

ด่วนที่สุด

ที่ สภมช ๐๗๐๐/ว๖๒๔๑

๑๙ สิงหาคม ๒๕๖๘

เรื่อง ขอประชาสัมพันธ์การจัดอบรมเชิงปฏิบัติการ ภายใต้กิจกรรมพัฒนาศักยภาพบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน

เรียน สำนักงานส่งเสริมการปกครองท้องถิ่นจังหวัดแม่ฮ่องสอน

ด้วย ปัจจุบันหน่วยงานต่าง ๆ ในประเทศไทยมีแนวโน้มถูกโจมตีจากภัยคุกคามทางไซเบอร์เพิ่มมากขึ้นเรื่อย ๆ ประกอบกับหลายหน่วยงานยังขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในการดูแลและปกป้ององค์กร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สภมช.) จึงดำเนินการจัดอบรมเชิงปฏิบัติการ ภายใต้กิจกรรมพัฒนาศักยภาพบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานสากลให้กับประชาชน ตามมาตรการและแนวทางตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่มุ่งเน้นการพัฒนาศักยภาพภาครัฐด้านดิจิทัลให้ผู้เข้าอบรมสามารถนำความรู้ไปประยุกต์ใช้ได้จริง รวมทั้งสร้างเครือข่ายบุคลากรและวิทยากรที่มีศักยภาพในการถ่ายทอดองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานที่เป็นที่ยอมรับในระดับสากล และส่งเสริมการดำเนินงานตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ในยุทธศาสตร์ที่ ๑ : สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากรองค์ความรู้ และเทคโนโลยี) (Capacity) และตามกลยุทธ์ที่ ๑.๑ เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ โดยผ่านการอบรมเชิงปฏิบัติการในหลักสูตรที่สำคัญจำนวน ๔ หลักสูตร ได้แก่

๑. หลักสูตรประกาศนียบัตรรับรองพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์
๒. หลักสูตรประกาศนียบัตรความมั่นคงปลอดภัยระบบคลาวด์
๓. หลักสูตรประกาศนียบัตรด้านการพิสูจน์หลักฐานทางดิจิทัล
๔. หลักสูตรประกาศนียบัตรด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับสูง

ในการนี้ สภมช. จึงใคร่ขอให้ท่านพิจารณาขอบข่ายบุคลากรในสังกัดที่ปฏิบัติงานเกี่ยวข้องเข้าร่วมการอบรมเชิงปฏิบัติการในครั้งนี้ เพื่อเพิ่มพูนความรู้ ความเข้าใจ และทักษะเชิงปฏิบัติการที่สามารถนำไปดูแลองค์กร พร้อมทั้งนำไปประยุกต์ใช้กับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ และขอความอนุเคราะห์ ในการแจ้งเวียนหนังสือประชาสัมพันธ์ไปยังหน่วยงานภายใต้การกำกับดูแลและประชาชนในพื้นที่ของท่าน เพื่อสมัครเข้าร่วมการฝึกอบรมในหลักสูตรที่สนใจ โดยไม่มีค่าใช้จ่าย

/ทั้งนี้...

ทั้งนี้ ท่านสามารถศึกษารายละเอียดเพิ่มเติม และดาวน์โหลดเอกสารรายละเอียดหลักสูตรได้ที่ QR Code ที่แนบมาท้ายหนังสือ ทั้งนี้ขอมอบหมายให้ คุณวรลักษณ์ สง่าลี หมายเลขโทรศัพท์ ๐๙ ๖๑๘๖ ๗๐๐๔ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณา และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

พลอากาศตรี 

(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โทรศัพท์ ๐ ๒๕๐๒ ๗๘๓๔

ไปรษณีย์อิเล็กทรอนิกส์ thnca@ncsa.or.th

รายละเอียดหลักสูตร



One Drive

ลงทะเบียน



www.thnca.or.th

หลักสูตรประกาศนียบัตรรับรองพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Certified in Cybersecurity)

1. คำอธิบายหลักสูตร

หลักสูตรการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ระดับเริ่มต้นที่มีเนื้อหาอ้างอิงตามหลักสูตรประกาศนียบัตรระดับสากลด้านความปลอดภัยไซเบอร์ ISC2 Certified in Cybersecurity (CC) ที่มุ่งเน้นให้ผู้เรียนมีความรู้พื้นฐานและทักษะเริ่มต้นในด้านความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามทางดิจิทัล โดยเน้นไปที่ผู้ที่ต้องการเริ่มต้นอาชีพในด้านความปลอดภัยไซเบอร์หรือผู้ที่ต้องการพัฒนาความรู้พื้นฐานด้านความปลอดภัยสารสนเทศ หลักสูตรนี้ได้รับการยกย่องอย่างกว้างขวางในอุตสาหกรรมความปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ

2. เนื้อหาในหลักสูตร

- บทเรียนที่ 1 หลักการด้านความมั่นคงปลอดภัย (Security Principles)
- บทเรียนที่ 2 การดำเนินงานด้านการรักษาความปลอดภัย (Security Operations)
- บทเรียนที่ 3 แนวคิดในการควบคุมการเข้าถึง (Access Controls Concepts)
- บทเรียนที่ 4 ความมั่นคงปลอดภัยของเครือข่าย (Network Security)
- บทเรียนที่ 5 แนวคิดการรับมือเหตุการณ์ ความต่อเนื่องทางธุรกิจ และการกู้คืนจากภัยพิบัติ (Incident Response, Business Continuity and Disaster Recovery Concepts)
- บทเรียนที่ 6 การประยุกต์ใช้หลักความมั่นคงปลอดภัยไซเบอร์ในบริบทกฎหมายไทย

3. เงื่อนไขการสมัครเข้าร่วมโครงการ

3.1 คุณสมบัติบุคคล

(1) บุคลากรของหน่วยงานควบคุมกำกับดูแล (Regulator) หรือ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือ
หน่วยงานของรัฐ (Government)

(2) นักเรียน นักศึกษา และบุคคลทั่วไป

3.2 เงื่อนไขอื่น ๆ ตามที่ สกมช. กำหนด

4. เกณฑ์การผ่านการคัดเลือกเข้าอบรมเชิงปฏิบัติการ (Onsite Workshop)

4.1 มีเวลาเข้าร่วมอบรมตลอดหลักสูตรไม่น้อยกว่า 80%

4.2 ทำข้อสอบวัดความรู้ก่อนเรียน

4.3 มีคะแนนข้อสอบวัดความรู้หลังเรียนไม่น้อยกว่า 70%

4.4 มีการลงทะเบียนสอบ Certified in Cybersecurity certification (CC)
ภายในระยะเวลาที่โครงการกำหนด

5. เกณฑ์การได้รับใบประกาศนียบัตรจาก สกมช.

