ประกาศนียบัตรผู้ปฏิบัติงานด้านการรักษาความปลอดภัยขั้นสูง (CASP+) ของ CompTIA

วัตถุประสงค์การสอบ

รหัสข้อสอบ: **CAS-004**

CompTIA

เกี่ยวกับข้อสอบ

ผู้สมัครสอบสามารถใช้เอกสารฉบับนี้เพื่อช่วยเตรียมความพร้อมสำหรับข้อสอบประกาศนียบัตรผู้ปฏิบัติงานด้านการรักษาความปลอดภัยขั้นสูง (CASP+) (CAS-004) ของ CompTIA ข้อสอบประกาศนียบัตร CASP+ ของ CompTIA จะรับรองว่าผู้สมัครซึ่งสอบผ่านมีความรู้และทักษะที่จำเป็นในการ:

- **ออกแบบสถาปัตยกรรม วางโครงสร้างวิศวกรรม ผสานรวม และดำเนินการใช้โซลูชันด้านความปลอดภัยทั่วทั้งสภาพแวดล้อมที่ซับซ้อน เพื่อสนับสนุนองค์กรให้มีความยืดหยุ่น**
- **ใช้การติดตามตรวจสอบ การตรวจจับ การตอบสนองต่อเหตุการณ์ และระบบอัตโนมัติเพื่อสนับสนุนปฏิบัติการด้านการรักษาความปลอดภัยที่กำลังดำเนินอยู่ในสภาพแวดล้อมขององค์กรในเชิงรุก**
- **นำแนวปฏิบัติด้านการรักษาความปลอดภัยไปใช้กับโครงสร้างพื้นฐานที่เป็นระบบคลาวด์ ระบบที่ตั้งอยู่ในสถานที่ ที่อุปกรณ์ปลายทาง และแบบเคลื่อนที่ พร้อมทั้งพิจารณาเทคโนโลยีและเทคนิคด้านวิทยาการเข้ารหัสลับ (cryptographic)**
- **พิจารณาผลกระทบของการกำกับดูแล ความเสี่ยง และข้อกำหนดด้านการปฏิบัติตามกฎระเบียบทั่วทั้งองค์กร**

สิ่งนี้เทียบเท่ากับประสบการณ์ภาคปฏิบัติด้าน IT ทั่วไปอย่างน้อย 10 ปี โดยเป็นประสบการณ์ภาคปฏิบัติด้านการรักษาความปลอดภัยในภาพกว้างอย่างน้อย 5 จาก 10 ปีนั้น ตัวอย่างเนื้อหาเหล่านี้ให้ไว้เพื่ออธิบายวัตถุประสงค์เท่านั้น ไม่ใช่รายการหัวข้อเนื้อหาทั้งหมดของข้อสอบชุดนี้

การรับรองข้อสอบ

ข้อสอบ CASP+ (CAS-004) ของ CompTIA ผ่านการรับรองจากสถาบันมาตรฐานอเมริกัน (ANSI) ตามมาตรฐาน ISO 17024 ซึ่งผ่านการทบทวนและปรับปรุงวัตถุประสงค์ของการสอบอย่างสม่ำเสมอ

การพัฒนาข้อสอบ

ข้อสอบ CompTIA เป็นผลจากการประชุมเชิงปฏิบัติการของผู้เชี่ยวชาญในหัวข้อเนื้อหาที่สำคัญ และผลสำรวจเกี่ยวกับทักษะและความรู้ที่จำเป็นสำหรับผู้เชี่ยวชาญวิชาชีพด้าน IT ระดับเริ่มต้นในอุตสาหกรรม

นโยบายการใช้เนื้อหาที่ได้รับอนุญาตของ CompTIA

CompTIA Certifications, LLC ไม่มีส่วนเกี่ยวข้องกับและไม่ได้อนุญาต สนับสนุน หรือยอมให้มีการใช้เนื้อหาใดที่จัดหาให้โดยเว็บไซต์การฝึกอบรมภายนอกที่ไม่ได้รับอนุญาต (หรือที่เรียกว่า “brain dump”) ผู้ที่ใช้เนื้อหาดังกล่าวเพื่อเตรียมความพร้อมสำหรับการสอบ CompTIA ใดๆ จะถูกเพิกถอนประกาศนียบัตรของตนและระงับการทดสอบในอนาคต ตามข้อตกลงผู้สมัครสอบ CompTIA ด้วยความพยายามที่จะสื่อสารนโยบายการสอบว่าด้วยเนื้อหาการเรียนรู้ที่ไม่ได้รับอนุญาตของ CompTIA ให้ชัดเจนยิ่งขึ้น CompTIA จึงแนะนำให้ผู้สมัครสอบประกาศนียบัตรทุกท่านไปที่**นโยบายการสอบประกาศนียบัตร CompTIA** โปรดทบทวนนโยบายทั้งหมดของ CompTIA ก่อนที่จะเริ่มต้นกระบวนการเรียนรู้สำหรับการสอบ CompTIA ใดๆ ผู้สมัครสอบจะต้องปฏิบัติตาม**ข้อตกลงผู้สมัครสอบ CompTIA** หากผู้สมัครสอบมีคำถามเกี่ยวกับเนื้อหาการเรียนรู้ที่ถือว่าไม่ได้รับอนุญาต (หรือที่เรียกว่า “brain dumps”) ผู้สมัครสอบควรติดต่อ CompTIA ที่ **examsecurity@comptia.org** เพื่อตรวจสอบยืนยัน

โปรดทราบ

รายการตัวอย่างที่ให้ไว้ในสัญลักษณ์แสดงหัวข้อย่อยเป็นเพียงรายการคร่าวๆ ตัวอย่างเทคโนโลยี กระบวนการ หรืองานอื่นที่สัมพันธ์กับวัตถุประสงค์แต่ละข้ออาจรวมอยู่ในข้อสอบแม้ว่าจะไม่ได้อยู่ในรายการหรือถูกกล่าวถึงในเอกสารวัตถุประสงค์ฉบับนี้ก็ตาม CompTIA ได้ทำการทบทวนเนื้อหาข้อสอบและปรับปรุงคำถามในข้อสอบอย่างต่อเนื่องเพื่อให้ข้อสอบของเราเป็นปัจจุบันและเพื่อรักษาความปลอดภัยในการเก็บรักษาคำถามให้เป็นความลับ ในกรณีที่จำเป็น เราจะจัดทำข้อสอบฉบับปรับปรุงโดยอ้างอิงจากวัตถุประสงค์ของข้อสอบเดิม โปรดทราบว่าสื่อเตรียมสอบทั้งหมดที่เกี่ยวข้องจะยังคงสามารถใช้ได้อยู่

รายละเอียดการทดสอบ

ข้อสอบที่กำหนด	CAS-004
จำนวนคำถาม	สูงสุด 90 ข้อ
ประเภทคำถาม	ข้อสอบแบบเลือกตอบและอ้างอิงตามผลการดำเนินงาน
ระยะเวลาการทดสอบ	165 นาที
ประสบการณ์ที่แนะนำ	• ประสบการณ์ภาคปฏิบัติด้าน IT ทั่วไปขั้นต่ำ 10 ปี โดยเป็นประสบการณ์ภาคปฏิบัติด้านการรักษาความปลอดภัยทาง IT ในภาพกว้างอย่างน้อย 5 จาก 10 ปีนั้น • Network+, Security+, CySA+, Cloud+ และ PenTest+ หรือประกาศนียบัตร/ความรู้ที่เทียบเท่า
คะแนนสอบผ่าน	มีแค่ ผ่าน/ไม่ผ่าน เท่านั้น — ไม่มีคะแนนที่อิงตามค่าเฉลี่ย (scaled score)

วัตถุประสงค์การสอบ (ขอบเขต)

ตารางด้านล่างแสดงขอบเขตการวัดผลของข้อสอบชุดนี้และสัดส่วนการให้คะแนน

ขอบเขต	อัตราส่วนร้อยละของข้อสอบ
1.0 สถาปัตยกรรมการรักษาความปลอดภัย	29%
2.0 การดำเนินการรักษาความปลอดภัย	30%
3.0 วิศวกรรมการรักษาความปลอดภัยและการเข้ารหัสลับ	26%
4.0 การกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อบังคับ	15%
รวม	**100%**

1.0 สถาปัตยกรรมการรักษาความปลอดภัย

1.1 วิเคราะห์ข้อกำหนดและวัตถุประสงค์ด้านการรักษาความปลอดภัยตามสถานการณ์สมมติ เพื่อให้มั่นใจว่าสถาปัตยกรรมเครือข่ายมีความเหมาะสมและปลอดภัยสำหรับเครือข่ายใหม่หรือเครือข่ายเดิมที่มีอยู่

- **บริการ**
  - เครื่องกระจายโหลด (load balancer)
  - ระบบตรวจจับการบุกรุก (IDS)/ระบบตรวจจับการบุกรุกเครือข่าย (NIDS)/ระบบตรวจจับการบุกรุกเครือข่ายแบบไร้สาย (WIDS)
  - ระบบป้องกันการบุกรุก (IPS)/ระบบป้องกันการบุกรุก เครือข่าย (NIPS)/ระบบป้องกันการบุกรุกเครือข่ายแบบไร้สาย (WIPS)
  - ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน (WAF)
  - การควบคุมการเข้าถึงเครือข่าย (NAC)
  - เครือข่ายส่วนตัวเสมือน (VPN)
  - การเพิ่มความปลอดภัยให้แก่ระบบโดเมนเนม (DNSSEC)
  - ไฟร์วอลล์/การจัดการภัยคุกคามแบบเบ็ดเสร็จ (UTM)/ไฟร์วอลล์ยุคถัดไป (NGFW)
  - เกตเวย์การแปลงที่อยู่เครือข่าย (NAT)
  - อินเทอร์เน็ตเกตเวย์
  - พร็อกซีส่งข้อมูล/พร็อกซีทรานส์แพเรนต์ (forward/transparent proxy)
  - พร็อกซีรับข้อมูล (reverse proxy)
  - การป้องกันการปฏิเสธการให้บริการ แบบกระจาย (DDoS)
  - เราเตอร์
  - การรักษาความปลอดภัยสำหรับจดหมาย
  - เกตเวย์ส่วนต่อประสาน โปรแกรมประยุกต์ (API)/เกตเวย์ภาษา Extension Markup (XML)
  - การทำสำเนาทราฟฟิก (traffic mirroring)
    - พอร์ตตัววิเคราะห์ พอร์ตแบบสวิตช์ (SPAN)
    - การทำสำเนาพอร์ต (port mirroring)
    - คลาวด์ส่วนตัวเสมือน (VPC)
    - แท็บเครือข่าย (network tap)
  - เซ็นเซอร์
    - การจัดการข้อมูลและเหตุการณ์ความปลอดภัย (SIEM)
    - การตรวจสอบความถูกต้องของไฟล์ (FIM)
    - การแจ้งเตือนด้วยโปรโตคอลพื้นฐานสำหรับการจัดการเครือข่าย (SNMP traps)
    - NetFlow
    - การป้องกันข้อมูลสูญหาย (DLP)
    - โปรแกรมป้องกันไวรัส (Antivirus)
- **การแบ่งส่วน**
  - การแบ่งส่วนแบบไมโคร (Microsegmentation)
  - เครือข่ายภายในพื้นที่ (LAN)/เครือข่ายเสมือนภายในพื้นที่ (VLAN)
  - จั๊มบอกซ์ (jump box)
  - ซับเน็ตที่ผ่านการคัดกรอง (screened subnet)
  - โซนข้อมูล (data zones)
  - สภาพแวดล้อมก่อนใช้งานจริง (staging environments)
  - สภาพแวดล้อมของผู้เยี่ยมชม (guest environments)
  - VPC/เครือข่ายเสมือน (VNET)
  - โซนพร้อมใช้งาน (availability zone)
  - รายการ NAC
  - นโยบาย/กลุ่มการรักษาความปลอดภัย
  - ภูมิภาค
  - รายการควบคุมการเข้าถึง (ACL)
  - เพียร์ทูเพียร์ (peer-to-peer)
  - การเว้นระยะห่าง (air gap)
- **Deperimeterization/Zero Trust**
  - ระบบคลาวด์ (Cloud)
  - การทำงานจากระยะไกล (remote work)
  - อุปกรณ์เคลื่อนที่ (mobile)
  - การจัดหาจากภายนอก (outsourcing) และการทำสัญญาจ้าง (contracting)
  - เครือข่ายความถี่สัญญาณไร้สาย/ความถี่วิทยุ (RF)
- **การควบรวมเครือข่ายจาก หลายองค์กร**
  - เพียริง (peering)
  - จากระบบคลาวด์ไปยังระบบในสถานที่
  - ระดับความอ่อนไหวของข้อมูล
  - การควบรวมและการครอบครอง
  - ข้ามโดเมน (cross-domain)
  - การเชื่อมต่อร่วมกับภายนอก (Federation)
  - บริการไดเรกทอรี
- **ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (software-defined networking - SDN)**
  - SDN แบบเปิด (Open SDN)
  - SDN แบบไฮบริด (Hybrid SDN)
  - โอเวอร์เลย์ SDN (SDN overlay)

