โครงการพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศด้วยมาตรฐานในระดับสากล

IT Cyber Security Certification Program

1. ที่มาของโครงการ

โครงการนี้จัดทำขึ้นเพื่อพัฒนาความรู้และทักษะที่จำเป็นในการสร้างความเข้าใจและความเชี่ยวชาญในความมั่นคงปลอดภัยของระบบ การระบุความเสี่ยง การลดความเสี่ยง ที่เกี่ยวกับความปลอดภัยของข้อมูลสารสนเทศ การดำเนินการด้านโครงสร้างพื้นฐาน การประยุกต์ใช้ข้อมูลสารสนเทศและการควบคุมความปลอดภัยในการรักษาความมั่งคงปลอดภัยสารสนเทศได้อย่างสัมฤทธิ์ผลในด้านการรักษาความลับ การรักษาความถูกต้องครบถ้วนและการรักษาความพร้อมใช้ของข้อมูลระบบสารสนเทศ เพื่อให้สามารถจัดการเทคโนโลยีและระบบสารสนเทศได้อย่างเหมาะสม สอดคล้องกับนโยบายองค์กร ระเบียบข้อบังคับของอุตสาหกรรมและกฎหมาย รวมถึงการเรียนรู้การตรวจหาการโจมตีเพื่อจัดทำเป็นรายงานเชิงอาชญากรรมได้และเพื่อป้องกันการโจมตีในอนาคต โดยทักษะที่ได้รับจะจัดอยู่ในระดับมาตรฐานสากล เพื่อส่งเสริมและพัฒนาให้เกิดผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีปริมาณมากขึ้นในตลาดแรงงานและความเท่าทันกับยุคเศรษฐกิจดิจิทัลต่อไป

2. วัตถุประสงค์

1) เพื่อส่งเสริมและพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ ให้มีปริมาณมากขึ้นในตลาดแรงงานและเท่าทันกับยุคเศรษฐกิจดิทัล
2) เพื่อส่งเสริมให้บุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ ได้รับประกาศนียบัตรในระดับสากล

3. กลุ่มเป้าหมายโครงการ (200 คน)

1) หน่วยงานภาคเอกชน
2) หน่วยงานภาครัฐ, รัฐวิสาหกิจ, องค์การมหาชน
3) สถาบันการเงิน, บริษัทประกันภัย, ประกันชีวิต, โรงพยาบาล
4) สถานบันการศึกษา ภาครัฐ และเอกชน
5) หน่วยงานอื่น ๆ ที่มีความสนใจ

4. การสมัครเข้าร่วมโครงการฯ

1) **ผู้สมัครสามารถเลือกอบรมได้เพียง 1 หลักสูตรเท่านั้น**
2) **หน่วยงานละไม่เกิน 5 ท่าน**
3) **คุณสมบัติ ผู้เข้าร่วมโครงการฯ**
   - เป็นบุคลากรที่ตรงตาม กลุ่มเป้าหมายโครงการ
   - มีตำแหน่งงาน หรือลักษณะงาน สอดคล้อง กับงาน **ด้านเทคโนโลยีสารสนเทศ ด้านความมั่นคงปลอดภัยสารสนเทศ เช่น IT Support, System Engineer, Network Engineer, IT Auditor, IT Manager,**

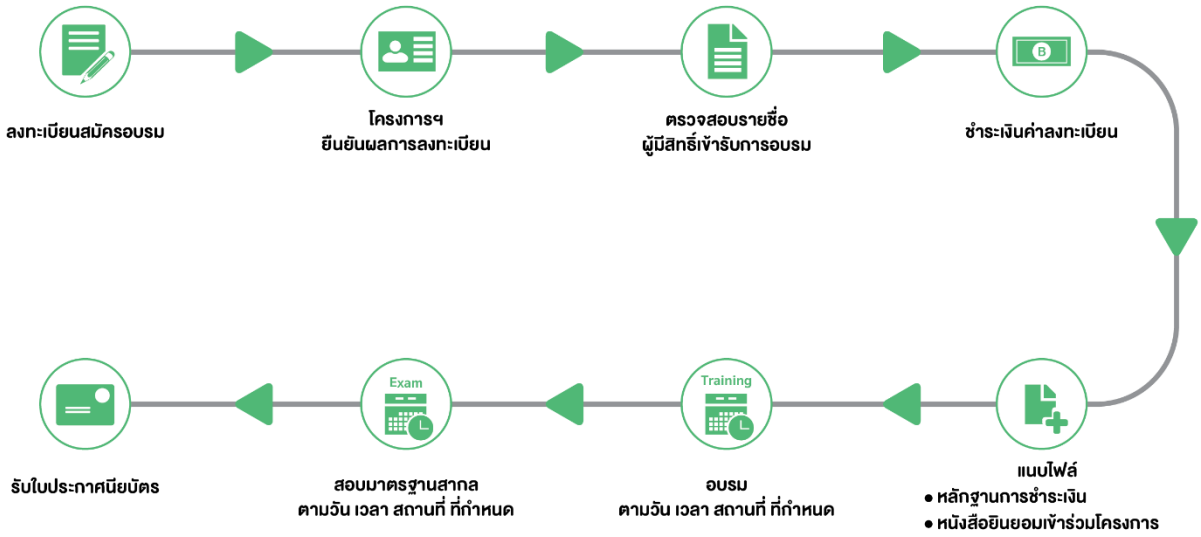
System Manager, Network Manager, IT Project Manager ตลอดจนผู้ที่ทำงานทางด้านพัฒนาโปรแกรม เช่น Programmer, System Analyst เป็นต้น

