วัตถุประสงค์ของ

CompTIA Security+ Certification Exam

รหัสข้อสอบ: **SY0-701**

เกี่ยวกับข้อสอบ

ข้อสอบ CompTIA Security+ จะรับรองว่าผู้สมัครซึ่งสอบผ่านมีความรู้และทักษะที่จำเป็นในการ:

- ประเมินสถานะด้านการรักษาความปลอดภัย (security posture) ของสภาพแวดล้อมองค์กร แนะนำและใช้โซลูชันการรักษาความปลอดภัยที่เหมาะสม
- เฝ้าติดตามและรักษาความปลอดภัยของสภาพแวดล้อมแบบไฮบริด ซึ่งรวมถึงระบบคลาวด์ อุปกรณ์เคลื่อนที่ และอินเทอร์เน็ตของสรรพสิ่ง (IoT)
- ปฏิบัติงานโดยมีความตระหนักถึงระเบียบข้อบังคับและนโยบายที่บังคับใช้ ซึ่งรวมถึงหลักการกำกับดูแล ความเสี่ยง และแนวทางการปฏิบัติตามข้อบังคับ
- ระบุ วิเคราะห์ และตอบสนองต่อเหตุการณ์และอุบัติเหตุด้านการรักษาความปลอดภัย

การจัดทำข้อสอบ

ข้อสอบ CompTIA เป็นผลจากการจัดเวิร์กช็อปสำหรับผู้เชี่ยวชาญในหัวข้อเนื้อหา และผลสำรวจระดับอุตสาหกรรมเกี่ยวกับทักษะและความรู้ที่จำเป็นสำหรับผู้ประกอบวิชาชีพด้าน IT

นโยบายการใช้เนื้อหาที่ได้รับอนุญาตของ CompTIA

CompTIA Certifications, LLC ไม่มีส่วนเกี่ยวข้องกับและไม่ได้อนุญาต สนับสนุน หรือยินยอมให้มีการใช้เนื้อหาใดที่จัดหาให้โดยเว็บไซต์การฝึกอบรมภายนอกที่ไม่ได้รับอนุญาต (หรือที่เรียกว่า "Brain Dump") ผู้ที่ใช้เนื้อหาดังกล่าวเพื่อเตรียมความพร้อมสำหรับการสอบ CompTIA ใด ๆ จะถูกเพิกถอนประกาศนียบัตรของตนและถูกระงับไม่ให้ดำเนินการทดสอบในอนาคตตามข้อตกลงผู้สมัครสอบ CompTIA เพื่อการสื่อสารที่ชัดเจนยิ่งขึ้นเกี่ยวกับนโยบายการสอบของ CompTIA ว่าด้วยการใช้เนื้อหาการเรียนรู้ที่ไม่ได้รับอนุญาต CompTIA ขอให้ผู้สมัครสอบประกาศนียบัตรทุกท่านไปที่นโยบายการสอบประกาศนียบัตร CompTIA โปรดทบทวนนโยบายทั้งหมดของ CompTIA ก่อนที่จะเริ่มต้นกระบวนการเรียนรู้สำหรับการสอบ CompTIA ใด ๆ ผู้สมัครสอบจะต้องปฏิบัติตามข้อตกลงผู้สมัครสอบ CompTIA หากผู้สมัครสอบมีข้อสงสัยว่าเนื้อหาการเรียนรู้ถือว่าไม่ได้รับอนุญาตหรือไม่ (หรือที่เรียกว่า "Brain Dump") ผู้สมัครสอบควรติดต่อ CompTIA ที่ examsecurity@comptia.org เพื่อตรวจสอบยืนยัน

โปรดทราบ

รายการตัวอย่างที่ระบุไว้ในรูปแบบหัวข้อย่อยเป็นเพียงรายการโดยสังเขป ตัวอย่างอื่น ๆ ของเทคโนโลยี กระบวนการ หรืองานที่เกี่ยวข้องกับวัตถุประสงค์แต่ละข้ออาจรวมอยู่ในข้อสอบด้วย แม้ว่าจะไม่ได้ระบุอยู่ในรายการหรือถูกกล่าวถึงในเอกสารวัตถุประสงค์ฉบับนี้ก็ตาม CompTIA มีการดำเนินการทบทวนเนื้อหาข้อสอบและปรับปรุงคำถามในข้อสอบอย่างสม่ำเสมอ เพื่อให้ข้อสอบของเรามีข้อมูลเป็นปัจจุบันและเพื่อรักษาความปลอดภัยในการเก็บรักษาคำถามให้เป็นความลับ ในกรณีที่จำเป็น เราจะออกข้อสอบฉบับปรับปรุงโดยอ้างอิงจากวัตถุประสงค์ของข้อสอบเดิม โปรดทราบว่าสื่อเตรียมสอบทั้งหมดที่เกี่ยวข้องจะยังคงสามารถใช้ได้อยู่

รายละเอียดการทดสอบ

ข้อสอบที่จำเป็น	SY0-701
จำนวนคำถาม	สูงสุด 90 ข้อ
ประเภทคำถาม	ข้อสอบแบบปรนัยและอ้างอิงจากประสิทธิภาพการทำงาน
ระยะเวลาการทดสอบ	90 นาที
ประสบการณ์ที่แนะนำ	ประสบการณ์ขั้นต่ำ 2 ปีในการดูแลระบบไอที โดยมุ่งเน้นด้านความปลอดภัย มีประสบการณ์ที่ผ่านการลงมือทำเกี่ยวกับความปลอดภัยของข้อมูลทางเทคนิค และมีความรู้กว้างขวางเกี่ยวกับแนวคิดด้านการรักษาความปลอดภัย

วัตถุประสงค์การสอบ (ขอบเขต)

ตารางด้านล่างแสดงขอบเขตที่ข้อสอบชุดนี้วัดผลและสัดส่วนการให้คะแนน

ขอบเขต		อัตราส่วนร้อยละของข้อสอบ
1.0	แนวคิดทั่วไปด้านการรักษาความปลอดภัย	12%
2.0	ภัย ช่องโหว่ และการบรรเทา	22%
3.0	สถาปัตยกรรมการรักษาความปลอดภัย	18%
4.0	การดำเนินการรักษาความปลอดภัย	28%
5.0	การจัดการและดูแลภาพรวมโครงการรักษาความปลอดภัย	20%
รวม		**100%**

1.0 แนวคิดทั่วไปด้านการรักษาความปลอดภัย

1.1 เปรียบเทียบความแตกต่างของมาตรการควบคุมความปลอดภัย

- **หมวดหมู่**
  - ด้านเทคนิค
  - ด้านการจัดการ
  - ด้านการปฏิบัติการ
  - ด้านกายภาพ
- **ประเภทการควบคุม**
  - ป้องกัน (Preventive)
  - ขัดขวาง (Deterrent)
  - ตรวจจับ (Detective)
  - แก้ไข (Corrective)
  - ชดเชย (Compensating)
  - สั่งการ (Directive)

1.2 สรุปแนวคิดด้านการรักษาความปลอดภัยพื้นฐาน

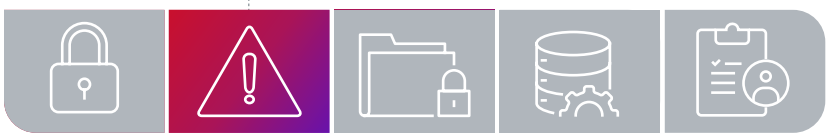
- **การรักษาความลับ ความซื่อสัตย์ และความพร้อมใช้งาน (CIA)**
- **การห้ามปฏิเสธความรับผิดชอบ**
- **การยืนยันตัวตน การอนุญาต และการบันทึก (AAA)**
  - การยืนยันตัวตนบุคคล
  - การยืนยันตัวตนระบบ
  - โมเดลการให้สิทธิ์
- **การวิเคราะห์ช่องว่าง (Gap analysis)**
- **Zero Trust**
  - คอนโทรลเพลน
    - Adaptive identity
    - การลดขอบเขตภัยคุกคาม
    - การควบคุมการเข้าถึงที่ขับเคลื่อนด้วยนโยบาย
    - ผู้ดูแลระบบนโยบาย
    - เครื่องมือกำหนดนโยบาย
  - ดาต้าเพลน
    - พื้นที่ที่เชื่อถือได้โดยนัย (Implicit trust zones)
    - เจ้าของข้อมูล/ระบบ
    - การบังคับใช้นโยบาย
- **การรักษาความปลอดภัยทางกายภาพ**
  - เสากั้น
  - ห้องตรวจสอบก่อนเข้าอาคาร (vestibule)
  - รั้ว
  - กล้องวิดีโอวงจรปิด
  - พนักงานรักษาความปลอดภัย
  - บัตรเข้าถึง
  - แสงสว่าง
  - เซนเซอร์
    - Infrared (อินฟราเรด)
    - ความดัน
    - ไมโครเวฟ
    - อัลตราโซนิก
- **เทคโนโลยีการลวงและสกัดกั้นการโจมตี**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