1.2 วิเคราะห์ข้อกำหนดระดับองค์กรตามสถานการณ์สมมติ เพื่อระบุการออกแบบการรักษาความปลอดภัยสำหรับโครงสร้างพื้นฐานที่เหมาะสม

- **ความสามารถในการปรับขนาด (scalability)**
  - แบบแนวตั้ง
  - แบบแนวนอน
- **ความยืดหยุ่น (resiliency)**
  - ความพร้อมใช้สูง (high availability)
  - ความหลากหลาย (diversity/heterogeneity)
  - การประสานวิธีดำเนินการให้ราบรื่น (course of action orchestration)
  - การจัดสรรแบบกระจาย (distributed allocation)
  - ความซ้ำซ้อน (redundancy)
  - การทำซ้ำ (replication)
  - การจับกลุ่ม (clustering)
- **การทำงานโดยอัตโนมัติ**
  - การปรับขนาดอัตโนมัติ (autoscaling)
  - การประสานการทำงานของระบบความปลอดภัยให้ราบรื่น เป็นอัตโนมัติ และเพิ่มความเร็วในการตอบสนองต่อเหตุการณ์ภัยไซเบอร์ (SOAR)
  - การบูตสแตรป (bootstrapping)
- **ประสิทธิภาพ**
- **การรันในคอนเทนเนอร์ (containerization)**
- **ระบบเสมือน (virtualization)**
- **เครือข่ายการนำเสนอคอนเทนต์**
- **การแคช (caching)**

1.3 ผสานรวมแอปพลิเคชันซอฟต์แวร์ลงในสถาปัตยกรรมองค์กรอย่างปลอดภัยตามสถานการณ์สมมติ

- **พื้นฐานและแม่แบบ**
  - รูปแบบการออกแบบที่ปลอดภัย/ประเภทของเทคโนโลยีเว็บ
    - รูปแบบการออกแบบพื้นที่จัดเก็บ
  - API ของคอนเทนเนอร์
  - มาตรฐานการเขียนโค้ดที่ปลอดภัย
  - กระบวนการคัดกรองแอปพลิเคชัน
  - การจัดการ API
  - มิดเดิลแวร์ (Middleware)
- **การรับประกันซอฟต์แวร์**
  - การทำพื้นที่ทดลอง (sandboxing)/สภาพแวดล้อมสำหรับการพัฒนา (development environment)
  - การตรวจสอบความถูกต้องไลบรารีของบุคคลภายนอก
  - ไพพ์ไลน์ DevOps ที่กำหนด (defined DevOps pipeline)
  - การเซ็นกำกับโค้ด (code signing)
  - การทดสอบการรักษาความปลอดภัยของแอพลิเคชัน แบบโต้ตอบ (IAST) เทียบกับการทดสอบการรักษาความปลอดภัยของแอปพลิเคชัน แบบไดนามิก (DAST) เทียบกับการทดสอบการรักษาความปลอดภัยของแอปพลิเคชันแบบคงที่ (SAST)
- **ข้อควรพิจารณาด้านการผสานรวม แอปพลิเคชันองค์กร**
  - การจัดการความสัมพันธ์ลูกค้า (CRM)
  - การวางแผนทรัพยากรขององค์กร (ERP)
  - ฐานข้อมูลการจัดการ การกำหนดค่า (CMDB)
  - ระบบการจัดการคอนเทนต์ (CMS)
  - ตัวเปิดใช้งานการผสานรวม
    - บริการไดเรกทอรี
    - ระบบโดเมนเนม (DNS)
    - สถาปัตยกรรมที่มุ่งเน้นบริการ (SOA)
    - บัสบริการองค์กร (ESB)
- **การผสานรวมการรักษาความปลอดภัยลงใน วงจรชีวิตการพัฒนา**
  - วิธีการที่เป็นทางการ (formal methods)
  - ข้อกำหนด
  - ฟิลดิง (fielding)
  - การสอดแทรกและอัปเกรด
  - การกำจัดทิ้งและการนำกลับมาใช้ใหม่
  - การทดสอบ
    - การถดถอย (regression)
    - การทดสอบหน่วย (unit testing)
    - การทดสอบการผสานรวม (integration testing)
  - แนวทางการพัฒนา (development approach)
    - SecDevOps
    - Agile
    - Waterfall
    - Spiral
    - Versioning
    - ไพพ์ไลน์การผสานรวมอย่างต่อเนื่อง/การส่งมอบอย่างต่อเนื่อง (CI/CD)
  - แนวปฏิบัติที่ดีที่สุด
    - โครงการ Open Web Application Security (OWASP)
    - HTTP เฮดเดอร์ที่เหมาะสม

1.4 ดำเนินการใช้เทคนิคด้านการรักษาความปลอดภัยข้อมูลตามสถานการณ์สมมุติ เพื่อรักษาสถาปัตยกรรมองค์กรให้ปลอดภัย

- **การป้องกันข้อมูลสูญหาย**
  - การปิดกั้นการใช้งานสื่อภายนอก
  - การปิดกั้นการพิมพ์
  - การปิดกั้นโปรโตคอล เดสก์ท็อประยะไกล (RDP)
  - การควบคุมความเป็นส่วนตัวของคลิปบอร์ด
  - การดำเนินการใช้โครงสร้างพื้นฐานเดสก์ท็อปเสมือน (VDI) แบบจำกัด
  - กรปิดกั้นการจำแนกประเภทข้อมูล
- **การตรวจจับข้อมูลสูญหาย**
  - การทำลายน้ำ (watermarking)
  - การจัดการสิทธิ์ดิจิทัล (DRM)
  - การถอดรหัสทราฟฟิกเครือข่าย/การตรวจสอบแพ็กเก็ตเชิงลึก
  - การวิเคราะห์ทราฟฟิกเครือข่าย
- **การจำแนกประเภท การติดป้ายกำกับ และการแท็กข้อมูล**
  - เมตาเดต้า/แอตทริบิวต์
- **การทำให้สับสน (obfuscation)**
  - การทำโทเค็น (tokenization)
  - การสครับ (scrubbing)
  - การปิดบัง (masking)
- **การทำให้ไม่ระบุชื่อ (anonymization)**
- **เข้ารหัส เทียบกับ ไม่เข้ารหัส**
- **วงจรชีวิตของข้อมูล**
  - สร้าง
  - ใช้
  - แชร์
  - จัดเก็บ
  - เก็บถาวร
  - ทำลาย
- **คลังจัดเก็บและการทำแผนผังข้อมูล**
- **การจัดการความสมบูรณ์ของข้อมูล**
- **การจัดเก็บ การสำรอง และการกู้คืนข้อมูล**
  - Redundant array of inexpensive disks (RAID)

1.5 วิเคราะห์ข้อกำหนดและวัตถุประสงค์ด้านความปลอดภัยตามสถานการณ์สมมติ เพื่อจัดหาการควบคุมการยืนยันตัวตนและการอนุญาตสิทธิ์ที่เหมาะสม

- **การจัดการข้อมูลการเข้าใช้งานระบบ**
  - แอปพลิเคชันเก็บรักษารหัสผ่าน
    - พื้นที่จัดเก็บรหัสผ่านของผู้ใช้ปลายทาง
    - การเก็บรักษาในสถานที่เทียบกับในระบบคลาวด์
  - ตัวจัดการคีย์ฮาร์ดแวร์
  - การจัดการการเข้าถึงตามสิทธิ์การใช้งาน
- **นโยบายรหัสผ่าน**
  - ความซับซ้อน
  - ความยาว
  - ประเภทอักขระ (character classes)
  - ประวัติ
  - อายุสูงสุด/ต่ำสุด
  - การตรวจสอบ (auditing)
  - การเข้ารหัสแบบย้อนกลับ (reversable encryption)
- **การติดต่อกับภายนอก (Federation)**
  - Transitive trust
  - OpenID
  - ภาษา Security Assertion Markup (SAML)
  - Shibboleth
- **การควบคุมการเข้าถึง**
  - การควบคุมการเข้าถึงแบบบังคับ (MAC)
  - การควบคุมการเข้าถึงแบบมีเงื่อนไข (DAC)
  - การควบคุมการเข้าถึงตามบทบาทหน้าที่ (role-based access control)
  - การควบคุมการเข้าถึงตามกฎ (rule-based access control)
  - การควบคุมการเข้าถึงตามแอตทริบิวต์ (attribute-based access control)
- **โปรโตคอล**
  - เซิร์ฟเวอร์การยืนยันตัวตน ผู้ใช้ที่ต้องการเชื่อมต่อจากระยะไกล (RADIUS)
  - ระบบควบคุมการเข้าถึง ตัวควบคุมการเข้าถึงเทอร์มินัล (TACACS)
  - ไดอะมีเทอร์ (Diameter)
  - โปรโตคอลที่ใช้ในการค้นหาและเข้าถึงข้อมูลหรือออบเจ็กต์ต่างๆ ได้อย่างรวดเร็วด้วยระบบไดเรกทอรี (LDAP)
  - Kerberos
  - OAuth
  - 802.1X
  - โปรโตคอลการยืนยันตัวตน แบบขยายได้ (EAP)
- **การยืนยันตัวตนแบบหลายปัจจัย (MFA)**
  - การยืนยันตัวตน 2 ขั้นตอน (2FA)
  - การตรวจสอบ 2 ขั้นตอน
  - In-band
  - Out-of-band
- **รหัสผ่านแบบใช้ครั้งเดียว (OTP)**
  - รหัสผ่านแบบใช้ครั้งเดียว ที่อิงตาม HMAC (HOTP)
  - รหัสผ่านแบบใช้ครั้งเดียวที่อิงตามเวลา (TOTP)
- **เพิ่มระบบรักษาความปลอดภัยที่ระดับของฮาร์ดแวร์**
- **การลงชื่อเข้าใช้ทุกระบบในครั้งเดียว (SSO)**
- **JavaScript Object Notation (JSON) เว็บโทเค็น (JWT)**
- **การพิสูจน์ยืนยันและการพิสูจน์ตัวตน**