- มีความรู้พื้นฐานตามหลักสูตรที่เข้าอบรม
- สามารถนำความรู้ที่ได้จากการอบรม นำไปประยุกต์ใช้ในการทำงานได้อย่างมีประสิทธิภาพ และมีประสิทธิผล
- ต้องมีความพร้อม และให้ความร่วมมือในการเข้าร่วมกิจกรรมต่าง ๆ ตลอดการฝึกอบรม

4) **วิธีการสมัครเข้าร่วมโครงการฯ**

- ผู้สนใจสามารถสมัครเข้าร่วมโครงการฯ ได้ตั้งแต่ 15 กรกฎาคม 2562 เป็นต้นไป โดยจะประกาศรายชื่อผู้มีสิทธิได้รับคัดเลือกเข้าอบรมก่อนการเข้าอบรม 15 - 30 วัน และสามารถติดตามการประกาศรายชื่อได้ที่ http://www.cybersecurity-cert.com/announce

5. ขั้นตอนการสมัครเข้าร่วมโครงการฯ



6. รายละเอียดขั้นตอนการสมัครเข้าร่วมโครงการฯ

ลำดับ	ขั้นตอน	รายละเอียด
1	ลงทะเบียนสมัครอบรมได้ที่เว็บไซต์โครงการ http://www.cybersecurity-cert.com/	▪ ศึกษารายละเอียดโครงการ รายละเอียดหลักสูตร ▪ ตรวจสอบคุณสมบัติผู้มีสิทธิ์เข้ารับการอบรม ▪ กรอกข้อมูลผู้สมัครตามความเป็นจริง และครบถ้วน
2	โครงการฯ ยืนยันการลงทะเบียน	▪ โครงการฯ ตรวจสอบคุณสมบัติผู้ลงทะเบียน ▪ โครงการฯ ส่งอีเมลแจ้งผลการลงทะเบียน ภายใน 3 วัน

ลำดับ	ขั้นตอน	รายละเอียด
3	ตรวจสอบรายชื่อผู้มีสิทธิ์เข้ารับการอบรม	■ โครงการฯ ประกาศรายชื่อผู้มีสิทธิ์เข้ารับการฝึกอบรม ○ ประกาศ ล่วงหน้า 15 - 30 วัน ก่อนการฝึกอบรมแต่ละรุ่น ผ่านเว็บไซต์ http://www.cybersecurity-cert.com/announce ○ ส่งอีเมลแจ้งไปยังผู้ผ่านการคัดเลือก ■ ผู้มีสิทธิ์เข้าอบรม ศึกษากำหนดการอบรม สถานที่จัดอบรมให้ครบถ้วน
4	ชำระเงินค่าลงทะเบียน	■ ผู้มีสิทธิ์เข้าอบรม ชำระเงินค่าลงทะเบียนอัตราตามรายวิชาที่ลงทะเบียน ภายใน 15 วันก่อนการฝึกอบรม ○ CompTIA Security+ ราคา 10,000 บาท ○ CompTIA Cybersecurity Analyst (CySA+) ราคา 12,000 บาท ○ CompTIA Advanced Security Practitioner+ (CASP+) ราคา 12,000 บาท **ราคาดังกล่าวยังไม่รวมภาษีมูลค่าเพิ่ม VAT 7% และได้รับการยกเว้นภาษีหักที่จ่าย 3% เนื่องจากเป็นหน่วยงานภาครัฐ**
5	แนบไฟล์เอกสาร	■ ผู้ผ่านการคัดเลือกแนบไฟล์เอกสาร ภายใน 15 วัน ก่อนวันที่ท่านอบรม ดังนี้ ○ หลักฐานการชำระเงิน ○ หนังสือยินยอมการเข้าร่วมโครงการ
6	อบรมตามวัน เวลา และสถานที่ที่กำหนดในแต่ละรุ่น	■ ระยะเวลาการฝึกอบรม 4 วัน/ 24 ชั่วโมง (9.00 – 16.00 น.) ○ CompTIA Security+ ○ CompTIA Cybersecurity Analyst (CySA+) ○ CompTIA Advanced Security Practitioner+ (CASP+)