1.3 อธิบายความสำคัญของกระบวนการจัดการการเปลี่ยนแปลงและผลกระทบต่อความปลอดภัย

- **กระบวนการทางธุรกิจที่มีผลต่อการดำเนินการรักษาความปลอดภัย**
  - กระบวนการอนุมัติ
  - ความเป็นเจ้าของ
  - ผู้มีส่วนได้ส่วนเสีย
  - การวิเคราะห์ผลกระทบ
  - ผลการทดสอบ
  - แผนการถอยกลับ
  - กรอบเวลาการซ่อมบำรุง
  - มาตรฐานขั้นตอนการปฏิบัติงาน (SOP)
- **การปรับใช้ทางเทคนิค**
  - รายการที่บล็อก/ปฏิเสธ
  - กิจกรรมที่ถูกจำกัด
  - ระยะเวลาหยุดชะงัก
  - การรีสตาร์ทบริการ
  - รีสตาร์ทแอปพลิเคชัน
  - แอปพลิเคชันล้าสมัย
  - การพึ่งพาองค์ประกอบภายนอก (Dependencies)
- **การจัดทำเอกสาร**
  - การปรับปรุงแก้ไขแผนภาพ
  - การปรับปรุงแก้ไขนโยบาย/กระบวนการ
- **การควบคุมเวอร์ชัน**

1.4 อธิบายความสำคัญของการใช้โซลูชันการเข้ารหัสที่เหมาะสม

- **โครงสร้างพื้นฐานของคีย์สาธารณะ (PKI)**
  - คีย์สาธารณะ
  - คีย์ส่วนตัว
  - ระบบฝากกุญแจ (Key escrow)
- **การเข้ารหัส**
  - ระดับ
    - ทั้งดิสก์
    - แบ่งพาร์ทิชัน
    - ไฟล์
    - ไดรฟ์ข้อมูล
    - ฐานข้อมูล
    - เรคคอร์ด
  - ระหว่างการส่ง/สื่อสาร
  - อสมมาตร
  - สมมาตร
  - การแลกเปลี่ยนคีย์
  - อัลกอริทึม
  - ความยาวของคีย์
- **เครื่องมือ**
  - โมดูลแพลตฟอร์มที่เชื่อถือ (TPM)
  - โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM)
  - ระบบการจัดการคีย์
  - Secure enclave
- **การทำให้สับสน (Obfuscation)**
  - การอำพรางข้อมูล (Steganography)
  - Tokenization
  - การปกปิดข้อมูล (Data masking)
- **การแฮช**
- **การใช้ Salt**
- **ลายเซ็นดิจิทัล**
- **การยืดความยาวของคีย์**
- **บล็อกเชน**
- **Open public ledger**
- **ใบรับรอง**
  - ผู้ออกใบรับรอง
  - รายการยกเลิกใบรับรอง (CRL)
  - Online Certificate Status Protocol (OCSP)
  - ลงชื่อด้วยตนเอง (Self-signed)
  - บุคคลภายนอก
  - Root of trust
  - การสร้างคำขอลงชื่อใบรับรอง (CSR)
  - Wildcard



2.0 ภัย ช่องโหว่ และการบรรเทา

2.1 เปรียบเทียบความแตกต่างของภัยคุกคามและแรงจูงใจ

- **ภัยคุกคาม**
  - ระดับชาติ (Nation-state)
  - ผู้โจมตีที่ไม่มีทักษะ
  - แฮกเกอร์นักเคลื่อนไหว (Hacktivist)
  - ภัยคุกคามที่เกิดขึ้นจากบุคคลภายในองค์กร
  - ขบวนการอาชญากรรม
  - Shadow IT
- **ลักษณะของภัยคุกคาม**
  - ภายใน/ภายนอก
  - ทรัพยากร/เงินทุน
  - ระดับความซับซ้อน/ความสามารถ
- **แรงจูงใจ**
  - การแอบดึงข้อมูล
  - การจารกรรม
  - การหยุดชะงักของบริการ
  - แบล็กเมล
  - ผลประโยชน์ทางการเงิน
  - ความเชื่อทางปรัชญา/การเมือง
  - จริยธรรม
  - แก้แค้น
  - การหยุดชะงัก/ความโกลาหล
  - สงคราม

2.2 อธิบายเส้นทางภัยคุกคามทั่วไปและพื้นที่ที่มีโอกาสโดนโจมตี

- **ใช้ข้อความเป็นหลัก**
  - o อีเมล
  - o บริการข้อความสั้น (SMS)
  - o ข้อความโต้ตอบแบบทันที (IM)
- **รูปภาพเป็นหลัก**
- **ไฟล์เป็นหลัก**
- **การโทรด้วยเสียง**
- **อุปกรณ์ที่นำออกได้**
- **ซอฟต์แวร์ที่มีช่องโหว่**
  - o ใช้ไคลเอนต์เป็นหลักเปรียบเทียบกับไม่ใช้เอเจนต์
- **ระบบและแอปพลิเคชันที่ไม่รองรับ**
- **เครือข่ายที่ไม่ปลอดภัย**
  - แบบไร้สาย
  - แบบมีสาย
  - Bluetooth
- **พอร์ตที่เปิดให้บริการ**
- **รหัสผ่านเริ่มต้นในการใช้งาน**
- **ห่วงโซ่อุปทาน**
  - ผู้ให้บริการด้านการจัดการ (MSP)
  - ผู้จำหน่าย
  - ซัพพลายเออร์
- **บุคคล/วิศวกรรมเชิงสังคม**
  - ฟิชชิง (Phishing)
  - วิชชิง (Vishing)
  - สมิชชิง (Smishing)
  - การให้ข้อมูลที่ผิด/บิดเบือนข้อมูล
  - การปลอมตัวเป็นผู้อื่น
  - การใช้ช่องทางการโจมตีด้วยการปลอดอีเมลธุรกิจ (BEC)
  - การแอบอ้างแบบ Pretexting
  - การโจมตีแบบ Watering hole
  - การสวมรอยเป็นบริษัทที่มีชื่อเสียง
  - การจดชื่อโดเมนที่มีการสะกดคล้ายคลึงกับชื่อเว็บเป้าหมาย (Typosquatting)

2.3 อธิบายประเภทช่องโหว่ต่าง ๆ

- **แอปพลิเคชัน**
  - Memory injection
  - การอ้างอิงข้อมูลเกินขอบเขตที่กำหนด (Buffer overflow)
  - Race conditions
    - Time-of-check (TOC)
    - Time-of-use (TOU)
  - อัปเดตที่เป็นอันตราย
- **ช่องโหว่บนระบบปฏิบัติการ**
- **ช่องโหว่บนเว็บไซต์**
  - Structured Query Language injection (SQLi)
  - การส่งสคริปต์ข้ามเว็บไซต์ (XSS)
- **ฮาร์ดแวร์**
  - เฟิร์มแวร์
  - ผลิตภัณฑ์ที่สิ้นสุดการจำหน่าย (EOL)
  - ผลิตภัณฑ์รุ่นเก่า
- **เวอร์ช่วลไร้เซชัน**
  - การหลบหนี Virtual machine (VM)
  - Resource reuse
- **ช่องโหว่บนระบบคลาวด์**
- **ห่วงโซ่อุปทาน**
  - ผู้ให้บริการ
  - ผู้ให้บริการฮาร์ดแวร์
  - ผู้ให้บริการซอฟต์แวร์
- **การเข้ารหัส**
- **การกำหนดค่าที่ไม่ถูกต้อง**
- **อุปกรณ์เคลื่อนที่**
  - Side loading
  - Jailbreaking
- **ช่องโหว่ของซอฟต์แวร์ที่ผู้พัฒนาซอฟต์แวร์ยังไม่ค้นพบ (Zero-day)**

