
- การเก็บค่าลงในตัวแปรเกินค่าสูงสุดที่กำหนด **(integer overflow)**
- การปลอมแปลงคำขอ **(request forgeries)**
  - ฝั่งเซิร์ฟเวอร์
  - ข้ามเว็บไซต์
- การโจมตี **Application programming interface (API)**
- การใช้ทรัพยากรหมดไป **(resource exhaustion)**
- หน่วยความจำรั่ว **(memory leak)**
- การถอด **Secure Sockets Layer (SSL)**
- การจัดการไดรเวอร์ **(driver manipulation)**
  - ชิมมิง (shimming)
  - รีแฟกเตอริง (refactoring)
- การใช้รหัสผ่านที่ถูกแฮชไว้โดยไม่ต้องแกะรหัสแฮช **(pass-the-hash)**

1.4 วิเคราะห์สัญญาณบ่งชี้ที่เกี่ยวข้องกับการโจมตีเครือข่ายตามสถานการณ์สมมติ

- แบบไร้สาย
  - การปล่อยสัญญาณปลอม (evil twin)
  - อุปกรณ์กระจายสัญญาณหลอกลวง (rogue access point)
  - การเชื่อมต่อโดยไม่ได้รับอนุญาตผ่านทางบลูทูธ (bluesnarfing)
  - บลูแจ็กกิง (bluejacking)
  - การแยกออก (disassociation)
  - แจมมิง (jamming)
  - การระบุความถี่วิทยุ (RFID)
  - การสื่อสารสนามใกล้ (NFC)
  - เวกเตอร์เริ่มต้น (IV)
- การโจมตีบนเส้นทาง (ก่อนหน้านี้เรียกว่าการที่มีผู้ไม่หวังดีเข้ามาแทรกกลางในการสนทนา **(man-in-the-middle)**/การที่มีโทรจันที่ฝังตัวอยู่คอยแก้ไขหน้าเว็บไซต์ **(man-in-the-browser)**
- การโจมตีชั้น 2
  - การปลอมแปลง Address Resolution Protocol (ARP)
  - การส่ง MAC Address ปลอดออกไปจำนวนมาก ๆ (MAC flooding)
  - การโคลน MAC (MAC cloning)
- ระบบโดเมนเนม (DNS)
  - การขโมยโดเมนเนม (domain hijacking)
  - การปลอมแปลง DNS (DNS poisoning)
  - การเปลี่ยนเส้นทาง Uniform Resource Locator (URL)
  - ชื่อเสียงของโดเมน (domain reputation)
- การปฏิเสธการให้บริการแบบกระจาย (DDoS)
  - เครือข่าย
  - แอปพลิเคชัน
  - เทคโนโลยีการปฏิบัติงาน (OT)
- การใช้โค้ดหรือสคริปต์ที่ประสงค์ร้าย
  - PowerShell
  - Python
  - Bash
  - Macros
  - Visual Basic for Applications (VBA)

1.5 อธิบายตัวภัยคุกคาม (threat actor) เส้นทางภัยคุกคาม (vector) และแหล่งข่าวกรองต่าง ๆ

- **ตัวภัยคุกคาม (actor) และเส้นทางภัยคุกคาม (vector)**
  - ภัยคุกคามแบบถาวรขั้นสูง (advanced persistent threat, APT)
  - ภัยคุกคามที่เกิดขึ้นจากภายในองค์กร (insider threat)
  - ตัวภัยคุกคามที่มีรัฐเป็นผู้ให้การสนับสนุน (state actor)
  - แฮกเกอร์นักเคลื่อนไหว (hacktivist)
  - Script kiddies
  - ขบวนการอาชญากรรม
  - แฮกเกอร์
    - ได้รับอนุญาต
    - ไม่ได้รับอนุญาต
    - กึ่งได้รับอนุญาต
  - Shadow IT
  - คู่แข่ง
- **ลักษณะของตัวภัยคุกคาม**
  - ภายใน/ภายนอก
  - ระดับความซับซ้อน/ความสามารถ
  - ทรัพยากร/เงินทุน
  - ความมุ่งหมาย/แรงจูงใต
- **เส้นทางภัยคุกคาม**
  - การเข้าถึงโดยตรง
  - แบบไร้สาย
  - อีเมล
  - ห่วงโซ่อุปทาน
  - สื่อสังคม
  - สื่อที่ถอดออกได้
  - ระบบกลุ่มเมฆ
- **แหล่งข่าวกรองภัยคุกคาม (threat intelligence sources)**
  - ข่าวกรองแบบโอเพ่นซอร์ส (open-source intelligence, OSINT)
  - แบบปิด/มีกรรมสิทธิ์
  - ฐานข้อมูลช่องโหว่ (vulnerability database)
  - ข้อมูลสาธารณะ/ส่วนตัว - ศูนย์แบ่งปันข้อมูล
  - ดาร์กเว็บ
  - สัญญาณบ่งชี้การละเมิด
  - การแบ่งปันสัญญาณบ่งชี้อัตโนมัติ (automated indicator sharing, AIS)
  - นิพจน์ข้อมูลภัยคุกคามแบบมีโครงสร้าง (Structured Threat Information eXpression, STIX)/บริการแลกเปลี่ยนข้อมูลสัญญาณบ่งชี้อัตโนมัติที่เชื่อถือได้ (Trusted Automated eXchange of Intelligence Information, TAXII)
  - การวิเคราะห์คาดการณ์
  - แผนที่ภัยคุกคาม
  - ที่เก็บไฟล์/โค้ด
- **แหล่งการค้นคว้า**
  - เว็บไซต์ของผู้จำหน่าย
  - ฟีดข้อมูลช่องโหว่ (vulnerability feed)
  - งานประชุม
  - วารสารทางวิชาการ
  - คำขอความคิดเห็น (request for comments, RFC)
  - กลุ่มอุตสาหกรรมในพื้นที่
  - สื่อสังคม
  - ฟีดข้อมูลภัยคุกคาม
  - ยุทธวิธี เทคนิค และขั้นตอน (TTP) การโจมตี

1.6 อธิบายข้อกังวลด้านการรักษาความปลอดภัยที่เกี่ยวข้องกับช่องโหว่ประเภทต่าง ๆ

- **ช่องโหว่บนระบบกลุ่มเมฆเทียบกับระบบที่ตั้งอยู่ในบริษัท**
- **ช่องโหว่ของซอฟต์แวร์ที่ผู้พัฒนาซอฟต์แวร์ยังไม่ค้นพบ (zero-day)**
- **การกำหนดค่าที่ไม่มีประสิทธิภาพ**
  - การอนุญาตแบบเปิด (open permission)
  - บัญชีรากที่ไม่ปลอดภัย (unsecure root account)
  - ข้อผิดพลาด
  - การเข้ารหัสที่ไม่ดี (weak encryption)
  - โพรโทคอลที่ไม่ปลอดภัย (unsecure protocol)
  - การตั้งค่าเริ่มต้น
  - พอร์ตและบริการที่เปิดอยู่
- **ความเสี่ยงจากภายนอก**
  - การจัดการผู้ให้บริการ
    - การรวมระบบ
    - การขาดการสนับสนุนจากผู้ให้บริการ
  - ห่วงโซ่อุปทาน
  - การพัฒนาโค้ดที่จัดจ้างหน่วยงานภายนอก
  - การจัดเก็บข้อมูล
- **การจัดการที่ไม่เหมาะสมหรือไม่มีประสิทธิภาพ**
  - เฟิร์มแวร์
  - ระบบปฏิบัติการ (OS)
  - แอปพลิเคชัน
- **แพลตฟอร์มรุ่นเก่า (legacy)**
- **ผลกระทบ**
  - การสูญเสียข้อมูล
  - การละเมิดข้อมูล
  - การแอบดึงข้อมูล (data exfiltration)
  - การโจรกรรมเอกลักษณ์บุคคล (identity theft)
  - การเงิน
  - ชื่อเสียง
  - การสูญเสียความพร้อมใช้

