



ที่ ศธ ๐๗๐๘๘/ ๖ ๒๒๒

สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดสตูล  
ต.คลองขุด อ.เมือง จ.สตูล ๙๑๐๐๐

๑๐ มีนาคม ๒๕๖๙

เรื่อง แนะนำการเรียนรู้หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบออนไลน์

เรียน ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอทุกอำเภอ

สิ่งที่ส่งมาด้วย เอกสารแนะนำการเรียนรู้หลักสูตร

จำนวน ๑ ชุด

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ร่วมมือกับกรมส่งเสริมการเรียนรู้ เพื่อส่งเสริมและสนับสนุนความรู้ด้านวิชาการความมั่นคงปลอดภัยไซเบอร์ให้แก่ครู บุคลากรทางการศึกษา และนักศึกษา ของกรมส่งเสริมการเรียนรู้ ให้มีโอกาพัฒนาความรู้และทักษะที่จำเป็นต่อการดำรงชีวิตในยุคดิจิทัล โดยในส่วนที่เกี่ยวข้องกับการแนะนำการเรียนรู้หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ทาง สกมช. ได้มีแพลตฟอร์มการเรียนรู้ผ่านระบบออนไลน์ จำนวน ๒ ช่องทาง ดังนี้

๑. NCSA MOOC : เรียนออนไลน์แนวฝึกปฏิบัติ/แล็บ มีสถานการณ์จำลองให้ลองทำจริง

๒. THNCA e Learning: เรียนออนไลน์ในรูปแบบหลักสูตรที่เป็นระบบ ประกอบด้วย บทเรียนและแบบทดสอบก่อน/หลังเรียน เมื่อประเมินผลผ่านเกณฑ์แล้วได้ใบรับรอง มีให้เลือกตั้งแต่ระดับพื้นฐาน ระดับผู้เชี่ยวชาญ และระดับเฉพาะทาง

ในการนี้ สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดสตูล ขอประชาสัมพันธ์ การเรียนรู้หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบออนไลน์เพื่อส่งเสริมให้ครู บุคลากรทางการศึกษา และผู้เรียนได้เข้าศึกษาเรียนรู้และพัฒนาทักษะที่เกี่ยวข้องต่อไป รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและดำเนินการ

ขอแสดงความนับถือ

(นางวาสนา อนุสรณ์ประเสริฐ)

ผู้อำนวยการสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดสตูล

กลุ่มยุทธศาสตร์และการพัฒนา

โทร. ๐ ๗๔๗๑ ๑๔๔๔

โทรสาร ๐ ๗๔๗๒ ๑๔๑๓

ไปรษณีย์อิเล็กทรอนิกส์ stn\_it@dole.go.th

“เรียนดี มีคุณธรรม”



กรมส่งเสริมการเรียนรู้

# แนะนำการเรียนรู้หลักสูตรด้านความมั่นคง ปลอดภัยไซเบอร์ ผ่านระบบออนไลน์ จาก (สกมช.)



จำนวน 2 ช่องทาง

คลิปวิดีโอแนะนำการเรียนรู้



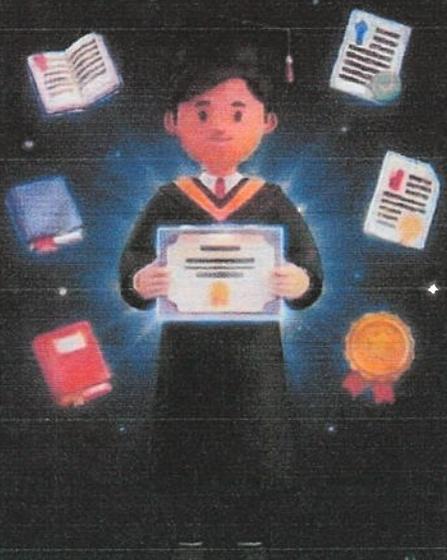
## 1. NCSA MOOC

เรียนออนไลน์แนวฝึกปฏิบัติ (Lab)  
มีสถานการณ์จำลองให้ได้ทดลองทำงานจริง



## 2. THNCA e-Learning

เรียนออนไลน์ในรูปแบบหลักสูตรที่เป็นระบบ  
ประกอบด้วยบทเรียนและแบบทดสอบก่อน-หลังเรียน  
เมื่อผ่านเกณฑ์การประเมินผลจะได้รับใบรับรอง  
มีให้เลือกตั้งแต่ระดับพื้นฐาน ระดับผู้เชี่ยวชาญ  
และระดับเฉพาะทาง



กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

NCSA  
สกนช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

THNCA  
Thailand National Cyber Academy  
สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ  
by NCSA

# THNCA ONLINE COURSES



## หลักสูตรในโครงการอบรมออนไลน์

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



[www.thnca.or.th](http://www.thnca.or.th)



0 2502 7831



Thailand National Cyber Academy



สำนักงานคณะกรรมการการรักษา  
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



## หลักสูตรในโครงการอบรมออนไลน์ (Online Courses)

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พ.ศ. 2569



**หลักสูตรในโครงการอบรมออนไลน์ (Online courses)**  
**ของสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ**  
**สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ**

**ระบบ THNCA e-Learning (<https://www.thnca.or.th>)**

THNCA e-Learning เป็นแพลตฟอร์มเรียนรู้ออนไลน์เพื่อพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชนและบุคลากรด้านไซเบอร์ทุกระดับ ผู้เรียนสามารถเข้าถึงเนื้อหาได้ทุกที่ ทุกเวลา และไม่มีค่าใช้จ่าย ประกอบด้วย 7 หลักสูตรที่มีความหลากหลาย ครอบคลุมเนื้อหาตั้งแต่ระดับพื้นฐานไปจนถึงระดับผู้เชี่ยวชาญ เฉพาะทาง ดังนี้

1. หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ระดับพื้นฐาน (ออนไลน์)
2. หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ระดับผู้เชี่ยวชาญ (ออนไลน์)
3. หลักสูตรผู้เชี่ยวชาญเฉพาะด้าน นักวิเคราะห์ความมั่นคงปลอดภัยทางไซเบอร์
4. หลักสูตรผู้เชี่ยวชาญเฉพาะด้าน การทดสอบเจาะระบบ (Penetration Test)
5. หลักสูตรความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องของระบบควบคุมอุตสาหกรรม (OT Security)
6. Microsoft AI Skills For All
7. Microsoft 365 Copilot



**NCSA**  
สทช.

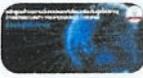
## ยกระดับความมั่นคงปลอดภัยไซเบอร์กับ NCSA e-learning

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA) เปิดโอกาสแห่งการเรียนรู้ผ่านหลักสูตรออนไลน์ที่ครอบคลุมทุกระดับ ตั้งแต่พื้นฐานไปจนถึงระดับผู้เชี่ยวชาญเฉพาะทาง เพื่อพัฒนาศักยภาพบุคลากรด้านไซเบอร์ของประเทศ

**หลักสูตรสำหรับทุกคนและทุกภาค-ดิจิทัล**

-  Microsoft AI Skills For All (ออนไลน์): เสริมสร้างความรู้เชิงปัญญาขั้นสูงด้านปัญญาประดิษฐ์
-  Microsoft 365 Copilot (ออนไลน์): เรียนรู้การใช้เครื่องมือ AI ช่วยเพิ่มประสิทธิภาพการทำงาน
-  Cybersecurity Foundation Course: เพิ่มความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

**หลักสูตรสำหรับผู้เชี่ยวชาญเฉพาะทาง**

-  Cybersecurity Professional Course: หลักสูตรสำหรับผู้จัดการด้านระดับมืออาชีพ
-  Cybersecurity Analyst: พัฒนาทักษะการเฝ้าระวังและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยไซเบอร์
-  Penetration Test: เรียนรู้เกี่ยวกับและกระบวนการทดสอบเจาะระบบ
-  OT Security: ความมั่นคงปลอดภัยทางไซเบอร์สำหรับระบบควบคุมอุตสาหกรรม

SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

## 1. หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ระดับพื้นฐาน (ออนไลน์) (Cybersecurity Foundation Course)

### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-learning

### คำอธิบายหลักสูตร

เป็นหลักสูตรพื้นฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยให้กับข้อมูล สารสนเทศ และระบบสารสนเทศ องค์ประกอบคุณสมบัติหลักด้านความมั่นคงปลอดภัยสารสนเทศ 3 ด้าน (การรักษาความลับ ความถูกต้อง และความพร้อมใช้) และองค์ประกอบสำคัญอื่นที่เกี่ยวข้อง แนวคิดความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย ฟังก์ชันการทำงาน และการใช้งาน (The Security, Functionality, and Usability Triangle) สำหรับการกำหนดระดับความมั่นคงปลอดภัยสารสนเทศ รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ ประเภทภัยคุกคามและช่องโหว่ ลักษณะภัยคุกคามไซเบอร์ แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารความเสี่ยงและมาตรการจัดการความเสี่ยง

