หลักสูตร CompTIA Security+

รายละเอียดหลักสูตร

CompTIA Security + คือใบประกาศนียบัตรการรับรองความรู้ด้านความปลอดภัย สำหรับผู้เชี่ยวชาญด้านไอที ซึ่งมีเนื้อหาอ้างอิงจากความรู้เบื้องต้นที่จำเป็นสำหรับงาน Cybersecurity และเป็นจุดเริ่มต้นทางด้านความคิดที่ใช้สำหรับงานด้านความปลอดภัยในระดับกลาง - ระดับสูง

ใบประกาศนียบัตรSecurity + ประกอบด้วยชุดฝึกฝน ที่สามารถลงมือปฏิบัติในการแก้ไขปัญหาได้จริง โดยผู้เข้ารับการทดสอบสามารถมั่นใจได้ว่า จะได้ฝึกฝน จนเกิดทักษะการแก้ปัญหาความปลอดภัย

CompTIA Security+ ได้รับการรับรองมาตรฐานโดย ANSI และยังสอดคล้องกับมาตรฐาน ISO 17024 ซึ่งเป็นการยืนยันถึงมาตรฐาน และการปรับปรุงคุณภาพอย่างต่อเนื่องของ CompTIA Security+ โดยที่หัวข้อต่างๆ ในวัตถุประสงค์การเรียนรู้ของ CompTIA Security+ เป็นผลลัพธ์จากการวิจัยและพัฒนาโดยผู้เชี่ยวชาญด้าน Information security ในทุกมิติ เพื่อให้สอดคล้องกับความต้องการขององค์กรต่างๆ อย่างแท้จริง

ทักษะที่ได้รับ

- ด้านภัยคุกคาม การโจมตี และช่องโหว่
  สามารถตรวจสอบความปลอดภัยประเภทต่าง ๆ และมีความเข้าใจในการทดสอบการเจาะ และแนวคิดในการสแกนช่องโหว่
- ด้านเทคโนโลยี และเครื่องมือ
  สามารถติดตั้งกำหนดค่า และปรับใช้คอมโพเนนต์เครือข่ายในขณะที่ประเมิน และแก้ไขปัญหาเพื่อสนับสนุนความปลอดภัยขององค์กรได้
- ด้านสถาปัตยกรรมและการออกแบบ
  สามารถใช้แนวคิดสถาปัตยกรรมเครือข่ายที่ปลอดภัย และการออกแบบระบบได้
- ด้านการจัดการข้อมูลประจำตัว และการเข้าถึง
  ติดตั้ง และกำหนดค่าข้อมูลประจำตัว และการเข้าถึงบริการ รวมถึงการบริหารจัดการได้
- ด้านการจัดการความเสี่ยง
  สามารถดำเนินการ และสรุปแนวทางปฏิบัติที่ดีที่สุดในการบริหารความเสี่ยง และผลกระทบทางธุรกิจได้
- CRYPTOGRAPHY & PKI
  สามารถติดตั้ง และกำหนดการตั้งค่าความปลอดภัยแบบไร้สาย และใช้โครงสร้างพื้นฐาน แบบกุญแจสาธารณะได้

คุณสมบัติของผู้เข้าอบรม

บุคลากรที่ปฏิบัติงานในตำแหน่งด้านไอที เกี่ยวข้องกับงานเทคนิคทั้งในระดับปฏิบัติการและระดับนโยบาย เช่น IT Support, System Engineer, Network Engineer, IT Auditor, IT Manager, System Manager, Network Manager,

สายงานที่มีความเกี่ยวข้องกับ CompTIA Security+

- ผู้ดูแลระบบ (Systems Administrator)
- ผู้ดูแลระบบเครือข่าย (Network Administrator)
- ผู้ดูแลระบบความปลอดภัย (Security Administrator)
- ผู้สอบบัญชีไอที / ผู้ตรวจการเจาะระบบ (Junior IT Auditor/ Penetration Tester)
- ผู้เชี่ยวชาญด้านความปลอดภัย (Security Specialist)
- ที่ปรึกษาด้านความปลอดภัย (Security Consultant)
- วิศวกรรักษาความปลอดภัย (Security Engineer)
- IT Project Manager ตลอดจนผู้ที่ทำงานทางด้านพัฒนาโปรแกรม เช่น Programmer, System Analyst

ระยะเวลาการอบรม

4 วัน (24 ชั่วโมง)