2.4 วิเคราะห์ข้อบ่งชี้กิจกรรมที่เป็นอันตรายในแต่ละสถานการณ์

- **โจมตีด้วยมัลแวร์**
  - แรนซัมแวร์
  - โทรจัน
  - เวิร์ม
  - สปายแวร์
  - โบลตแวร์ (Bloatware)
  - ไวรัส
  - ตัวบันทึกการพิมพ์ (Keylogger)
  - Logic bomb
  - รูทคิท
- **การโจมตีทางกายภาพ**
  - การบุกรุกโดยตรง
  - การโคลน RFID
  - การใช้ประโยชน์จากสิ่งแวดล้อม
- **การโจมตีเครือข่าย**
  - การปฏิเสธการให้บริการแบบ DDoS
    - Amplified
    - Reflected
  - การโจมตีโดเมนเนม (DNS)
  - แบบไร้สาย
  - การถูกแทรกแซงโดยผู้ไม่หวังดี (On-path)
  - Credential replay
  - โค้ดที่เป็นอันตราย
- **การโจมตีผ่านแอปพลิเคชัน**
  - Injection
  - การอ้างอิงข้อมูลเกินขอบเขตที่กำหนด (Buffer overflow)
  - Replay
  - การยกระดับสิทธิ์ (Privilege escalation)
  - Forgery
  - การเข้าถึงผ่านไดเรกทอรี (Directory traversal)
- **การโจมตีเข้ารหัสลับ**
  - การดาวน์เกรด
  - การชน
  - Birthday attack
- **การโจมตีรหัสผ่าน**
  - การโจมตีหลายบัญชีด้วยรหัสผ่านที่คนมักใช้ (Spraying)
  - การบุกรุกโดยตรง
- **สัญญาณบ่งชี้การโจมตี (IOC)**
  - การล็อกบัญชีผู้ใช้ (Account Lockout)
  - การใช้หลายเซสชันพร้อมกัน
  - เนื้อหาที่ถูกปิดกั้น
  - การเดินทางที่เป็นไปไม่ได้ (Impossible travel)
  - การใช้ทรัพยากร
  - การไม่สามารถเข้าถึงทรัพยากร
  - การบันทึกล็อกที่ไม่ตรงตามเวลาจริง
  - เผยแพร่แล้ว/มีการบันทึกเอกสาร
  - ข้อมูลล็อกสูญหาย

2.5 อธิบายจุดประสงค์ของเทคนิคการบรรเทาที่ใช้เพื่อรักษาความปลอดภัยขององค์กร

- **การแบ่งส่วน**
- **การควบคุมการเข้าถึง**
  - รายการควบคุมการเข้าถึง (ACL)
  - การอนุญาต
- **รายการแอปพลิเคชันที่ได้รับอนุญาต**
- **การแยก (Isolation)**
- **การติดตั้งแพทช์**
- **การเข้ารหัส**
- **การตรวจสอบ**
- **การให้สิทธิ์ให้น้อยที่สุดเท่าที่เป็นไปได้**
- **การบังคับใช้การกำหนดค่า**
- **การเลิกใช้งาน**
- **เทคนิคการเสริมความปลอดภัย**
  - การเข้ารหัส
  - การติดตั้งระบบปกป้อง endpoint
  - ไฟร์วอลล์แบบโฮสต์เบส
  - ระบบป้องกันการบุกรุกแบบโฮสต์เบส (HIPS)
  - การปิดใช้งานพอร์ต/โปรโตคอล
  - การเปลี่ยนรหัสผ่านที่เป็นค่าเริ่มต้น
  - การลบซอฟต์แวร์ที่ไม่จำเป็น

3.0 สถาปัตยกรรมการรักษาความปลอดภัย

3.1 เปรียบเทียบความแตกต่างของการรักษาความปลอดภัยในแต่ละสถาปัตยกรรม

- **แนวคิดทางสถาปัตยกรรมและโครงสร้าง**
  - คลาวด์
    - เกณฑ์ความรับผิดชอบ
    - ข้อควรพิจารณาแบบไฮบริดคลาวด์
    - ผู้ให้บริการที่เป็นบุคคลที่สาม
  - การกำหนดโครงสร้างพื้นฐานจากโค้ด (IaC)
  - เซิร์ฟเวอร์เลส
  - ไมโครเซอร์วิส
  - โครงสร้างพื้นฐานของเครือข่าย
    - การจำแนกเชิงกายภาพ
      - การเว้นช่องว่าง (Air gap)
    - การแบ่งส่วนเชิงลอจิคอล
    - ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (SDN)
  - ระบบที่ตั้งภายในองค์กร (On-premises)
  - แบบรวมศูนย์เปรียบเทียบกับไม่รวมศูนย์
  - การรันในคอนเทนเนอร์ (Containerization)
  - เวอร์ช่วลไร้เซชัน
  - IoT
  - ระบบควบคุมทางอุตสาหกรรม (ICS)/การควบคุมกำกับดูแลและเก็บข้อมูล (SCADA)
  - ระบบปฏิบัติการแบบเรียลไทม์ (RTOS)
  - ระบบฝังตัว (Embedded systems)
  - ความพร้อมใช้งานสูง
- **ข้อควรพิจารณา**
  - ความพร้อมใช้งาน
  - ความทนต่อการเปลี่ยนแปลง
  - ต้นทุน
  - ระดับตอบสนอง
  - ความสามารถในการขยายสเกล
  - ความง่ายในการติดตั้ง
  - การถ่ายโอนความเสี่ยง
  - ความง่ายในการกู้คืน
  - ความพร้อมของแพทช์
  - การไม่สามารถแพทช์ได้
  - พลังงานไฟฟ้า
  - ทรัพยากรประมวลผล

3.2 นำหลักการรักษาความปลอดภัยไปใช้เพื่อรักษาความปลอดภัยของโครงสร้างพื้นฐานในองค์กรในแต่ละสถานการณ์

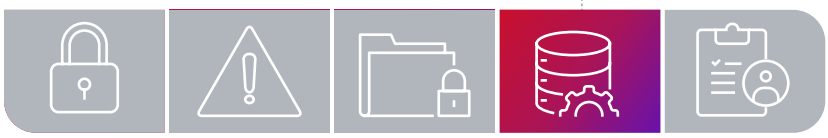
- **ข้อควรพิจารณาด้านโครงสร้างพื้นฐาน**
  - การวางอุปกรณ์
  - โซนที่ปลอดภัย
  - พื้นที่ที่มีโอกาสโดนโจมตี
  - การเชื่อมต่อ
  - โหมดการทำงานเมื่อล้มเหลว
    - เปิดเมื่อล้มเหลว
    - ปิดเมื่อล้มเหลว
  - รูปแบบในการทำงานของอุปกรณ์
    - เชิงรุกเทียบกับเชิงรับ
    - อินไลน์เทียบกับแทป/มอนิเตอร์
  - อุปกรณ์เครือข่าย
    - Jump server
    - เซิร์ฟเวอร์พรอกซี
    - ระบบป้องกันการบุกรุก (IPS)/ระบบตรวจจับการบุกรุก (IDS)
    - อุปกรณ์กระจายโหลด
    - เซนเซอร์
  - การรักษาความปลอดภัยของพอร์ต
    - 802.1X
    - โปรโตคอลการยืนยันตัวตนแบบ EAP
  - ประเภทไฟร์วอลล์
    - ไฟร์วอลล์เว็บแอปพลิเคชัน (WAF)
    - การจัดการภัยคุกคามแบบเบ็ดเสร็จ (UTM)
    - ไฟร์วอลล์แบบ Nextgen
    - เลเยอร์ 4/เลเยอร์ 7
- **การเชื่อมต่อ/การเข้าถึงที่ปลอดภัย**
  - เครือข่ายส่วนตัวเสมือน (VPN)
  - การเข้าถึงระยะไกล
  - Tunneling
    - Transport Layer Security (TLS)
    - Internet protocol security (IPSec)
  - Software-defined wide area network (SD-WAN)
  - Secure access service edge (SASE)
- **การเลือกการควบคุมที่มีประสิทธิภาพ**