1.6 ดำเนินการใช้โซลูชันระบบคลาวด์และการจำลองระบบเสมือนที่ปลอดภัยตามกลุ่มข้อกำหนดที่ให้มา

- **กลยุทธ์การจำลองระบบเสมือน (virtualization)**
  - ไฮเปอร์ไวเซอร์ไทป์ 1 เทียบกับไทป์ 2
  - คอนเทนเนอร์
  - การจำลอง (emulation)
  - การจำลองระบบเสมือนของแอปพลิเคชัน (application virtualization)
  - VDI
- **การเตรียมใช้งาน (provisioning) และการยกเลิกการเตรียมใช้งาน (deprovisioning)**
- **มิดเดิลแวร์ (Middleware)**
- **เมตาเดต้าและแท็ก**
- **โมเดลและข้อควรพิจารณาด้านการปรับใช้**
  - ข้อกำหนด/ทิศทางธุรกิจ
    - ต้นทุน
    - ความสามารถในการปรับขนาด (scalability)
    - ทรัพยากร
    - สถานที่ตั้ง
    - การคุ้มครองข้อมูล
  - โมเดลการปรับใช้ระบบคลาวด์
    - ส่วนตัว (private)
    - สาธารณะ (public)
    - ลูกผสม (hybrid)
    - ชุมชน (community)
- **แบบจำลองการโฮสต์ (hosting models)**
  - แบบรองรับการใช้งานหลายราย (multitenant)
  - แบบรองรับการใช้งานรายเดียว (single-tenant)
- **โมเดลการให้บริการ**
  - การให้บริการซอฟต์แวร์ (SaaS)
  - การให้บริการแพลตฟอร์ม (PaaS)
  - การให้บริการโครงสร้างพื้นฐาน (IaaS)
- **เงื่อนไขข้อจำกัดของผู้ให้บริการระบบคลาวด์**
  - แบบ IP Address
  - เพียริง VPC
- **การขยายการควบคุม ระบบที่ตั้งในสถานที่อย่างเหมาะสม**
- **โมเดลพื้นที่จัดเก็บ**
  - พื้นที่จัดเก็บแบบอ็อบเจกต์ (object storage)/พื้นที่จัดเก็บตามไฟล์ (file-based storage)
  - พื้นที่จัดเก็บฐานข้อมูล (database storage)
  - พื้นที่จัดเก็บแบบบล็อก (block storage)
  - พื้นที่จัดเก็บแบบบล็อบ (blob storage)
  - การจับคู่คีย์กับค่า

1.7 อธิบายว่าวิทยาการเข้ารหัสลับและโครงสร้างพื้นฐานคีย์สาธารณะ (public key infrastructure, PKI) สนับสนุนวัตถุประสงค์และข้อกำหนดด้านการรักษาความปลอดภัยอย่างไร

- **ข้อกำหนดด้านความเป็นส่วนตัวและการรักษาความลับ**
- **ข้อกำหนดด้านความถูกต้องสมบูรณ์**
- **การห้ามปฏิเสธความรับผิดชอบ**
- **ข้อกำหนดด้านการปฏิบัติตามข้อบังคับและนโยบาย**
- **กรณีการใช้วิทยาการเข้ารหัสลับที่พบบ่อย**
  - ข้อมูลที่พักอยู่
  - ข้อมูลที่มีการเคลื่อนย้าย
  - ข้อมูลที่อยู่ระหว่างประมวลผล/ข้อมูลที่กำลังถูกใช้งาน
  - การคุ้มครองการให้บริการบนเว็บ
  - ระบบฝังตัว (embedded systems)
  - ระบบ/การจัดการรับฝากกุญแจ (key escrow/management)
  - การรักษาความปลอดภัยอุปกรณ์เคลื่อนที่
  - การยืนยันตัวตนที่ปลอดภัย
  - บัตรสมาร์ท
- **กรณีการใช้ PKI ที่พบบ่อย**
  - การให้บริการบนเว็บ (web services)
  - อีเมล
  - การเซ็นกำกับโค้ด (code signing)
  - การเชื่อมต่อร่วมกับภายนอก (Federation)
  - แบบจำลองความเชื่อมั่น (trust models)
  - VPN
  - การทำงานโดยอัตโนมัติ/การทำงานอย่างราบรื่น ขององค์กรและการรักษาความปลอดภัย

1.8 อธิบายผลกระทบของเทคโนโลยีใหม่ๆ ที่มีต่อการรักษาความปลอดภัยและนโยบายขององค์กร

- **ปัญญาประดิษฐ์ (artificial intelligence)**
- **แมชชีนเลิร์นนิ่ง (machine learning)**
- **การประมวลผลแบบควอนตัม (quantum computing)**
- **บล็อกเชน (blockchain)**
- **การเข้ารหัส homomorphic**
  - การดึงข้อมูลส่วนตัว (private information retrieval)
  - การประเมินฟังก์ชันความปลอดภัย (secure function evaluation)
  - การประเมินฟังก์ชันความเป็นส่วนตัว (private function evaluation)
- **การคำนวณความปลอดภัยแบบหลายฝ่าย (secure multiparty computation)**
- **ฉันทามติแบบกระจาย (distributed consensus)**
- **บิ๊กดาต้า (Big Data)**
- **ความเป็นจริงเสมือน/ความเป็นจริงเสริม (virtual/augmented reality)**
- **การพิมพ์ 3 มิติ (3-D printing)**
- **การยืนยันตัวตนโดยไม่ใช้รหัสผ่าน (passwordless authentication)**
- **นาโนเทคโนโลยี (nano technology)**
- **ดีปเลิร์นนิง (deep learning)**
  - การประมวลผลด้วยภาษาธรรมชาติ (natural language processing)
  - ดีปเฟค (deep fake)
- **การเลียนแบบข้อมูลชีวภาพ (biometric impersonation)**

2.0 การดำเนินการรักษาความปลอดภัย

2.1 ให้ดำเนินกิจกรรมการจัดการภัยคุกคามตามสถานการณ์สมมติ

- **ประเภทข่าวกรอง**
  - แบบกลวิธี (tactical)
    - มัลแวร์โจมตีแบบเน้นปริมาณ (commodity malware)
  - แบบกลยุทธ์ (strategic)
    - การโจมตีแบบกำหนดเป้าหมาย (targeted attacks)
  - ระดับดำเนินการ (operational)
    - การตรวจหาภัยคุกคามเชิงรุก (threat hunting)
    - การเลียนแบบภัยคุกคาม (threat emulation)
- **ประเภทผู้กระทำ**
  - ภัยคุกคามแบบถาวร ขั้นสูง (APT)/ระดับชาติ
  - ภัยคุกคามที่เกิดขึ้นจากภายในองค์กร (insider threat)
  - คู่แข่ง (competitor)
  - แฮกเกอร์นักเคลื่อนไหว (hacktivist)
  - สคริปต์คิดดี้ (script kiddie)
  - ขบวนการอาชญากรรม (organized crime)
- **อุปกรณ์ประกอบของผู้ก่อภัยคุกคาม**
  - ทรัพยากร
    - เวลา
    - เงิน
  - การเข้าถึงห่วงโซ่อุปทาน
  - การสร้างช่องโหว่
  - ความสามารถ/การตบตา
  - การระบุเทคนิค
- **วิธีรวบรวมข่าวกรอง**
  - ฟีดข่าวกรอง
  - เว็บมืด (deep web)
  - กรรมสิทธิ์
  - ข่าวกรองแบบโอเพ่นซอร์ส (OSINT)
  - ปัญญาของมนุษย์ (HUMINT)
- **กรอบการทำงาน**
  - MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK)
    - ATT&CK สำหรับระบบ การควบคุมระดับอุตสาหกรรม (ICS)
  - การวิเคราะห์การบุกรุกในแบบ Diamond Model
  - Cyber Kill Chain

2.2 วิเคราะห์สัญญาณบ่งชี้การละเมิดและกำหนดการตอบสนองที่เหมาะสมตามสถานการณ์สมมติ

- **สัญญาณบ่งชี้การละเมิด**
  - การจับแพ็กเก็ต (PCAP)
  - บันทึก
    - บันทึกเครือข่าย
    - บันทึกช่องโหว่
    - บันทึกระบบปฏิบัติการ
    - บันทึกการเข้าถึง
    - บันทึก NetFlow
  - การแจ้งเตือน
    - การแจ้งเตือน FIM
    - การแจ้งเตือน SIEM
    - การแจ้งเตือน DLP
    - การแจ้งเตือน IDS/IPS
    - การแจ้งเตือนระบบป้องกันไวรัส
  - ความรุนแรง/ลำดับความสำคัญของการแจ้งเตือน
  - กิจกรรมการประมวลผลที่ไม่ปกติ
- **การตอบสนอง**
  - กฎไฟร์วอลล์
  - กฎ IPS/IDS
  - กฎ ACL
  - กฎ Signature
  - กฎ Behavior
  - กฎ DLP
  - สคริปต์/นิพจน์ทั่วไป

2.3 กำหนดสถานการณ์สมมติ ให้ดำเนินกิจกรรมการจัดการช่องโหว่

- **การสแกนช่องโหว่**
  - มีข้อมูลสิทธิ์เข้าระบบเทียบกับไม่มีข้อมูลสิทธิ์เข้าระบบ
  - อิงตามเอเจนต์/อิงตามเซิร์ฟเวอร์
  - การจัดอันดับความร้ายแรง
  - เชิงรุกเทียบกับเชิงรับ
- **โปรโตคอลรักษาความปลอดภัย เนื้อหาอัตโนมัติ (SCAP)**
  - รูปแบบการอธิบายรายการตรวจสอบ การกำหนดค่าแบบขยายได้ (XCCDF)
  - ภาษาการประเมิน ช่องโหว่แบบเปิด (OVAL)
  - การระบุแพลตฟอร์มทั่วไป (CPE)
  - ช่องโหว่และการสัมผัสความเสี่ยง ที่พบได้บ่อย (CVE)
  - ระบบการจัดลำดับ ช่องโหว่ทั่วไป (CVSS)
  - การระบุการกำหนดค่า ที่พบได้บ่อย (CCE)
  - รูปแบบการรายงานสินทรัพย์ (ARF)
- **การประเมินตัวเองเทียบกับการประเมินของผู้จำหน่ายบุคคลภายนอก**
- **การจัดการแพตช์**
- **แหล่งข้อมูล**
  - ที่ปรึกษา
  - กระดานข่าว
  - เว็บไซต์ของผู้จำหน่าย
  - ศูนย์การวิเคราะห์ และแบ่งปันข้อมูล (ISAC)
  - รายงานข่าว

2.4 ใช้การประเมินช่องโหว่ รวมถึงวิธีและเครื่องมือการทดสอบการเจาะระบบที่เหมาะสมตามสถานการณ์สมมติ