ลำดับ	ขั้นตอน	รายละเอียด
7	สอบมาตรฐานสากล ตามวัน เวลา สถานที่ ที่กำหนด	■ ภายใน 15 วันหลังจากจบการอบรมในแต่ละรุ่น ผู้อบรมดำเนินการดังนี้ ○ ทำชุดฝึกฝนให้เกิดความชำนาญ และความพร้อมในการสอบมาตรฐานสากล ○ ตกลง วัน เวลา ในการเข้าสอบกับเจ้าหน้าที่ศูนย์สอบฯ ○ เข้าสอบ ตามวัน เวลา ที่ตกลงกับเจ้าหน้าที่ศูนย์สอบฯ
8	การรับใบประกาศนียบัตร	■ ประกาศนียบัตรมาตรฐานสากล ○ ศูนย์สอบจัดส่ง Digital Certification ทางอีเมลผู้ที่สอบผ่าน ○ Person VUE จัดส่งประกาศนียบัตรตามที่อยู่ของผู้ที่สอบผ่าน ■ ประกาศนียบัตรการเข้าร่วมโครงการอบรม (Software Park Thailand) ○ หลังจากผู้อบรมสอบมาตรฐานสากลแล้วเสร็จ ทางโครงการฯ จัดส่งประกาศนียบัตรที่ออกโดย Software Park Thailand ตามที่อยู่ที่ผู้อบรมลงทะเบียนไว้

กรรมการโครงการฯ ขอสงวนสิทธิ์ในการคัดเลือกผู้มีสิทธิเข้าร่วมโครงการฯ โดยพิจาณาจากตำแหน่งงานที่ตรงกับหลักสูตรที่สมัครเข้ารับการอบรม ลำดับการสมัครเข้าร่วมโครงการ และเอกสารประกอบการสมัครครบถ้วน ***ทั้งนี้การพิจารณาอยู่ในดุลยพินิจของผู้จัดโครงการ และผลการคัดเลือกถือว่าเป็นที่สิ้นสุด***

7. ตารางการฝึกอบรม

ที่	หลักสูตร	ระยะเวลาอบรม	จำนวนคน/รุ่น	รุ่นที่ 1	รุ่นที่ 2	รุ่นที่ 3	รุ่นที่ 4	รุ่นที่ 5
1	CompTIA Security+	4 วัน/24 ช.ม.	30	27-30 ส.ค.62	24-27 ก.ย.62	29 ต.ค.- 1 พ.ย. 62	21-24 ม.ค.63	18-21 ก.พ.63
2	CompTIA Cybersecurity Analyst (CySA+)	4 วัน/24 ช.ม.	30	19-22 พ.ย.62	-	-	-	-
3	CompTIA Advanced Security Practitioner+ (CASP+)	4 วัน/24 ช.ม.	30	10-13 มี.ค.63	-	-	-	-

หมายเหตุ วันที่และเวลา อาจมีการเปลี่ยนแปลงตามความเหมาะสม

8. สถานที่จัดอบรม

ณ ห้องอบรม ชั้น 3 อาคารซอฟต์แวร์พาร์ค ถนนแจ้งวัฒนะ ปากเกร็ด นนทบุรี หรือ หน่วยงานหรือบริษัทฯ ในเครือข่าย

9. ข้อกำหนดการอบรม

1) ผู้เข้ารับการอบรมต้องเข้ารับการอบรมตามวัน เวลา และสถานที่ ที่กำหนด
2) มีชั่วโมงการร่วมกิจกรรมไม่น้อยกว่าร้อยละ 80
3) ก่อนการสอบมาตรฐานสากล ผู้อบรมต้องฝึกทำระบบฝึกฝนออนไลน์ (Learning Management System) โดยมีคะแนนไม่น้อยกว่าร้อยละ 80 จึงจะสามารถลงทะเบียนสอบมาตรฐานสากลได้
4) ภายใน 15 หลังจากอบรม ผู้อบรมต้องสอบมาตรฐานสากล ตามสถานที่ฯ โครงการฯ กำหนด
5) หลังจากสอบมาตรฐานสากลผ่านแล้ว จึงจะได้รับใบประกาศนียบัตรเข้าร่วมโครงการจาก Software Park Thailand