1.7 สรุปเทคนิคที่ใช้ในการประเมินการรักษาความปลอดภัย

- การตรวจหาภัยคุกคามเชิงรุก **(threat hunting)**
  - การรวมข่าวกรอง (intelligence fusion)
  - ฟีดข้อมูลภัยคุกคาม
  - คำแนะนำ (advisory) และรายงานเผยแพร่ (bulletin)
  - Maneuver
- การสแกนช่องโหว่
  - ผลบวกลวง
  - ผลลบลวง
  - การทบทวนบันทึก
  - มีข้อมูลประจำตัว (credentialed) กับไม่มีข้อมูลประจำตัว (non-credentialed)
  - บุกรุก (intrusive) กับไม่บุกรุก (non-intrusive)
  - แอปพลิเคชัน
  - เว็บแอปพลิเคชัน
  - เครือข่าย
  - ช่องโหว่และความเสี่ยงที่พบได้บ่อย (CVE)/ระบบกาให้คะแนนช่องโหว่ที่พบได้บ่อย (CVSS)
  - การทบทวนการกำหนดค่า
- **Syslog/ข้อมูลการรักษาความปลอดภัยและการจัดการกิจกรรม (SIEM)**
  - รายงานการทบทวน
  - การดักจับแพคเก็ต (packet capture)
  - ข้อมูลนำเข้า
  - การวิเคราะห์พฤติกรรมผู้ใช้
  - การวิเคราะห์ความเชื่อมั่น
  - การเฝ้าติดตามการรักษาความปลอดภัย
  - การรวมบันทึก (log aggregation)
  - การรวบรวมบันทึก (log collector)
- **การเชื่อมต่อเทคโนโลยีความปลอดภัยเข้าไว้ด้วยกัน ระบบอัตโนมัติ และการตอบสนอง (SOAR)**

1.8 อธิบายเทคนิคที่ใช้ในการทดสอบเจาะระบบ

- การทดสอบเจาะระบบ
  - สภาพแวดล้อมที่ทราบ
  - สภาพแวดล้อมที่ไม่ทราบ
  - สภาพแวดล้อมที่ทราบบางส่วน
  - กฎการปะทะ
  - การเคลื่อนย้ายทางด้านข้าง (lateral movement)
  - การยกระดับสิทธิ์ (privilege escalation)
  - การคงอยู่ (persistence)
  - การล้าง (cleanup)
  - Bug bounty
  - Pivoting
- การลาดตระเวน **(reconnaissance)** เชิงรับและเชิงรุก
  - โดรน
  - War flying
  - War driving
  - Footprinting
  - OSINT
- ประเภทการฝึกซ้อม
  - ทีมสีแดง
  - ทีมสีน้ำเงิน
  - ทีมสีขาว
  - ทีมสีม่วง

2.0 สถาปัตยกรรมและการออกแบบ

2.1 อธิบายความสำคัญของแนวคิดด้านการรักษาความปลอดภัยในสภาพแวดล้อมองค์กร

- การจัดการการกำหนดค่า
  - แผนภาพ
  - การกำหนดค่าพื้นฐาน
  - แบบแผนการตั้งชื่อมาตรฐาน
  - แบบแผนโพรโทคอลอินเทอร์เน็ต (IP)
- อธิบไตยด้านข้อมูล
- การคุ้มครองข้อมูล
  - การป้องกันการสูญหายของข้อมูล (DLP)
  - การปิดบัง (masking)
  - การเข้ารหัสลับ
  - พักอยู่ (at rest)
  - ระหว่างส่งต่อ/เคลื่อนย้าย
  - ระหว่างประมวลผล
  - การทำโทเค็น (tokenization)
  - การจัดการสิทธิ
- ข้อควรพิจารณาด้านภูมิศาสตร์
- การควบคุมในการรับมือและการกู้คืน
- การตรวจสอบ **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)**
- การ **Hash**
- ข้อควรพิจารณาด้าน **API**
- ความพร้อมรับมือของสถานที่
  - Hot site
  - Cold site
  - Warm site
- การหลอกลวงและการหยุดชะงัก
  - Honeypot
  - Honeyfile
  - Honeynet
  - การได้รับข้อมูลทางไกลปลอม
  - หลุม DNS (DNS sinkhole)

2.2 สรุปแนวคิดเกี่ยวกับระบบเสมือนและการประมวลผลแบบกลุ่มเมฆ

- แบบจำลองระบบกลุ่มเมฆ
  - การให้บริการโครงสร้างพื้นฐาน (IaaS)
  - การให้บริการแพลตฟอร์ม (PaaS)
  - การให้บริการซอฟต์แวร์ (SaaS)
  - การให้บริการครบวงจร (XaaS)
  - สาธารณะ
  - ชุมชน
  - ส่วนตัว
  - ลูกผสม
- ผู้ให้บริการระบบกลุ่มเมฆ
- ผู้ให้บริการที่มีการบริหารจัดการ **(MSP)/** ผู้ให้บริการการรักษาความปลอดภัยที่มีการบริหารจัดการ **(MSSP)**
- ในสถานที่กับนอกสถานที่
- การประมวลผลแบบหมอก **(fog computing)**
- **Edge computing**
- ธินไคลเอ็นต์ **(thin client)**
- คอนเทนเนอร์
- ไมโครเซอร์วิส/API
- โครงสร้างพื้นฐานเป็นโค้ด **(infrastructure as code)**
  - ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (software-defined networking, SDN)
  - การมองเห็นที่กำหนดโดยซอฟต์แวร์ (software-defined visibility, SDV)
- สถาปัตยกรรมไร้เซิร์ฟเวอร์
- การรวมบริการ
- นโยบายทรัพยากร
- **Transit gateway**
- ระบบเสมือน
  - การหลีกเลี่ยงการมีเครื่องเสมือน (VM) จำนวน (VM sprawl)
  - การป้องกันการหลบหนี VM (VM escape)

2.3 สรุปแนวคิดเกี่ยวกับการพัฒนาแอปพลิเคชันที่ปลอดภัย การใช้งาน และการทำงานอัตโนมัติ

- สภาพแวดล้อม
  - การพัฒนา
  - การทดสอบ
  - การทดสอบก่อนเอาขึ้นใช้งานจริง (staging)
  - การผลิต
  - การประกันคุณภาพ (QA)
- การเตรียมใช้งาน **(provisioning)** และการยกเลิกการเตรียมใช้งาน **(deprovisioning)**
- การวัดความสมบูรณ์
- เทคนิคการเขียนโค้ดอย่างปลอดภัย
  - การจัดให้อยู่ในรูปแบบบรรทัดฐาน (normalization)
  - ขั้นตอนที่จัดเก็บไว้ (stored procedures)
  - การทำให้สับสน (obfuscation)/การพรางตัว (camouflage)
  - การนำโค้ดกลับมาใช้ใหม่ (code reuse)/โค้ดที่ไม่ได้นำไปใช้งาน (dead code)
  - การใช้งานและการตรวจสอบฝั่งเซิร์ฟเวอร์กับฝั่งไคลเอ็นต์
  - การจัดการหน่วยความจำ
  - การใช้ไลบรารีของบุคคลภายนอกและชุดพัฒนาซอฟต์แวร์ (SDK)
  - การเปิดเผยข้อมูล (data exposure)
- โครงการความปลอดภัยของเว็บแอปพลิเคชันแบบเปิด **(Open Web Application Security Project, OWASP)**
- ความหลากหลายของซอฟต์แวร์ **(software diversity)**
  - คอมไพเลอร์ (compiler)
  - ฐานสอง (binary)
- ระบบอัตโนมัติ/การเขียนสคริปต์
  - การดำเนินการโดยอัตโนมัติ
  - การติดตามอย่างต่อเนื่อง
  - การตรวจสอบอย่างต่อเนื่อง
  - การรวมอย่างต่อเนื่อง
  - การส่งมอบอย่างต่อเนื่อง
  - การปรับใช้อย่างต่อเนื่อง
- ความยืดหยุ่น
- ความสามารถในการปรับขนาด **(scalability)**
- การควบคุมเวอร์ชัน