3.3 เปรียบเทียบความแตกต่างของกลยุทธ์ในการปกป้องข้อมูล

- **ประเภทข้อมูล**
  - อยู่ภายใต้การควบคุมดูแล
  - ความลับทางการค้า
  - ทรัพย์สินทางปัญญา
  - ข้อมูลทางกฎหมาย
  - ข้อมูลการเงิน
  - ข้อมูลที่อ่านได้โดยมนุษย์และอ่านไม่ได้โดยมนุษย์
- **การจำแนกประเภทข้อมูล**
  - ละเอียดอ่อน
  - เป็นความลับ
  - สาธารณะ
  - จำกัด
  - ส่วนตัว
  - วิกฤติ
- **ข้อควรพิจารณาทั่วไปด้านข้อมูล**
  - สถานะข้อมูล
    - ข้อมูลที่เก็บไว้บนอุปกรณ์
    - ข้อมูลระหว่างการเคลื่อนย้าย (Data in transit)
    - ข้อมูลที่อยู่ระหว่างการใช้งาน (Data in use)
  - อธิปไตยด้านข้อมูล
  - พิกัดทางภูมิศาสตร์
- **วิธีในการรักษาความปลอดภัยข้อมูล**
  - ข้อจำกัดทางภูมิศาสตร์
  - การเข้ารหัส
  - การแฮช
  - การปิดบัง
  - การทำโทเค็น
  - การทำให้สับสน
  - การแบ่งส่วน
  - การจำกัดสิทธิ์อนุญาต

3.4 อธิบายความสำคัญของความทนต่อการเปลี่ยนแปลงและการกู้คืนในสถาปัตยกรรมการรักษาความปลอดภัย

- **ความพร้อมใช้งานสูง**
  - การกระจายโหลดเปรียบเทียบกับการทำคลัสเตอร์
- **ข้อควรพิจารณาเกี่ยวกับสถานที่**
  - Hot
  - Cold
  - Warm
  - การกระจายทางภูมิศาสตร์
- **ความหลากหลายของแพลตฟอร์ม**
- **ระบบมัลติคลาวด์**
- **ความต่อเนื่องของการดำเนินงาน**
- **การวางแผนความจุ** (Capacity)
  - บุคลากร
  - เทคโนโลยี
  - โครงสร้างพื้นฐาน
- **การทดสอบ**
  - การฝึกซ้อมแผนบนโต๊ะ
  - Fail over
  - การจำลอง
  - การประมวลผลแบบคู่ขนาน
- **การสำรองข้อมูล**
  - ในสถานที่/นอกสถานที่
  - ความถี่
  - การเข้ารหัส
  - สแนปช็อต
  - การกู้คืน
  - การทำซ้ำข้อมูล
  - การสำรองข้อมูลแบบ Journaling
- **พลังงานไฟฟ้า**
  - เครื่องกำเนิดไฟฟ้า
  - ระบบสำรองไฟฟ้า (UPS)



4.0 การดำเนินการรักษาความปลอดภัย

4.1 การใช้เทคนิคด้านการรักษาความปลอดภัยกับทรัพยากรประมวลผลในแต่ละสถานการณ์

- **มาตรฐานในการตั้งค่าระบบ (Baseline)**
  - การสร้างมาตรฐาน
  - การนำมาตรฐานไปใช้
  - การปรับปรุงมาตรฐาน
- **เสริมการป้องกันให้อุปกรณ์**
  - อุปกรณ์เคลื่อนที่
  - เวิร์กสเตชัน
  - สวิตช์
  - เราเตอร์
  - โครงสร้างพื้นฐานระบบคลาวด์
  - เซิร์ฟเวอร์
  - ICS/SCADA
  - ระบบฝังตัว (Embedded systems)
  - RTOS
  - อุปกรณ์ IoT
- **อุปกรณ์ไร้สาย**
  - ข้อควรพิจารณาด้านการติดตั้ง
    - การสำรวจสถานที่
    - แผนที่ความร้อน (Heat map)
- **โซลูชันสำหรับโมบาย**
  - การจัดการอุปกรณ์เคลื่อนที่ (MDM)
  - รูปแบบการใช้งาน
    - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานเอง (BYOD)
    - การที่บริษัทเป็นเจ้าของอุปกรณ์ที่จะแจกจ่ายให้พนักงานได้เลือกใช้ (COPE)
    - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานโดยบริษัทเป็นผู้กำหนด (CYOD)
  - วิธีการเชื่อมต่อ
    - แบบเซลลูลาร์
    - Wi-Fi
    - Bluetooth
- **การตั้งค่าการรักษาความปลอดภัยระบบไร้สาย**
  - Wi-Fi Protected Access 3 (WPA3)
  - AAA/Remote Authentication Dial-In User Service (RADIUS)
  - โปรโตคอลการเข้ารหัส
  - โปรโตคอลการตรวจสอบสิทธิ์
- **การรักษาความปลอดภัยของแอปพลิเคชัน**
  - การตรวจสอบอินพุต
  - คุกกี้ที่ปลอดภัย
  - การวิเคราะห์โค้ดคงที่ (Static)
  - การเข็นกำกับโค้ด
- **การทำแซนด์บ็อกซ์**
- **การตรวจสอบ**

4.2 อธิบายประเด็นด้านความปลอดภัยในการจัดการสินทรัพย์ทั้งฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล

- **กระบวนการจัดหา/จัดซื้อ**
- **การมอบหมาย/การอนุมัติ**
  - ความเป็นเจ้าของ
  - การจัดประเภท
- **ตรวจสอบ/ติดตามสินทรัพย์**
  - ทะเบียนสินทรัพย์
  - การระบุแจกแจง
- **การกำจัดทิ้ง/การเลิกใช้งาน**
  - การล้างข้อมูล
  - การทำลายสื่อเก็บข้อมูล
  - ใบรับรอง
  - การเก็บรักษาข้อมูล

4.3 อธิบายกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่

- **วิธีการระบุ**
  - การสแกนช่องโหว่
  - การรักษาความปลอดภัยของแอปพลิเคชัน
    - การวิเคราะห์โค้ดแบบสแตติก (static analysis)
    - การวิเคราะห์โค้ดแบบไดนามิก (dynamic analysis)
    - การติดตามแพ็กเกจ
  - หน้าฟีดภัยคุกคาม
    - ข่าวกรองแบบโอเพ่นซอร์ส (OSINT)
    - จากผู้ให้บริการภายนอก
    - องค์กรที่ร่วมแบ่งปันข้อมูล
    - ดาร์กเว็บ (dark web)
  - การทดสอบเจาะระบบ
  - โครงการที่เปิดให้หาช่องโหว่ในผลิตภัณฑ์
    - โครงการ Bug bounty
  - การตรวจสอบระบบ/กระบวนการ
- **การวิเคราะห์**
  - การยืนยัน
    - ผลแบบ false positive
    - ผลแบบ false negative
  - การจัดลำดับความสำคัญ
  - ระบบการจัดลำดับช่องโหว่ทั่วไป (CVSS)
  - Common Vulnerability Enumeration (CVE)
  - การจำแนกประเภทช่องโหว่
  - ปัจจัยที่ถูกเปิดเผย (Exposure factor)
  - ตัวแปรสภาพแวดล้อม
  - ผลกระทบต่ออุตสาหกรรม/องค์กร
  - ความเสี่ยงที่รับได้
- **การตอบสนองและการแก้ไขช่องโหว่**
  - การติดตั้งแพทช์
  - ประกันภัย
  - การแบ่งส่วน
  - การควบคุมแบบชดเชย
  - ข้อยกเว้นและข้อละเว้น
- **การตรวจสอบความถูกต้องของการแก้ไข**
  - สแกนอีกครั้ง
  - ตรวจ Audit
  - การทวนสอบ
- **การรายงาน**

