

TTCT01 : CompTIA Security+ โครงการอบรมเชิงปฏิบัติการมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยสารสนเทศระดับพื้นฐาน

Description :

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

Instructor :



Training Date : 27 ส.ค. 2568 - 29 ส.ค. 2568

fee : 35,000 ฿ (ราคายังไม่รวม Vat 7%)

Days & Duration : 3 Day(s) | 18 Hour(s)

Time : 09:00:00 - 16:00:00

Language : Thai

Venue : การอบรมในรูปแบบ Online

Type : Online

Category : CompTIA Certification Program

อาจารย์ทรงพล นครศรีเรืองศักดิ์

นักวิชาการอิสระ

Objectives :

โครงการอบรมเชิงปฏิบัติการพร้อมสอบใบรับรองวิชาชีพด้านความมั่นคงปลอดภัยสารสนเทศระดับพื้นฐาน (CompTIA Security+) เป็นความร่วมมือระหว่าง เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทยและบริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS Professional Center) พร้อมทั้งได้รับการสนับสนุนใบรับรองโดย CompTIA สมาคมการค้าระดับโลกที่พิทักษ์ผลประโยชน์ทางด้านธุรกิจของอุตสาหกรรมเทคโนโลยีสารสนเทศ จากประเทศสหรัฐอเมริกา ซึ่งเป็นใบรับรองทางมาตรฐานวิชาชีพที่เป็นกลางไม่อิงผู้ชาย และผู้ผลิตอุปกรณ์รายใด อีกทั้งยังเป็นที่ยอมรับในระดับสากลด้านความรู้และทักษะการรักษามั่นคงปลอดภัยที่นำไปประยุกต์ใช้อย่างแพร่หลายในองค์กรและผู้เชี่ยวชาญด้านการรักษาความปลอดภัยทั่วโลก CompTIA Security+ ได้รับการรับรองมาตรฐานโดย ANSI และยังคงสอดคล้องกับมาตรฐาน ISO 17024 ซึ่งเป็นการยืนยันถึงมาตรฐาน และการปรับปรุงคุณภาพอย่างต่อเนื่องของ CompTIA Security+ โดยที่หัวข้อต่างๆ ในวัตถุประสงค์การเรียนรู้ของ CompTIA Security+ เป็นผลลัพธ์จากการวิจัยและพัฒนาโดยผู้เชี่ยวชาญด้าน Information security ในทุกมิติ เพื่อให้สอดคล้องกับความต้องการขององค์กรต่างๆ อย่างแท้จริง

Objectives:

- + เพื่อขยายฐานการผลิตบุคลากรที่มีความรู้ความเชี่ยวชาญ ด้านความมั่นคงปลอดภัยสารสนเทศ ระดับพื้นฐาน (IT Security Foundation) ให้มีปริมาณมากขึ้นในตลาดแรงงานด้าน IT Security
- + เพื่อสร้างมาตรฐานของบุคลากรด้าน Security ให้มีความทัดเทียมในระดับสากล เป็นการรองรับ การเปิดการค้าเสรีอาเซียน (AEC) ในเร็ววัน
- + เพื่อพัฒนาศักยภาพของบุคลากรด้าน IT Security ให้เท่าทันกับยุคเศรษฐกิจดิจิทัลที่จะเกิดขึ้นอย่างเต็มรูปแบบ

Target Group :

CompTIA Security+ เหมาะสำหรับผู้ที่ปฏิบัติงานในตำแหน่งทางด้านไอที ซึ่งต้องเกี่ยวข้องกับงานเทคนิคทั้งในระดับปฏิบัติการและระดับนโยบาย เช่น IT Support, System Engineer, Network Engineer, IT Auditor, IT Manager, System Manager, Network Manager, IT Project Manager ตลอดจนผู้ที่ทำงานทางด้านพัฒนาโปรแกรม เช่น Programmer, System Analyst เป็นต้น

Benefits :

ผู้ที่สอบผ่านมาตรฐาน CompTIA Security+ จะมีความรู้และทักษะที่จำเป็นในการระบุความเสี่ยง (Risk Identification) การลดความเสี่ยง (Risk Mitigation) ที่เกี่ยวกับ Information security การดำเนินการด้านโครงสร้างพื้นฐาน การประยุกต์ใช้ข้อมูลสารสนเทศและ Security control ในการรักษาความมั่นคงปลอดภัยสารสนเทศได้อย่างสัมฤทธิ์ผลในด้าน การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน(Integrity) และ การรักษาความพร้อมใช้ (Availability) ของข้อมูลระบบสารสนเทศ เพื่อช่วยให้ผู้เรียนมีความสามารถในการจัดการเทคโนโลยีและระบบสารสนเทศได้อย่างเหมาะสมสอดคล้องกับนโยบายองค์กร ระเบียบข้อบังคับของอุตสาหกรรมและ กฎหมาย

Course Outline :

Network Security

- + คุณสมบัติและการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย เช่น Firewall, Router, Switch, Load Balancer, Proxy, IDS/IPS
- + ข้อควรคำนึงถึงด้านความปลอดภัยของเทคโนโลยี Virtualization และ Cloud Computing
- + รู้จักกับโปรโตคอลที่ใช้งานบนเครือข่าย TCP/IP เช่น IPv4, IPv6, HTTP, FTP, IPsec, SNMP, SSL, TLS
- + การเข้ารหัสและวิธีการรักษาความปลอดภัยของเครือข่ายไร้สาย เช่น WEP, WPA/WPA2, TKIP, CCMP, EAP, Mac filter