2.4 สรุปแนวคิดการออกแบบการตรวจสอบสิทธิ์และการอนุญาต

- วิธีการตรวจสอบสิทธิ์
  - บริการไดเรกทอรี
  - การติดต่อกับภายนอก (Federation)
  - การพิสูจน์ (attestation)
  - เทคโนโลยี
    - รหัสผ่านแบบใช้ครั้งเดียวที่อิงตามเวลา (TOTP)
    - รหัสผ่านแบบใช้ครั้งเดียวที่อิงตาม HMAC (HOTP)
    - บริการข้อความสั้น (SMS)
    - คีย์โทเค็น
    - โค้ดคงที่ (static code)
    - แอปพลิเคชันการตรวจสอบสิทธิ์
    - การแจ้งเตือนแบบพุช
    - โทรศัพท์
  - การตรวจสอบสิทธิ์ด้วยสมาร์ทการ์ด
- ชีวมาตร
  - ลายนิ้วมือ
  - จอตา
  - ม่านตา
  - ใบหน้า
  - เสียง
  - เส้นเลือดดำ
  - การวิเคราะห์ท่าเดิน
  - อัตราประสิทธิผล (efficacy rate)
  - การอนุญาตผิดพลาด (false acceptance)
  - การปฏิเสธผิดพลาด (false rejection)
  - อัตราความผิดพลาดทั้งหมด (crossover error rate)
- ระดับหรือคุณลักษณะของการตรวจสอบตัวตนแบบหลายขั้นตอน **(MFA)**
  - ระดับ
    - สิ่งที่คุณทราบ
    - สิ่งที่คุณมี
    - สิ่งที่คุณเป็น
  - คุณลักษณะ
    - สถานที่ที่คุณอยู่
    - สิ่งที่คุณสามารถทำได้
    - สิ่งที่คุณแสดงออก
    - คนที่คุณรู้จัก
- การตรวจสอบสิทธิ์ การอนุญาต และการบัญชี **(AAA)**
- ข้อกำหนดบนระบบกลุ่มเมฆเทียบกับที่ตั้งอยู่ในบริษัท

2.5 ใช้การเตรียมพร้อมรับมือด้านความปลอดภัยทางไซเบอร์ (cybersecurity resilience) ตามสถานการณ์สมมติ

- ความซ้ำซ้อน **(redundancy)**
  - การกระจายทางภูมิศาสตร์
  - ดิสก์
    - ระดับของ redundant array of inexpensive disks (RAID)
    - หลายเส้นทาง (multipath)
  - เครือข่าย
    - เครื่องกระจายโหลด (load balancer)
    - การทำงานร่วมกันของ Network interface card (NIC)
  - พลังงาน
    - ระบบกำลังไฟฟ้าต่อเนื่อง (uninterruptible power supply)
    - เครื่องกำเนิดไฟฟ้า
    - แหล่งจ่ายไฟสองแหล่ง
    - อุปกรณ์ควบคุมและแจกจ่ายกระแสไฟฟ้าแบบมีการจัดการ (Managed power distribution unit, PDU)
- การทำซ้ำ
  - Storage Area Network
  - VM
- ในสถานที่กับระบบกลุ่มเมฆ
- ประเภทการสำรองข้อมูล
  - ทั้งหมด (full)
  - เฉพาะส่วนที่เพิ่มขึ้นมา (incremental)
  - Snapshot
  - ส่วนที่มีการเปลี่ยนแปลงหรือเพิ่มเข้ามาใหม่ (differential)
  - เทป
  - ดิสก์
  - สำเนา
  - ที่จัดเก็บผ่านเครือข่าย (Network-attached storage, NAS)
  - Storage Area Network
  - ระบบกลุ่มเมฆ
  - อิมเมจ
  - ออนไลน์เทียบกับออฟไลน์
  - ที่จัดเก็บนอกสถานที่
    - ข้อควรพิจารณาเกี่ยวกับระยะทาง
- แบบไม่คงอยู่ **(non-persistence)**
  - ย้อนกลับไปเป็นสถานะที่ทราบ
  - การกำหนดค่าล่าสุดที่ทราบว่าใช้ได้ (last known-good configuration)
  - สื่อการบูตแบบไลฟ์ (live boot media)
- ความพร้อมใช้สูง
  - ความสามารถในการปรับขนาด (scalability)
- ลำดับการคืนค่า
- ความหลากหลาย
  - เทคโนโลยี
  - ผู้ให้บริการ
  - คริปโต
  - การควบคุม

2.6 อธิบายผลกระทบด้านการรักษาความปลอดภัยจากระบบฝังตัวและระบบเฉพาะทาง

- ระบบฝังตัว **(embedded system)**
  - Raspberry Pi
  - อาร์เรย์ของเกตแบบตั้งโปรแกรมด้วยเขตข้อมูลได้ (FPGA)
  - Arduino
- การควบคุมตรวจตราและการได้มาซึ่งข้อมูล **(SCADA)**/ระบบการควบคุมของอุตสาหกรรม **(ICS)**
  - โรงงาน
  - อุตสาหกรรม
  - การผลิต
  - พลังงาน
  - โลจิสติกส์
- อินเทอร์เน็ตในทุกสรรพสิ่ง **(IoT)**
  - เซนเซอร์
  - อุปกรณ์แบบสมาร์ท
  - อุปกรณ์ที่สวมใส่ได้
  - ระบบอัตโนมัติของโรงงาน
  - ค่าเริ่มต้นที่ไม่ดี
- เฉพาะทาง
  - ระบบทางการแพทย์
  - ยานพาหนะ
  - เครื่องบิน
  - มิเตอร์แบบสมาร์ท
- เสียงผ่าน IP **(VoIP)**
- การทำความร้อน ระบายอากาศ และปรับอากาศ **(HVAC)**
- โดรน
- เครื่องพิมพ์มัลติฟังก์ชัน **(MFP)**
- ระบบปฏิบัติการในเวลาจริง **(RTOS)**
- ระบบตรวจตรา
- ระบบบนชิป **(SoC)**
- ข้อควรพิจารณาด้านการสื่อสาร
  - 5G
  - แถบความถี่แคบ (narrow-band)
  - วิทยุเบสแบนด์ (Baseband radio)
  - การ์ด subscriber identity module (SIM)
  - Zigbee
- ข้อจำกัด
  - พลังงาน
  - คำนวณ
  - เครือข่าย
  - คริปโต
  - การไม่สามารถแพทช์ได้
  - การตรวจสอบสิทธิ์
  - ช่วง
  - ต้นทุน
  - ทรัสต์โดยปริยาย

2.7 อธิบายความสำคัญของการควบคุมการรักษาความปลอดภัยทางกายภาพ

- เสากั้น/รั้ว
- ห้องโถงที่มีการควบคุมการเข้าถึง
- การติดเครื่องหมาย
- ระบบแจ้งเหตุ
- ป้าย
- กล้อง
  - การรับรู้การเคลื่อนไหว
  - การตรวจจับวัตถุ
- กล้องวงจรปิด (CCTV)
- การพรางตัวทางอุตสาหกรรม
- บุคลากร
  - ยาม
  - หุ่นยนต์รักษาการณ์
  - แผนกต้อนรับ
  - ความสมบูรณ์/การควบคุมด้วยคนสองคน
- ล็อก
  - ชีวมาตร
  - อิเล็กทรอนิกส์
  - กายภาพ
  - การล็อกสายเคเบิล
- USB บล็อกข้อมูล (USB data blocker)
- แสงสว่าง
- รั้ว
- ระบบควบคุมเพลิง
- เซนเซอร์
  - การตรวจจับการเคลื่อนไหว
  - การตรวจจับเสียง
  - ตัวอ่านบัตรทาบสำหรับเปิดปิด (Proximity reader)
  - การตรวจจับความชื้น
  - บัตร
  - อุณหภูมิ
- โดรน
- บันทึกผู้เยี่ยมชม
- กรงฟาราเดย์ (Faraday cage)
- การเว้นช่องว่าง (air gap)
- Screened subnet (ก่อนหน้านี้เรียกว่า demilitarized zone)
- การกระจายสายเคเบิลที่ได้รับการป้องกัน
- พื้นที่ที่มีการรักษาความปลอดภัย
  - การเว้นช่องว่าง (air gap)
  - ตู้นิรภัย
  - ตู้เซฟ
  - ห้องกักลมร้อน
  - ห้องกักลมเย็น
- การทำลายข้อมูลอย่างปลอดภัย
  - การเผา
  - การใช้เครื่องทำลายเอกสาร
  - การทำเยื่อ (pulping)
  - การบด (pulverizing)
  - การใช้สนามแม่เหล็ก (degaussing)
  - โซลูชันของบุคคลภายนอก