5.1 มีเวลาเข้าร่วมอบรมตลอดหลักสูตรไม่น้อยกว่า 80%

5.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (ถ้ามี)

5.3 มีคะแนนข้อสอบวัดความรู้หลังเรียนไม่น้อยกว่า 70%

5.4 ทำแบบประเมินความพึงพอใจหลังการฝึกอบรม

5.5 มีการลงทะเบียนสอบ Certified in Cybersecurity certification (CC)
ภายในระยะเวลาที่โครงการกำหนด

6. เกณฑ์การได้รับสิทธิ์สอบใบประกาศนียบัตร ISC2 Certified in Cybersecurity (CC)

โดยคัดเลือกจากผู้มีคะแนนสูงสุดตามลำดับ จำนวนสิทธิ์ทั้งหมด 120 สิทธิ์
ตลอดโครงการ

- 6.1 คะแนนการเข้าร่วมอบรมตลอดหลักสูตร (20 คะแนน)
- 6.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (10 คะแนน)
- 6.3 คะแนนข้อสอบวัดความรู้หลังเรียน (70 คะแนน)

หมายเหตุ

- หากพบว่าข้อมูลหรือสิ่งที่ท่านนำเสนอเพื่อประกอบการพิจารณาไม่เป็นจริง และ/หรือ หากท่านไม่เข้าร่วมการอบรมตามที่ได้แจ้งยืนยันโดยไม่มีเหตุอันควร สกมช. ขอสงวนสิทธิ์ในการตัดสิทธิ์การเข้าร่วมโครงการนี้และโครงการอื่น ๆ ของท่านต่อไป
- ผู้สมัครเข้ารับการอบรม ต้องไม่เป็นผู้ที่อยู่ในรายชื่อผู้ถูกตัดสิทธิ์การเข้าร่วมกิจกรรม ของ สกมช.
- ผลการพิจารณาคัดเลือกจาก สกมช. ถือเป็นที่สุด

ช่องทางติดต่อเพิ่มเติม



www.thnca.or.th



09 6186 7004 (คุณวราลักษณ์ สง่าลี) หรือ
โทร. 02 502 7834 (ในวันเวลาราชการ)



Line Official Account @thnca

7. ขั้นตอนการรับสมัคร และการฝึกอบรม

- 7.1 เปิดรับสมัครเข้าสนใจเข้ารับการฝึกอบรม ระหว่างวันที่ 4 สิงหาคม – 26 กันยายน 2568 ผ่านช่องทาง www.thnca.or.th
- 7.2 ผู้สมัครเข้ารับการฝึกอบรม จะได้รับอีเมลแจ้งให้เข้าทำแบบทดสอบก่อนเรียน และแจ้งผลการทดสอบหลังการทดสอบ ระหว่างวันที่ 1 – 26 กันยายน 2568 ผ่านช่องทาง www.thnca.or.th
- 7.3 เข้ารับการฝึกอบรมในรูปแบบออนไลน์ ผ่านระบบ Zoom ระหว่างวันที่ 6 – 10 ตุลาคม 2568
- 7.4 แจ้งผู้มีสิทธิเข้ารับการฝึกอบรม ในรูปแบบปฏิบัติการ (Workshop) ผ่านช่องทางอีเมล ของผู้อบรม ในวันที่ 24 ตุลาคม พ.ศ 2568
- 7.5 เข้ารับการฝึกอบรมในรูปแบบปฏิบัติการ (Workshop) ตามรุ่นที่ผู้เข้าอบรม ได้ทำการเลือกไว้ และมีการทำแบบทดสอบหลังการอบรมในรูปแบบปฏิบัติการฯ เพื่อคัดเลือกผู้ได้รับการสนับสนุนการสอบประเมินทักษะตามมาตรฐานสากล ของวันสุดท้ายของการอบรมในรูปแบบปฏิบัติการ (Workshop) เวลา 13.00 – 16.00 น. (3 ชั่วโมง)

-  รุ่นที่ 1 ณ โรงแรม เดอะเนเจอร์ ภูเก็ต จังหวัดภูเก็ต จำนวน 40 ท่าน
ระหว่างวันที่ 10 – 12 พฤศจิกายน 2568
-  รุ่นที่ 2 ณ โรงแรมคุ้มภูคำ จังหวัดเชียงใหม่ จำนวน 40 ท่าน
ระหว่างวันที่ 17 – 19 พฤศจิกายน 2568
-  รุ่นที่ 3 ณ โรงแรมอวานี ขอนแก่น โฮเทล แอนด์ คอนเวนชั่น เซ็นเตอร์
จังหวัดขอนแก่น จำนวน 40 ท่าน
ระหว่างวันที่ 24 – 26 พฤศจิกายน 2568
-  รุ่นที่ 4 ณ โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น จังหวัดกรุงเทพฯ
จำนวน 40 ท่าน
ระหว่างวันที่ 15 – 17 ธันวาคม 2568

7.6 ผู้ได้รับสิทธิการสนับสนุน ดำเนินการสอบประเมินทักษะตามมาตรฐานสากล CC ณ ศูนย์สอบ ภายใน 30 วัน หลังประกาศรายชื่อ

หลักสูตรประกาศนียบัตรความมั่นคงปลอดภัยระบบบคลาวด์ (Certified in Cloud Security)

1. คำอธิบายหลักสูตร

หลักสูตรประกาศนียบัตรความมั่นคงปลอดภัยระบบบคลาวด์ที่มีเนื้อหาอ้างอิงตามหลักสูตรประกาศนียบัตรระดับสากลด้านเทคโนโลยีคลาวด์ CompTIA Cloud+ ที่มุ่งเน้นให้ผู้เรียนมีความรู้และทักษะในด้านการออกแบบ นำไปใช้ จัดการ และการรักษาความปลอดภัยของโครงสร้างพื้นฐานคลาวด์ โดยเน้นไปที่ผู้มีความเชี่ยวชาญในด้านการบริหารจัดการระบบคลาวด์ การทำงานร่วมกันของระบบ และการแก้ไขปัญหาเทคโนโลยีคลาวด์ หลักสูตรนี้ได้รับการยกย่องอย่างกว้างขวางในอุตสาหกรรมเทคโนโลยีสารสนเทศและการให้บริการคลาวด์

2. เนื้อหาในหลักสูตร

- บทเรียนที่ 1 ความเข้าใจเกี่ยวกับสถาปัตยกรรมระบบบคลาวด์
(Understanding Cloud Architecture Concepts)
- บทเรียนที่ 2 การวางแผนบริการระบบบคลาวด์ (Planning Cloud Services)
- บทเรียนที่ 3 การจัดเตรียมและย้ายทรัพยากรไปยังคลาวด์
(Provisioning and Migrating Cloud Resources)
- บทเรียนที่ 4 การเปรียบเทียบระบบจัดเก็บข้อมูลบนคลาวด์
(Comparing Cloud Storage)
- บทเรียนที่ 5 การแก้ไขปัญหาการปรับใช้และต้นทุน
(Troubleshooting Deployment Issues and Cost)
- บทเรียนที่ 6 การใช้เทคโนโลยีเวอร์ชวลไลเซชันและฐานข้อมูล
(Using Virtualization and Databases)
- บทเรียนที่ 7 การเข้าใจระบบเครือข่ายบนคลาวด์
(Comprehending Cloud Networking)

2. เนื้อหาในหลักสูตร (ต่อ)