4.4 อธิบายการแจ้งเตือนความปลอดภัย รวมทั้งแนวคิดและเครื่องมือในการติดตาม

- **ติดตามทรัพยากรด้านการประมวลผล**
  - ระบบ
  - แอปพลิเคชัน
  - โครงสร้างพื้นฐาน
- **กิจกรรม**
  - การรวมบันทึกล็อก
  - การแจ้งเตือน
  - การสแกน
  - การรายงาน
  - การเก็บถาวร (Archiving)
  - การตรวจสอบการตอบสนองและการแก้ไขเมื่อได้รับการแจ้งเตือน
    - การจำกัดบริเวณ
    - การปรับแต่งการแจ้งเตือน
- **เครื่องมือ**
  - เครื่องมือรักษาความปลอดภัยอัตโนมัติ (SCAP)
  - เกณฑ์มาตรฐานที่เทียบในกลุ่มอุตสาหกรรม (Benchmarks)
  - แบบที่ใช้เอเจนต์/แบบที่ไม่ใช้เอเจนต์
  - การจัดการข้อมูลและเหตุการณ์ความปลอดภัย (SIEM)
  - โปรแกรมป้องกันไวรัส
  - ระบบป้องกันการสูญหายของข้อมูล (DLP)
  - การแจ้งเตือนด้วยโปรโตคอลพื้นฐานสำหรับการจัดการเครือข่าย (SNMP)
  - NetFlow
  - เครื่องมือสแกนช่องโหว่

4.5 แก้ไขความสามารถขององค์กรเพื่อเพิ่มประสิทธิภาพด้านความปลอดภัยในแต่ละสถานการณ์

- **ไฟร์วอลล์**
  - กฎ
  - รายการควบคุมการเข้าถึง
  - พอร์ต/โปรโตคอล
  - ขับเน็ตที่ผ่านการคัดกรอง
- **ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก**
  - วิเคราะห์ตามแนวโน้ม
  - ตรวจจับตาม Signature
- **ตัวกรองเว็บ**
  - แบบที่ใช้เอเจนต์
  - พร็อกซีแบบรวมศูนย์
  - การสแกน Universal Resource Locator (URL)
  - การจัดหมวดหมู่เนื้อหา
  - กฎการบล็อก
  - กรองตามชื่อเสียงเว็บไซต์
- **การอัปเดตระบบปฏิบัติการ**
  - Group Policy
  - SELinux
- **การใช้โปรโตคอลอย่างปลอดภัย**
  - การเลือกใช้โปรโตคอล
  - การเลือกพอร์ต
  - วิธีการสื่อสาร
- **การกรอง DNS**
- **ความปลอดภัยของอีเมล**
  - Domain-based Message Authentication Reporting and Conformance (DMARC)
  - DomainKeys Identified Mail (DKIM)
  - เฟรมเวิร์กนโยบายผู้ส่ง (SPF)
  - เกตเวย์
- **การติดตามความสมบูรณ์ของไฟล์**
- **DLP**
- **การควบคุมการเข้าถึงเครือข่าย (NAC)**
- **การตรวจสอบและตอบสนอง Endpoint/การตรวจสอบและตอบสนองแบบขั้นสูง (XDR)**
- **การวิเคราะห์พฤติกรรมผู้ใช้**

4.6 การวางระบบและดูแลการจัดการข้อมูลตัวตนในแต่ละสถานการณ์

- **จัดสรร/เลิกจัดสรรบัญชีผู้ใช้**
- **การมอบหมายและการปรับใช้สิทธิ์อนุญาต**
- **การพิสูจน์ตัวตน**
- **การเชื่อมต่อร่วมกับภายนอก (Federation)**
- **การลงชื่อเข้าใช้เพียงครั้งเดียว (SSO)**
  - Lightweight Directory Access Protocol (LDAP)
  - Open authorization (OAuth)
  - Security Assertion Markup Language (SAML)
- **การทำงานระหว่างกันได้**
- **การพิสูจน์**
- **การควบคุมการเข้าถึง**
  - แบบบังคับ
  - ตามวิจารณญาณของเจ้าของข้อมูล
  - ตามบทบาทหน้าที่
  - ตามกฎ
  - ตามคุณลักษณะ
  - จำกัดการเข้าถึงตามช่วงเวลา
  - ใช้หลักการให้สิทธิ์ให้น้อยที่สุด
- **การตรวจสอบสิทธิ์ผู้ใช้แบบหลายปัจจัย**
  - การใช้งาน
    - Biometrics
    - โทเค็นตรวจสอบสิทธิ์แบบใช้อุปกรณ์/แบบดิจิทัล
    - คีย์รักษาความปลอดภัย
  - ปัจจัย
    - สิ่งที่คุณทราบ (Something you know)
    - สิ่งที่คุณมี (Something you have)
    - สิ่งที่คุณเป็น (Something you are)
    - สถานที่ที่คุณอยู่ (somewhere you are)
- **แนวคิดของรหัสผ่าน**
  - แนวทางปฏิบัติที่ดีที่สุดเกี่ยวกับรหัสผ่าน
    - ความยาว
    - ความซับซ้อน
    - การนำมาใช้ซ้ำ
    - การหมดอายุ
    - อายุ
  - ตัวจัดการรหัสผ่าน
  - การไม่ต้องใช้รหัสผ่าน
- **การจัดการการเข้าถึงตามสิทธิการใช้งาน**
  - สิทธิ์อนุญาตแบบจำกัดช่วงเวลา
  - ระบบจัดเก็บรหัสผ่าน
  - ข้อมูลเข้าสู่ระบบแบบชั่วคราว (Ephemeral)

4.7 อธิบายความสำคัญของระบบอัตโนมัติและการทำ orchestration ในการรักษาความปลอดภัย

- **กรณีการใช้งานระบบอัตโนมัติและสคริปต์**
  - การจัดสรรผู้ใช้
  - การจัดสรรทรัพยากร
  - Guard rails
  - กลุ่มการรักษาความปลอดภัย
  - การสร้าง ticket
  - การยกระดับสิทธิ์
  - การเปิดหรือปิดการเข้าใช้งานและการเข้าถึงบริการ
  - การทดสอบต่อเนื่องตามระบบ CI/CD
  - การใช้ API
- **ประโยชน์**
  - ประสิทธิภาพ/ประหยัดเวลา
  - บังคับใช้เป็นมาตรฐานเดียวกันได้
  - การกำหนดโครงสร้างพื้นฐานที่เป็นมาตรฐาน
  - ปรับขนาดระบบได้อย่างปลอดภัย
  - ช่วยแบ่งเบาภาระพนักงาน
  - ตอบสนองได้รวดเร็ว
  - เพิ่มขีดความสามารถของพนักงาน
- **ข้อควรพิจารณาอื่น ๆ**
  - ความซับซ้อน
  - ต้นทุน
  - Single point of failure
  - หนี้ทางเทคนิค
  - ความสามารถในการสนับสนุนอย่างต่อเนื่อง

4.8 อธิบายกิจกรรมการตอบสนองต่อเหตุการณ์ที่เหมาะสม

- **กระบวนการ**
  - การเตรียมการ
  - การตรวจจับ
  - การวิเคราะห์
  - การจำกัดบริเวณ (Containment)
  - การกำจัด (Eradication)
  - การกู้คืน
  - การถอดบทเรียน
- **การฝึกอบรม**
- **การทดสอบ**
  - การฝึกซ้อมแผนบนโต๊ะ
  - การจำลอง
- **การวิเคราะห์สาเหตุที่แท้จริง**
- **การตรวจหาภัยคุกคามเชิงรุก**
- **นิติเวชทางดิจิทัล**
  - คำสั่งให้เก็บข้อมูลเพื่อการดำเนินคดี
  - เส้นทางการรับ-ส่งพยานหลักฐาน
  - การได้มาซึ่งหลักฐาน
  - การรายงาน
  - การรักษาสภาพหลักฐาน (Preservation)
  - การค้นพบทางอิเล็กทรอนิกส์ (E-discovery)

4.9 ใช้แหล่งข้อมูลที่เหมาะสมเพื่อสนับสนุนการตรวจสอบในแต่ละสถานการณ์

- **ข้อมูลล็อก**
  - ล็อกไฟร์วอลล์
  - ล็อกแอปพลิเคชัน
  - ล็อกเอนด์พอยต์
  - ล็อกความปลอดภัยที่เจาะจงระบบปฏิบัติการ
  - ล็อก IPS/IDS
  - ล็อกเครือข่าย
  - ข้อมูลเมตา
- **แหล่งข้อมูล**
  - การสแกนช่องโหว่
  - การรายงานอัตโนมัติ
  - แดชบอร์ด
  - การดักจับแพคเก็ต