หมายเหตุ

กรณีผู้อบรมเข้ารับการอบรม *แต่ไม่สอบมาตรฐานสากล ตามวัน เวลา ที่ตกลงไว้กับโครงการฯ* ผู้อบรมจะต้องชำระเงินค่าอบรมเต็มจำนวนในอัตรา ดังต่อไปนี้

- CompTIA Security + ราคา 25,000 บาท
- CompTIA Cybersecurity Analyst (CySA+) ราคา 35,000 บาท
- CompTIA Advanced Security Practitioner+ (CASP+) ราคา 45,000 บาท

10. อัตราค่าลงทะเบียนการเข้าร่วมโครงการ

ลำดับ	หลักสูตร	ระยะเวลาอบรม	ค่าลงทะเบียน
1	CompTIA Security+	4 วัน/24 ช.ม.	10,000 บาท
2	CompTIA Cybersecurity Analyst (CySA+)	4 วัน/24 ช.ม.	12,000 บาท
3	CompTIA Advanced Security Practitioner+ (CASP+)	4 วัน/24 ช.ม.	12,000 บาท

หมายเหตุ อัตราค่าลงทะเบียนดังกล่าว ยังไม่รวมภาษีมูลค่าเพิ่ม 7% และได้รับการยกเว้นภาษีหักที่จ่าย 3% เนื่องจากเป็นหน่วยงานภาครัฐ

11. อัตราค่าสอบซ่อม

ลำดับ	หลักสูตร	ค่าสอบ (อัตราพิเศษ)
1	CompTIA Security+	จะแจ้งให้ทราบอีกครั้ง
2	CompTIA Cybersecurity Analyst (CySA+)	
3	CompTIA Advanced Security Practitioner+ (CASP+)	

หมายเหตุ

1) การสอบซ่อมเป็นความประสงค์ของผู้สอบ ทางโครงการฯ ไม่บังคับ
2) อัตราค่าสอบ (ซ่อม) ยังไม่รวมภาษีมูลค่าเพิ่ม

12. สิ่งที่ผู้เข้าอบรมจะได้รับ

1) คอมพิวเตอร์ในการอบรม 1 เครื่อง/ท่าน
2) อาหารว่าง 2 มื้อ/วัน
3) อาหารกลางวัน 1 มื้อ/วัน
4) เอกสารประกอบการฝึกอบรม
5) ระบบฝึกฝนออนไลน์ (Learning Management System)
6) Voucher สำหรับการสอบมาตรฐานสากล ตามหลักสูตรที่ลงทะเบียนไว้ จำนวน 1 ชุด

13. การชำระเงินค่าลงทะเบียน

ผู้ลงทะเบียนรอการยืนยันร่วมอบรมจากเจ้าหน้าที่ ก่อนการชำระเงิน เมื่อได้รับการยืนยันแล้ว ผู้ลงทะเบียนต้องดำเนินการชำระค่าลงทะเบียนภายใน 7 – 15 วัน ก่อนการอบรม โดยสามารถโอนเงินค่าลงทะเบียนได้ ตามเลขบัญชีดังนี้

ลำดับ	ธนาคาร	สาขา	ชื่อบัญชี	เลขที่บัญชี
1	ไทยพาณิชย์	ถนนแจ้งวัฒนะ	เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย#2	324-256262-0
2	กรุงศรีอยุธยา	ถนนแจ้งวัฒนะ (ซอฟต์แวร์ พาร์ค)	เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย#2	329-1-34850-3

เมื่อโอนเงินเรียบร้อยแล้ว กรุณาสแกนหลักฐานการโอนเงิน (Pay-in Slip) พร้อมระบุชื่อ-สกุล บริษัท หัวข้อการอบรม ส่งมาที่อีเมล์ cybersecurity@swpark.or.th หรือ แนบไฟล์ได้ที่เมนู Attach File

14. ผู้บริหารโครงการ

เขตอุสาหกรรมซอฟต์แวร์ประเทศ (Software Park Thailand)

เลขที่ 99/31 หมู่ที่ 4 อาคารซอฟต์แวร์ปาร์ค ถนนแจ้งวัฒนะ ตำบลคลองเกลือ อำเภอปากเกร็ด จังหวัดนนทบุรี 11120