- **วิธีการ**
  - การวิเคราะห์โค้ดแบบคงที่
  - การวิเคราะห์โค้ดแบบไดนามิก
  - การวิเคราะห์โดยใช้ช่องทางข้างเคียง (side-channel)
  - วิศวกรรมย้อนกลับ
    - ซอฟต์แวร์
    - ฮาร์ดแวร์
  - การสแกนช่องโหว่แบบไร้สาย
  - การวิเคราะห์องค์ประกอบซอฟต์แวร์
  - การทดสอบแบบฟัซ (fuzz testing)
  - Pivoting
  - Post-exploitation
  - การคงอยู่ (persistence)
- **เครื่องมือ**
  - เครื่องสแกน SCAP
  - เครื่องวิเคราะห์ทราฟฟิกเครือข่าย
  - เครื่องสแกนช่องโหว่
  - เครื่องวิเคราะห์โปรโตคอล
  - เครื่องสแกนพอร์ต
  - HTTP interceptor
  - กรอบการทำงานโดยใช้ประโยชน์จากช่องโหว่
  - โปรแกรมเจาะรหัสผ่าน
- **การจัดการสิ่งที่จำเป็น/สิ่งที่เกี่ยวข้อง (dependency)**
- **ข้อกำหนด**
  - ขอบเขตงาน
  - กฎการปะทะ
  - แบบล่วงล้ำเทียบกับแบบไม่ล่วงล้ำ
  - คลังจัดเก็บสินทรัพย์
  - การอนุญาตและการเข้าถึง
  - ข้อควรพิจารณาด้านนโยบายระดับองค์กร
  - ข้อควรพิจารณาด้านสิ่งอำนวยความสะดวก
  - ข้อควรพิจารณาด้านการรักษาความปลอดภัยทางกายภาพ
  - การสแกนซ้ำเพื่อหาการแก้ไข/การเปลี่ยนแปลง

2.5 วิเคราะห์ช่องโหว่และแนะนำการลดความเสี่ยงตามสถานการณ์สมมติ

- **ช่องโหว่**
  - สภาวะการแข่งขัน (race condition)
  - Overflows
    - Buffer
    - Integer
  - ระบบการยืนยันตัวตนที่ถูกทำลาย
  - การอ้างอิงที่ไม่ปลอดภัย
  - การจัดการข้อยกเว้นที่ไม่ดี
  - การกำหนดค่าการรักษาความปลอดภัยไม่ถูกต้อง
  - เฮดเดอร์ที่ไม่เหมาะสม
  - การเปิดเผยข้อมูล
  - ความผิดพลาดของใบรับรอง
  - การใช้งานวิทยาการเข้ารหัสลับที่เปราะบาง
  - cipher ที่เปราะบาง
  - การใช้ cipher suite ที่เปราะบาง
  - การวิเคราะห์องค์ประกอบซอฟต์แวร์
  - การใช้กรอบการทำงาน และโมดูลซอฟต์แวร์ที่มีช่องโหว่
  - การใช้ฟังก์ชันที่ไม่ปลอดภัย
  - ไลบรารีของบุคคลภายนอก
  - สิ่งที่จำเป็น/สิ่งที่เกี่ยวข้อง
  - การโจมตีด้วย code injections/ การเปลี่ยนแปลงที่เป็นอันตราย
  - ผลิตภัณฑ์ไม่ได้รับการสนับสนุนแล้ว/ผลิตภัณฑ์ตกรุ่น
  - ประเด็นการถดถอย
- **ระบบ/แอปพลิเคชัน ที่มีช่องโหว่แฝง**
  - การประมวลผลฝั่งไคลเอ็นต์เทียบกับ การประมวลผลฝั่งเซิร์ฟเวอร์
  - JSON/representational state transfer (REST)
  - ส่วนขยายเบราว์เซอร์
    - แฟลช
    - ActiveX
  - ภาษามาร์กอัปแบบ Hypertext 5 (HTML5)
  - Asynchronous JavaScript และ XML (AJAX)
  - โปรโตคอลเข้าถึงอ็อบเจกต์พื้นฐาน (SOAP)
  - Machine code เทียบกับ bytecode หรือ แบบ interpreted เทียบกับ emulated
- **การโจมตี**
  - การเข้าถึงผ่านไดเรกทอรี (directory traversal)
  - การเขียนสคริปต์ข้ามไซต์ (XSS)
  - การปลอมแปลงคำขอข้ามไซต์ (CSRF)
  - การฉีด (injection)
    - XML
    - LDAP
    - Structure Query Language (SQL)
    - คำสั่ง (command)
    - กระบวนการ
  - Sandbox escape
  - Virtual machine (VM) hopping
  - VM escape
  - การโจมตีแบบ Border Gateway Protocol (BGP)/route hijacking
  - การโจมตี interception
  - การปฏิเสธการให้บริการ (DoS)/DDoS
  - การหลบเลี่ยงระบบยืนยันตัวตน
  - วิศวกรรมสังคม
  - การโจมตีแบบ VLAN hopping

2.6 ใช้กระบวนการในการลดความเสี่ยงตามสถานการณ์สมมติ

- **การดำเนินการเชิงรุกและการตรวจจับ**
  - การค้นหา
  - การพัฒนามาตรการรับมือ
  - เทคโนโลยีที่หลอกลวง
    - Honeynet
    - Honeypot
    - ไฟล์กับดัก (decoy file)
    - ตัวจำลอง (simulator)
    - การกำหนดค่าเครือข่ายแบบไดนามิก
- **การวิเคราะห์ข้อมูลด้านการรักษาความปลอดภัย**
  - การประมวลผลไพพ์ไลน์
    - ข้อมูล
    - สตรีม
  - การทำดัชนีและการค้นหา
  - การรวบรวมและการคัดสรรบันทึก
  - การติดตามตรวจสอบกิจกรรมฐานข้อมูล
- **ป้องกัน (preventive)**
  - โปรแกรมป้องกันไวรัส (Antivirus)
  - ระบบแบบ Immutable
  - การเสริมความปลอดภัย (hardening)
  - Sandbox detonation
- **การควบคุมแอปพลิเคชัน**
  - เทคโนโลยีการให้สิทธิ์ใช้งาน
  - รายการที่อนุญาตเทียบกับรายการที่ถูกบล็อก
  - เวลาตรวจสอบเทียบกับเวลาที่ใช้
  - การดำเนินการแบบอะตอมมิค
- **การทำงานโดยอัตโนมัติของการรักษาความปลอดภัย**
  - Cron/งานที่มีกำหนดเวลา
  - Bash
  - PowerShell
  - Python
- **การรักษาความปลอดภัยทางกายภาพ**
  - การตรวจสอบแสง
  - การตรวจสอบบันทึกของผู้เยี่ยมชม
  - การตรวจสอบกล้อง
  - พื้นที่เปิดโล่งเทียบกับพื้นที่อับอากาศ

2.7 ดำเนินการใช้การตอบสนองที่เหมาะสมตามสถานการณ์สมมติ

- **การจำแนกประเภทเหตุการณ์**
  - False positive
  - False negative
  - True positive
  - True negative
- **เหตุการณ์กลั่นกรอง (triage event)**
- **การยกระดับเหตุการณ์ล่วงหน้า (preescalation tasks)**
- **กระบวนการตอบสนองต่อเหตุการณ์**
  - การเตรียมการ
  - การตรวจจับ
  - การวิเคราะห์
  - การกักกัน
  - การกู้คืน
  - การเรียนรู้บทเรียน
- **คู่มือ/กระบวนการตอบสนองที่เฉพาะเจาะจง**
  - สถานการณ์จำลอง
    - ไวรัสเรียกค่าไถ่ (Ransomware)
    - การแอบดึงข้อมูล (data exfiltration)
    - วิศวกรรมสังคม
  - วิธีการตอบสนองแบบไม่อัตโนมัติ
  - วิธีการตอบสนองแบบอัตโนมัติ
    - Runbooks
    - SOAR
- **แผนการสื่อสาร**
- **การจัดการผู้มีส่วนได้เสีย (stakeholder management)**

2.8 อธิบายความสำคัญของแนวคิดทางการตรวจพิสูจน์หลักฐาน

- **วัตถุประสงค์ขององค์กรในทางกฎหมายเทียบกับภายใน**
- **กระบวนการตรวจพิสูจน์หลักฐาน**
  - การระบุ (identification)
  - การรวบรวมหลักฐาน (evidence collection)
    - เส้นทางการรับ-ส่งพยานหลักฐาน (chain of custody)
    - ลำดับความลบเลือนได้ของข้อมูล (order of volatility)
      - การบันทึกภาพของข้อมูลในหน่วยความจำ (memory snapshots)
      - อิมเมจข้อมูล
      - การโคลน
  - การรักษาหลักฐาน (evidence preservation)
    - พื้นที่จัดเก็บที่ปลอดภัย (secure storage)
    - การสำรองข้อมูล
  - การวิเคราะห์
    - เครื่องมือการตรวจพิสูจน์หลักฐาน
  - การทวนสอบ (verification)
  - การนำเสนอ (presentation)
- **การรักษาบูรณภาพ (integrity preservation)**
  - การแฮช (hashing)
- **การวิเคราะห์เพื่อถอดรหัส (cryptanalysis)**
- **การวิเคราะห์การอำพรางข้อมูล (steganalysis)**

2.9 ใช้เครื่องมือวิเคราะห์การตรวจพิสูจน์หลักฐานตามสถานการณ์สมมติ

- **เครื่องมือชำแหละไฟล์ (file carving tools)**
  - Foremost
  - Strings
- **เครื่องมือวิเคราะห์แบบไบนารี**
  - Hex dump
  - Binwalk
  - Ghidra
  - เครื่องมือแก้บั๊กโครงการแบบ GNU (GDB)
  - OllyDbg
  - readelf
  - objdump
  - strace
  - ldd
  - file
- **เครื่องมือวิเคราะห์**
  - ExifTool
  - Nmap
  - Aircrack-ng
  - Volatility
  - The Sleuth Kit
  - Dynamically vs. statically linked
- **เครื่องมือการสร้างอิมเมจ**
  - Forensic Toolkit (FTK) Imager
  - dd
- **ยูทิลิตีสำหรับการแฮช (hashing utilities)**
  - sha256sum
  - ssdeep
- **เครื่องมือเก็บรวบรวมระหว่างเกิดเหตุการณ์เทียบกับเครื่องมือเก็บรวมรวมหลักฐานหลังเหตุการณ์**
  - netstat
  - ps
  - vmstat
  - ldd
  - lsof
  - netcat
  - tcpdump
  - conntrack
  - Wireshark