5.0 การจัดการและดูแลภาพรวมโครงการรักษาความปลอดภัย

5.1 สรุปองค์ประกอบของการกำกับดูแลด้านความปลอดภัยที่มีประสิทธิภาพ

- **แนวทาง**
- **นโยบาย**
  - นโยบายการใช้งานที่ยอมรับได้ (AUP)
  - นโยบายการรักษาความปลอดภัยของข้อมูล
  - ความต่อเนื่องทางธุรกิจ
  - การฟื้นฟูธุรกิจหลังภัยพิบัติ
  - การตอบสนองต่อเหตุการณ์
  - วงจรการพัฒนาซอฟต์แวร์ (SDLC)
  - การจัดการการเปลี่ยนแปลง
- **มาตรฐาน**
  - รหัสผ่าน
  - การควบคุมการเข้าถึง
  - การรักษาความปลอดภัยทางกายภาพ
  - การเข้ารหัส
- **ขั้นตอน**
  - การจัดการการเปลี่ยนแปลง
  - การดำเนินการเมื่อรับเข้าและเมื่อสิ้นสุดสภาพพนักงาน
  - แผนรับมือเหตุการณ์ (Playbook)
- **ข้อควรพิจารณาภายนอก**
  - ข้อกำหนด
  - กฎหมาย
  - อุตสาหกรรม
  - ท้องถิ่น/ภูมิภาค
  - ระดับประเทศ
  - สากล
- **การติดตามและแก้ไข**
- **ประเภทโครงสร้างการกำกับดูแล**
  - คณะกรรมการบริหาร
  - คณะกรรมการ
  - หน่วยงานรัฐบาล
  - แบบรวมศูนย์/แบบไม่รวมศูนย์
- **บทบาทและความรับผิดชอบสำหรับระบบและข้อมูล**
  - เจ้าของ
  - ผู้ควบคุม
  - ผู้ประมวลผล
  - ผู้ปกครอง/ผู้ดูแล

5.2 อธิบายองค์ประกอบในการจัดการความเสี่ยง

- **การระบุความเสี่ยง**
- **การประเมินความเสี่ยง**
  - เฉพาะกิจ (Ad hoc)
  - เกิดขึ้นซ้ำ (Recurring)
  - ครั้งเดียว (One time)
  - ต่อเนื่อง (Continuous)
- **การวิเคราะห์ความเสี่ยง**
  - เชิงคุณภาพ
  - เชิงปริมาณ
  - ค่าความสูญเสียที่อาจเกิดขึ้นครั้งเดียว (SLE)
  - ค่าความสูญเสียที่อาจเกิดขึ้นต่อปี (ALE)
  - อัตราการเกิดเหตุการณ์ต่อปี (ARO)
  - ความน่าจะเป็น
  - โอกาสที่จะเกิด
  - ปัจจัยที่ถูกเปิดเผย (Exposure factor)
  - ผลกระทบ
- **การทำทะเบียนข้อมูลความเสี่ยง**
  - สัญญาณบ่งชี้ความเสี่ยงสำคัญ
  - ผู้เป็นเจ้าของความเสี่ยง
  - เกณฑ์ความเสี่ยงสูงสุด
- **ความเสี่ยงที่ทนยอมรับได้**
- **ความเสี่ยงที่ตั้งใจยอมรับ**
  - แบบ Expansionary
  - แบบ Conservative
  - แบบ Neutral
- **กลยุทธ์การจัดการความเสี่ยง**
  - ถ่ายโอน
  - ยอมรับ
    - การละเว้น (Exemption)
    - การยกเว้น (Exception)
  - หลีกเลี่ยง
  - บรรเทา
- **การรายงานความเสี่ยง**
- **การวิเคราะห์ผลกระทบทางธุรกิจ**
  - เวลากู้คืนระบบที่ยอมรับได้ (RTO)
  - ปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้ (RPO)
  - ระยะเวลาเฉลี่ยตั้งแต่เสียหายจนใช้งานได้แต่ละครั้ง (MTTR)
  - ระยะเวลาเฉลี่ยก่อนการเสียหายแต่ละครั้ง (MTBF)

5.3 อธิบายกระบวนการที่เกี่ยวข้องกับการประเมินและการจัดการความเสี่ยงจากบุคคลที่สาม

- **การประเมินผู้ให้บริการ**
  - การทดสอบเจาะระบบ
  - ข้อกำหนดเกี่ยวกับสิทธิในการตรวจสอบ
  - หลักฐานการตรวจสอบภายใน
  - การประเมินอิสระ
  - การวิเคราะห์ห่วงโซ่อุปทาน
- **การเลือกผู้ให้บริการ**
  - การสอบทานทางธุรกิจ (Due diligence)
  - ความขัดแย้งทางผลประโยชน์
- **ประเภทข้อตกลง**
  - ข้อตกลงระดับการบริการ (SLA)
  - บันทึกข้อตกลง (MOA)
  - บันทึกความเข้าใจ (MOU)
  - ข้อตกลงต้นแบบการให้บริการ (MSA)
  - คำสั่งการทำงาน (WO)/คำชี้แจงในการทำงาน (SOW)
  - ข้อตกลงการไม่เปิดเผยข้อมูล (NDA)
  - ข้อตกลงว่าด้วยการเป็นคู่ค้าทางธุรกิจ (BPA)
- **การตรวจสอบผู้ให้บริการ**
- **แบบสอบถาม**
- กฎการปะทะ (rules of engagement)

5.4 สรุปองค์ประกอบของการปฏิบัติตามข้อกำหนดด้านความปลอดภัยที่มีประสิทธิภาพ

- **รายงานการปฏิบัติตาม**
  - ภายใน
  - ภายนอก
- **ผลที่ตามมาจากการไม่ปฏิบัติตาม**
  - ค่าปรับ
  - บทลงโทษ
  - ความเสียหายต่อชื่อเสียง
  - การสูญเสียใบอนุญาต
  - ผลกระทบทางสัญญา
- **การติดตามการปฏิบัติตาม**
  - การสอบทานทางธุรกิจ (Due diligence/care)
  - การพิสูจน์และการรับทราบ
  - ภายในและภายนอก
  - ระบบอัตโนมัติ
- **ความเป็นส่วนตัว**
  - ประเด็นทางกฎหมาย
    - ท้องถิ่น/ภูมิภาค
    - ระดับประเทศ
    - สากล
  - เจ้าของข้อมูล
  - ผู้ควบคุมและผู้ประมวลผล
  - ความเป็นเจ้าของ
  - การจัดเก็บและทำทะเบียนข้อมูล
  - สิทธิ์ในการถูกลืม

5.5 อธิบายประเภทและจุดประสงค์ของการตรวจสอบและการประเมิน

- **การพิสูจน์**
- **ภายใน**
  - การปฏิบัติตาม
  - คณะกรรมการตรวจสอบ
  - การประเมินตนเอง
- **ภายนอก**
  - ข้อกำหนด
  - การตรวจสอบ
  - การประเมิน
  - การตรวจสอบอิสระโดยบุคคลที่สาม
- **การทดสอบเจาะระบบ**
  - กายภาพ
  - เชิงรุก
  - เชิงป้องกัน
  - แบบบูรณาการ
  - แบบที่ทราบข้อมูลระบบทั้งหมด
  - แบบที่ทราบข้อมูลระบบบางส่วน
  - แบบที่ไม่ทราบข้อมูลระบบ
  - การลาดตระเวน (Reconnaissance)
    - แบบเชิงรับ
    - แบบเชิงรุก