### เงื่อนไขการสมัครเข้าร่วมโครงการ

นักเรียน นักศึกษา และบุคคลทั่วไป ที่ยังไม่มีความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

### ขั้นตอนการเข้าเรียนด้วยตนเอง

1. ลงทะเบียนเพื่อสมัครเป็นสมาชิก THNCA e-Learning ที่ [www.thnca.or.th](http://www.thnca.or.th)
2. เลือกหลักสูตรที่ต้องการ แล้วสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

### เกณฑ์การผ่านและได้รับใบประกาศนียบัตรจาก สกมช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ทำข้อสอบวัดความรู้หลังเรียนได้คะแนนไม่น้อยกว่า 60%

## รายวิชาในหลักสูตร (จำนวนรวม 21 ชั่วโมง)

- หน่วยที่ 01 หลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ
- หน่วยที่ 02 ภัยคุกคามและการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ
- หน่วยที่ 03 วิศวกรรมทางสังคม (การหลอกลวงทางไซเบอร์)
- หน่วยที่ 04 ระบบแฟ้มข้อมูล
- หน่วยที่ 05 วิทยาการเข้ารหัสลับ
- หน่วยที่ 06 วิทยาการอำพรางข้อมูล
- หน่วยที่ 07 จริยธรรมและกฎหมาย
- หน่วยที่ 08 หลักการพื้นฐานด้านเครือข่ายสื่อสาร
- หน่วยที่ 09 โพรโตคอลการเชื่อมต่อเครือข่ายที่ปลอดภัย
- หน่วยที่ 10 อุปกรณ์ความปลอดภัยเครือข่าย
- หน่วยที่ 11 ระบบการตรวจจับการบุกรุก
- หน่วยที่ 12 เครือข่ายส่วนตัวแบบเสมือน
- หน่วยที่ 13 ความมั่นคงปลอดภัยของเครือข่ายไร้สาย
- หน่วยที่ 14 การระบุตัวตน การพิสูจน์ตัวตน และการให้สิทธิ
- หน่วยที่ 15 ศูนย์ข้อมูลและการสำรองข้อมูล
- หน่วยที่ 16 การตอบสนองต่อเหตุขัดข้อง
- หน่วยที่ 17 การวิเคราะห์ข้อมูลบันทึกกิจกรรม
- หน่วยที่ 18 กระบวนการทดสอบเจาะระบบ
- หน่วยที่ 19 การเจาะระบบและการทดสอบเจาะระบบทางเทคนิค
- หน่วยที่ 20 ความมั่นคงปลอดภัยซอฟต์แวร์และระบบเว็บ
- หน่วยที่ 21 หลักการพื้นฐานด้านนิติคอมพิวเตอร์
- หน่วยที่ 22 หลักฐานดิจิทัล
- หน่วยที่ 23 นิติวิทยาระบบปฏิบัติการวินโดวส์
- หน่วยที่ 24 นิติวิทยาระบบเครือข่าย
- หน่วยที่ 25 อาชญากรรมทางจดหมายอิเล็กทรอนิกส์และนิติคอมพิวเตอร์
- หน่วยที่ 26 การจัดทำรายงานการตรวจพิสูจน์หลักฐาน
- หน่วยที่ 27 การรักษาความปลอดภัยบนคลาวด์ขั้นพื้นฐาน

## 2. หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ระดับผู้เชี่ยวชาญ (ออนไลน์) (Cybersecurity Professional Course)

### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-Learning

### คำอธิบายหลักสูตร

เป็นหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับมืออาชีพที่สอดคล้องกับหลักสูตรประกาศนียบัตรสากลด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ CompTIA Security+ เวอร์ชัน 601 ซึ่งประกอบไปด้วยเนื้อหาที่มีความเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในเชิงลึกยิ่งขึ้นจากหลักสูตรในระดับพื้นฐาน ซึ่งจะนำไปสู่การต่อยอดความชำนาญเฉพาะด้านในหลักสูตรขั้นสูงขึ้นไป

### เงื่อนไขการสมัครเข้าร่วมโครงการ

เป็นผู้ได้รับใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐานจาก สกมช.