3.0 วิศวกรรมการรักษาความปลอดภัย และวิทยาการเข้ารหัสลับ

3.1 นำการกำหนดค่าที่ปลอดภัยไปใช้กับอุปกรณ์เคลื่อนที่ขององค์กรตามสถานการณ์สมมติ

- **การกำหนดค่าที่มีการจัดการ**
  - การควบคุมแอปพลิเคชัน
  - รหัสผ่าน
  - ข้อกำหนดด้าน MFA
  - การเข้าถึงตามโทเค็น
  - การเก็บรักษาแพตช์
  - การอัปเดตเฟิร์มแวร์ทางอากาศ (Firmware Over-the-Air)
  - การลบข้อมูลจากระยะไกล (remote wipe)
  - WiFi
    - การเข้าใช้งาน WiFi ที่ได้รับการป้องกัน (WPA2/3)
    - ใบรับรองอุปกรณ์
  - โปรไฟล์
  - บลูทูธ
  - การสื่อสารไร้สายระยะใกล้ (NFC)
  - อุปกรณ์ต่อพ่วง
  - การกำหนดขอบเขตปลอดภัย (geofencing)
  - การตั้งค่า VPN
  - การติดแท็กสถานที่ตั้ง (geotagging)
  - การจัดการใบรับรอง
  - การเข้ารหัสทั้งอุปกรณ์
  - แบบการปล่อยสัญญาณ (tethering)
  - โหมดเครื่องบิน
  - บริการหาตำแหน่งที่ตั้ง
  - DNS บน HTTPS (DoH)
  - Custom DNS
- **สถานการณ์ที่มีการปรับใช้**
  - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานเอง (BYOD)
  - อุปกรณ์ที่บริษัทเป็นเจ้าของ (corporate-owned)
  - การที่บริษัทเป็นเจ้าของอุปกรณ์, ที่จะแจกจ่ายให้พนักงานได้เลือกใช้ (COPE)
  - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานโดยบริษัทเป็นผู้กำหนด (CYOD)
- **ข้อควรพิจารณาด้านการรักษาความปลอดภัย**
  - การเปิดใช้งาน/การปิดใช้งานอุปกรณ์หรือคุณสมบัติจากระยะไกลโดยไม่ได้รับอนุญาต
  - ข้อกังวลด้านการสื่อสาร ที่มีการเข้ารหัสและไม่มีการเข้ารหัส
  - การลาดตระเวนทางกายภาพ (physical reconnaissance)
  - การขโมยข้อมูลส่วนบุคคล
  - ความเป็นส่วนตัวด้านสุขภาพ
  - ความตั้งใจในการใช้อุปกรณ์สวมใส่
  - การตรวจพิสูจน์หลักฐานทางดิจิทัลของข้อมูลที่เก็บรวบรวมไว้
  - ร้านค้าแอปพลิเคชันที่ไม่ได้รับอนุญาต
  - กระบวนการดัดแปลงระบบปฏิบัติการของอุปกรณ์เคลื่อนที่ (jailbreaking/rooting)
  - Side loading
  - การรันในคอนเทนเนอร์ (containerization)
  - ความแตกต่างของผู้ผลิตอุปกรณ์ดั้งเดิม (OEM) และผู้ให้บริการ
  - ปัญหาด้านห่วงโซ่อุปทาน
  - eFuse

3.2 กำหนดและดำเนินการใช้การควบคุมด้านความปลอดภัยที่ปลายทางตามสถานการณ์สมมติ

- **เทคนิคการเสริมความปลอดภัย (hardening techniques)**
  - การลบบริการที่ไม่จำเป็นออก
  - การปิดบัญชีที่ไม่ได้ใช้งาน
  - อิมเมจ/แม่แบบ
  - นำอุปกรณ์ตกรุ่นออก
  - นำอุปกรณ์ที่ไม่ได้รับการสนับสนุนแล้วออก
  - การเข้ารหัสไดรฟ์ภายใน
  - เปิดใช้งาน no execute (NX)/execute never (XN) bit
  - การปิดใช้งานการสนับสนุนระบบเสมือนของหน่วยประมวลผลกลาง (CPU)
  - การเข้ารหัสที่ปลอดภัย/การเข้ารหัสหน่วยความจำ
  - การจำกัด Shell
  - การสุ่มตำแหน่ง พื้นที่ที่อยู่ (ASLR)
- **กระบวนการ**
  - การใช้แพตช์
    - เฟิร์มแวร์
    - แอปพลิเคชัน
  - การบันทึก
  - การตรวจสอบ
- **การควบคุมการเข้าถึงแบบบังคับ**
  - Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid)
  - Kernel เทียบกับ Middleware
- **การประมวลผลที่เชื่อถือได้ (trustworthy computing)**
  - โมดูลแพลตฟอร์มที่เชื่อถือได้ (TPM)
  - การบูตอย่างปลอดภัย
  - การปกป้อง Unified Extensible Firmware Interface (UEFI)/basic input/output system (BIOS)
  - บริการพิสูจน์
  - โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM)
  - การบูตที่วัดได้
  - ไดรฟ์เข้ารหัสตัวเอง (SED)
- **การควบคุมแบบชดเชย**
  - โปรแกรมป้องกันไวรัส (Antivirus)
  - การควบคุมแอปพลิเคชัน
  - ระบบตรวจจับการบุกรุก แบบอิงตามโฮสต์ (HIDS)/ระบบ ป้องกันการบุกรุกแบบอิงตามโฮสต์ (HIPS)
  - ไฟร์วอลล์แบบอิงตามโฮสต์ (host-based firewall)
  - การตรวจจับและตอบสนองปลายทาง (EDR)
  - ฮาร์ดแวร์ซ้ำซ้อน
  - ฮาร์ดแวร์ที่ซ่อมแซมตัวเองได้
  - การวิเคราะห์พฤติกรรมผู้ใช้ และเอนทิตี (UEBA)

3.3 อธิบายข้อควรพิจารณาด้านการรักษาความปลอดภัยที่ส่งผลกระทบต่อภาคส่วนและเทคโนโลยีการดำเนินการที่เฉพาะเจาะจง

- **แบบฝังตัว**
  - อินเทอร์เน็ตแห่งสรรพสิ่ง (IoT)
  - ระบบบนชิป (SoC)
  - วงจรผสานรวมเฉพาะ แอปพลิเคชัน (ASIC)
  - อาร์เรย์ของเกตแบบตั้งโปรแกรมด้วยเขตข้อมูลได้ (FPGA)
- **ICS/การควบคุมกำกับดูแล และเก็บข้อมูล (SCADA)**
  - ตัวควบคุมลอจิกแบบตั้งโปรแกรมได้ (PLC)
  - Historian
  - Ladder logic
  - ระบบรักษาความปลอดภัยด้วยเครื่องมือวัด
  - การทำความร้อน ระบายอากาศ และปรับอากาศ (HVAC)
- **โปรโตคอล**
  - บัสการควบคุมพื้นที่เครือข่าย (CAN)
  - Modbus
  - โปรโตคอลเครือข่ายแบบกระจาย 3 (DNP3)
  - Zigbee
  - โปรโตคอลระดับอุตสาหกรรมที่พบได้บ่อย (CIP)
  - บริการกระจายข้อมูล
- **ภาคส่วน**
  - พลังงาน
  - การผลิต
  - สาธารณสุข
  - สาธารณูปโภค
  - บริการสารธารณะ
  - บริการสิ่งอำนวยความสะดวก

3.4 อธิบายว่าการปรับใช้เทคโนโลยีระบบคลาวด์ส่งผลกระทบต่อการรักษาความปลอดภัยระดับองค์กรอย่างไร

- **การทำงานโดยอัตโนมัติและความราบรื่น**
- **การกำหนดค่าการเข้ารหัส**
- **บันทึก**
  - ความพร้อมใช้งาน
  - การรวบรวมข้อมูล
  - การตรวจสอบ
  - การกำหนดค่า
  - การแจ้งเตือน
- **การตรวจสอบการกำหนดค่า**
- **การเป็นเจ้าของคีย์และตำแหน่งที่ตั้ง**
- **การจัดการวงจรชีวิตคีย์**
- **วิธีการสำรองข้อมูลและการกู้คืน**
  - การใช้ระบบคลาวด์เพื่อความต่อเนื่องทางธุรกิจ และการฟื้นฟูธุรกิจหลังภัยพิบัติ (BCDR)
  - ผู้ให้บริการ BCDR หลัก
  - ผู้ให้บริการ BCDR สำรอง
- **การประมวลผลด้านโครงสร้างพื้นฐานเทียบกับแบบไร้เซิร์ฟเวอร์**
- **การจำลองระบบเสมือนของแอปพลิเคชัน (application virtualization)**
- **ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์ (software-defined networking)**
- **การกำหนดค่าที่ไม่ถูกต้อง**
- **เครื่องมือการทำงานร่วมกัน**
- **การกำหนดค่าพื้นที่จัดเก็บ**
  - การแยกบิต (bit splitting)
  - การกระจายของข้อมูล (data dispersion)
- **ผู้ให้บริการตรวจสอบและบริหารจัดการสิทธิด้านความปลอดภัยบนระบบคลาวด์ (CASB)**

3.5 ปรับใช้โซลูชัน PKI ที่เหมาะสมตามข้อกำหนดทางธุรกิจที่ให้มา

- **ลำดับชั้นของ PKI**
  - ผู้ให้บริการออกใบรับรอง (CA)
  - ผู้ให้บริการออกใบรับรองในสังกัด/กลาง (subordinate/intermediate CA)
  - เจ้าหน้าที่รับลงทะเบียน (RA)
- **ประเภทใบรับรอง**
  - ใบรับรองแบบ wildcard
  - Extended validation
  - Multidomain
  - ใช้งานได้หลายด้าน
- **การใช้งาน/โปรไฟล์/แม่แบบใบรับรอง**
  - การยืนยันตัวตนไคลเอ็นต์
  - การยืนยันตัวตนเซิร์ฟเวอร์
  - ลายเซ็นดิจิทัล
  - การเซ็นกำกับโค้ด (code signing)
- **นามสกุล**
  - ชื่อสามัญ (CN)
  - ชื่อสำรองของซับเจ็กต์ (SAN)
- **ผู้ให้บริการที่เชื่อถือได้**
- **แบบจำลองความเชื่อมั่น**
- **การรับรองแบบข้ามสาย**
- **กำหนดค่าโปรไฟล์**
- **การจัดการวงจรชีวิต**
- **คีย์สาธารณะและส่วนตัว**
- **ลายเซ็นดิจิทัล**
- **Certificate pinning**
- **Certificate stapling**
- **คำขอลงชื่อใบรับรอง (CSR)**
- **โปรโตคอลสถานะใบรับรองออนไลน์ (OCSP) เทียบกับรายการเพิกถอนใบรับรอง (CRL)**
- **การรักษาความปลอดภัยในการส่งข้อมูล HTTP แบบเข้มงวด (HSTS)**

3.6 ปรับใช้โปรโตคอลและอัลกอริธึมวิทยาการเข้ารหัสลับที่เหมาะสมตามข้อกำหนดทางธุรกิจที่ให้มา

- **การแฮช**
  - อัลกอริธึมแฮชเพื่อความปลอดภัย (SHA)
  - โค้ดตรวจสอบข้อความ อิงตามแฮช (HMAC)
  - เมสเสจไดเจสต์ (MD)
  - เมสเสจไดเจสต์การประเมินความสมบูรณ์ของ RACE เบื้องต้น (RIPEMD)
  - Poly1305
- **อัลกอริธึมแบบสมมาตร**
  - โหมดการทำงาน
    - Galois/โหมดตัวนับ (GCM)
    - Electronic codebook (ECB)
    - Cipher block chaining (CBC)
    - Counter (CTR)
    - ข้อมูลย้อนกลับของเอาต์พุต (OFB)
  - สตรีมและบล็อก
    - มาตรฐานการเข้ารหัส ขั้นสูง (AES)
    - มาตรฐานการเข้ารหัส ทางดิจิทัลแบบสามเท่า (3DES)
    - ChaCha
    - Salsa20
- **อัลกอริธึมแบบอสมมาตร**
  - ความพ้องกันของคีย์
    - Diffie-Hellman
    - Elliptic-curve Diffie-Hellman (ECDH)
  - การลงชื่อ (Signing)
    - อัลกอริธึมลายเซ็นดิจิทัล (DSA)
    - Rivest, Shamir, and Adleman (RSA)
    - อัลกอริธึมลายเซ็นดิจิทัล แบบ Elliptic-curve (ECDSA)
- **โปรโตคอล**
  - Secure Socket Layer (SSL)/ Transport Layer Security (TLS)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Internet Protocol Security (IPSec)
  - Secure Shell (SSH)
  - EAP
- **วิทยาการเข้ารหัสลับแบบ elliptic curve**
  - P256
  - P384
- **การรักษาความปลอดภัยในอนาคต (forward secrecy)**
- **การเข้ารหัสโดยมีการยืนยันตัวตน ด้วยข้อมูลที่เกี่ยวข้อง**
- **การยืดความยาวของคีย์ (key stretching)**
  - ฟังก์ชันการหาคีย์ ด้วยรหัสผ่าน 2 (PBKDF2)
  - Bcrypt