Website: http://www.cybersecurity-cert.com

Email: cybersecurity@swpark.or.th

15. ผู้ดูแลโครงการ

คุณศาสตรา นะรารัมย์	มือถือ	087-444-5526
คุณหัสยา แซ่ฉั่ว	มือถือ	085-553-5679
คุณทรงศิริ สิทธิคุณ	เบอร์ติดต่อ	02-583-9992 ต่อ 1426
คุณภัสสร พรทิพย์	เบอร์ติดต่อ	02-583-9992 ต่อ 1422

16. รายละเอียดหลักสูตร

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

3 วัน (18 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

ที่	เนื้อหาหลักสูตร
	วิเคราะห์และแปลความหมายของผลลัพธ์ที่ได้จากการเครื่องมือในการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ
	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

ที่	เนื้อหาหลักสูตร
	แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan) และแผน Continuity Of Operation Plan (COOP)
	เปรียบเทียบความแตกต่างประเภทของการควบคุม
	นโยบายความเป็นส่วนตัวและการส่งข้อมูลออกไปภายนอก
6	Cryptography and PKI
	เปรียบเทียบและอธิบายความแตกต่างของการเข้ารหัสขั้นพื้นฐาน
	อธิบายถึงอัลกอริทึ่มและคุณลักษณะพื้นฐานของการเข้ารหัส
	ติดตั้งและปรับแต่งค่าความปลอดภัยของระบบเครือข่ายแบบไร้สาย
	การเข้ารหัสแบบแบบกุญแจสาธารณะ (Public key)

หลักสูตร CompTIA Cybersecurity Analyst (CySA+)

รายละเอียดหลักสูตร

เมื่อผู้โจมตีบนโลกออนไลน์เรียนรู้ที่จะหลบเลี่ยงโซลูชันที่ใช้วิธีการแบบดั้งเดิม เช่น ไฟร์วอลล์ ทักษะการวิเคราะห์ที่ใช้ในอุตสาหกรรมความปลอดภัยด้านไอทีจึงมีความสำคัญมากขึ้นสำหรับองค์กรส่วนใหญ่

โดยใบประกาศนียบัตรการรับรองความรู้ CompTIA Cybersecurity Analyst (CySA+) คลอบคลุมทักษะการวิเคราะห์พฤติกรรม และการต่อสู้กับมัลแวร์และภัยคุกคามถาวรขั้นสูง (APTs) ซึ่งส่งผลให้ผู้วิเคราะห์สามารถมองเห็นภัยคุกคามได้ดีขึ้น สำหรับใบประกาศนียบัตร CompTIA CySA + เหมาะสำหรับผู้เชี่ยวชาญด้านไอทีที่ต้องการทักษะในการวิเคราะห์ความปลอดภัย ดังต่อไปนี้

- ดำเนินการวิเคราะห์ข้อมูล และตีความหมายเพื่อระบุช่องโหว่ของภัยคุกคาม รวมถึงความเสี่ยงต่อองค์กร
- กำหนดค่า และใช้เครื่องมือตรวจจับภัยคุกคาม
- รักษาความปลอดภัย และป้องกันแอปพลิเคชัน และระบบภายในองค์กร

ทักษะที่ได้รับ

- ด้านการจัดการภัยคุกคาม
  ใช้เทคนิคการสอดแนมสิ่งแวดล้อมโดยใช้เครื่องมือที่เหมาะสม สามารถวิเคราะห์ผลลัพธ์ พร้อมตอบสนองและสามารถนำไปใช้งานตามข้อแนะนำได้
- ด้านการจัดการความเสี่ยง
  ใช้กระบวนการจัดการช่องโหว่ และวิเคราะห์ผลลัพธ์ของการสแกน
- ด้านสถาปัตยกรรมในการรักษาความปลอดภัย และชุดเครื่องมือ
  สามารถใช้ข้อมูลเพื่อแนะนำการแก้ไขปัญหาด้านความปลอดภัยที่เกี่ยวข้องกับข้อมูลประจำตัว และการจัดการการเข้าถึง และแนะนำกลยุทธ์การใช้งานในขณะที่อยู่ร่วมกันในวงจรการพัฒนาซอฟต์แวร์ (SDLC)
- ด้านการตอบโต้เหตุการณ์บนโลกไซเบอร์
  สามารถแยกแยะข้อมูลภัยคุกคาม เพื่อกำหนดผลกระทบของเหตุการณ์ และเตรียมชุดเครื่องมือที่เหมาะสม, สร้างกลยุทธ์การสื่อสาร พร้อมแนวทางปฏิบัติในการตอบโต้