- บทเรียนที่ 8 การทำงานแบบอัตโนมัติของทรัพยากรคลาวด์ (Automating Cloud Resources)
- บทเรียนที่ 9 การบริหารจัดการด้านความมั่นคงปลอดภัยในระบบคลาวด์ (Implementing Security Management)
- บทเรียนที่ 10 ความเข้าใจด้านการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการแก้ไขปัญหา (Comprehending Security Compliance and Troubleshooting)
- บทเรียนที่ 11 การดำเนินการด้านประสิทธิภาพและการตรวจสอบระบบ (Implementing Performance and Monitoring)
- บทเรียนที่ 12 การจัดการการกู้คืนจากภัยพิบัติและความต่อเนื่องทางธุรกิจ (Managing Disaster Recovery and Business Continuity)
- บทเรียนที่ 13 การประยุกต์ใช้คลาวด์คอมพิวติงภายใต้กรอบกฎหมายและข้อบังคับของไทย (Applying Cloud Computing within the Thai Legal and Regulatory Framework)

3. เงื่อนไขการสมัครเข้าร่วมโครงการ

3.1 คุณสมบัติบุคคล

- (1) เป็นบุคลากรที่อยู่ภายใต้สังกัดหน่วยงานควบคุมกำกับดูแล (Regulator) หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือหน่วยงานของรัฐ
- (2) หน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (3) นักเรียน นักศึกษา และบุคคลทั่วไป

➡ แสดงหลักฐาน

 ข้อมูลในระบบ THNCA ที่ยอมรับว่าเป็นความจริง (เสมือนเป็นการรับรองตนเอง) ดังนี้

- หน่วยงานต้นสังกัด
- ตำแหน่งงาน
- การศึกษา
- ประสบการณ์ทำงาน

3. เงื่อนไขการสมัครเข้าร่วมโครงการ (ต่อ)

3.2 ทักษะ/ความเชี่ยวชาญ (อย่างน้อย 1 ข้อ)

- (1) เป็นผู้ได้รับใบประกาศนียบัตรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ (สกมช.) โดยสามารถเข้าเรียนได้ที่ระบบ e-Learning ของ THNCA
- (2) เป็นผู้มีความรู้หรือความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ หรือเทียบเท่า โดยพิจารณาจากใบรับรองสากลด้านไซเบอร์ตามที่ สกมช. กำหนด

➡ แสดงหลักฐาน

- 🖥️ ใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ จาก สกมช.
- 🖥️ หรือ ได้รับใบรับรองสากลด้านความมั่นคงปลอดภัยไซเบอร์อื่น ๆ ที่เทียบเท่าหรือไม่ต่ำกว่า ดังนี้
 - ★ ISC2 Certified in Cybersecurity (CC)
 - ★ CompTIA Security+
 - ★ EC-Council Certified Security Specialist (ECSS)
 - ★ ฯลฯ

3.3 เงื่อนไขอื่น ๆ ตามที่ สกมช. กำหนด

4. เกณฑ์การผ่านการคัดเลือกเข้าอบรมเชิงปฏิบัติการ (Onsite Workshop)

- 4.1 เป็นบุคลากรที่อยู่ภายใต้สังกัดหน่วยงานควบคุมกำกับดูแล (Regulator) หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือหน่วยงานของรัฐ (จะได้รับการพิจารณาเป็นลำดับแรก)
- 4.2 มีเวลาเข้าร่วมอบรมออนไลน์ตลอดหลักสูตรไม่น้อยกว่า 80%
- 4.3 มีคะแนนสอบวัดความรู้หลังเรียนออนไลน์ ไม่น้อยกว่า 70%

5. เกณฑ์การได้รับใบประกาศนียบัตรจาก สกมช.

- 5.1 มีเวลาเข้าร่วมอบรมตลอดหลักสูตรไม่น้อยกว่า 80%
- 5.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (ถ้ามี)
- 5.3 มีคะแนนข้อสอบวัดความรู้หลังเรียน ไม่น้อยกว่า 70%
- 5.4 ทำแบบประเมินความพึงพอใจหลังการฝึกอบรม

6. เกณฑ์การได้รับสิทธิ์สอบใบประกาศนียบัตร CompTIA Cloud+

โดยคัดเลือกจากผู้มีคะแนนสูงสุดตามลำดับ จำนวนสิทธิ์ทั้งหมด 90 สิทธิ์
ตลอดโครงการ

- 6.1 คะแนนการเข้าร่วมอบรมตลอดหลักสูตร (20 คะแนน)
- 6.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (10 คะแนน)
- 6.3 คะแนนข้อสอบวัดความรู้หลังเรียน (70 คะแนน)

หมายเหตุ

- หากพบว่าข้อมูลหรือสิ่งที่ท่านนำเสนอเพื่อประกอบการพิจารณาไม่เป็นจริง และ/หรือ หากท่านไม่เข้าร่วมการอบรมตามที่ได้แจ้งยืนยันโดยไม่มีเหตุอันควร สกมช. ขอสงวนสิทธิ์ในการตัดสิทธิ์การเข้าร่วมโครงการนี้และโครงการอื่น ๆ ของท่านต่อไป
- ผู้สมัครเข้ารับการอบรม ต้องไม่เป็นผู้ที่อยู่ในรายชื่อผู้ถูกตัดสิทธิ์การเข้าร่วมกิจกรรม ของ สกมช.
- ผลการพิจารณาคัดเลือกจาก สกมช. ถือเป็นที่สุด

7. ขั้นตอนการรับสมัคร และการฝึกอบรม

- 7.1 เปิดรับสมัครเข้าสนใจเข้ารับการฝึกอบรม ระหว่างวันที่ 4 สิงหาคม – 26 กันยายน พ.ศ 2568 ผ่านช่องทาง www.thnca.or.th
- 7.2 ผู้สมัครเข้ารับการฝึกอบรม จะได้รับอีเมลแจ้งให้เข้าทำแบบทดสอบก่อนเรียน และแจ้งผลการทดสอบหลังการทดสอบ ระหว่างวันที่ 1 – 26 กันยายน 2568 ผ่านช่องทาง www.thnca.or.th
- 7.3 เข้ารับการฝึกอบรมในรูปแบบออนไลน์ ผ่านระบบ Zoom ระหว่างวันที่ 14 – 18 ตุลาคม 2568
- 7.4 แจ้งผู้มีสิทธิเข้ารับการฝึกอบรม ในรูปแบบปฏิบัติการ (Workshop) ผ่านช่องทางอีเมลของผู้อบรม ในวันที่ 31 ตุลาคม 2568
- 7.5 เข้ารับการฝึกอบรมในรูปแบบปฏิบัติการ (Workshop) ตามรุ่นที่ผู้เข้าอบรมได้ทำการเลือกไว้ และมีการทำแบบทดสอบหลังการอบรมในรูปแบบปฏิบัติการฯ เพื่อคัดเลือกผู้ได้รับการสนับสนุนการสอบประเมินทักษะตามมาตรฐานสากล ของวันสุดท้ายของการอบรมในรูปแบบปฏิบัติการ (Workshop) เวลา 13.00 – 16.00 น. (3 ชั่วโมง)
 -  รุ่นที่ 1 ณ โรงแรม เดอะเนเจอร์ ภูเก็ต จังหวัดภูเก็ต จำนวน 40 ท่าน ระหว่างวันที่ 13 – 15 พฤศจิกายน 2568
 -  รุ่นที่ 2 ณ โรงแรมคุ้มภูคำ จังหวัดเชียงใหม่ จำนวน 40 ท่าน ระหว่างวันที่ 20 – 22 พฤศจิกายน 2568
 -  รุ่นที่ 3 ณ โรงแรมอวานี ขอนแก่น โฮเทล แอนด์ คอนเวนชั่น เซ็นเตอร์ จังหวัดขอนแก่น จำนวน 40 ท่าน ระหว่างวันที่ 27 – 29 พฤศจิกายน พ.ศ 2568
- 7.6 ผู้ได้รับสิทธิการสนับสนุน ดำเนินการสอบประเมินทักษะตามมาตรฐานสากล Cloud+ ณ ศูนย์สอบ ภายใน 30 วัน หลังประกาศรายชื่อ