### ขั้นตอนการเข้าเรียนด้วยตนเอง

1. เข้าระบบ THNCA e-Learning
2. เลือกหลักสูตรที่ต้องการ แล้วสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

### เกณฑ์การผ่านและได้รับใบประกาศนียบัตรจาก สกมช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ทำข้อสอบวัดความรู้หลังเรียนได้คะแนนไม่น้อยกว่า 60%

### รายวิชาในหลักสูตร (จำนวนรวม 20 ชั่วโมง)

- บทเรียนที่ 1 การเปรียบเทียบบทบาทด้านความปลอดภัยและการควบคุมความปลอดภัย  
(Comparing Security Roles and Security Controls)
- บทเรียนที่ 2 ผู้ประสังคร้ายและข่าวกรองภัยคุกคาม  
(Explaining Threat Actors and Threat Intelligence)

- บทเรียนที่ 3 การประเมินความปลอดภัย (Performing Security Assessments)
- บทเรียนที่ 4 การระบุการโจมตีด้วยวิศวกรรมสังคมและมัลแวร์  
(Identifying Social Engineering and Malware)
- บทเรียนที่ 5 การสรุปแนวคิดการเข้ารหัสขั้นพื้นฐาน (Summarizing Basic Cryptographic Concepts)
- บทเรียนที่ 6 การใช้งานโครงสร้างพื้นฐานกุญแจสาธารณะ  
(Implementing Public Key Infrastructure)
- บทเรียนที่ 7 การใช้งานการควบคุมการพิสูจน์ตัวตน (Implementing Authentication Controls)
- บทเรียนที่ 8 การใช้งานการจัดการบัญชีและตัวตน  
(Implementing Identity and Account Management Controls)
- บทเรียนที่ 9 การออกแบบเครือข่ายที่ปลอดภัย (Implementing Secure Networking Designs)
- บทเรียนที่ 10 การใช้งานอุปกรณ์ความปลอดภัยเครือข่าย  
(Implementing Network Security Appliances)
- บทเรียนที่ 11 การใช้งานโปรโตคอลเครือข่ายที่ปลอดภัย (Implementing Secure Network Protocols)
- บทเรียนที่ 12 การใช้งานโซลูชันความปลอดภัยของโฮสต์ (Implementing Host Security Solutions)
- บทเรียนที่ 13 การใช้งานโซลูชันความปลอดภัยมือถือ (Implementing Secure Mobile Solutions)
- บทเรียนที่ 14 การวิเคราะห์สัญญาณของการโจมตีแอปพลิเคชัน  
(Analyze Indicators of Application Attacks)
- บทเรียนที่ 15 การใช้งานโซลูชันคลาวด์ที่ปลอดภัย (Implementing Secure Cloud Solutions)
- บทเรียนที่ 16 การอธิบายแนวคิดความเป็นส่วนตัวและการป้องกันข้อมูล  
(Explaining Data Privacy and Protection Concepts)
- บทเรียนที่ 17 การตอบสนองต่อเหตุการณ์ (Performing Incident Response)
- บทเรียนที่ 18 นิติวิทยาศาสตร์ดิจิทัล (Explaining Digital Forensic)
- บทเรียนที่ 19 การสรุปแนวคิดการจัดการความเสี่ยง (Summarizing Risk Management Concepts)
- บทเรียนที่ 20 การใช้งานความปลอดภัยไซเบอร์ (Implementing Cybersecurity)
- บทเรียนที่ 21 ความปลอดภัยทางกายภาพ (Explaining Physical Security)
- บทเรียนที่ 22 ทำความเข้าใจแนวคิดความปลอดภัยบนคลาวด์  
(Understanding Cloud Security Concepts)

### 3. หลักสูตรผู้เชี่ยวชาญเฉพาะด้าน นักวิเคราะห์ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Analyst)

#### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-learning

#### คำอธิบายหลักสูตร

เป็นหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับผู้เชี่ยวชาญเฉพาะด้าน ที่เป็นภาษาไทย ซึ่งสอดคล้องกับหลักสูตรประกาศนียบัตรสากลด้านการวิเคราะห์ความมั่นคงปลอดภัยทางไซเบอร์ CompTIA CySA+ เวอร์ชัน CS0-003 ประกอบด้วยเนื้อหาที่ครอบคลุมตั้งแต่การทำความเข้าใจเกี่ยวกับแนวคิดที่สำคัญ การทำความเข้าใจการปรับปรุงกระบวนการในการปฏิบัติการดำเนินการเกี่ยวกับช่องโหว่ การตอบสนองต่อเหตุการณ์ การวิเคราะห์กิจกรรมที่เป็นอันตราย การใช้เครื่องมือที่เกี่ยวข้อง ตลอดจนแนวทางปฏิบัติที่ดีที่สุด ด้านความปลอดภัยของแอปพลิเคชันและการบรรเทาการโจมตีอีกด้วย ซึ่งจะเป็นความรู้ที่สำคัญสำหรับการต่อยอด ความชำนาญด้านความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในการทำงานและการศึกษาเพิ่มเติมในหลักสูตรขั้นสูงอื่น ๆ ต่อไป