คุณสมบัติของผู้เข้าอบรม

บุคลากรที่มีประสบการณ์ด้านเทคนิคการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย 3 - 4 ปี

สายงานที่มีความเกี่ยวข้องกับ CompTIA Cybersecurity Analyst (CySA+)

- นักวิเคราะห์ความปลอดภัยด้านไอที (IT Security Analyst)
- นักวิเคราะห์ ศูนย์ปฏิบัติการรักษาความปลอดภัย (Security Operations Center (SOC) Analyst)
- นักวิเคราะห์ช่องโหว่ (Vulnerability Analyst)
- ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Specialist)
- นักวิเคราะห์ข้อมูลภัยคุกคาม (Threat Intelligence Analyst)
- วิศวกรรักษาความปลอดภัย (Security Engineer)
- นักวิเคราะห์ความปลอดภัยทางไซเบอร์ (Cybersecurity Analyst)

ระยะเวลาการอบรม

3 วัน (18 ชั่วโมง)

รายละเอียดหลักสูตร

ที่	เนื้อหาหลักสูตร
1	**Threat Management**
	การใช้เครื่องมือ (Tools) และเทคนิคที่เหมาะสมในการเก็บรวบรวมข้อมูลเป้าหมาย เช่น NMAP, IDS/IPS, Syslog
	การวิเคราะห์ผลระบบเครือข่ายที่ได้จากการเก็บรวบรวมข้อมูล เช่น Event log, IDS Report, Firewalls log
	วิธีการป้องกันและรับมือภัยคุกคามทางระบบเครือข่ายอย่างเหมาะสม เช่น Network Isolation, Honeypot, Hardening
	อธิบายวัตถุประสงค์ของการรักษาความปลอดภัยทางสารสนเทศภายในองค์กร
2	**Vulnerability Management**
	ขั้นตอนการบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ
	วิเคราะห์ผลลัพธ์ที่ได้จากการสแกนหาช่องโหว่
	เปรียบเทียบและหาความแตกต่างของช่องโหว่พื้นฐานกับช่องโหว่ที่พบภายในองค์กร
3	**Cyber Incident Response**
	แยกความแตกต่างระหว่างภัยคุกคามกับพฤติกรรมที่ส่งผลกระทบต่อ Incident เช่น Threat classification
	เลือกและใช้เครื่องมือที่เหมาะสมในการรวบรวมพยานหลักฐานทางดิจิทัล เช่น Forensics kit, Forensic investigation suite

ที่	เนื้อหาหลักสูตร
	ความสำคัญของการสื่อสารระหว่างเกิดเหตุการณ์ Incident เช่น การสื่อสารกับ Stakeholder, วัตถุประสงค์ของการสื่อสาร (Purpose of communication processes), บทบาทและความรับผิดชอบ (Role-based responsibilities)
	วิเคราะห์อาการที่พบบ่อยเพื่อเลือกทางเลือกที่ดีที่สุดในการตอบสนองต่อเหตุการณ์ Incident เช่น Bandwidth consumption, Memory consumption, Unauthorized software, Unauthorized privileges, Memory overflows
	สรุปรวบรวม Incident ที่เกิดขึ้นและขั้นตอนหลังจากเกิด Incident แล้ว เช่น Reverse engineering, Patching, Reconstruction/reimage, Update incident response plan
4	**Security Architecture and Tool Sets**
	อธิบายความสัมพันธ์ของกรอบการทำงาน (Frameworks), นโยบาย (Policies), การควบคุม (Controls), ขั้นตอนการปฏิบัติงาน (Procedures) เช่น NIST, ISO, COBIT, ITIL, Password policy, Physical controls, Control testing procedures
	ใช้ข้อมูลเพื่อบรรเทาปัญหาด้านความปลอดภัยทางสารสนเทศ เช่น Security issues associated with context-based authentication, Security issues associated with identities, Security issues associated with federation and single sign-on
	ตรวจสอบสถาปัตยกรรมความปลอดภัยทางเทคโนโลยีสารสนเทศและนำข้อเสนอแนะมาปรับปรุงแผนการดำเนินงานให้ดีขึ้น เช่น Security data analytics, Defense in depth
	ใช้แอปพลิเคชันที่ปลอดภัยในขณะที่อยู่ในช่วงพัฒนาโปรแกรม (SDLC) เช่น Best practices during software development, Secure coding best practices
	เปรียบเทียบและหาความแตกต่างของวัตถุประสงค์พร้อมเหตุผลในการใช้เครื่องมือที่หลากหลายด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น การเลือกใช้เครื่องมือสำหรับรวบรวมข้อมูล (Collective), การใช้เครื่องมือสำหรับป้องกัน (Preventative), การใช้เครื่องมือสำหรับวิเคราะห์ (Analytical), การใช้เครื่องมือสำหรับหาช่องโหว่ (Exploit), การใช้เครื่องมือสำหรับการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Forensics)