ช่องทางติดต่อเพิ่มเติม



www.thnca.or.th



09 6186 7004 (คุณวราลักษณ์ สง่าลี) หรือ โทร. 02 502 7834 (ในวันเวลาราชการ)



Line Official Account @thnca

หลักสูตรประกาศนียบัตรด้านความปลอดภัยระบบสารสนเทศระดับสูง (Certified Information Systems Security Professional)

1. คำอธิบายหลักสูตร

เป็นหลักสูตรการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ในระดับผู้เชี่ยวชาญเฉพาะด้านที่มีเนื้อหาอ้างอิงตามหลักสูตรประกาศนียบัตรระดับสากลด้านความปลอดภัยระบบสารสนเทศระดับสูง ISC2 CISSP ที่มุ่งเน้นให้ผู้เรียนมีความรู้และทักษะในด้านความปลอดภัยของระบบสารสนเทศและเทคโนโลยีสารสนเทศ โดยเน้นไปที่ผู้มีความเชี่ยวชาญในด้านความปลอดภัยของระบบสารสนเทศและเทคโนโลยีสารสนเทศ หลักสูตรนี้ได้รับการยกย่องอย่างกว้างขวางในอุตสาหกรรมความปลอดภัยและเทคโนโลยีสารสนเทศ

2. เนื้อหาในหลักสูตร

- บทเรียนที่ 1 หลักการความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity principles)
- บทเรียนที่ 2 กฎหมายและจริยธรรม (Law and ethics)
- บทเรียนที่ 3 การบริหารความเสี่ยง (Risk management)
- บทเรียนที่ 4 นโยบายความมั่นคงปลอดภัย (Security policies)
- บทเรียนที่ 5 สินทรัพย์สารสนเทศ (Information assets)
- บทเรียนที่ 6 เทคนิคการเข้ารหัสวิทยา (Cryptographic techniques)
- บทเรียนที่ 7 หลักการความปลอดภัยของระบบ (System security principles)
- บทเรียนที่ 8 สถาปัตยกรรมองค์กรที่ปลอดภัย (Secure enterprise architecture)
- บทเรียนที่ 9 ความมั่นคงปลอดภัยของระบบเฉพาะทาง
(Specialized system security)
- บทเรียนที่ 10 การออกแบบระบบที่มั่นคงปลอดภัย (Secure system design)
- บทเรียนที่ 11 พื้นฐานของเครือข่าย (Network fundamentals)
- บทเรียนที่ 12 โพรโทคอลเครือข่าย (Network protocols)

2. เนื้อหาในหลักสูตร (ต่อ)

- บทเรียนที่ 14 สถาปัตยกรรมความมั่นคงปลอดภัยเครือข่าย
(Network security architecture)
- บทเรียนที่ 15 การกำหนดค่าเครือข่ายที่ปลอดภัย (Secure network configuration)
- บทเรียนที่ 16 การบริหารจัดการตัวตน (Identity management)
- บทเรียนที่ 17 เทคโนโลยีการควบคุมการเข้าถึง (Access control technologies)
- บทเรียนที่ 18 การประเมินและทดสอบความมั่นคงปลอดภัย
(Security assessment and testing)
- บทเรียนที่ 19 การปฏิบัติการด้านความมั่นคงปลอดภัย (Security operations)
- บทเรียนที่ 20 การสแกนและการตรวจสอบ (Scanning and monitoring)
- บทเรียนที่ 21 การรับมืออุบัติการณ์ (Incident response)
- บทเรียนที่ 22 การวางแผนรับมือภัยพิบัติ (Disaster planning)
- บทเรียนที่ 23 การพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure software development)
- บทเรียนที่ 24 การประยุกต์ใช้หลักการ CISSP ในบริบทกฎหมายและกรณีศึกษาของประเทศไทย

3. เจาะลึกการสมัครเข้าร่วมโครงการ

3.1 คุณสมบัติบุคคล

- (1) เป็นบุคลากรที่อยู่ภายใต้สังกัดหน่วยงานควบคุมกำกับดูแล (Regulator) หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือหน่วยงานของรัฐ
- (2) หน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (3) นักเรียน นักศึกษา และบุคคลทั่วไป



แสดงหลักฐาน



ข้อมูลในระบบ THNCA ที่ยอมรับว่าเป็นความจริง (เสมือนเป็นการรับรองตนเอง) ดังนี้

- หน่วยงานต้นสังกัด
- ตำแหน่งงาน
- การศึกษา
- ประสบการณ์ทำงาน

3. เงื่อนไขการสมัครเข้าร่วมโครงการ (ต่อ)

3.2 มีประสบการณ์ทำงานด้านความมั่นคงปลอดภัยไซเบอร์ หรือด้านเทคโนโลยีสารสนเทศ ไม่น้อยกว่า 5 ปี

3.3 ทักษะ/ความเชี่ยวชาญ (อย่างน้อย 1 ข้อ)

(1) เป็นผู้ได้รับใบประกาศนียบัตรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ (สกมช.) โดยสามารถเข้าเรียนได้ที่ระบบ e-Learning ของ THNCA

(2) เป็นผู้มีความรู้หรือความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ หรือเทียบเท่า โดยพิจารณาจากใบรับรองสากลด้านไซเบอร์ตามที่ สกมช. กำหนด

➡ แสดงหลักฐาน

 ใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ จาก สกมช.