#### เงื่อนไขการสมัครเข้าเรียน

เป็นผู้ได้รับใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐานจาก สกมช.

#### ขั้นตอนการเข้าเรียนด้วยตนเอง

1. เข้าระบบ THNCA e-Learning
2. เลือกหลักสูตรที่ต้องการ แล้วสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

#### เกณฑ์การผ่านและได้รับใบประกาศนียบัตรจาก สกมช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ทำข้อสอบวัดความรู้หลังเรียนได้คะแนนไม่น้อยกว่า 60%

## รายวิชาในหลักสูตร (จำนวนรวม 22 ชั่วโมง)

- บทที่ 1 ความเข้าใจเกี่ยวกับการจัดการและการตอบสนองต่อช่องโหว่  
(Understanding Vulnerability Response, Handling, and Management)
  - บทที่ 2 การสำรวจแนวคิดเกี่ยวกับข่าวกรองด้านภัยคุกคามและการติดตามภัยคุกคาม  
(Exploring Threat Intelligence and Threat Hunting Concepts)
  - บทที่ 3 การอธิบายแนวคิดของระบบและสถาปัตยกรรมเครือข่ายที่สำคัญ  
(Explaining Important System and Network Architecture Concepts)
  - บทที่ 4 การทำความเข้าใจการปรับปรุงกระบวนการในการปฏิบัติการด้านความปลอดภัย  
(Understanding Process Improvement in Security Operations)
  - บทที่ 5 การนำวิธีการสแกนช่องโหว่ไปใช้ (Implementing Vulnerability Scanning Methods)
  - บทที่ 6 การวิเคราะห์ช่องโหว่ (Performing Vulnerability Analysis)
  - บทที่ 7 การสื่อสารข้อมูลเกี่ยวกับช่องโหว่ (Communicating Vulnerability Information)
  - บทที่ 8 อธิบายกิจกรรมการตอบสนองต่อเหตุการณ์ (Explaining Incident Response Activities)
  - บทที่ 9 การสาธิตการสื่อสารการตอบสนองต่อเหตุการณ์  
(Demonstrating Incident Response Communication)
  - บทที่ 10 การใช้เครื่องมือเพื่อระบุกิจกรรมที่เป็นอันตราย  
(Applying Tools to Identify Malicious Activity)
  - บทที่ 11 การวิเคราะห์กิจกรรมที่อาจเป็นอันตราย (Analyzing Potentially Malicious Activity)
  - บทที่ 12 การทำความเข้าใจการประเมินช่องโหว่ของแอปพลิเคชัน  
(Understanding Application Vulnerability Assessment)
  - บทที่ 13 การสำรวจเครื่องมือการเขียนสคริปต์และแนวคิดการวิเคราะห์  
(Exploring Scripting Tools and Analysis Concepts)
  - บทที่ 14 การทำความเข้าใจแนวทางปฏิบัติที่ดีที่สุด ด้านความปลอดภัยของแอปพลิเคชันและการบรรเทา  
การโจมตี (Understanding Application Security and Attack Mitigation Best Practices)
- บทเรียนฝึกปฏิบัติหลักสูตรผู้เชี่ยวชาญเฉพาะด้านการวิเคราะห์ความมั่นคงปลอดภัยทางไซเบอร์  
การอบรมตรวจสอบ CompTIA CySA+ Certificate

ผู้ที่เรียนผ่านหลักสูตรนี้แล้ว สามารถศึกษาและทำแบบฝึกหัดเพิ่มเติมผ่านระบบ MOOC เพื่อต่อยอดความรู้และ  
ความเชี่ยวชาญ