หลักสูตร CompTIA Advanced Security Practitioner (CASP+)

รายละเอียดหลักสูตร

ใบประกาศนียบัตร CASP+ เป็นสมรรถนะขั้นสูงในเรื่องการบริหารจัดการความเสี่ยง การดำเนินด้านความปลอดภัยขององค์กรและสถาปัตยกรรม การวิจัยและความร่วมมือ และการบูรณาการด้านความปลอดภัยขององค์กร สำหรับผู้ที่สนใจหลักสูตร ใบประกาศนียบัตร CASP+ ควรมีความรู้ความเข้าใจดังต่อไปนี้

- สามารถขยายความปลอดภัยของโดเมนในองค์กรเพื่อรวมการบริหารจัดการและแนวคิดสถาปัตยกรรม เทคนิค และข้อกำหนดได้
- ให้ความสำคัญกับการวิเคราะห์ความเสี่ยงโดยการตีความข้อมูลแนวโน้ม และการคาดการณ์การป้องกันทางไซเบอร์ เพื่อให้บรรลุเป้าหมายทางธุรกิจ
- ขยายหัวข้อการควบคุมความปลอดภัย ให้ครอบคลุมอุปกรณ์มือถือ และอุปกรณ์ขนาดเล็ก รวมถึงช่องโหว่ของซอฟต์แวร์
- ครอบคลุมการรวมเทคโนโลยีคลาวด์ และการจำลองเสมือน เข้ากับสถาปัตยกรรมขององค์กรได้อย่างปลอดภัย
- สามารถรวมการใช้เทคนิคการเข้ารหัส เช่น Block chain- Crypto currency และการเข้ารหัสอุปกรณ์มือถือ

ทักษะที่ได้รับ

- ด้านการจัดการความเสี่ยง
  สามารถวิเคราะห์ความเสี่ยง และกรอบความปลอดภัยที่มาพร้อมกับภัยคุกคามในอุตสาหกรรมแบบเฉพาะได้ เข้าใจข้อกำหนดขององค์กร และบริหารกลยุทธ์ในการลดความเสี่ยงได้
- ด้านการดำเนินงานด้านความปลอดภัยขององค์กร
  สามารถตอบสนองเหตุการณ์ต่างๆ ที่เกิดขึ้น และมีความรู้ในการกระบวนการกู้คืนข้อมูล ดำเนินการประเมินความปลอดภัยโดยใช้เครื่องมือที่เหมาะสม
- การบูรณาการด้านเทคนิคความปลอดภัยขององค์กร
  สามารถรวบรวมโฮสต์ ที่เก็บข้อมูล เครือข่าย และแอปพลิเคชันเข้ากับสถาปัตยกรรมองค์กรได้อย่างปลอดภัยโดยใช้เทคโนโลยีคลาวด์ และระบบเสมือนจริง
- ด้านการวิจัย การพัฒนา และความร่วมมือ
  สามารถใช้การวิจัย เพื่อกำหนดแนวโน้มของอุตสาหกรรม และผลกระทบที่มีต่อองค์กร

คุณสมบัติของผู้เข้าอบรม

มีประสบการณ์ในการบริหารเทคโนโลยีสารสนเทศอย่างน้อย 10 ปี รวมถึงมีประสบการณ์ด้านความปลอดภัยในเชิงปฏิบัติการอย่างน้อย 5 ปี

สายงานที่มีความเกี่ยวข้องกับ CompTIA Advanced Security Practitioner (CASP+)

- สถาปนิกด้านการรักษาความปลอดภัย (Security Architect)
- นักวิเคราะห์เชิงผู้นำด้านเทคโนโลยี (Technical Lead Analyst)
- วิศวกรด้านความปลอดภัยของโปรแกรม (Application Security Engineer)
- วิศวกรด้านความปลอดภัย (Security Engineer)

ระยะเวลาการอบรม

3 วัน (18 ชั่วโมง)