 หรือได้รับใบรับรองสากลด้านความมั่นคงปลอดภัยไซเบอร์อื่น ๆ ที่เทียบเท่าหรือไม่ต่ำกว่า ดังนี้

★ ISC2 Certified in Cybersecurity (CC)

★ CompTIA Security+

★ EC-Council Certified Security Specialist (ECSS)

★ ฯลฯ

3.4 เงื่อนไขอื่น ๆ ตามที่ สกมช. กำหนด

4. เกณฑ์การผ่านการคัดเลือกเข้าอบรมเชิงปฏิบัติการ (Onsite Workshop)

4.1 เป็นบุคลากรที่อยู่ภายใต้สังกัดหน่วยงานควบคุมกำกับดูแล (Regulator) หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือหน่วยงานของรัฐ (จะได้รับการพิจารณาเป็นลำดับแรก)

4.2 มีประสบการณ์ทำงานด้านความมั่นคงปลอดภัยไซเบอร์ หรือด้านเทคโนโลยีสารสนเทศ ไม่น้อยกว่า 5 ปี

4.3 มีเวลาเข้าร่วมอบรมออนไลน์ตลอดหลักสูตรไม่น้อยกว่า 80%

4.4 มีคะแนนสอบวัดความรู้หลังเรียนออนไลน์ไม่น้อยกว่า 70%

5. เกณฑ์การได้รับใบประกาศนียบัตรจาก สกมช.

- 5.1 มีเวลาเข้าร่วมอบรมตลอดหลักสูตรไม่น้อยกว่า 80%
- 5.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (ถ้ามี)
- 5.3 มีคะแนนข้อสอบวัดความรู้หลังเรียน ไม่น้อยกว่า 70%
- 5.4 ทำแบบประเมินความพึงพอใจหลังการฝึกอบรม
- 5.5 ผ่านการสอบคัดเลือกเพื่อเข้าฝึกอบรมในรูปแบบเชิงปฏิบัติการ (Workshop) ในรูปแบบ Onsite
- 5.6 ผ่านการสอบคัดเลือกโดยวิธีสัมภาษณ์ผ่านระบบ Zoom

6. เกณฑ์การได้รับสิทธิ์สอบใบประกาศนียบัตร ISC2 CISSP

โดยคัดเลือกจากผู้มีคะแนนสูงสุดตามลำดับ จำนวนสิทธิ์ทั้งหมด 40 สิทธิ์ ตลอดโครงการ

- 6.1 คะแนนการเข้าร่วมอบรมตลอดหลักสูตร (20 คะแนน)
- 6.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (10 คะแนน)
- 6.3 คะแนนข้อสอบวัดความรู้หลังเรียน (70 คะแนน)

หมายเหตุ

- หากพบว่าข้อมูลหรือสิ่งที่ท่านนำเสนอเพื่อประกอบการพิจารณาไม่เป็นจริง และ/หรือ หากท่านไม่เข้าร่วมการอบรมตามที่ได้แจ้งยืนยันโดยไม่มีเหตุอันควร สกมช. ขอสงวนสิทธิ์ในการตัดสิทธิ์การเข้าร่วมโครงการนี้และโครงการอื่น ๆ ของท่านต่อไป
- ผู้สมัครเข้ารับการอบรม ต้องไม่เป็นผู้ที่อยู่ในรายชื่อผู้ถูกตัดสิทธิ์การเข้าร่วมกิจกรรมของ สกมช.
- ผลการพิจารณาคัดเลือกจาก สกมช. ถือเป็นขั้นสิ้นสุด

7. ขั้นตอนการรับสมัคร และการฝึกอบรม

- 7.1 เปิดรับสมัครเข้าสนใจเข้ารับการฝึกอบรม ระหว่างวันที่ 4 สิงหาคม – 19 กันยายน พ.ศ 2568 ผ่านช่องทาง www.thnca.or.th
- 7.2 ผู้สมัครเข้ารับการฝึกอบรม จะได้รับอีเมลแจ้งให้เข้าทำแบบทดสอบก่อนเรียน และแจ้งผลการทดสอบหลังการทดสอบ ระหว่างวันที่ 1 – 19 กันยายน 2568 ผ่านช่องทาง www.thnca.or.th
- 7.3 เข้ารับการฝึกอบรมในรูปแบบออนไลน์ ผ่านระบบ Zoom ระหว่างวันที่ 29 กันยายน – 3 ตุลาคม 2568
- 7.4 ผู้เข้ารับการฝึกอบรม ดำเนินการทำแบบทดสอบหลังอบรมออนไลน์ จำนวน 100 คน ผ่านระบบ Proctor ในวันที่ 3 ตุลาคม 2568 เวลา 13.00 - 16.00 น. (3 ชั่วโมง)
- 7.5 แจ้งผู้ผ่านการทำแบบทดสอบหลังอบรมออนไลน์ เพื่อสอบคัดเลือกออนไลน์ ผ่านช่องทางอีเมล ในวันที่ 16 ตุลาคม 2568
- 7.6 ผู้ผ่านเกณฑ์การทดสอบหลังอบรมออนไลน์ การทบทวนเนื้อหาหลักสูตร ในรูปแบบออนไลน์ ผ่านระบบ Zoom ระหว่างวันที่ 17 – 20 ตุลาคม 2568
- 7.7 ดำเนินการสอบ เพื่อคัดเลือกผู้เข้ารับการฝึกอบรมในรูปแบบเชิงปฏิบัติการ (Workshop) โดยการสอบเป็นรูปแบบการสอบออนไลน์ จำนวน 100 คน วันที่ 21 ตุลาคม 2568 (ข้อสอบเป็นภาษาอังกฤษ)
- 7.8 สอบสัมภาษณ์ผ่านระบบ Zoom แจ้งผู้มีสิทธิเข้าการฝึกอบรมในรูปแบบเชิงปฏิบัติการ (Workshop) และผู้มีสิทธิสอบประเมินทักษะตาม มาตรฐานสากล จำนวน 50 คน ณ โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น จังหวัดกรุงเทพฯ ระหว่างวันที่ 4 – 7 พฤศจิกายน 2568
- 7.9 เข้ารับการฝึกอบรมในรูปแบบปฏิบัติการ (Workshop) ระหว่างวันที่ 15 – 19 ธันวาคม 2568 และมีการทำแบบทดสอบหลังการอบรมในรูปแบบปฏิบัติการ (Workshop) เพื่อคัดเลือกผู้ได้รับการสนับสนุนการสอบประเมิน ทักษะตามมาตรฐานสากล ในวันที่ 19 ธันวาคม 2568 เวลา 13.00 – 16.00 น. (3 ชั่วโมง)
- 7.10 ผู้ได้รับสิทธิการสนับสนุน ดำเนินการสอบประเมินทักษะตามมาตรฐานสากล CISSP ณ ศูนย์สอบ ภายใน 30 วัน หลังประกาศรายชื่อ

ช่องทางติดต่อเพิ่มเติม



www.thnca.or.th



09 6186 7004 (คุณวราลักษณ์ สง่าลี) หรือ
โทร. 02 502 7834 (ในวันเวลาราชการ)



Line Official Account @thnca

หลักสูตรประกาศนียบัตรด้านการพิสูจน์หลักฐานทางดิจิทัล (Computer Hacking Forensic Investigator)