3.7 แก้ไขปัญหาด้วยการใช้วิทยาการเข้ารหัสลับตามสถานการณ์สมมติ

- **ปัญหาด้านการดำเนินการใช้และการกำหนดค่า**
  - วันที่มีผลใช้งานได้ (validity dates)
  - ประเภทใบรับรองที่ไม่ถูกต้อง
  - ใบรับรองที่ถูกเพิกถอน
  - ชื่อที่ไม่ถูกต้อง
  - ปัญหาห่วงโซ่
    - รูตหรือ CA กลางไม่ถูกต้อง
    - ลงชื่อด้วยตนเอง
  - อัลกอริธึมการลงชื่อที่เปราะบาง
  - cipher suite ที่เปราะบาง
  - การอนุญาตที่ไม่ถูกต้อง
  - การจับคู่ cipher ที่ไม่ถูกต้อง
  - การดาวน์เกรด
- **คีย์**
  - จับคู่ไม่ถูกต้อง
  - การจัดการคีย์ไม่เหมาะสม
  - คีย์แบบฝังตัว
  - การใส่คีย์ซ้ำ (rekeying)
  - คีย์ส่วนตัวที่มีความเสี่ยง
  - การลบข้อมูลโดยเขียนคีย์เข้ารหัสทับ (crypto shredding)
  - การปกปิดวิทยาการเข้ารหัสลับ (cryptographic obfuscation)
  - การหมุนเวียนคีย์ (key rotation)
  - คีย์ที่ถูกบุกรก (compromised keys)

4.0 การกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อบังคับ

4.1 นำกลยุทธ์ด้านความเสี่ยงที่เหมาะสมไปใช้ตามชุดข้อกำหนดที่ให้มา

- **การประเมินความเสี่ยง**
  - ความเป็นไปได้
  - ผลกระทบ
  - เชิงคุณภาพเทียบกับเชิงปริมาณ
  - ปัจจัยการสัมผัสความเสี่ยง
  - มูลค่าสินทรัพย์
  - ต้นทุนการเป็นเจ้าของโดยรวม (TCO)
  - ผลตอบแทนจากการลงทุน (ROI)
  - ระยะเวลาเฉลี่ยในการกู้คืน (MTTR)
  - ระยะเวลาเฉลี่ยระหว่างเกิดความล้มเหลว (MTBF)
  - ค่าความสูญเสียที่อาจเกิดขึ้นต่อปี (ALE)
  - อัตราการเกิดเหตุการณ์ต่อปี (ARO)
  - ค่าความสูญเสียที่อาจเกิดขึ้นครั้งเดียว (SLE)
  - การวิเคราะห์ช่องว่าง (gap analysis)
- **เทคนิคการจัดการความเสี่ยง**
  - ถ่ายโอน
  - ยอมรับ
  - หลีกเลี่ยง
  - บรรเทา
- **ประเภทความเสี่ยง**
  - ที่แฝงอยู่
  - ที่เหลือตกค้าง
  - ข้อยกเว้น
- **วงจรชีวิตการจัดการความเสี่ยง**
  - ระบุปัญหา
  - ประเมิน
  - การควบคุม
    - บุคลากร
    - กระบวนการ
    - เทคโนโลยี
    - ปกป้อง
    - ตรวจจับ
    - ตอบสนอง
    - กู้คืน
  - ทบทวน
  - กรอบการทำงาน
- **การติดตามร่องรอยความเสี่ยง**
  - ทะเบียนข้อมูลความเสี่ยง
  - สัญญาณบ่งชี้ประสิทธิภาพสำคัญ
    - ความสามารถในการปรับขนาด (scalability)
    - ความน่าเชื่อถือ
    - ความพร้อมใช้งาน
  - สัญญาณบ่งชี้ความเสี่ยงสำคัญ
- **ความเสี่ยงที่ยอมรับได้เทียบกับความเสี่ยงที่ทนได้**
  - การวิเคราะห์จุดสมดุล
  - ข้อกำหนดด้านความสามารถในการใช้งานเทียบกับการรักษาความปลอดภัย
- **นโยบายและแนวปฏิบัติด้านการรักษาความปลอดภัย**
  - การแบ่งแยกหน้าที่
  - การหมุนเวียนเปลี่ยนงาน
  - การบังคับลาพักร้อน
  - การให้สิทธิ์ให้น้อยที่สุดเท่าที่เป็นไปได้
  - ระเบียบการจ้างงาน และการเลิกจ้าง
  - การฝึกอบรมและการสร้างความตระหนักสำหรับผู้ใช้
  - ข้อกำหนดการตรวจสอบและความถี่

4.2 อธิบายความสำคัญของการจัดการและการบรรเทาความเสี่ยงของผู้จำหน่าย

- **โมเดลความรับผิดชอบร่วมกัน (บทบาท/ความรับผิดชอบ)**
  - ผู้ให้บริการระบบคลาวด์ (CSP)
    - ตำแหน่งทางภูมิศาสตร์
    - โครงสร้างพื้นฐาน
    - หน่วยประมวลผล
    - พื้นที่จัดเก็บ
    - การสร้างเครือข่าย
    - บริการ
  - ไคลเอ็นต์
    - การเข้ารหัสลับ
    - ระบบปฏิบัติการ
    - แอปพลิเคชัน
    - ข้อมูล
- **vendor lock-in และ vendor lockout**
- **ความสามารถในการอยู่รอดของผู้จำหน่าย (vendor viability)**
  - ความเสี่ยงด้านการเงิน
  - ความเสี่ยงด้านการควบรวมหรือการครอบครอง
- **การปฏิบัติตามข้อกำหนดของลูกค้า**
  - ฝ่ายกฎหมาย
  - การจัดการการเปลี่ยนแปลง
  - อัตราการลาออกของพนักงาน
  - อุปกรณ์และการกำหนดค่าทางเทคนิค
- **ความพร้อมด้านการสนับสนุน**
- **ข้อควรพิจารณาด้านภูมิศาสตร์**
- **ทัศนวิสัยในระบบห่วงโซ่อุปทาน**
- **ข้อกำหนดด้านการรายงานอุบัติการณ์**
- **ระบบรับฝากซอร์สโค้ด (source code escrows)**
- **เครื่องมือประเมินผู้จำหน่ายที่ดำเนินการอยู่**
- **การพึ่งพาบุคคลภายนอก**
  - โค้ด
  - ฮาร์ดแวร์
  - โมดูล
- **ข้อควรพิจารณาทางเทคนิค**
  - การทดสอบทางเทคนิค
  - การแบ่งส่วนเครือข่าย
  - การควบคุมการส่งต่อ
  - ข้อมูลการเข้าใช้ระบบที่ใช้ร่วมกัน

4.3 อธิบายกรอบการทำงานด้านการปฏิบัติตามข้อบังคับและข้อควรพิจารณาทางกฎหมาย รวมทั้งผลกระทบระดับองค์กรของสิ่งเหล่านั้น

- **ข้อกังวลด้านความปลอดภัยในการผสานรวมอุตสาหกรรมที่มีความหลากหลาย**
- **ข้อควรพิจารณาด้านข้อมูล**
  - อธิปไตยด้านข้อมูล
  - ความเป็นเจ้าของข้อมูล
  - การจำแนกประเภทข้อมูล
  - การเก็บรักษาข้อมูล
  - ชนิดข้อมูล
    - สุขภาพ
    - การเงิน
    - ทรัพย์สินทางปัญญา
    - ข้อมูลที่ระบุตัวบุคคลได้ (PII)
  - การลบ การกำจัด และการทำลายข้อมูล
- **ข้อควรพิจารณาด้านภูมิศาสตร์**
  - ตำแหน่งที่ตั้งของข้อมูล
  - ตำแหน่งที่ตั้งของซับเจกต์ของข้อมูล
  - ตำแหน่งที่ตั้งของผู้ให้บริการระบบคลาวด์
- **การพิสูจน์การปฏิบัติตามข้อบังคับของบุคคลที่ภายนอก**
- **กฎระเบียบ การรับรอง และมาตรฐาน**
  - มาตรฐานความปลอดภัย ของข้อมูลบัตรชำระเงินในอุตสาหกรรม (PCI DSS)
  - กฎระเบียบว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคลทั่วไป (GDPR)
  - องค์การระหว่างประเทศว่าด้วย การวางมาตรฐาน (ISO)
  - การผสานรวมโมเดลวัดวุฒิภาวะ ความสามารถ (CMMI)
  - สถาบันมาตรฐาน และเทคโนโลยีแห่งชาติ (NIST)
  - กฎหมายคุ้มครองความเป็นส่วนตัว ทางออนไลน์ของเด็ก (COPPA)
  - หลักเกณฑ์ทั่วไป
  - Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)
- **ข้อควรพิจารณาทางกฎหมาย**
  - การสอบทานทางธุรกิจ
  - ความระมัดระวังตามสมควร
  - การควบคุมการนำออก
  - คำสั่งให้เก็บข้อมูลเพื่อการดำเนินคดี (legal hold)
  - การค้นพบทางอิเล็กทรอนิกส์ (E-discovery)
- **ประเภทสัญญาและข้อตกลง**
  - สัญญาระดับการให้บริการ (SLA)
  - สัญญาต้นแบบการให้บริการ (MSA)
  - ข้อตกลงไม่เปิดเผยข้อมูล (NDA)
  - บันทึกความเข้าใจ (MOU)
  - ข้อตกลงการรักษาความปลอดภัยในการเชื่อมต่อระหว่างกัน (ISA)
  - ข้อตกลงระดับการดำเนินการ
  - ข้อตกลงระดับความเป็นส่วนตัว

4.4 อธิบายความสำคัญของแนวคิดด้านความต่อเนื่องทางธุรกิจและการฟื้นฟูธุรกิจหลังภัยพิบัติ

- **การวิเคราะห์ผลกระทบทางธุรกิจ**
  - ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายได้
  - เวลากู้คืนระบบที่ยอมรับได้
  - ระดับการให้บริการกู้คืนระบบ
  - การทำงานที่จำเป็นสำหรับภารกิจ
- **การประเมินผลกระทบด้านความเป็นส่วนตัว**
- **แผนการฟื้นฟูธุรกิจหลังภัยพิบัติ (DRP)/แผนความต่อเนื่องทางธุรกิจ (BCP)**
  - Cold site
  - Warm site
  - Hot site
  - Mobile site
- **แผนการตอบสนองต่อเหตุการณ์**
  - บทบาท/ความรับผิดชอบ
  - รายงานหลังการดำเนินการ
- **แผนการทดสอบ**
  - รายการตรวจสอบ
  - การอธิบายอย่างละเอียด
  - การฝึกซ้อมแผนบนโต๊ะ
  - การทดสอบเสมือนเหตุการณ์จริงเต็มรูปแบบ (full interruption test)
  - การทดสอบแบบคู่ขนาน/การทดสอบด้วยสถานการณ์จำลอง

รายการคำย่อของ CASP+ (CAS-004)

รายการต่อไปนี้คืออักษรย่อที่ปรากฏในข้อสอบประกาศนียบัตร CompTIA CASP+ ผู้สมัครสอบควรทบทวนรายการทั้งหมดและศึกษาหาความรู้ในการปฏิบัติงานเกี่ยวกับอักษรย่อทั้งหมดเพื่อการเตรียมความพร้อมสำหรับการสอบที่ครอบคลุม