รายละเอียดหลักสูตร

ที่	เนื้อหาหลักสูตร
1	**Threats, Attacks and Vulnerabilities**
	ชนิดและประเภทของ Malware เช่น Viruses, Ransomware, Worm, Trojan, Rootkit
	เปรียบเทียบและระบุความแตกต่างชนิดของการโจมตีประเภทต่าง ๆ เช่น Social engineering, Application/service attacks, Wireless attacks, Cryptographic attacks
	อธิบายถึงประเภทของผู้บุกรุก เช่น Script kiddies, Hacktivist, Insiders, Competitors
	อธิบายถึงภาพรวมของการทดสอบการเจาะระบบ เช่น Active reconnaissance, Passive reconnaissance, Black box, White box, Gray box
	อธิบายถึงภาพรวมของการค้นหาช่องโหว่ (Vulnerability) ของระบบ เช่น Identify vulnerability, Identify lack of security controls, Identify common misconfigurations
	อธิบายถึงผลกระทบที่เกี่ยวข้องกับประเภทของช่องโหว่ เช่น Improper input handling, Misconfiguration, Memory/buffer vulnerability
2	**Technologies and Tools**
	ติดตั้งและปรับแต่งอุปกรณ์ระบบเครือข่ายให้มีความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น Firewall, VPN concentrator, Router, Switch
	ใช้ซอฟต์แวร์สำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น Protocol analyzer, Network scanners, Vulnerability scanner, Honeypot, Command line tools
	การวิเคราะห์และแก้ไขปัญหาด้านมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศขั้นพื้นฐาน
	วิเคราะห์และแปลความหมายของผลลัพธ์ที่ได้จากการเครื่องมือในการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ

ที่	เนื้อหาหลักสูตร
	การรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้กับอุปกรณ์เคลื่อนที่
	การใช้งานโปรโตคอลอย่างปลอดภัย เช่น DNSSEC, SSH, SSL/TLS, SNMPv3
3	**Architecture and Design**
	อธิบายถึงวัตถุประสงค์และกรณีศึกษาที่เกี่ยวกับการตั้งค่าอย่างปลอดภัย เช่น Defense-in-depth/layered security
	สถาปัตยกรรมความปลอดภัยระบบเครือข่าย เช่น Zones/topologies, Segregation/segmentation/isolation, Tunneling/VPN
	การออกแบบระบบให้มีความปลอดภัย เช่น TPM, Secure boot and attestation, Patch management, Disabling unnecessary ports and services
	อธิบายถึงความสำคัญของความปลอดภัยในแต่ละช่วงเวลา
	การรักษาความปลอดภัยให้กับระบบ Embedded systems เช่น SCADA, HVAC, Smart devices/IoT
	การพัฒนาแอปพลิเคชันอย่างปลอดภัย เช่น Secure DevOps, Provisioning and deprovisioning, Secure coding techniques
	ระบบคลาวด์ (Cloud) และระบบเสมือน (Virtualization) เช่น Cloud Model, VDI/VDE
	กลยุทธ์เพื่อลดความเสี่ยงด้วยการใช้ระบบอัตโนมัต (Automation)
	ความสำคัญของการรักษาความปลอดภัยทางกายภาพ
4	**Identity and Access Managemen**
	เปรียบเทียบและบอกถึงความแตกต่างของการพิสูจน์ตัวตนและการจัดการการเข้าถึงระบบ (Access Management)
	การติดตั้งและปรับแต่งระบบพิสูจน์ตัวตนและการเข้าถึงระบบ
	การใช้งานระบบพิสูจน์ตัวตนและการจัดการการเข้าถึงระบบ
	การบริหารจัดการบัญชีผู้ใช้ (Account Management) เช่น Account types, Account policy enforcement
5	**Risk Management**
	ความสำคัญของนโยบาย, แผนการดำเนินงาน, ขั้นตอนการปฏิบัติ ที่ส่งผลกระทบกับความปลอดภัยขององค์กร
	วิเคราะห์ปัจจัยที่ผลกระทบกับธุรกิจ
	กระบวนการการจัดการความเสี่ยง
	การติดตามและตอบสนองต่อ Incident
	การเก็บรวบรวมพยานหลักฐานทางดิจิทัลขั้นพื้นฐาน
	แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan) และแผน Continuity Of Operation Plan (COOP)
	เปรียบเทียบความแตกต่างประเภทของการควบคุม

ที่	เนื้อหาหลักสูตร
	นโยบายความเป็นส่วนตัวและการส่งข้อมูลออกไปภายนอก
6	Cryptography and PKI
	เปรียบเทียบและอธิบายความแตกต่างของการเข้ารหัสขั้นพื้นฐาน
	อธิบายถึงอัลกอริทึ่มและคุณลักษณะพื้นฐานของการเข้ารหัส
	ติดตั้งและปรับแต่งค่าความปลอดภัยของระบบเครือข่ายแบบไร้สาย
	การเข้ารหัสแบบแบบกุญแจสาธารณะ (Public key)