1. คำอธิบายหลักสูตร

เป็นหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับผู้เชี่ยวชาญเฉพาะด้านที่มีเนื้อหาอ้างอิงตามหลักสูตรประกาศนียบัตรระดับสากลด้านการพิสูจน์หลักฐานทางดิจิทัล EC-Council CHFI ซึ่งการฝึกอบรมเน้นการสอนให้ผู้เรียนมีความรู้และทักษะในการสอบสวนอาชญากรรมทางดิจิทัลด้วยกระบวนการทางนิติวิทยาศาสตร์ การวิเคราะห์ข้อมูลที่เกี่ยวข้องกับการบุกรุกทางไซเบอร์ การตรวจพิสูจน์หลักฐานทางดิจิทัล ตรวจสอบการละเมิดความปลอดภัยของระบบสารสนเทศ โดยมุ่งเน้นการศึกษาเกี่ยวกับกระบวนการที่ใช้ในการสอบสวนด้านนิติวิทยาศาสตร์ทางไซเบอร์

2. เนื้อหาในหลักสูตร

- บทเรียนที่ 1 นิติวิทยาศาสตร์คอมพิวเตอร์ในโลกยุคปัจจุบัน
(Computer Forensics in Today's World)
- บทเรียนที่ 2 กระบวนการสืบสวนทางนิติวิทยาการคอมพิวเตอร์
(Computer Forensics Investigation)
- บทเรียนที่ 3 การทำความเข้าใจเกี่ยวกับฮาร์ดดิสก์และระบบไฟล์
(Understanding Hard Disks and File Systems)
- บทเรียนที่ 4 การได้มาซึ่งข้อมูลและการทำซ้ำ (Data Acquisition and Duplication)
- บทเรียนที่ 5 การรับมือกับเทคนิคต่อต้านนิติวิทยาศาสตร์
(Defeating Anti-forensics Techniques)
- บทเรียนที่ 6 การพิสูจน์หลักฐานบนระบบ Windows (Windows Forensics)

2. เนื้อหาในหลักสูตร (ต่อ)

- บทเรียนที่ 7 การพิสูจน์หลักฐานในระบบ Linux และ macOS (Linux and Mac Forensics)
- บทเรียนที่ 8 การพิสูจน์หลักฐานในเครือข่าย (Network Forensics)
- บทเรียนที่ 9 การพิสูจน์หลักฐานจากมัลแวร์ (Malware Forensics)
- บทเรียนที่ 10 การสืบสวนการโจมตีผ่านเว็บไซต์ (Investigating Web Attacks)
- บทเรียนที่ 11 ดำเนินการพิสูจน์หลักฐานบนเครือข่ายดาร์กเว็บ (Dark Web Forensics)
- บทเรียนที่ 12 การพิสูจน์หลักฐานในระบบคลาวด์ (Cloud Forensics)
- บทเรียนที่ 13 การพิสูจน์หลักฐานจากอีเมลและโซเชียลมีเดีย (Email and Social Media Forensics)
- บทเรียนที่ 14 การพิสูจน์หลักฐานจากอุปกรณ์เคลื่อนที่ (Mobile Forensics)
- บทเรียนที่ 15 การพิสูจน์หลักฐานดิจิทัลในอุปกรณ์ IoT (IoT Forensics)
- บทเรียนที่ 16 นิติวิทยาศาสตร์ดิจิทัลในบริบทของกฎหมายและกระบวนการยุติธรรมไทย

3. เงื่อนไขการสมัครเข้าร่วมโครงการ

3.1 คุณสมบัติบุคคล

- (1) เป็นบุคลากรที่อยู่ภายใต้สังกัดหน่วยงานควบคุมกำกับดูแล (Regulator) หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือหน่วยงานของรัฐ
- (2) หน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (3) นักเรียน นักศึกษา และบุคคลทั่วไป

➡ แสดงหลักฐาน

 ข้อมูลในระบบ THNCA ที่ยอมรับว่าเป็นความจริง (เสมือนเป็นการรับรองตนเอง) ดังนี้

- หน่วยงานต้นสังกัด
- ตำแหน่งงาน
- การศึกษา
- ประสบการณ์ทำงาน

3. เงื่อนไขการสมัครเข้าร่วมโครงการ (ต่อ)

3.2 ทักษะ/ความเชี่ยวชาญ (อย่างน้อย 1 ข้อ)

- (1) เป็นผู้ได้รับใบประกาศนียบัตรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ (สกมช.) โดยสามารถเข้าเรียนได้ที่ระบบ e-Learning ของ THNCA
- (2) เป็นผู้มีความรู้หรือความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ หรือเทียบเท่า โดยพิจารณาจากใบรับรองสากลด้านไซเบอร์ตามที่ สกมช. กำหนด

➡ แสดงหลักฐาน

- 🖥️ ใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ จาก สกมช.
- 🖥️ หรือได้รับใบรับรองสากลด้านความมั่นคงปลอดภัยไซเบอร์อื่น ๆ ที่เทียบเท่าหรือไม่ต่ำกว่า ดังนี้
 - ★ ISC2 Certified in Cybersecurity (CC)
 - ★ CompTIA Security+
 - ★ EC-Council Certified Security Specialist (ECSS)
 - ★ ฯลฯ

3.3 เงื่อนไขอื่น ๆ ตามที่ สกมช. กำหนด

4. เกณฑ์การผ่านการคัดเลือกเข้าอบรมเชิงปฏิบัติการ (Onsite Workshop)

- 4.1 เป็นบุคลากรที่อยู่ภายใต้สังกัดหน่วยงานควบคุมกำกับดูแล (Regulator) หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือหน่วยงานของรัฐ (จะได้รับการพิจารณาเป็นลำดับแรก)
- 4.2 มีเวลาเข้าร่วมอบรมออนไลน์ตลอดหลักสูตรไม่น้อยกว่า 80%
- 4.3 มีคะแนนสอบวัดความรู้หลังเรียนออนไลน์ ไม่น้อยกว่า 70%

5. เกณฑ์การได้รับใบประกาศนียบัตรจาก สกมช.

- 5.1 มีเวลาเข้าร่วมอบรมตลอดหลักสูตรไม่น้อยกว่า 80%
- 5.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (ถ้ามี)
- 5.3 มีคะแนนข้อสอบวัดความรู้หลังเรียน ไม่น้อยกว่า 70%
- 5.4 ทำแบบประเมินความพึงพอใจหลังการฝึกอบรม

6. เกณฑ์การได้รับสิทธิสอบใบประกาศนียบัตร EC-Council CHFI

โดยคัดเลือกจากผู้มีคะแนนสูงสุดตามลำดับ จำนวนสิทธิ์ทั้งหมด 40 สิทธิ์ ตลอดโครงการ

- 6.1 คะแนนการเข้าร่วมอบรมตลอดหลักสูตร (20 คะแนน)
- 6.2 มีส่วนร่วมกิจกรรมเสริมระหว่างการอบรม ทั้งแบบเดี่ยวและกลุ่ม (10 คะแนน)
- 6.3 คะแนนข้อสอบวัดความรู้หลังเรียน (70 คะแนน)

หมายเหตุ

- หากพบว่าข้อมูลหรือสิ่งที่ท่านนำเสนอเพื่อประกอบการพิจารณาไม่เป็นจริง และ/หรือ หากท่านไม่เข้าร่วมการอบรมตามที่ได้แจ้งยืนยันโดยไม่มีเหตุอันควร สกมช. ขอสงวนสิทธิ์ในการตัดสิทธิ์การเข้าร่วมโครงการนี้และโครงการอื่น ๆ ของท่านต่อไป
- ผู้สมัครเข้ารับการอบรม ต้องไม่เป็นผู้ที่อยู่ในรายชื่อผู้ถูกตัดสิทธิ์การเข้าร่วมกิจกรรมของ สกมช.
- ผลการพิจารณาคัดเลือกจาก สกมช. ถือเป็นขั้นสิ้นสุด