คำย่อ	คำเต็ม
2FA	Two-Factor Authentication (การยืนยันตัวตน 2 ขั้นตอน)
3DES	Triple Digital Encryption Standard (มาตรฐานการเข้ารหัสทางดิจิทัลแบบสามเท่า)
ACL	Access Control List (รายการควบคุมการเข้าถึง)
AES	Advanced Encryption Standard (มาตรฐานการเข้ารหัสลับขั้นสูง)
AJAX	Asynchronous JavaScript และ XML
ALE	Annualized Loss Expectancy (ค่าความสูญเสียที่อาจเกิดขึ้นต่อปี)
API	Application Programming Interface (ส่วนต่อประสานโปรแกรมประยุกต์)
APT	Advanced Persistent Threat (ภัยคุกคามแบบถาวรขั้นสูง)
ARF	Asset Reporting Format (รูปแบบการรายงานสินทรัพย์)
ARO	Annualized Rate of Occurrence (อัตราการเกิดเหตุการณ์ต่อปี)
ASIC	Application-Specific Integrated Circuit (วงจรผสานรวมเฉพาะแอปพลิเคชัน)
ASLR	Address Space Layout Randomization (การสุ่มตำแหน่งพื้นที่ที่อยู่)
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge (แพลตฟอร์มจัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ)
BCDR	Business Continuity and Disaster Recovery (ความต่อเนื่องทางธุรกิจและการฟื้นฟูธุรกิจหลังภัยพิบัติ)
BCP	Business Continuity Plan (แผนความต่อเนื่องทางธุรกิจ)
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BYOD	Bring Your Own Device (การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานเอง)
CA	Certificate Authority (ผู้ให้บริการออกใบรับรอง)
CAN	Controller Area Network (การควบคุมพื้นที่เครือข่าย)
CASB	Cloud Access Security Broker (ผู้ให้บริการตรวจสอบและบริหารจัดการสิทธิด้านความปลอดภัยบนระบบคลาวด์)
CBC	Cipher Block Chaining
CCE	Common Configuration Enumeration (การระบุการกำหนดค่าที่พบได้บ่อย)
CI/CD	Continuous Integration (การบูรณาการอย่างต่อเนื่อง) / Continuous Delivery (การส่งมอบอย่างต่อเนื่อง)
CIP	Common Industrial Protocol (โปรโตคอลระดับอุตสาหกรรมที่พบได้บ่อย)
CMDB	Configuration Database Management (การจัดการฐานข้อมูลการกำหนดค่า)
CMMI	Capability Maturity Model Integration (การผสานรวมโมเดลวัดวุฒิภาวะความสามารถ)
CN	Common Name (ชื่อสามัญ)
COPE	Corporate Owned, Personally Enabled (การที่บริษัทเป็นเจ้าของอุปกรณ์ที่จะแจกจ่ายให้พนักงานได้เลือกใช้)
COPPA	Children's Online Privacy Protection Act (กฎหมายคุ้มครองความเป็นส่วนตัวทางออนไลน์ของเด็ก)
CPE	Common Platform Enumeration (การระบุแพลตฟอร์มทั่วไป)
CPU	Central Processing Unit (หน่วยประมวลผลกลาง)
CRL	Certificate Revocation List (รายการเพิกถอนใบรับรอง)
CRM	Customer Relationship Management (การจัดการความสัมพันธ์ลูกค้า)
CSA	Cloud Security Alliance
CSP	Cloud Service Provider (ผู้ให้บริการระบบคลาวด์)
CSR	Certificate Signing Request (คำขอลงชื่อใบรับรอง)
CSRF	Cross-Site Request Forgery (การปลอมแปลงคำขอข้ามไซต์)
CVE	Common Vulnerabilities and Exposures (ช่องโหว่และการสัมผัสความเสี่ยงที่พบได้บ่อย)
CVSS	Common Vulnerability Scoring System (ระบบการจัดลำดับช่องโหว่ทั่วไป)
CYOD	Choose Your Own Device (การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานโดยบริษัทเป็นผู้กำหนด)
DAC	Discretionary Access Control (การควบคุมการเข้าถึงแบบมีเงื่อนไข)
DAST	Dynamic Application Security Testing (การทดสอบการรักษาความปลอดภัยของแอปพลิเคชันแบบไดนามิก)
DDoS	Distributed Denial of Service (การโจมตีโดยปฏิเสธการให้บริการ)
DEP	Data Execution Prevention (การป้องกันการดำเนินการข้อมูล)
DLP	Data Loss Prevention (การป้องกันข้อมูลสูญหาย)
DNP3	Distributed Network Protocol 3 (โปรโตคอลเครือข่ายแบบกระจาย 3)
DNS	Domain Name System (ระบบที่มีไว้สำหรับบริหารจัดการข้อมูลของชื่อโดเมนเนม)
DNSSEC	Domain Name System Security Extensions (ระบบรักษาความปลอดภัยที่คอยดูแลข้อมูลต่างๆ ที่อยู่บนโลกอินเทอร์เน็ต)
DoH	DNS over HTTPS
DoS	Denial of Service (การปฏิเสธการให้บริการ)
DRM	Digital Rights Management (การจัดการสิทธิ์ดิจิทัล)
DRP	Disaster Recovery Plan (แผนการฟื้นฟูธุรกิจหลังภัยพิบัติ)

คำย่อ	คำเต็ม
DSA	Digital Signature Algorithm (อัลกอริธึมลายเซ็นดิจิทัล)
EAP	Extensible Authentication Protocol (โปรโตคอลการยืนยันตัวตนแบบขยายได้)
ECB	Electronic Codebook
ECDH	Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response (การตรวจจับและการตอบสนองต่อภัยคุกคามไซเบอร์ให้แก่ระบบ Endpoint)
ERP	Enterprise Resource Planning (การวางแผนทรัพยากรขององค์กร)
ESB	Enterprise Service Bus (บัสบริการองค์กร)
FIM	File Integrity Monitoring (การติดตามตรวจสอบความสมบูรณ์ของไฟล์)
FPGA	Field-Programmable Gate Array (อาร์เรย์ของเกตแบบตั้งโปรแกรมด้วยเขตข้อมูลได้)
FTK	Forensic Toolkit (เครื่องมือการตรวจพิสูจน์หลักฐาน)
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation (กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลทั่วไป)
HIDS	Host-based Intrusion Detection System (ระบบตรวจจับการบุกรุกแบบอิงตามโฮสต์)
HIPS	Host-based Intrusion Prevention System (ระบบป้องกันการบุกรุกแบบอิงตามโฮสต์)
HMAC	Hash-based Message Authentication Code (โค้ดตรวจสอบข้อความอิงตามแฮช)
HOTP	HMAC-based One-Time Password (รหัสผ่านแบบใช้ครั้งเดียวที่อิงตาม HMAC)
HSM	Hardware Security Module (โมดูลรักษาความปลอดภัยของฮาร์ดแวร์)
HSTS	HTTP Strict Transport Security (การรักษาความปลอดภัยในการส่งข้อมูล HTTP แบบเข้มงวด)
HTML	Hypertext Markup Language (ภาษามาร์กอัปแบบ Hypertext)
HTTP	Hypertext Transfer Protocol (โปรโตคอลสื่อสารสำหรับการแลกเปลี่ยนสารสนเทศผ่านอินเทอร์เน็ต)
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, and Air Conditioning (การทำความร้อน ระบายอากาศ และปรับอากาศ)
IaaS	Infrastructure as a Service (การให้บริการโครงสร้างพื้นฐาน)
IAST	Interactive Application Security Testing (การทดสอบการรักษาความปลอดภัยของแอปพลิเคชันแบบโต้ตอบ)
ICS	Industrial Control System (ระบบควบคุมทางอุตสาหกรรม)
IDS	Intrusion Detection System (ระบบตรวจจับการบุกรุก)
IoT	Internet of Things (อินเทอร์เน็ตแห่งสรรพสิ่ง)
IP	Internet Protocol (อินเทอร์เน็ตโปรโตคอล)
IPS	Intrusion Prevention System (ระบบป้องกันการบุกรุก)
IPSec	Internet Protocol Security (การรักษาความปลอดภัยอินเทอร์เน็ตโปรโตคอล)
ISA	Interconnection Security Agreement (ข้อตกลงการรักษาความปลอดภัยในการเชื่อมต่อระหว่างกัน)
ISAC	Information Sharing Analysis Center (ศูนย์การวิเคราะห์และแบ่งปันข้อมูล)
ISO	International Organization for Standardization (องค์การระหว่างประเทศว่าด้วยการวางมาตรฐาน)
ISP	Internet Service Provider (ผู้ให้บริการอินเทอร์เน็ต)
JSON	JavaScript Object Notation
JWT	JSON Web Token
KVM	Keyboard, Video, and Mouse (แป้นพิมพ์ วิดีโอ และเมาส์)
LAN	Local Area Network (ระบบเครือข่ายภายในพื้นที่)
LDAP	Lightweight Directory Access Protocol (โปรโตคอลที่ใช้ในการค้นหาและเข้าถึงข้อมูลหรือออบเจ็กต์ต่างๆ ได้อย่างรวดเร็วด้วยระบบไดเรกทอรี)
MAC	Mandatory Access Control (การควบคุมการเข้าถึงแบบบังคับ)
MD	Message Digest
MFA	Multifactor Authentication (การยืนยันตัวตนแบบหลายปัจจัย)
MOU	Memorandum of Understanding (บันทึกความเข้าใจ)
MSA	Master Service Agreement (สัญญาต้นแบบการให้บริการ)
MTBF	Mean Time Between Failure (ระยะเวลาเฉลี่ยระหว่างเกิดความล้มเหลว)
MTTR	Mean Time to Recovery (ระยะเวลาเฉลี่ยในการกู้คืน)
NAC	Network Access Control (การควบคุมการเข้าถึงเครือข่าย)
NAT	Network Address Translation (การแปลงที่อยู่เครือข่าย)
NDA	Non-Disclosure Agreement (ข้อตกลงไม่เปิดเผยข้อมูล)
NFC	Near Field Communication (การสื่อสารไร้สายระยะใกล้)
NGFW	Next Generation Firewall (ไฟร์วอลล์รุ่นถัดไป)
NIC	Network Interface Controller (ตัวควบคุมการเชื่อมต่อเครือข่าย)
NIDS	Network Intrusion Detection System (ระบบตรวจจับการบุกรุกบนเครือข่าย)
NIPS	Network Intrusion Prevention System (ระบบป้องกันการบุกรุกบนเครือข่าย)
NIST	National Institute of Standards and Technology (สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ)
NX	No Execute
OCSP	Online Certificate Status Protocol (โปรโตคอลสถานะใบรับรองออนไลน์)
OEM	Original Equipment Manufacturer (ผู้ผลิตอุปกรณ์ดั้งเดิม)
OFB	Output Feedback (ข้อมูลย้อนกลับของเอาต์พุต)
OS	Operating System (ระบบปฏิบัติการ)
OSINT	Open-Source Intelligence (ข่าวกรองแบบโอเพ่นซอร์ส)
OTP	One-Time Password (รหัสผ่านแบบใช้ครั้งเดียว)
OVAL	Open Vulnerability and Assessment Language (ภาษาการประเมินช่องโหว่แบบเปิด)
OWASP	Open Web Application Security Project (องค์กรรักษาความปลอดภัยด้านโอเพ่นเว็บแอปพลิเคชัน)
PaaS	Platform as a Service (การให้บริการแพลตฟอร์ม)
PBKDF2	Password-Based Key Derivation Function 2 (ฟังก์ชันการหาคีย์ด้วยรหัสผ่าน 2)
PBX	Private Branch Exchange
PCAP	Packet Capture (การจับแพ็กเก็ต)
PCI DSS	Payment Card Industry Data Security Standard (มาตรฐานความปลอดภัยของข้อมูลบัตรชำระเงินในอุตสาหกรรม)
PGP	Pretty Good Privacy
PII	Personal Identifiable Information (ข้อมูลที่ระบุตัวบุคคลได้)
PKI	Public Key Infrastructure (โครงสร้างพื้นฐานคีย์สาธารณะ)
PLC	Programmable Logic Controller (ตัวควบคุมลอจิกแบบตั้งโปรแกรมได้)
PSK	Pre-Shared Key
QoS	Quality of Service (คุณภาพการบริการ)