2.8 สรุปพื้นฐานแนวคิดเกี่ยวกับรหัสลับ (cryptographic)

- ลายเซ็นดิจิทัล
- ความยาวของคีย์
- การยืดความยาวของคีย์ (key stretching)
- การ Salt
- การ Hash
- การแลกเปลี่ยนคีย์
- การเข้ารหัสแบบวงรีรูปไข่ (elliptic-curve cryptography)
- การรักษาความปลอดภัยในอนาคต (perfect forward secrecy)
- เชิงควอนตัม
  - การสื่อสาร
  - การคำนวณ
- หลังควอนตัม (post-quantum)
- ชั่วคราว (Ephemeral)
- โหมดการทำงาน
  - มีการตรวจสอบสิทธิ์
  - ไม่มีการตรวจสอบสิทธิ์
  - เคาน์เตอร์
- บล็อกเชน (blockchain)
  - บัญชีสาธารณะ
- Cipher suite
  - สตรีม
  - บล็อก
- สมมาตรกับอสมมาตร
- การเข้ารหัสแบบเบา (lightweight cryptography)
- การอำพรางข้อมูล (steganography)
  - เสียง
  - วิดีโอ
  - ภาพ
- การเข้ารหัส Homomorphic
- กรณีการใช้ที่พบบ่อย
  - อุปกรณ์พลังงานต่ำ
  - เวลาแฝงต่ำ
  - ความพร้อมรับมือสูง
  - สนับสนุนการรักษาความลับ
  - สนับสนุนความสมบูรณ์
  - สนับสนุนการทำให้สับสน (obfuscation)
  - สนับสนุนการตรวจสอบสิทธิ์
  - สนับสนุนการห้ามปฏิเสธความรับผิดชอบ (non-repudiation)
- ข้อจำกัด
  - ความเร็ว
  - ขนาด
  - คีย์ไม่มีประสิทธิภาพ
  - เวลา
  - ช่วงชีวิต
  - ความสามารถในการคาดการณ์
  - การนำมาใช้ซ้ำ
  - เอนโทรปี
  - โอเวอร์เฮดในการประมวลผล
  - ข้อจำกัดของทรัพยากรเทียบกับการรักษาความปลอดภัย

3.0 การใช้งาน

3.1 ใช้โพรโทคอลที่ปลอดภัยตามสถานการณ์สมมติ

- โปรโตคอล
  - Domain Name System Security Extensions (DNSSEC)
  - SSH
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-time Transport Protocol (SRTP)
  - Lightweight Directory Access Protocol Over SSL (LDAPS)
  - File Transfer Protocol, Secure (FTPS)
  - SSH File Transfer Protocol (SFTP)
  - Simple Network Management Protocol, เวอร์ชัน 3 (SNMPv3)
  - Hypertext transfer protocol over SSL/TLS (HTTPS)
  - IPSec
    - Authentication header (AH)/ Encapsulating Security Payloads (ESP)
    - Tunnel/transport
  - Post Office Protocol (POP)/ Internet Message Access Protocol (IMAP)
- กรณีการใช้งาน
  - เสียงและวิดีโอ
  - การซิงค์เวลา (time synchronization)
  - อีเมลและเว็บ
  - การถ่ายโอนไฟล์
  - บริการไดเรกทอรี
  - การเข้าถึงระยะไกล
  - กระบวนการใช้ชื่อโดเมนสืบค้น (domain name resolution)
  - การกำหนดเส้นทางและการสวิตช์
  - การแจกจ่ายที่อยู่เครือข่าย (network address allocation)
  - บริการบอกรับเป็นสมาชิก (subscription)

3.2 ใช้โซลูชันด้านการรักษาความปลอดภัยของโฮสต์หรือแอปพลิเคชันตามสถานการณ์สมมติ

- การปกป้องจุดสิ้นสุด
  - โปรแกรมป้องกันไวรัส
  - โปรแกรมป้องกันมัลแวร์
  - การตรวจจับและตอบสนองที่ระดับจุดสิ้นสุด (EDR)
  - DLP
  - ไฟร์วอลล์ยุคถัดไป (NGFW)
  - ระบบป้องกันการบุกรุกแบบโฮสต์เบส (HIPS)
  - ระบบตรวจจับการบุกรุกแบบโฮสต์เบส (HIDS)
  - ไฟร์วอลล์แบบโฮสต์เบส (host-based firewall)
- ความสมบูรณ์ในการบูต
  - ความปลอดภัยในการบูต/Unified Extensible Firmware Interface (UEFI)
  - Measured boot
  - การพิสูจน์การบูต
- ฐานข้อมูล
  - การทำโทเค็น (tokenization)
  - การ Salt
  - การ Hash
- การรักษาความปลอดภัยของแอปพลิเคชัน
  - การตรวจสอบข้อมูลนำเข้า (input validation)
  - คุกกี้ที่ปลอดภัย (secure cookies)
  - ส่วนหัวของ Hypertext Transfer Protocol (HTTP)
  - การเซ็นกำกับโค้ด (code signing)
  - รายการที่อนุญาต (allow list)
  - รายการที่บล็อก/ปฏิเสธ (block list/deny list)
  - หลักปฏิบัติในการเขียนโค้ดอย่างปลอดภัย
  - การวิเคราะห์โค้ดคงที่ (static code)
    - การทบทวนโค้ดโดยผู้ใช้
  - การวิเคราะห์โค้ดแบบไดนามิก (dynamic code)
  - การทดสอบเพื่อหาบั๊ก (fuzzing)
- การเสริมความปลอดภัย **(hardening)**
  - พอร์ตและบริการที่เปิดอยู่
  - รีจิสทรี
  - การเข้ารหัสดิสก์
  - OS
  - การจัดการแพทช์
    - อัปเดตจากบุคคลภายนอก
    - อัปเดตอัตโนมัติ
- ไดร์ฟแบบเข้ารหัสได้เอง **(SED)**/ การเข้ารหัสทั้งดิสก์ **(FDE)**
  - Opal
- ระบบรักษาความปลอดภัยที่ระดับของฮาร์ดแวร์ **(hardware root of trust)**
- **Trusted Platform Module (TPM)**
- **Sandboxing**

3.3 ใช้การออกแบบเครือข่ายที่ปลอดภัยตามสถานการณ์สมมติ

- การกระจายโหลด **(load balancing)**
  - Active/active
  - Active/passive
  - การจัดกำหนดการ
  - Virtual IP
  - การคงอยู่ (persistence)
- การแบ่งส่วนเครือข่าย **(network segmentation)**
  - เครือข่ายท้องถิ่นแบบเสมือน (VLAN)
  - Screened subnet (ก่อนหน้านี้เรียกว่า demilitarized zone)
  - ทราฟฟิกแบบ East-west
  - เอ็กซ์ทราเน็ต
  - อินทราเน็ต
  - Zero Trust
- เครือข่ายส่วนตัวเสมือน **(VPN)**
  - Always-on
  - อุโมงค์แบบแยกกับอุโมงค์แบบเต็ม
  - การเข้าถึงระยะไกลกับจากไซต์ถึงไซต์
  - IPSec
  - SSL/TLS
  - HTML5
  - Layer 2 tunneling protocol (L2TP)
- **DNS**
- การควบคุมการเข้าถึงเครือข่าย **(NAC)**
  - Agent และ Agentless
- การจัดการนอกแบนด์
- การรักษาความปลอดภัยพอร์ต
  - การป้องกันพายุ Broadcast
  - การป้องกัน Bridge Protocol Data Unit (BPDU)
  - การป้องกันลูป
  - การสอดแนม Dynamic Host Configuration Protocol (DHCP)
  - การกรอง Media access control (MAC)
- อุปกรณ์เครือข่าย
  - Jump server
  - เซิร์ฟเวอร์พรอกซี
    - Forward
    - Reverse
  - ระบบตรวจจับการบุกรุกแบบเน็ตเวิร์กเบส (NIDS)/ระบบป้องกันการบุกรุกแบบเน็ตเวิร์กเบส (NIPS)
    - ซิกเนเจอร์เบส
    - ฮิวริสติก/พฤติกรรม
    - สิ่งผิดปกติ
    - อินไลน์กับพาสซีฟ
  - HSM
  - เซนเซอร์
  - ตัวเก็บรวบรวม
  - ตัวรวม
  - ไฟร์วอลล์
    - ไฟร์วอลล์เว็บแอปพลิเคชัน (WAF)
    - NGFW
    - การจดจำสถานะ (stateful)
    - การไม่จดจำสถานะ (stateless)
    - Unified threat management (UTM)
    - เกตเวย์ Network address translation (NAT)
    - เนื้อหา/ตัวกรอง URL
    - โอเพ่นซอร์สและเพื่อการพาณิชย์
    - ฮาร์ดแวร์และซอฟต์แวร์
    - อุปกรณ์และโฮสต์เบสและระบบเสมือน
- รายการควบคุมการเข้าถึง **(ACL)**
- การรักษาความปลอดภัยของเส้นทาง
- คุณภาพการบริการ **(QoS)**
- ความหมายของ **IPv6**
- **Port spanning/port mirroring**
  - Port tap
- บริการเฝ้าติดตาม
- การติดตามความสมบูรณ์ของไฟล์