7. ขั้นตอนการรับสมัคร และการฝึกอบรม

- 7.1 เปิดรับสมัครเข้าสนใจเข้ารับการฝึกอบรม ระหว่างวันที่ 4 สิงหาคม – 26 กันยายน 2568 ผ่านช่องทาง www.thnca.or.th
- 7.2 ผู้สมัครเข้ารับการฝึกอบรม จะได้รับอีเมลแจ้งให้เข้าทำแบบทดสอบก่อนเรียน และแจ้งผลการทดสอบหลังการทดสอบ ระหว่างวันที่ 1 – 26 กันยายน 2568 ผ่านช่องทาง www.thnca.or.th
- 7.3 เข้ารับการฝึกอบรมในรูปแบบออนไลน์ ผ่านระบบ Zoom ระหว่างวันที่ 27 - 31 ตุลาคม 2568
- 7.4 แจ้งผู้มีสิทธิ เข้ารับการฝึกอบรม ในรูปแบบปฏิบัติการ (Workshop) ผ่านช่องทางอีเมลของผู้อบรม ในวันที่ 14 พฤศจิกายน 2568
- 7.5 เข้ารับการฝึกอบรมในรูปแบบปฏิบัติการ (Workshop) ระหว่างวันที่ 11 - 13 ธันวาคม 2568 ณ โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น จังหวัดกรุงเทพฯ และมีการทำแบบทดสอบหลังการอบรมในรูปแบบปฏิบัติการ (Workshop) เพื่อคัดเลือกผู้ได้รับการสนับสนุนการสอบประเมินทักษะตามมาตรฐานสากล ในวันที่ 13 ธันวาคม 2568 เวลา 13.00 – 16.00 น. (3 ชั่วโมง)
- 7.6 ผู้ได้รับสิทธิการสนับสนุน ดำเนินการสอบประเมินทักษะตามมาตรฐานสากล CHFI ณ ศูนย์สอบ ภายใน 30 วัน หลังประกาศรายชื่อ

ช่องทางติดต่อเพิ่มเติม



www.thnca.or.th



09 6186 7004 (คุณวรลักษณ์ สง่าลี) หรือ
โทร. 02 502 7834 (ในวันเวลาราชการ)



Line Official Account @thnca

อบรม
ฟรี

พร้อมรับสนับสนุน
สอบใบเซอร์สากล



สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดอบรมและสอบ
ISC2 Certified in Cybersecurity Certification

หลักสูตรพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคง
ปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน

เปิดลงทะเบียนการอบรม วันที่ – 26 กันยายน 2568

คัดเลือกอบรมออนไลน์ จำนวน 160 คน (4 รุ่น)

หลักสูตร
มูลค่ากว่า
25,000 บาท

วันที่ 6 - 10 ต.ค. 2568

- อบรมในรูปแบบออนไลน์

ภาคเหนือ รุ่นที่ 2
จังหวัดเชียงใหม่

- วันที่ 17 - 19 พ.ย. 2568
- ณ โรงแรม คันทันท์

ภาคตะวันออกเฉียงเหนือ รุ่นที่ 3
จังหวัดขอนแก่น

- วันที่ 24 - 26 พ.ย. 2568
- ณ โรงแรม อวานี ขอนแก่น โฮเทล แอนด์ คอนเวนชันเซ็นเตอร์

ภาคกลาง รุ่นที่ 4
จังหวัดกรุงเทพมหานคร

- วันที่ 15 - 17 ธ.ค. 2568
- ณ โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชัน

ภาคใต้ รุ่นที่ 1 จังหวัดภูเก็ต

- วันที่ 10 - 12 พ.ย. 2568
- ณ โรงแรม เดอะ เมเจอร์ ภูเก็ต

เนื้อหา

Security Principles

Incident Response,
Business Continuity
and Disaster
Recovery Concepts

Access Controls
Concepts

Network Security

Security Operations

พร้อมรับใบรับรอง
การเข้าร่วมอบรม
จาก สกมช.

หลักสูตรนี้เหมาะกับ

นักเรียน นิสิต นักศึกษา ผู้ที่ต้องการเปลี่ยนสายงาน
มาด้านไซเบอร์ และบุคลากรทั่วไปที่ต้องการสร้าง
ความเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์



Register

สอบถามข้อมูลเพิ่มเติมได้ที่

E - Mail : thnca@thnca.or.th

Tel. : 0961867004 (คุณวราลักษณ์ สง่าลี)

Line OA : @thnca

(สามารถติดต่อได้ตามวันและเวลาดำเนินการ 08:30-16:30 น.)

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดอบรมและสอบ
Computer Hacking Forensic Investigator: CHFI

หลักสูตรประกาศนียบัตรด้านการพิสูจน์หลักฐานทางดิจิทัล

ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยาการด้านความมั่นคง
ปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน

อบรม

ฟรี

พร้อมรับสนับสนุน
สอบใบเซอร์สากล

เปิดลงทะเบียนการอบรม

วันนี้ – 26 กันยายน 2568

คัดเลือกอบรมออนไลน์

50 คน



หลักสูตร
มูลค่ากว่า

50,000 บาท

27 - 31 ต.ค. 2568

– อบรมในรูปแบบออนไลน์

14 พ.ย. 2568

– ประกาศรายชื่อผู้ผ่านเข้าอบรม ในรูปแบบเชิงปฏิบัติการ (ออนไลน์)

11 - 13 ส.ค. 2568

– อบรมออนไลน์ จำนวน 50 คน
– อบรมเชิงปฏิบัติการ (Workshop)

จังหวัดกรุงเทพมหานคร ณ โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น



14 ส.ค. 2568

– ประกาศรายชื่อผู้ได้รับการคัดเลือก เข้ารับการประเมิน
ทักษะตามมาตรฐานสากล

เนื้อหา

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Malware Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Cloud Forensics
- Email and Social Media Forensics
- Mobile Forensics
- IoT Forensics

หลักสูตรนี้เหมาะกับ

เจ้าหน้าที่ด้านความมั่นคงปลอดภัย ผู้ตรวจสอบระบบ
สารสนเทศ และผู้ที่ต้องการเป็นผู้เชี่ยวชาญในการ
แกะรอยและวิเคราะห์ภัยคุกคามทางไซเบอร์



พร้อมรับใบรับรอง
การเข้าร่วมอบรม
จาก สกมช.



Register

คุณสมบัติผู้สมัคร

- มีประสบการณ์ด้าน IT/Technology Digital ไม่น้อยกว่า 2 ปี
- มี Certificate ด้าน Cybersecurity จะได้รับการพิจารณาเป็นอันดับแรก

สอบถามข้อมูลเพิ่มเติมได้ที่

E - Mail : thnca@ncsa.or.th

Tel. : 0961867004 (คุณวรลักษณ์ สง่าสี)

Line OA : @thnca

(สามารถติดต่อได้ตามวันและเวลาราชการ 08:30-16:30 น.)