รายละเอียดหลักสูตร

ที่	เนื้อหาหลักสูตร
1	**Risk Management**
	อิทธิพลของความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่มีต่อธุรกิจและอุตสาหกรรม เช่น ปัจจัยภายใน, ปัจจัยภายนอก, การเปลี่ยนรูปแบบ (Model) ทางธุรกิจ
	เปรียบเทียบและแยกความแตกต่างระหว่างความปลอดภัยทางเทคโนโลยีสารสนเทศ, นโยบายด้านความเป็นส่วนตัว, ขั้นตอนการปฏิบัติงานให้เป็นไปตามความต้องการขององค์กร เช่น Memorandum of understanding (MOU), Service-level agreement (SLA), Non-disclosure agreement (NDA), Incident response
	กลยุทธ์การบรรเทาความเสี่ยง (risk mitigation) เช่น กระบวนการบริหารจัดการความเสี่ยง (Risk management processes), ROI, RTO, RPO, MTTR, MTBF
	วิเคราะห์ตัวชี้วัด (Metric) ด้านความเสี่ยงของความปลอดภัยทางเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อองค์กร เช่น KPIs, KRIs, Metrics and attributes to ensure meet business needs
2	**Enterprise Security Architecture**
	วิเคราะห์ภาพรวมและสถาปัตยกรรมของระบบเครือข่ายให้ตรงกับความต้องการด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น ความปลอดภัยของอุปกรณ์ภายในระบบเครือข่าย, การออกแบบระบบเครือข่ายให้มีความปลอดภัย, การตั้งค่าความปลอดภัยให้กับอุปกรณ์ภายในระบบเครือข่าย
	การตั้งค่าความปลอดภัยให้กับอุปกรณ์ต่าง ๆ เช่น Trusted OS, Endpoint security software, Host hardening, Boot loader protections
	การตั้งค่าความปลอดภัยให้กับอุปกรณ์เคลื่อนที่และคอมพิวเตอร์แบบ Small Form Factor เช่น Enterprise mobility management, Security implications/privacy concerns, Wearable technology
	การป้องกันช่องโหว่ (Vulnerability) ของซอฟต์แวร์อย่างเหมาะสม เช่น การป้องกัน SQL injection, การป้องกัน Buffer overflow, การป้องกัน Click-jacking

ที่	เนื้อหาหลักสูตร
3	**Enterprise Security Operations**
	ประเมินความปลอดภัยโดยการใช้เครื่องมือที่เหมาะสม เช่น Malware sandboxing, Penetration testing, Vulnerability assessment
	วิเคราะห์สถานการณ์หรือผลลัพธ์และเลือกเครื่องมือที่เหมาะสมสำหรับการประเมินความปลอดภัย เช่น Port scanners, Vulnerability scanners, Protocol analyzer, Command line tools
	การตอบสนองต่อ Incident และขั้นตอนการกู้คืน (Recovery) เช่น E-discovery, Incident and emergency response, Incident response support tools
4	**Technical Integration of Enterprise Security**
	การผสาน (Integrate) ระบบคอมพิวเตอร์เพื่อสร้างความปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กร เช่น Data security considerations, Resources provisioning and deprovisioning, Network secure segmentation and delegation, Security and privacy considerations of storage integration
	การผสานระบบคลาวด์และระบบเสมือน (Virtualization) เพื่อสร้างความปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กร เช่น Cloud augmented security services, Security advantages and disadvantages of virtualization
	การผสานและแก้ไขปัญหาของระบบการพิสูจน์ตัวตน (Authentication and Authorization) เพื่อสร้างความปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กร เช่น Single sign-on, 802.1x, OpenID, LDAP, AD, RADIUS
	เทคนิคการเข้ารหัส (Cryptographic) เช่น Hashing, Digital signature, Steganography, Cryptocurrency, PKI
	เลือกเครื่องมือที่เหมาะสมในการควบคุมความปลอดภัยด้านการสื่อสารและการทำงานร่วมกัน เช่น Remote access, Instant messaging, Email, Social media
5	**Research, Development and Collaboration**
	ประยุกต์ใช้งานวิจัยและทฤษฎีเพื่อวิเคราะห์แนวโน้มของอุตสาหกรรมที่ส่งผลกระทบต่อองค์กร เช่น Threat intelligence, Research security implications of emerging business tools
	การออกแบบวงจรการพัฒนาเทคโนโลยี (Technology Life Cycle) ให้มีความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น Systems development life cycle, Software development life cycle, Asset management
	อธิบายถึงความสำคัญของความเกี่ยวข้องและความมีปฏิสัมพันธ์ระหว่างหน่วยธุรกิจที่ส่งผลต่อความสำเร็จในเรื่องความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