3.4 ติดตั้งและกำหนดค่าการตั้งค่ารักษาความปลอดภัยระบบไร้สายตามสถานการณ์สมมติ

- โพรโทคอลการเข้ารหัส
  - WiFi Protected Access 2 (WPA2)
  - WiFi Protected Access 3 (WPA3)
  - Counter-mode/CBC-MAC Protocol (CCMP)
  - Simultaneous Authentication of Equals (SAE)
- โพรโทคอลการตรวจสอบสิทธิ์
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Authentication Protocol (PEAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) Federation
- วิธีการ
  - คีย์ที่แจ้งให้ทราบล่วงหน้า (pre-shared key (PSK) กับขององค์กร (Enterprise) กับแบบเปิด (Open)
  - การตั้งค่า WiFi แบบป้องกัน (WiFi Protected Setup, WPS)
  - พอร์ทัลคัดกรอง
- ข้อควรพิจารณาด้านการติดตั้ง
  - การสำรวจสถานที่
  - แผนที่ความร้อน
  - เครื่องวิเคราะห์ WiFi
  - การทับซ้อนของช่อง
  - การจัดวางอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (WAP)
  - ความปลอดภัยของตัวควบคุมและอุปกรณ์กระจายสัญญาณ

3.5 ใช้โซลูชันเคลื่อนที่ที่ปลอดภัยตามสถานการณ์สมมติ

- **วิธีการเชื่อมต่อและตัวรับ**
  - แบบเซลลูลาร์
  - WiFi
  - Bluetooth
  - NFC
  - อินฟราเรด
  - USB
  - จุดต่อจุด (point-to-point)
  - จุดต่อหลายจุด (point-to-multipoint)
  - ระบบการหาตำแหน่งทั่วโลก (GPS)
  - RFID
- **การจัดการอุปกรณ์เคลื่อนที่ (MDM)**
  - การจัดการแอปพลิเคชัน
  - การจัดการเนื้อหา
  - การลบข้อมูลจากระยะไกล (remote wipe)
  - การกำหนดขอบเขตปลอดภัย (geofencing)
  - พิกัดทางภูมิศาสตร์ (geolocation)
  - การล็อกหน้าจอ
  - การแจ้งเตือนแบบพุช
  - รหัสผ่านและ PIN
  - ชีวมาตร
  - การตรวจสอบสิทธิ์ที่คำนึงถึงบริบท
  - การรันในคอนเทนเนอร์ (containerization)
  - การแบ่งส่วนที่จัดเก็บ (storage segmentation)
  - การเข้ารหัสทั้งอุปกรณ์
- **อุปกรณ์เคลื่อนที่**
  - Hardware security module (HSM) ของ MicroSD
  - MDM/Unified Endpoint Management (UEM)
  - การจัดการแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ (MAM)
  - SEAndroid
- **การบังคับใช้และการติดตาม:**
  - ร้านค้าแอปพลิเคชันภายนอก
  - การรูท (rooting)/เจลเบรก (jailbreaking)
  - ไซด์โหลด (sideloading)
  - เฟิร์มแวร์แบบกำหนดเอง
  - การปลดล็อกผู้ให้บริการ (carrier unlocking)
  - การอัปเดตเฟิร์มแวร์ผ่านทางอากาศ (OTA)
  - การใช้งานกล้อง
  - SMS/บริการส่งข้อความมัลติมีเดีย (MMS)/Rich Communication Services (RCS)
  - สื่อภายนอก
  - USB On-The-Go (USB OTG)
  - การบันทึกไมโครโฟน
  - การติดแท็ก GPS
  - WiFi direct/แบบกลุ่มส่วนตัว (ad hoc)
  - แบบการปล่อยสัญญาณ
  - ฮอตสปอต
  - วิธีการชำระเงิน
- **แบบจำลองการปรับใช้**
  - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานเอง (BYOD)
  - การที่บริษัทเป็นเจ้าของอุปกรณ์ที่จะแจกจ่ายให้พนักงานได้เลือกใช้ (COPE)
  - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานโดยบริษัทเป็นผู้กำหนด (CYOD)
  - บริษัทเป็นเจ้าของ
  - โครงสร้างพื้นฐานเดสก์ทอปเสมือนจริง (VDI)

3.6 ใช้โซลูชันความปลอดภัยทางไซเบอร์กับระบบกลุ่มเมฆตามสถานการณ์สมมติ

- **การควบคุมการรักษาความปลอดภัยบนระบบกลุ่มเมฆ**
  - ความพร้อมใช้สูงในหลายโซน
  - นโยบายทรัพยากร
  - การจัดการความลับ
  - การบูรณาการและการตรวจสอบ
  - การจัดเก็บ
    - การอนุญาต
    - การเข้ารหัสลับ
    - การทำซ้ำ
    - ความพร้อมใช้สูง
  - เครือข่าย
    - เครือข่ายเสมือน
    - เครือข่ายย่อยสาธารณะและส่วนตัว
    - การแบ่งส่วน (segmentation)
    - การตรวจสอบและการรวม API
  - คำนวณ
    - กลุ่มการรักษาความปลอดภัย
    - การจัดสรรทรัพยากรแบบไดนามิก
    - ความตระหนักเกี่ยวกับอินสแตนซ์ (instance awareness)
    - จุดสิ้นสุดของ Virtual private cloud (VPC)
    - ความปลอดภัยของคอนเทนเนอร์
- **โซลูชัน**
  - CASB
  - การรักษาความปลอดภัยของแอปพลิเคชัน
  - Secure web gateway (SWG) ยุคใหม่
  - ข้อควรพิจารณาเกี่ยวกับไฟร์วอลล์ในสภาพแวดล้อมบนระบบกลุ่มเมฆ
    - ต้นทุน
    - ความจำเป็นที่ต้องมีการแบ่งส่วน
    - ชั้น Open Systems Interconnection (OSI)
- **การควบคุมดั้งเดิมบนระบบกลุ่มเมฆกับโซลูชันของบุคคลภายนอก**

3.7 ใช้การควบคุมเอกลักษณ์บุคคลและการจัดการบัญชีตามสถานการณ์สมมติ

- ตัวตน
  - ผู้พิสูจน์และยืนยันตัวตน (IdP)
  - คุณลักษณะ
  - ใบรับรอง
  - โทเค็น
  - คีย์ SSH
  - สมาร์ทการ์ด
- ประเภทบัญชี
  - บัญชีผู้ใช้
  - บัญชี/ข้อมูลประจำตัวที่ใช้ร่วมกันและทั่วไป
  - บัญชีผู้เยี่ยมชม
  - บัญชีบริการ
- นโยบายเกี่ยวกับบัญชี
  - ความซับซ้อนของรหัสผ่าน
  - ประวัติรหัสผ่าน
  - การใช้รหัสผ่านซ้ำ
  - ตำแหน่งที่ตั้งของเครือข่าย
  - การกำหนดขอบเขตปลอดภัย (geofencing)
  - การติดแท็กสถานที่ตั้ง (geotagging)
  - พิกัดทางภูมิศาสตร์ (geolocation)
  - การเข้าสู่ระบบที่อิงตามเวลา
  - นโยบายเกี่ยวกับสิทธิเข้าถึง
  - การอนุญาตของบัญชี
  - การตรวจสอบบัญชี
  - เวลาเดินทางที่เป็นไปไม่ได้/การเข้าสู่ระบบที่เสี่ยง
  - การถูกล็อก
  - ความไม่สามารถกระทำการ