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดอบรมและสอบ
ISC2 CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL

CISSP

หลักสูตรความปลอดภัยระบบสารสนเทศระดับสูง

ภายใต้กิจกรรมพัฒนาศักยภาพบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากลให้กับประชาชน

อบรม

ฟรี

พร้อมรับสนับสนุน
สอบใบเซอร์สากล

เปิดลงทะเบียนการอบรม >>

วันนี้ - 19 กันยายน 2568

คัดเลือกอบรมออนไลน์

50 คน

หลักสูตร
มูลค่ากว่า
60,000 บาท

29 กันยายน - 3 ตุลาคม 2568

อบรมผ่านสื่ออิเล็กทรอนิกส์



16 ตุลาคม 2568

ประกาศรายชื่อผู้ผ่านการคัดเลือกเบื้องต้น

17 - 20 ตุลาคม 2568

ทบทวนข้อสอบ

21 ตุลาคม 2568

สอบคัดเลือกผู้มีคุณสมบัติในการเข้าอบรมเชิงปฏิบัติการ ณ มสร.

28 ตุลาคม 2568

ประกาศรายชื่อผู้มีสิทธิ์สอบสัมภาษณ์ 70 คน

4 - 7 พฤศจิกายน 2568

สอบสัมภาษณ์

24 พฤศจิกายน 2568

ประกาศรายชื่อผู้ผ่านเข้าอบรมเชิงปฏิบัติการ
และผู้ที่ได้รับสิทธิ์สอบประเมินทักษะตามมาตรฐานสากล

15 - 19 ธันวาคม 2568

เข้าอบรมเชิงปฏิบัติ จำนวน 70 คน

อบรมเชิงปฏิบัติ ณ โรงแรม ทีเค.พาเลซ แอนด์ คอนเวนชั่น



5 - 9 มกราคม 2569

ผู้ผ่านการอบรมทบทวนบทเรียนด้วยตนเองผ่านระบบ LMS
ตัวผ่านระบบ ZOOM

9 - 24 มกราคม 2569

ผู้เข้าอบรมเข้าสอบประเมินทักษะตามมาตรฐานสากล ณ ศูนย์สอบ
ภายในระยะเวลา 30 วันหลังจากประกาศผล

หลักสูตร Cyber Security

- มีประสบการณ์ด้าน Cybersecurity ไม่น้อยกว่า 5 ปี
- มี Certificate ด้าน Cybersecurity จะได้รับการพิจารณาเป็นพิเศษ

เกณฑ์การได้รับสิทธิ์สอบ ISC2 CISSP

- ผ่านการสอบคัดเลือก รอบที่ 1 ข้อสอบภาษาไทย 50 ข้อ
 Online
- ผ่านการสอบคัดเลือก รอบที่ 2 ข้อสอบภาษาไทย 100 ข้อ
 Onsite
- ผ่านการสอบคัดเลือกโดยการสัมภาษณ์
 Online
- ผ่านการอบรมหลักสูตร CISSP เป็นเวลา 5 วัน
 Onsite
- ผ่านการอบรมทบทวนข้อสอบ CISSP Boot Camp เป็นเวลา 5 วัน
 Onsite

หลักสูตรนี้เหมาะกับ

ผู้บริหารระดับสูง ผู้จัดการด้านความมั่นคงปลอดภัย
ที่ปรึกษา ผู้ออกแบบสถาปัตยกรรมระบบ
และผู้เชี่ยวชาญที่มีประสบการณ์ในสายงานอย่างน้อย 5 ปี ซึ่ง
ต้องการการรับรองความเป็นมืออาชีพระดับสากล
พร้อมรับใบรับรองการเข้าร่วมอบรม จาก สกมช.



รายละเอียดเพิ่มเติม

สอบถามข้อมูลเพิ่มเติมได้ที่

E - Mail : thnca@thnca.or.th
Tel. : 0961867004 (คุณวรลักษณ์ สง่าสี)
Line OA : @thnca
(สามารถติดต่อได้ตามวันและเวลาราชการ 08:30-16:30 น.)

อบรม
ฟรี

พร้อมรับสนับสนุน
สอบใบเซอร์สากล



สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดอบรมและสอบ
CompTIA Cloud+

หลักสูตรประกาศนียบัตรความมั่นคง ปลอดภัยระบบคลาวด์



ภายใต้กิจกรรมพัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัย
ไซเบอร์ตามมาตรฐานสากลให้กับประชาชน

หลักสูตร
มูลค่ากว่า
25,000 บาท

เปิดลงทะเบียนการอบรม
วันนี้ – 26 กันยายน 2568

คัดเลือกอบรมออนไลน์ จำนวน 120 คน (3 รุ่น)

8 ต.ค. 2568

— ประกาศรายชื่อผู้เข้าอบรม ในรูปแบบออนไลน์

ภาคเหนือ รุ่นที่ 2
จังหวัดเชียงใหม่

- วันที่ 20 - 22 พ.ย. 2568
- ณ โรงแรม คันทัน



ภาคตะวันออกเฉียงเหนือ
รุ่นที่ 3 จังหวัดขอนแก่น

- วันที่ 27 - 29 พ.ย. 2568
- ณ โรงแรม อวานี ขอนแก่น
ไฮเทล แอนด์ คอนเวนชัน
เซ็นเตอร์

ภาคใต้ รุ่นที่ 1 จังหวัดภูเก็ต

- วันที่ 13 - 15 พ.ย. 2568
- ณ โรงแรม เดอะ เมเจอร์ ภูเก็ต

พร้อมรับใบรับรอง
การเข้าร่วมอบรม
จาก สกมช.

หลักสูตรนี้เหมาะกับ

เจ้าหน้าที่ดูแลระบบคลาวด์ วิศวกรระบบ
และบุคลากรผู้รับผิดชอบการวางแผน
และดูแลโครงสร้างพื้นฐานบนระบบคลาวด์

คุณสมบัติผู้สมัคร

- มีประสบการณ์ด้าน IT/Technology Digital ไม่น้อยกว่า 2 ปี
- มี Certificate ด้าน Cybersecurity จะได้รับการพิจารณาเป็นอันดับแรก

เนื้อหา

Understanding Cloud Architecture Concept

Planning Cloud Services

Provisioning and Migrating Cloud Resources

Comparing Cloud Storage

Troubleshooting Deployment Issues and Cost

Using Virtualization and Databases

Comprehending Cloud Networking

Automating Cloud Resources

Implementing Security Management

Comprehending Security Compliance and Troubleshooting

Implementing Performance and Monitoring

Managing Disaster Recovery and Business Continuity



Register

สอบถามข้อมูลเพิ่มเติมได้ที่

E - Mail : thnca@ncsa.or.th

Tel. : 0961867004 (คุณวราลักษณ์ สง่าลี)

Line OA : @thnca

(สามารถติดต่อได้ตามวันและเวลาราชการ 08:30-16:30 น.)