คำย่อ	คำเต็ม
RA	Registration Authority (เจ้าหน้าที่รับลงทะเบียน)
RACE	Research and Development in Advanced Communications Technologies in Europe (การวิจัยและพัฒนาด้านเทคโนโลยีการสื่อสารขั้นสูงในยุโรป)
RADIUS	Remote Authentication Dial-in User Server (เซิร์ฟเวอร์การยืนยันตัวตนผู้ใช้ที่ต้องการเชื่อมต่อจากระยะไกล)
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol (โปรโตคอลเดสก์ท็อประยะไกล)
REST	Representational State Transfer (การถ่ายโอนสถานะที่เป็นตัวแทน)
RF	Radio Frequency (ความถี่วิทยุ)
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment (ผลตอบแทนจากการลงทุน)
RPO	Recovery Point Objective (ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายได้)
RSA	Rivest, Shamir, and Adleman
RTO	Recovery Time Objective (เวลากู้คืนระบบที่ยอมรับได้)
RTU	Remote Terminal Unit (ระบบควบคุมและหน่วยทำงานระยะไกล)
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service (การให้บริการซอฟต์แวร์)
SAE	Simultaneous Authentication of Equals
SAML	Security Assertion Markup Language (ภาษามาร์กอัปเพื่อยืนยันความปลอดภัย)
SAN	Subject Alternate Name (ชื่อสำรองของซับเจ็กต์)
SASE	Secure Access Service Edge
SAST	Static Application Security Testing (การทดสอบการรักษาความปลอดภัยของแอปพลิเคชันแบบคงที่)
SCADA	Supervisory Control and Data Acquisition (การควบคุมกำกับดูแลและเก็บข้อมูล)
SCAP	Security Content Automation Protocol (โปรโตคอลรักษาความปลอดภัยเนื้อหาอัตโนมัติ)
SDN	Software-Defined Networking (ระบบเครือข่ายที่กำหนดโดยซอฟต์แวร์)
SDR	Software-Defined Radio (การสื่อสารทางคลื่นวิทยุที่กำหนดโดยซอฟต์แวร์)
SD-WAN	Software-Defined Wide Area Network (เครือข่ายบริเวณกว้างที่กำหนดโดยซอฟต์แวร์)
SEAndroid	Security Enhanced Android
SED	Self-Encrypting Drive (ไดรฟ์เข้ารหัสตัวเอง)
SELinux	Security Enhanced Linux
SFTP	SSH File Transfer Protocol (โปรโตคอลการถ่ายโอนไฟล์ SSH อย่างปลอดภัย)
SHA	Secure Hashing Algorithm (อัลกอริธึมการแฮชที่ปลอดภัย)
SIEM	Security Information Event Management (การจัดการเหตุการณ์ข้อมูลด้านความปลอดภัย)
SLA	Service-Level Agreement (สัญญาระดับการให้บริการ)
SLE	Single Loss Expectancy (ค่าความสูญเสียที่อาจเกิดขึ้นครั้งเดียว)
SMB	Server Message Block (โปรโตคอลมาตรฐานเครือข่ายที่ใช้แชร์ไฟล์)
SNMP	Simple Network Management Protocol (โปรโตคอลการจัดการเครือข่ายอย่างง่าย)
SOA	Start of Authority
SOAP	Simple Object Access Protocol (โปรโตคอลเข้าถึงอ็อบเจกต์อย่างง่าย)
SOAR	Security Orchestration, Automation, and Response (การทำงานของระบบความปลอดภัยให้ราบรื่น ทำงานแบบอัตโนมัติ เพิ่มความเร็วในการตอบสนองต่อเหตุการณ์ภัยไซเบอร์)
SoC	System-on-Chip (ระบบบนชิป)
SPAN	Switched Port Analyzer (ตัววิเคราะห์พอร์ตแบบสวิตช์)
SQL	Structured Query Language (ภาษามาตรฐานในการเข้าถึงฐานข้อมูล)
SSH	Secure Shell (โปรโตคอลสำหรับเครือข่ายคอมพิวเตอร์ ที่ออกแบบมาเพื่อให้เข้าถึงไปยังคอมพิวเตอร์เครื่องอื่น)
SSL	Secure Sockets Layer (ชั้นซ็อกเก็ตปลอดภัย)
SSO	Single Sign-On (การลงชื่อเข้าใช้ทุกระบบในครั้งเดียว)
STAR	Security Trust Assurance and Risk
TACACS	Terminal Access Controller Access Control System (ระบบควบคุมการเข้าถึงตัวควบคุมการเข้าถึงเทอร์มินัล)
TAP	Test Access Points (อุปกรณ์กระจายสัญญาณทดสอบ)
TCO	Total Cost of Ownership (ต้นทุนการเป็นเจ้าของโดยรวม)
TLS	Transport Layer Security (โปรโตคอลความปลอดภัยที่เข้ารหัสอีเมล)
TOTP	Time-Based One-Time Password (รหัสผ่านแบบใช้ครั้งเดียวที่อิงตามเวลา)
TPM	Trusted Platform Module (โมดูลแพลตฟอร์มที่เชื่อถือได้)
UEBA	User and Entity Behavior Analytics (การวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี)
UEFI	Unified Extensible Firmware Interface (ส่วนต่อประสานเฟิร์มแวร์ที่ขยายได้แบบรวมกัน)
UTM	Unified Threat Management (การจัดการภัยคุกคามเบ็ดเสร็จในเครื่องเดียว)
VDI	Virtual Desktop Infrastructure (โครงสร้างพื้นฐานเดสก์ท็อปเสมือนจริง)
VLAN	Virtual Local Area Network (การแยกการเชื่อมต่อเครือข่ายคอมพิวเตอร์เป็นส่วนๆ)
VM	Virtual Machine
VNET	Virtual Network (เครือข่ายเสมือน)
VNET	Virtual Network (เครือข่ายเสมือน)
VoIP	Voice over Internet Protocol (วอยซ์โอเวอร์ไอพี)
VPC	Virtual Private Cloud (คลาวด์ส่วนตัวเสมือน)
VPN	Virtual Private Network (เครือข่ายส่วนตัวเสมือน)
WAF	Web Application Firewall (ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน)
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System (ระบบตรวจจับการบุกรุกแบบไร้สาย)
WIPS	Wireless Intrusion Prevention System (ระบบป้องกันการบุกรุกแบบไร้สาย)
WPA	WiFi Protected Access (การเข้าใช้งาน WiFi ที่ได้รับการป้องกัน)
WS	Web Services (การให้บริการบนเว็บ)
XCCDF	Extensible Configuration Checklist Description Format (รูปแบบการอธิบายรายการตรวจสอบการกำหนดค่าแบบขยายได้)
XML	Extensible Markup Language (ภาษามาร์กอัปแบบขยายได้)
XN	Execute Never
XSS	Cross-Site Scripting (การเขียนสคริปต์ข้ามไซต์)

รายการฮาร์ดแวร์และซอฟต์แวร์ที่มีการเสนอสำหรับข้อสอบ CASP+

CompTIA แนบตัวอย่างรายการฮาร์ดแวร์และซอฟต์แวร์มาในที่นี้เพื่อช่วยเหลือผู้สมัครสอบในการเตรียมตัวสอบ CASP+ รายการนี้อาจมีประโยชน์ต่อบริษัทฝึกอบรมที่ต้องการสร้างองค์ประกอบห้องปฏิบัติการสำหรับจัดการฝึกอบรม รายการย่อยในแต่ละหัวข้อเป็นเพียงตัวอย่างโดยคร่าวเท่านั้น

อุปกรณ์

- แล็ปท็อป
- ฮาร์ดแวร์เซิร์ฟเวอร์พื้นฐาน (เซิร์ฟเวอร์อีเมล/เซิร์ฟเวอร์ไดเรกทอรีแบบแอคทีฟ, OS ที่เชื่อถือได้)
- โทเค็น
- อุปกรณ์เคลื่อนที่ (Android และ iOS)
- สวิตช์ (สวิตช์ประเภท managed)—สามารถใช้งาน IPv6
- เกตเวย์/เราเตอร์—สามารถใช้งาน IPv6 (แบบสาย/แบบไร้สาย)
- ไฟร์วอลล์
- VoIP
- เซิร์ฟเวอร์พรอกซี
- เครื่องกระจายโหลด (Load Balancer)
- NIPS
- HSM
- อุปกรณ์กระจายสัญญาณ
- คริปโตการ์ด (Crypto cards)
- สมาร์ทการ์ด
- ตัวอ่านสมาร์ทการ์ด
- อุปกรณ์ตรวจสอบทางชีวภาพ
- Arduino/Raspberry Pi
- ระบบ SCADA: RTUs และ PLCs

ฮาร์ดแวร์สำรอง

- แป้นพิมพ์
- สายเคเบิล
- NICs
- อุปกรณ์จ่ายไฟ
- สื่อที่ถอดออกได้
- การ์ดจอกำลังไฟสูง

เครื่องมือ

- เครื่องวิเคราะห์สเปคตรัม
- เสาอากาศ
- ฮาร์ดแวร์การแฮก RF/SDR
- โทเค็น RSA
- สวิตช์ KVM

ซอฟต์แวร์

- อุปกรณ์เสมือน (ไฟร์วอลล์, IPS, โซลูชัน SIEM, การยืนยันตัวตน RSA, asterisk PBX)
- Windows
- Linux distros
- VMware Player/VirtualBox
- เครื่องมือการประเมินช่องโหว่
- ยูทิลิตี SSH และ Telnet
- เครื่องมือจำลองภัยคุกคาม
- IPS/IDS, HIPS
- WIPS
- เครื่องมือการตรวจพิสูจน์หลักฐาน
- ผู้ออกใบรับรอง
- ชุดเครื่องมือ Kali และ all Kali
- ซอฟต์แวร์แก้ไขปัญหาที่ตรวจพบ
- GNS และเฟิร์มแวร์ที่เกี่ยวข้อง
- เครื่องมือวิเคราะห์แบบไดนามิก
- APIs
- ELK Stack
- Graylog
- Python 3+
- เครื่องมือ Security Onion
- Metasploitable 2

อื่น ๆ

- ตัวอย่างบันทึก
- ตัวอย่างทราฟฟิกของเครือข่าย (การดักจับแพ็กเก็ต)
- ตัวอย่างโครงสร้างองค์กร
- ตัวอย่างเอกสารเครือข่าย
- การเชื่อมต่ออินเทอร์เน็ตบรอดแบนด์
- 4G/5G และ/หรือฮอตสปอต
- อุปกรณ์ต่อพ่วงคอมพิวเตอร์และเคลื่อนที่
- บริการระบบคลาวด์
- Visio/Excel
- Open Office