Compliance and Operational Security

- + หลักการและทฤษฎีด้านความปลอดภัยกับการบริการความเสี่ยง เช่น Control type, Security policy, Vulnerability, RTO/RPO
- + ความเสี่ยงของธุรกิจที่อาจเกิดจาก Business Partner และ Social Media Network ความสำคัญของ SLA และ MOU
- + กลยุทธ์และเครื่องมือลดความเสี่ยง เช่น Change and Incident management, Routine audits, Data loss preventions (DLP)
- + ขั้นตอนการเก็บหลักฐานในกรณีที่เกิดเหตุการณ์ความไม่ปลอดภัยเกิดขึ้นกับระบบ IT เช่น Order of volatility, Chain of custody
- + ขั้นตอนของกระบวนการตอบสนองต่อเหตุการณ์ไม่ปกติที่เกิดขึ้น เช่น Incident identification, Mitigation steps, First responder
- + ความสำคัญของ Security Awareness เช่น Personally identifiable information (PII), Information classification

- + รู้จักประเภทของเครื่องมือควบคุมหรือ Control ทางด้านความปลอดภัย ได้แก่ Environmental controls, Physical security
- + หลักการพื้นฐานของ Business continuity, Fault tolerance และ Disaster recovery (Hot site, Warm site, Cold site)
- + เป้าหมายของ Information Security ได้แก่ Confidentiality (ความลับ), Integrity (ความถูกต้อง) และ Availability (ความพร้อมใช้)

Threats and Vulnerabilities

- + ประเภทของ Malware เช่น Virus, Spyware, Trojan, Rootkit, Botnet
- + ประเภทของ Attack (การโจมตี) เช่น Man-in-the-middle, DoS, DDoS, Spam, Phishing, Pharming
- + ประเภทของ Social engineering attack (โจมตีที่ช่องโหว่ที่เกิดจากของตัวบุคคล) เช่น Shoulder surfing, Tailgating, Hoax, Whaling
- + ประเภทของ Wireless attack (โจมตีทางเครือข่ายไร้สาย) เช่น Rogue access points, Evil twin, War driving, War chalking
- + ประเภทของ Application attack (โจมตีช่องโหว่ของโปรแกรม) เช่น Cross-site scripting (XSS), SQL injection, Buffer overflow
- + เทคนิควิธีการลดและป้องกันความเสี่ยง เช่น Monitoring logs, Hardening, Network security, Detection vs. prevention controls
- + เครื่องมือทางเทคนิคที่ใช้เพื่อตรวจสอบช่องโหว่และกู้คืน เช่น Port scanner, Baseline report, Code review
- + วัตถุประสงค์ของการใช้งาน Penetration testing, Vulnerability scanning, Black box, White box, Grey box

Application, Data and Host Security

- + Application security เช่น Fuzzing, Error and exception handling, Input validating, Hardening, Patch management
- + Mobile device security เช่น Full drive encryption, Screen-locks, BYOD (Bring Your Own Device)
- + Host security เช่น OS hardening, Hardware security, Host software baseline
- + Data security เช่น Cloud storage, SAN, Hardware based encryption devices (TPM, HSM)
- + เทคนิควิธีการด้านความปลอดภัยอื่นๆ เช่น SCADA, Android, iOS, Application firewalls

Access Control and Identity Management

- + ระบบ Authentication (พิสูจน์ตัวตน) เช่น RADIUS, Kerberos, LDAP
- + Identification (Biometric, Username), Authentication (Token, Smart card), Authorization และการพิสูจน์ตัวตนด้วย
- + Something you are, Something you have, Something you know
- + การบริหารจัดการ Account เช่น Policy enforcement (Group policy, Password complexity, Expiration), User access review

Cryptography

- + หลักการของ Cryptography (การเข้ารหัส) เช่น Symmetric vs. asymmetric, Hashing, Digital signatures
- + อัลกอริทึมในการเข้ารหัสและการใช้งาน เช่น WEP, WPA/WPA2, MD5, SHA, DES, 3DES, AES
- + วิธีการของ Public Key Infrastructure ได้แก่ CA, PKI, Public key, Private key

Payment Condition :

Payment can be made by:

1. Cash or Credit Card or Bank Cheque payable to "สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ" (a post-dated cheque is not accepted) on the first day of the service or within the last day of the service.
2. Account transfer and send the proof of the payment (the deposit slip) via email ttd@swpark.or.th
 - ธนาคารกรุงเทพ สาขาอุทยานวิทยาศาสตร์
Saving Account Number: 080-0-00001-0
Account Name: สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
 - ธนาคารกรุงไทย สาขาตลาดไท
Saving Account Number: 152-1-32668-1
Account Name: สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

Notes:

- Withholding tax (3%) is exempt.
- Should you need to withdraw, you must send the notice of the withdrawal in writing no later than 7 working days before the commencement date. The cancellation less than 7 days will be subject to a fine of 40% of the fee.
- Software Park Thailand reserves the rights to cancel courses due to unforeseen circumstances.

Contact Person :

For more information, contact our course coordinator on:

Songsiri Sittikun

Tel: +66-2583-9992 Ext. 81426

Email: songsiri@swpark.or.th

You are encouraged to use the course schedule as a guide to plan your training. The schedule is accessible at www.swpark.or.th for more information.