5.6 การสร้างความตระหนักในการรักษาความปลอดภัยในแต่ละสถานการณ์

- **ฟิชชิง (Phishing)**
  - แคมเปญ
  - การตระหนักรู้ถึงความพยายามฟิชชิง
  - การตอบสนองต่อข้อความที่ถูกรายงานว่าต้องสงสัย
- **การตระหนักรู้ถึงพฤติกรรมผิดปกติ**
  - มีความเสี่ยงสูง
  - ไม่คาดคิด
  - ไม่จงใจ
- **การให้คำแนะนำและการฝึกอบรมผู้ใช้**
  - นโยบาย/คู่มือ
  - การรับรู้สถานการณ์
  - ภัยคุกคามที่เกิดขึ้นจากบุคคลภายในองค์กร
  - ตัวจัดการรหัสผ่าน
  - สื่อและสายเคเบิลที่ถอดเข้าออกได้
  - วิศวกรรมสังคม
  - การรักษาความปลอดภัยในการปฏิบัติงาน
  - สภาพแวดล้อมในการทำงานแบบไฮบริด/แบบระยะไกล
- **การรายงานและการติดตาม**
  - การเริ่มใช้งาน
  - เกิดขึ้นซ้ำ
- **การพัฒนา**
- **การดำเนินการ**

รายการคำย่อของ CompTIA Security+ SY0-701

รายการต่อไปนี้คืออักษรย่อที่ปรากฏในข้อสอบ CompTIA Security+ SY0-701 ผู้สมัครสอบควรทบทวนรายการทั้งหมดและศึกษาหาความรู้ในการปฏิบัติงานเกี่ยวกับอักษรย่อทั้งหมดที่ระบุไว้เพื่อเป็นการเตรียมความพร้อมสำหรับการสอบอย่างครอบคลุม

คำย่อ	คำเต็ม
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List (รายการควบคุมการเข้าถึง)
AES	Advanced Encryption Standard (มาตรฐานการเข้ารหัสขั้นสูง)
AES-256	Advanced Encryption Standards 256-bit
AH	Authentication Header
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy (ค่าความสูญเสียที่อาจเกิดขึ้นต่อปี)
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat (ภัยคุกคามแบบถาวรขั้นสูง)
ARO	Annualized Rate of Occurrence (อัตราการเกิดเหตุการณ์ต่อปี)
ARP	Address Resolution Protocol (โปรโตคอลการสื่อสารที่ใช้ในการค้นหาที่อยู่เลเยอร์ลิงก์)
ASLR	Address Space Layout Randomization (การสุ่มตำแหน่งพื้นที่ที่อยู่)
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge (แพลตฟอร์มจัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ)
AUP	Acceptable Use Policy (นโยบายการใช้งานที่ยอมรับได้)
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
BYOD	Bring Your Own Device (นำอุปกรณ์ของคุณมาเอง)
CA	Certificate Authority (ใบรับรองอิเล็กทรอนิกส์)
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR	Corrective Action Report

คำย่อ	คำเต็ม
CASB	Cloud Access Security Broker (ผู้ให้บริการตรวจสอบและบริหารจัดการสิทธิด้านความปลอดภัยบนระบบคลาวด์)
CBC	Cipher Block Chaining
CCMP	Counter-Mode/CBC-MAC Protocol
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge-Handshake Authentication Protocol
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operations Planning
COPE	Corporate Owned, Personally Enabled (การที่บริษัทเป็นเจ้าของอุปกรณ์ที่จะแจกจ่ายให้พนักงานได้เลือกใช้)
CP	Contingency Planning
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Cloud Service Provider (ผู้ให้บริการระบบคลาวด์)
CSR	Certificate Signing Request (คำขอลงชื่อใบรับรอง)
CSRF	Cross-site Request Forgery
CSU	Channel Service Unit
CTM	Counter Mode
CTO	Chief Technology Officer
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System (ระบบการจัดลำดับช่องโหว่ทั่วไป)
CYOD	Choose Your Own Device (การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานโดยบริษัทเป็นผู้กำหนด)
DAC	Discretionary Access Control (การควบคุมการเข้าถึงแบบมีเงื่อนไข)
DBA	Database Administrator
DDoS	Distributed Denial of Service (การโจมตีโดยปฏิเสธการให้บริการ)
DEP	Data Execution Prevention (การป้องกันการดำเนินการข้อมูล)

คำย่อ	คำเต็ม
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol (โปรโตคอลที่ใช้ในการจัดการที่รวดเร็วอัตโนมัติและการจัดการส่วนกลาง)
DHE	Diffie-Hellman Ephemeral
DKIM	DomainKeys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention (การป้องกันข้อมูลสูญหาย (DLP))
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Translation
DNS	Domain Name System (ระบบที่มีไว้สำหรับบริหารจัดการข้อมูลของชื่อโดเมนเนม)
DoS	Denial of Service
DPO	Data Privacy Officer
DRP	Disaster Recovery Plan (แผนการฟื้นฟูธุรกิจหลังภัยพิบัติ)
DSA	Digital Signature Algorithm (อัลกอริธึมลายเซ็นดิจิทัล)
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 (การตรวจจับและการตอบสนองต่อภัยคุกคามไซเบอร์ให้แก่ระบบ Endpoint)
EFS	Encrypted File System
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Management
FPGA	Field Programmable Gate Array
FRR	False Rejection Rate
FTP	File Transfer Protocol (โปรโตคอลการโอนย้ายไฟล์)
FTPS	Secured File Transfer Protocol
GCM	Galois Counter Mode
GDPR	General Data Protection Regulation (กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลทั่วไป)
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 (ระบบตรวจจับการบุกรุกแบบอิงตามโฮสต์)

คำย่อ	คำเต็ม
HIPS	Host-based Intrusion Prevention System (ระบบป้องกันการบุกรุกแบบอิงตามโฮสต์)
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-time Password
HSM	Hardware Security Module (โมดูลความปลอดภัยของฮาร์ดแวร์)
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol (โปรโตคอลการถ่ายโอนข้อความหลายมิติ)
HTTPS	Hypertext Transfer Protocol Secure (โปรโตคอลการถ่ายโอนข้อความหลายมิติอย่างปลอดภัย)
HVAC	Heating, Ventilation Air Conditioning
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code (โครงสร้างพื้นฐานเป็นรหัส)
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol (เกณฑ์วิธีข้อความควบคุมบนอินเทอร์เน็ต)
ICS	Industrial Control Systems
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System (ระบบตรวจจับการบุกรุก)
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol (เกณฑ์วิธีเข้าถึงข้อความบนอินเทอร์เน็ต)
IoC	Indicators of Compromise
IoT	Internet of Things (อินเทอร์เน็ตของสรรพสิ่ง)
IP	Internet Protocol (โปรโตคอลอินเทอร์เน็ต)
IPS	Intrusion Prevention System (ระบบตรวจสอบการบุกรุก)
IPSec	Internet Protocol Security (การรักษาความปลอดภัยของโปรโตคอลอินเทอร์เน็ต)
IR	Incident Response
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISO	International Standards Organization (องค์การระหว่างประเทศว่าด้วยการมาตรฐาน)
ISP	Internet Service Provider (ผู้ให้บริการอินเทอร์เน็ต)
ISSO	Information Systems Security Officer
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network (เครือข่ายเฉพาะที่)

คำย่อ	คำเต็ม
LDAP	Lightweight Directory Access Protocol (โปรโตคอลที่ใช้ในการค้นหาและเข้าถึงข้อมูลหรืออ็อบเจกต์ต่าง ๆ ได้อย่างรวดเร็วด้วยระบบไดเรกทอรี)
LEAP	Lightweight Extensible Authentication Protocol
MaaS	Monitoring as a Service (การให้บริการตรวจสอบ)
MAC	Mandatory Access Control (การควบคุมการเข้าถึงแบบบังคับ)
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5 (การเข้ารหัสแบบแฮชเอ็มดี 5)
MDF	Main Distribution Frame
MDM	Mobile Device Management (ซอฟต์แวร์สำหรับบริหารจัดการ และควบคุมอุปกรณ์ภายในองค์กร)
MFA	Multifactor Authentication (การยืนยันตัวตนโดยใช้หลายปัจจัย)
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning
MMS	Multimedia Message Service
MOA	Memorandum of Agreement (บันทึกข้อตกลง)
MOU	Memorandum of Understanding (บันทึกความเข้าใจ)
MPLS	Multi-protocol Label Switching
MSA	Master Service Agreement (สัญญาการให้บริการหลัก)
MSCHAP	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 Recover
MTU	Maximum Transmission Unit
NAC	Network Access Control (การควบคุมการเข้าถึงเครือข่าย)
NAT	Network Address Translation
NDA	Non-disclosure Agreement (ข้อตกลงไม่เปิดเผยข้อมูล)
NFC	Near Field Communication (การสื่อสารไร้สายระยะใกล้)
NGFW	Next-generation Firewall
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier

คำย่อ	คำเต็ม
OS	Operating System (ระบบปฏิบัติการ)
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over the Air
OVAL	Open Vulnerability Assessment Language
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 (การจับแพ็กเก็ต)
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure (เทคโนโลยีระบบรหัสแบบกุญแจสาธารณะ)
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
PTZ	Pan-tilt-zoom
PUP	Potentially Unwanted Program
RA	Recovery Agent
RA	Registration Authority (เจ้าหน้าที่รับลงทะเบียน)
RACE	Research and Development in Advanced Communications Technologies in Europe (การวิจัยและพัฒนาด้านเทคโนโลยีการสื่อสารขั้นสูงในยุโรป)
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service (เกณฑ์วิธีการเชื่อมต่อเพื่อพิสูจน์ตัวจริงระยะไกลในบริการของผู้ใช้)

คำย่อ	คำเต็ม
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol (โปรโตคอลเดสก์ท็อประยะไกล)
RFID	Radio Frequency Identifier
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment (ผลตอบแทนจากการลงทุน)
RPO	Recovery Point Objective (ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายได้)
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System (ระบบปฏิบัติการแบบเรียลไทม์)
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 (ภาษามาร์กอัปเพื่อยืนยันความปลอดภัย)
SAN	Storage Area Network (เครือข่ายพื้นที่จัดเก็บ)
SAN	Subject Alternative Name (ชื่อสำรองของซับเจ็กต์)
SASE	Secure Access Service Edge
SCADA	Supervisory Control and Data Acquisition (การควบคุมกำกับดูแลและเก็บข้อมูล)
SCAP	Security Content Automation Protocol (โพรโทคอลรักษาความปลอดภัยเนื้อหาอัตโนมัติ)
SCEP	Simple Certificate Enrollment Protocol
SD-WAN	Software-defined Wide Area Network (เครือข่ายบริเวณกว้างที่กำหนดโดยซอฟต์แวร์)
SDK	Software Development Kit
SDLC	Software Development Lifecycle
SDLM	Software Development Lifecycle Methodology
SDN	Software-defined Networking
SE Linux	Security-enhanced Linux
SED	Self-encrypting Drives
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm (อัลกอริธึมการแฮชที่ปลอดภัย)
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management (การจัดการข้อมูลด้านความปลอดภัยและการจัดการเหตุการณ์)
SIM	Subscriber Identity Module
SLA	Service-level Agreement
SLE	Single Loss Expectancy (ค่าความสูญเสียที่อาจเกิดขึ้นครั้งเดียว)

คำย่อ	คำเต็ม
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 (โปรโตคอลเข้าถึงอ็อบเจกต์พื้นฐาน)
SOAR	Security Orchestration, Automation, Response
SoC	System on Chip (ระบบบนชิป)
SOC	Security Operations Center (ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ)
SOW	Statement of Work
SPF	Sender Policy Framework (วิธีการตรวจสอบอีเมลจากผู้ส่งจริง)
SPIM	Spam over Internet Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell (โปรโตคอลสำหรับเครือข่ายคอมพิวเตอร์ที่ออกแบบมาเพื่อให้เข้าถึงไปยังคอมพิวเตอร์เครื่องอื่น)
SSL	Secure Sockets Layer (ชั้นซ็อกเก็ตปลอดภัย)
SSO	Single Sign-on (ลงชื่อพิสูจน์ตัวตนเพียงครั้งเดียว)
STIX	Structured Threat Information eXchange
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Indicator Information
TCP/IP	Transmission Control Protocol/ Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security (โปรโตคอลความปลอดภัยที่เข้ารหัสอีเมล)
TOC	Time-of-check
TOTP	Time-based One-time Password
TOU	Time-of-use
TPM	Trusted Platform Module (โมดูลแพลตฟอร์มที่เชื่อถือได้)
TTP	Tactics, Techniques, and Procedures
TSIG	Transaction Signature
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol (โปรโตคอลดาตาแกรมของผู้ใช้)
UEFI	Unified Extensible Firmware Interface (ส่วนต่อประสานเฟิร์มแวร์ที่ขยายได้แบบรวมกัน)
UEM	Unified Endpoint Management (ระบบการจัดการครบวงจรที่รวมความต้องการขององค์กร)
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus (ระบบยูเอสบี)

คำย่อ	คำเต็ม
USB OTG	USB On the Go
UTM	Unified Threat Management (การจัดการภัยคุกคามเบ็ดเสร็จในเครื่องเดียว)
UTP	Unshielded Twisted Pair
VBA	Visual Basic
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure (โครงสร้างพื้นฐานจำลองคอมพิวเตอร์เสมือน)
VLAN	Virtual Local Area Network (การแยกการเชื่อมต่อเครือข่ายคอมพิวเตอร์เป็นส่วน ๆ)
VLSM	Variable Length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPC	Virtual Private Cloud (คลาวด์ส่วนตัวเสมือน)
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall (ไฟร์วอลล์แอปพลิเคชันบนเว็บ)
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System (ระบบตรวจจับการบุกรุกแบบไร้สาย)
WIPS	Wireless Intrusion Prevention System (ระบบป้องกันการบุกรุกแบบไร้สาย)
WO	Work Order
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WTLS	Wireless TLS
XDR	Extended Detection and Response
XML	Extensible Markup Language (ภาษามาร์กอัปแบบขยายได้)
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

รายการฮาร์ดแวร์และซอฟต์แวร์ที่เสนอของ CompTIA Security+ SY0-701

CompTIA แนบตัวอย่างรายการฮาร์ดแวร์และซอฟต์แวร์มาในที่นี้เพื่อช่วยเหลือผู้สมัครสอบในการเตรียมตัวสอบ Security+ SY0-701 รายการนี้อาจมีประโยชน์ต่อบริษัทฝึกอบรมที่ต้องการสร้างองค์ประกอบห้องปฏิบัติการสำหรับจัดการฝึกอบรม รายการย่อยในแต่ละหัวข้อเป็นเพียงตัวอย่างโดยคร่าวเท่านั้น

อุปกรณ์

- แท็บเล็ต
- แล็ปท็อป
- เว็บเซิร์ฟเวอร์
- ไฟร์วอลล์
- เราเตอร์
- สวิตช์
- IDS
- IPS
- อุปกรณ์กระจายสัญญาณไร้สาย
- เครื่องระบบเสมือน
- ระบบอีเมล
- การเข้าถึงอินเทอร์เน็ต
- เซิร์ฟเวอร์ DNS
- อุปกรณ์ IoT
- โทเค็นฮาร์ดแวร์
- สมาร์ตโฟน

ฮาร์ดแวร์สำรอง

- NICs
- แหล่งจ่ายไฟ
- GBICs
- SFPs
- สวิตช์ประเภทที่มีการจัดการ
- อุปกรณ์กระจายสัญญาณไร้สาย
- UPS

เครื่องมือ

- ตัววิเคราะห์สัญญาณ Wi-Fi
- ตัวแมปเครือข่าย
- ตัววิเคราะห์ NetFlow

ซอฟต์แวร์

- Windows OS
- Linux OS
- Kali Linux
- ซอฟต์แวร์การจับแพ็กเก็ต
- ซอฟต์แวร์ทดสอบการเจาะระบบ
- เครื่องมือการวิเคราะห์โค้ดแบบคงที่และแบบไดนามิก
- เครื่องมือสแกนช่องโหว่
- ตัวจำลองเครือข่าย
- โค้ดตัวอย่าง
- เครื่องมือแก้ไขโค้ด
- SIEM
- ตัวบันทึกการพิมพ์ (Keylogger)
- ซอฟต์แวร์ MDM
- VPN
- บริการ DHCP
- บริการ DNS

อื่น ๆ

- การเข้าถึงสภาพแวดล้อมระบบคลาวด์
- ตัวอย่างเอกสาร/แผนภูมิเครือข่าย
- ตัวอย่างล็อก