3.8 ใช้โซลูชันการตรวจสอบสิทธิ์และการอนุญาตตามสถานการณ์สมมติ

- การจัดการการตรวจสอบสิทธิ์
  - คีย์รหัสผ่าน
  - ที่เก็บรหัสผ่าน
  - TPM
  - HSM
  - การตรวจสอบสิทธิ์ตามข้อมูลที่มี
- การตรวจสอบสิทธิ์/การอนุญาต
  - EAP
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - 802.1X
  - RADIUS
  - การพิสูจน์ตัวตนครั้งเดียว (SSO)
  - Security Assertion Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos
- แผนการควบคุมการเข้าถึง
  - การควบคุมการเข้าถึงตามแอตทริบิวต์ (Attribute-based access control, ABAC)
  - การควบคุมการเข้าถึงตามบทบาทหน้าที่ (role-based access control)
  - การควบคุมการเข้าถึงตามกฎ (rule-based access control)
  - MAC
  - การควบคุมการเข้าถึงแบบมีเงื่อนไข (discretionary access control)
  - การเข้าถึงตามเงื่อนไข (conditional access)
  - การจัดการการเข้าถึงตามสิทธิการใช้งาน (privileged access management)
  - การอนุญาตระบบไฟล์ (filesystem permission)

3.9 ใช้โครงสร้างพื้นฐานกุญแจสาธารณะตามสถานการณ์สมมติ

- โครงสร้างพื้นฐานของคีย์สาธารณะ **(public key infrastructure, PKI)**
  - การจัดการคีย์
  - ผู้ออกใบรับรอง (certificate authority, CA)
  - ใบรับรองกลาง (intermediate CA)
  - เจ้าหน้าที่รับลงทะเบียน (registration authority, RA)
  - ตรายการยกเลิกใบรับรอง (certificate revocation list, CRL)
  - คุณลักษณะของใบรับรอง (certificate attribute)
  - Online Certificate Status Protocol (OCSP)
  - คำขอลงชื่อใบรับรอง (certificate signing request, CSR)
  - CN
  - ใบรับรองชื่อสำรอง (subject alternative name)
  - การหมดอายุ
- ประเภทใบรับรอง
  - Wildcard
  - ใบรับรองชื่อสำรอง (subject alternative name)
  - การเซ็นกำกับโค้ด (code signing)
  - ลงชื่อด้วยตนเอง (self-signed)
  - เครื่อง/คอมพิวเตอร์
  - อีเมล
  - ผู้ใช้
  - ราก
  - Domain validation
  - Extended validation
- รูปแบบใบรับรอง
  - Distinguished encoding rules (DER)
  - Privacy enhanced mail (PEM)
  - Personal information exchange (PFX)
  - .cer
  - P12
  - P7B
- แนวคิด
  - CA ออนไลน์กับออฟไลน์
  - การผูกติด (stapling)
  - การปักหมุด (pinning)
  - แบบจำลองความเชื่อมั่น
  - ระบบฝากกุญแจ (key escrow)
  - สายใบรับรอง (certificate chaining)

4.0 การปฏิบัติงานและการตอบสนองต่อเหตุการณ์

4.1 ใช้เครื่องมือที่เหมาะสมเพื่อประเมินการรักษาความปลอดภัยขององค์กรตามสถานการณ์สมมติ

- การลาดตระเวน **(reconnaissance)** เครือข่ายและการค้นพบ
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - เครื่องสแกน IP
  - arp
  - route
  - curl
  - theHarvester
  - sn1per
  - scanless
  - dnsenum
  - Nessus
  - Cuckoo
- การจัดการไฟล์
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- สภาพแวดล้อมเชลล์และสคริปต์
  - SSH
  - PowerShell
  - Python
  - OpenSSL
- การดักจับแพคเก็ต **(packet capture)** และทำซ้ำ **(replay)**
  - Tcpreplay
  - Tcpdump
  - Wireshark
- การพิสูจน์พยานหลักฐาน
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- โปรแกรมเจาะระบบ **(exploitation framework)**
- โปรแกรมเจาะรหัสผ่าน **(password cracker)**
- การทำลายข้อมูลเพื่อไม่ให้สามารถกู้กลับคืนมาได้ **(data sanitization)**

4.2 สรุปความสำคัญของนโยบาย กระบวนการ และขั้นตอนเพื่อการตอบสนองต่อเหตุการณ์

- แผนการตอบสนองต่อเหตุการณ์
- กระบวนการตอบสนองต่อเหตุการณ์
  - การเตรียมการ (preparation)
  - การระบุ (identification)
  - การควบคุม (containment)
  - การกำจัด (eradication)
  - การกู้คืน (Recovery)
  - การเรียนรู้บทเรียน (lessons learned)
- การฝึกซ้อม
  - การฝึกซ้อมแผนบนโต๊ะ (tabletop)
  - Walkthrough
  - การจำลอง (simulation)
- แนวทางการโจมตี
  - MITRE ATT&CK
  - แบบจำลองการวิเคราะห์การบุกรุกแบบเพชร (Diamond Model of Intrusion Analysis)
  - Cyber Kill Chain
- การจัดการผู้มีส่วนได้เสีย **(stakeholder management)**
- แผนการสื่อสาร
- แผนการฟื้นฟูธุรกิจหลังภัยพิบัติ
- แผนความต่อเนื่องทางธุรกิจ
- การวางแผนความต่อเนื่องในการปฏิบัติงาน **(COOP)**
- ทีมตอบสนองต่อเหตุการณ์
- นโยบายการเก็บรักษา

4.3 ใช้แหล่งข้อมูลที่เหมาะสมเพื่อสนับสนุนการตรวจสอบตามสถานการณ์สมมติ

- ผลลัพธ์การสแกนช่องโหว่
- แดชบอร์ด **SIEM**
  - เซนเซอร์
  - ความไว
  - แนวโน้ม
  - การแจ้งเตือน
  - ความสัมพันธ์
- ไฟล์บันทึก
  - เครือข่าย
  - ระบบ
  - แอปพลิเคชัน
  - การรักษาความปลอดภัย
  - เว็บ
  - DNS
  - การตรวจสอบสิทธิ์
  - ไฟล์ Dump
  - VoIP และผู้จัดการการโทร
  - ทราฟฟิก Session Initiation Protocol (SIP)
- **syslog/rsyslog/syslog-ng**
- **journalctl**
- **NXLog**
- การตรวจสอบแบนด์วิดท์
- เมตาดาต้า
  - อีเมล
  - อุปกรณ์เคลื่อนที่
  - เว็บ
  - ไฟล์
- **Netflow/sFlow**
  - Netflow
  - sFlow
  - IPFIX
- ผลลัพธ์เครื่องวิเคราะห์โพรโทคอล

4.4 ใช้เทคนิคการลดความเสียหายหรือการควบคุมเพื่อรักษาความปลอดภัยของสภาพแวดล้อมตามสถานการณ์สมมติ

- กำหนดค่าโซลูชันด้านความปลอดภัยของจุดสิ้นสุดใหม่
  - รายการแอปพลิเคชันที่ได้รับอนุญาต
  - รายการแอปพลิเคชันที่บล็อก/ปฏิเสธ (blocklist/deny list)
  - การกักกัน
  - ตัวกรองเนื้อหา/ตัวกรอง URL
  - อัปเดตหรือเพิกถอนใบรับรอง
- การเปลี่ยนแปลงการกำหนดค่า
  - กฎไฟร์วอลล์
  - MDM
  - DLP
- การแยก **(isolation)**
- การกักกัน **(containment)**
- การแบ่งส่วน **(segmentation)**
- **SOAR**
  - Runbook
  - Playbook

4.5 อธิบายด้านต่าง ๆ ที่สำคัญของการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

- เอกสาร/หลักฐาน
  - คำสั่งให้เก็บข้อมูลเพื่อการดำเนินคดี (legal hold)
  - วิดีโอ
  - การรับฟังพยานหลักฐาน
  - เส้นทางการรับ-ส่งพยานหลักฐาน
  - ลำดับระยะเวลาเหตุการณ์
    - ข้อมูลวันที่และเวลา
    - การชดเชยเวลา
  - แท็ก
  - รายงาน
  - บันทึกเหตุการณ์
  - การสัมภาษณ์
- การได้มา
  - ลำดับความลบเลือนได้ของข้อมูล (order of volatility)
  - ดิสก์
  - Random-access memory (RAM)
  - Swap/pagefile
  - OS
  - อุปกรณ์
  - เฟิร์มแวร์
  - Snapshot
  - แคช
  - เครือข่าย
  - ภาพเป็นเส้น
- ในสถานที่กับระบบกลุ่มเมฆ
  - ข้อกำหนดเกี่ยวกับสิทธิในการตรวจสอบ
  - การกำกับดูแล/เขตอำนาจ
  - กฎหมายการแจ้งเตือนเกี่ยวกับการละเมิดข้อมูล
- ความถูกต้อง **(integrity)**
  - การ Hash
  - Checksums
  - ที่มา (provenance)
- การสงวนรักษา
- การค้นพบทางอิเล็กทรอนิกส์ **(E-discovery)**
- การกู้คืนข้อมูล **(data recovery)**
- การห้ามปฏิเสธความรับผิดชอบ
- ข่าวกรองเชิงกลยุทธ์ **(strategic intelligence)**/ข่าวกรองต่อต้าน **(counterintelligence)**

5.0 การกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อบังคับ

5.1 เปรียบเทียบข้อเหมือนและต่างของการควบคุมประเภทต่าง ๆ

- หมวดหมู่
  - จัดการ
  - ปฏิบัติงาน
  - เทคนิค
- ประเภทการควบคุม
  - ป้องกัน (Preventive)
  - ตรวจจับ (Detective)
  - แก้ไข (Corrective)
  - ขัดขวาง (Deterrent)
  - ชดเชย (Compensating)
  - กายภาพ

5.2 อธิบายความสำคัญของข้อบังคับ มาตรฐาน หรือกรอบการทำงานที่มีผลบังคับใช้ ซึ่งส่งผลต่อสถานะด้านการรักษาความปลอดภัย (security posture) ขององค์กร

- กฎระเบียบ มาตรฐาน และกฎหมาย
  - กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลทั่วไป (GDPR)
  - กฎหมายของประเทศ เขตแดน หรือรัฐ
  - มาตรฐานความปลอดภัยของข้อมูลบัตรชำระเงินในอุตสาหกรรม (PCI DSS)
- กรอบการทำงานด้านคีย์
  - Center for Internet Security (CIS)
  - กรอบการทำงานด้านการจัดการความเสี่ยง (Risk Management Framework, RMF)/กรอบการทำงานด้านการรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity Framework, CSF) ของ National Institute of Standards and Technology (NIST)
  - องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance
    - Cloud control matrix
    - สถาปัตยกรรมอ้างอิง (reference architecture)
- เกณฑ์มาตรฐาน/แนวทางการกำหนดค่าที่ปลอดภัย
  - แนวทางเฉพาะแพลตฟอร์ม/เฉพาะผู้ให้บริการ
    - เว็บเซิร์ฟเวอร์
    - OS
    - เซิร์ฟเวอร์แอปพลิเคชัน
    - อุปกรณ์โครงสร้างพื้นฐานของเครือข่าย

5.3 อธิบายความสำคัญของนโยบายต่อการรักษาความปลอดภัยขององค์กร

- บุคลากร
  - นโยบายการใช้งานที่ยอมรับได้
  - การหมุนเวียนเปลี่ยนงาน
  - การบังคับลาพักร้อน
  - การแบ่งแยกหน้าที่
  - การให้สิทธิ์ให้น้อยที่สุดเท่าที่เป็นไปได้
  - พื้นที่ทำงานที่สะอาด
  - การตรวจสอบประวัติ
  - สัญญาไม่เปิดเผยข้อมูล (NDA)
  - การวิเคราะห์ข้อมูลสื่อสังคม
  - การปฐมนิเทศพนักงานใหม่ (onboarding)
  - การดำเนินขั้นตอนต่าง ๆ หลังการแจ้งลาออก (offboarding)
  - การฝึกอบรมผู้ใช้
    - การนำรูปแบบเกมมาใช้
    - ชิงธง
    - แคมเปญฟิชชิง
      - การจำลองการฟิชชิง
    - การฝึกอบรมผ่านคอมพิวเตอร์ (CBT)
    - การฝึกอบรมตามบทบาทหน้าที่
- ความหลากหลายของเทคนิคการฝึกอบรม
- การจัดการความเสี่ยงจากภายนอก
  - ผู้ให้บริการ
  - ห่วงโซ่อุปทาน
  - พันธมิตรทางธุรกิจ
  - สัญญาระดับการบริการ (SLA)
  - บันทึกความเข้าใจ (MOU)
  - การวิเคราะห์ระบบการวัด (MSA)
  - สัญญาพันธมิตรทางธุรกิจ (BPA)
  - ผลิตภัณฑ์ตกรุ่น (EOL)
  - สิ้นสุดระยะเวลาการบริการ (EOSL)
  - NDA
- ข้อมูล
  - การจัดประเภท
  - การกำกับดูแล
  - การเก็บรักษา
- นโยบายเกี่ยวกับข้อมูลประจำตัว
  - บุคลากร
  - บุคคลภายนอก
  - อุปกรณ์
  - บัญชีบริการ
  - ผู้ดูแลระบบ/บัญชีราก
- นโยบายระดับองค์กร
  - การจัดการการเปลี่ยนแปลง
  - การควบคุมการเปลี่ยนแปลง
  - การจัดการสินทรัพย์

CompTIA

5.4 สรุปแนวคิดและกระบวนการจัดการความเสี่ยง

- ประเภทความเสี่ยง
  - ภายนอก
  - ภายใน
  - ระบบดั้งเดิม
  - หลายฝ่าย
  - การโจรกรรม IP
  - การให้อนุญาต/การปฏิบัติตามข้อกำหนดซอฟต์แวร์
- กลยุทธ์การจัดการความเสี่ยง
  - การยอมรับ
  - การหลีกเลี่ยง
  - การถ่ายโอน
    - การประกันภัยไซเบอร์
  - การบรรเทาเหตุ
- การวิเคราะห์ความเสี่ยง
  - ทะเบียนข้อมูลความเสี่ยง
  - เมทริกซ์ความเสี่ยง/แผนที่ความร้อน
  - การประเมินการควบคุมความเสี่ยง
  - การประเมินตนเองเกี่ยวกับการควบคุมความเสี่ยง
  - การรับรู้ความเสี่ยง
  - ความเสี่ยงที่แฝงอยู่
  - ความเสี่ยงที่คงเหลือ
  - ความเสี่ยงในการควบคุม
  - ความเสี่ยงที่ยอมรับได้
  - กฎระเบียบที่ส่งผลต่อสถานะความเสี่ยง
  - ประเภทการประเมินความเสี่ยง
    - เชิงคุณภาพ
    - เชิงปริมาณ
  - ความเป็นไปได้ของเหตุการณ์
  - ผลกระทบ
  - มูลค่าสินทรัพย์
  - ค่าความสูญเสียที่อาจเกิดขึ้นครั้งเดียว (SLE)
  - ค่าความสูญเสียที่อาจเกิดขึ้นต่อปี (ALE)
  - อัตราการเกิดเหตุการณ์ต่อปี (ARO)
- ภัยพิบัติ
  - สิ่งแวดล้อม
  - มนุษย์สร้างขึ้น
  - ภายในและภายนอก
- การวิเคราะห์ผลกระทบต่อธุรกิจ
  - เวลากู้คืนระบบที่ยอมรับได้ (RTO)
  - ปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้ (RPO)
  - ระยะเวลาเฉลี่ยตั้งแต่เสียหายจนใช้งานได้แต่ละครั้ง (MTTR)
  - ระยะเวลาเฉลี่ยก่อนการเสียหายแต่ละครั้ง (MTBF)
  - แผนการฟื้นฟูการทำงาน
  - จุดเดียวของความล้มเหลว (single point of failure)
  - แผนการฟื้นฟูธุรกิจหลังภัยพิบัติ (DRP)
  - การทำงานที่จำเป็นสำหรับภารกิจ (mission essential function)
  - การระบุระบบที่สำคัญวิกฤติ
  - การประเมินความเสี่ยงสถานที่

5.5 อธิบายแนวคิดเกี่ยวกับความเป็นส่วนตัวและข้อมูลละเอียดอ่อนในส่วนที่เกี่ยวข้องกับการรักษาความปลอดภัย

- ผลลัพธ์ของการละเมิดข้อมูลและความเป็นส่วนตัวต่อองค์กร
  - ความเสียหายต่อชื่อเสียง
  - การโจรกรรมเอกลักษณ์บุคคล (identity theft)
  - ค่าปรับ
  - การโจรกรรม IP
- การแจ้งการละเมิด
  - การยกระดับ
  - การแจ้งและการเปิดเผยต่อสาธารณะ
- ประเภทข้อมูล
  - การจัดประเภท
    - สาธารณะ
    - ส่วนตัว
    - ละเอียดอ่อน
    - เป็นความลับ
    - สำคัญวิกฤติ
    - มีกรรมสิทธิ์
  - ข้อมูลที่ระบุตัวบุคคลได้ (PII)
  - ข้อมูลสุขภาพ
  - ข้อมูลการเงิน
  - ข้อมูลของรัฐบาล
  - ข้อมูลลูกค้า
- เทคโนโลยีเพิ่มความเป็นส่วนตัว
  - การจัดเก็บข้อมูลเฉพาะที่จำเป็น (Data minimization)
  - การปิดบังข้อมูล (data masking)
  - การทำโทเค็น (tokenization)
  - การทำให้ไม่ระบุชื่อ (anonymization)
  - การทำให้ไม่ระบุชื่อแบบเทียม (pseudo-anonymization)
- บทบาทและความรับผิดชอบ
  - เจ้าของข้อมูล (data owner)
  - ผู้ควบคุมข้อมูล (data controller)
  - ผู้ประมวลผลข้อมูล (data processor)
  - ผู้ดูแลข้อมูล (data custodian)/ผู้พิทักษ์ข้อมูล (steward)
  - เจ้าหน้าที่คุ้มครองข้อมูล
- วงจรชีวิตของข้อมูล
- การประเมินผลกระทบ
- เงื่อนไขข้อตกลง
- ประกาศความเป็นส่วนตัว

รายการคำย่อของ Security+ (SY0-601)

รายการต่อไปนี้คืออักษรย่อที่ปรากฏในข้อสอบ CompTIA Security+ ผู้สมัครสอบควรทบทวนรายการทั้งหมดและศึกษาหาความรู้ในการปฏิบัติงานเกี่ยวกับอักษรย่อทั้งหมดเพื่อการเตรียมความพร้อมสำหรับการสอบที่ครอบคลุม

คำย่อ	คำจำกัดความ
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standards 256bit
AH	Authentication Header
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ASP	Active Server Pages
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
AV	Antivirus
BASH	Bourne Again Shell
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partnership Agreement
BPDU	Bridge Protocol Data Unit
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart

คำย่อ	คำจำกัดความ
CAR	Corrective Action Report
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CBT	Computer-based Training
CCMP	Counter-Mode/CBC-MAC Protocol
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge-Handshake Authentication Protocol
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CMS	Content Management System
CN	Common Name
COOP	Continuity of Operations Planning
COPE	Corporate-owned Personally Enabled
CP	Contingency Planning
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSP	Cloud Service Provider
CSR	Certificate Signing Request
CSRF	Cross-Site Request Forgery
CSU	Channel Service Unit
CTM	Counter-Mode
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial-of-Service
DEP	Data Execution Prevention

คำย่อ	คำจำกัดความ
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	Domain Keys Identified Mail
DLL	Dynamic-link Library
DLP	Data Loss Prevention
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Transaction
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial-of-Service
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic-curve Cryptography
ECDHE	Elliptic-curve Diffie-Hellman Ephemeral
ECDSA	Elliptic-curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EFS	Encrypted File System
EIP	Extended Instruction Pointer
EOL	End of Life
EOS	End of Service
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identifier
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Monitoring
FPGA	Field Programmable Gate Array
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	Secured File Transfer Protocol
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation
GPG	GNU Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
HA	High Availability
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based One-time Password

คำย่อ	คำจำกัดความ
HSM	Hardware Security Module
HSMaaS	Hardware Security Module as a Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, Air Conditioning
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP4	Internet Message Access Protocol v4
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISFW	Internal Segmentation Firewall
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
ITCP	IT Contingency Plan
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MaaS	Monitoring as a Service
MAC	Media Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning

คำย่อ	คำจำกัดความ
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Measurement Systems Analysis
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAS	Network-attached Storage
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near-field Communication
NFV	Network Function Virtualization
NGFW	Next-generation Firewall
NG-SWG	Next-generation Secure Web Gateway
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NOC	Network Operations Center
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSI	Open Systems Interconnection
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over-The-Air
OTG	On-The-Go
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
P12	PKCS #12
P2P	Peer-to-Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
PAM	Privileged Access Management
PAM	Pluggable Authentication Modules
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture

คำย่อ	คำจำกัดความ
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PE	Portable Executable
PEAP	Protected Extensible Authentication Protocol
PED	Portable Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PoC	Proof of Concept
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Preshared Key
PTZ	Pan-Tilt-Zoom
PUP	Potentially Unwanted Program
QA	Quality Assurance
QoS	Quality of Service
PUP	Potentially Unwanted Program
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RAS	Remote Access Server
RAT	Remote Access Trojan
RC4	Rivest Cipher version 4
RCS	Rich Communication Services
RFC	Request for Comments
RFID	Radio Frequency Identification
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol

คำย่อ	คำจำกัดความ
SCEP	Simple Certificate Enrollment Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDLM	Software Development Life-cycle Methodology
SDN	Software-defined Networking
SDP	Service Delivery Platform
SDV	Software-defined Visibility
SED	Self-Encrypting Drives
SEH	Structured Exception Handling
SFTP	SSH File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, Response
SoC	System on Chip
SOC	Security Operations Center
SPF	Sender Policy Framework
SPIM	Spam over Instant Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-time Transport Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
STP	Shielded Twisted Pair
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Intelligence Information
TCP/IP	Transmission Control Protocol/Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOTP	Time-based One Time Password
TPM	Trusted Platform Module
TSIG	Transaction Signature
TTP	Tactics, Techniques, and Procedures
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On-The-Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VBA	Visual Basic for Applications
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable-length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WORM	Write Once Read Many
WPA	WiFi Protected Access
WPS	WiFi Protected Setup
XaaS	Anything as a Service
XML	Extensible Markup Language
XOR	Exclusive OR
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

รายการฮาร์ดแวร์และซอฟต์แวร์ที่มีการเสนอสำหรับข้อสอบ Security+

CompTIA แนบตัวอย่างรายการฮาร์ดแวร์และซอฟต์แวร์มาในที่นี้เพื่อช่วยเหลือผู้สมัครสอบในการเตรียมตัวสอบ Security+ รายการนี้อาจมีประโยชน์ต่อบริษัทฝึกอบรมที่ต้องการสร้างองค์ประกอบห้องปฏิบัติการสำหรับจัดการฝึกอบรม รายการย่อยในแต่ละหัวข้อเป็นเพียงตัวอย่างโดยคร่าวเท่านั้น

ฮาร์ดแวร์
- แล็ปท็อปที่สามารถเข้าถึงอินเทอร์เน็ต
- NIC ไร้สายแยกต่างหาก
- WAP
- ไฟร์วอลล์
- UTM
- อุปกรณ์เคลื่อนที่
- เซิร์ฟเวอร์/เซิร์ฟเวอร์ระบบกลุ่มเมฆ
- อุปกรณ์ IoT

ซอฟต์แวร์
- ซอฟต์แวร์ระบบเสมือน (Virtualization software)
- การกระจาย/OS การทดสอบเจาะระบบ (เช่น Kali Linux, Parrot OS)
- SIEM
- Wireshark
- Metasploit
- tcpdump

อื่น ๆ
- การเข้าถึง CSP