#### 4. หลักสูตรผู้เชี่ยวชาญเฉพาะด้าน การทดสอบเจาะระบบ (Penetration Test)

##### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-learning

##### คำอธิบายหลักสูตร

เป็นหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับผู้เชี่ยวชาญเฉพาะด้าน ที่เป็นภาษาไทย ซึ่งสอดคล้องกับหลักสูตรประกาศนียบัตรสากลด้านการวิเคราะห์ความมั่นคงปลอดภัยทางไซเบอร์ CompTIA PenTest+ เวอร์ชัน PTO-002 ประกอบไปด้วยเนื้อหาที่ครอบคลุมตั้งแต่การวางแผนงานด้านการทดสอบเจาะระบบ การเก็บรวบรวมข้อมูลแบบต่าง ๆ การใช้ประโยชน์จากช่องโหว่ส่วนต่าง ๆ ไปจนถึงการเตรียมรายงานและติดตามผลอีกด้วย ซึ่งจะเป็นความรู้ที่สำคัญสำหรับการต่อยอดความชำนาญด้านความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในการทำงานและการศึกษาเพิ่มเติมในหลักสูตรขั้นสูงอื่น ๆ ต่อไป

##### เงื่อนไขการสมัครเข้าเรียน

เป็นผู้ได้รับใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐานจาก สกมช.

##### ขั้นตอนการเข้าเรียนด้วยตนเอง

1. เข้าระบบ THNCA e-Learning
2. เลือกหลักสูตรที่ต้องการ แล้วสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

##### เกณฑ์การผ่านและได้รับใบประกาศนียบัตรจาก สกมช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ทำข้อสอบวัดความรู้หลังเรียนได้คะแนนไม่น้อยกว่า 60%

### รายวิชาในหลักสูตร (จำนวนรวม 28 ชั่วโมง)

- บทที่ 1 การวางแผนงานด้านการทดสอบเจาะระบบ (Engagement Planning)
- บทที่ 2 การเก็บรวบรวมข้อมูล (Reconnaissance)
- บทที่ 3 การเก็บรวบรวมข้อมูลแบบเชิงรุก (แอคทีฟ) (Active Reconnaissance)
- บทที่ 4 การใช้ประโยชน์จากช่องโหว่ (Leveraging Target Information)
- บทที่ 5 การใช้ประโยชน์จากช่องโหว่ขององค์กร (Exploit Organizational Vulnerabilities)
- บทที่ 6 การใช้ประโยชน์จากช่องโหว่บนเครือข่าย (Exploit Network Vulnerabilities)
- บทที่ 7 การใช้ประโยชน์จากช่องโหว่บนแอปพลิเคชัน (Exploiting Application)
- บทที่ 8 การใช้ประโยชน์จากช่องโหว่ของโฮสต์ (Host Exploitation)
- บทที่ 9 การติดตามผล (Engagement Follow-up)
- บทเรียนฝึกปฏิบัติ หลักสูตรผู้เชี่ยวชาญเฉพาะด้าน การทดสอบเจาะระบบ (Penetration Test)
- การอบรมตัวข้อสอบ CompTIA PenTest+ Certificate

ผู้ที่เรียนผ่านหลักสูตรนี้แล้ว สามารถศึกษาและทำแบบฝึกหัดเพิ่มเติมผ่านระบบ MOOC เพื่อต่อยอดความรู้และความเชี่ยวชาญ

## 5. หลักสูตรความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องของระบบควบคุมอุตสาหกรรม

### (OT Security)

#### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-learning

#### คำอธิบายหลักสูตร

เป็นหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับผู้เชี่ยวชาญเฉพาะด้านที่สอดคล้องกับหลักสูตรประกาศนียบัตรสากลด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องของระบบควบคุมอุตสาหกรรม EC-Council ICS/SCADA Cybersecurity ที่เป็นภาษาไทย ซึ่งประกอบไปด้วยเนื้อหาที่ออกแบบมาเป็นพิเศษสำหรับผู้เชี่ยวชาญด้านเทคโนโลยีเชิงปฏิบัติการ ที่เกี่ยวข้องกับการจัดการหรือกำกับโครงสร้างพื้นฐานด้านเทคโนโลยีขององค์กร ผู้รับผิดชอบในการสร้างและรักษาโยบาย แนวปฏิบัติ และขั้นตอนการรักษาความปลอดภัยของข้อมูล หลักสูตรนี้ มุ่งเน้นระบบควบคุมอุตสาหกรรม (ICS) และระบบควบคุมดูแลและการได้มาซึ่งข้อมูล (SCADA) ซึ่งจะช่วยให้เรียนรู้พื้นฐานของการรักษาความปลอดภัยและการปกป้องสถาปัตยกรรมจากการโจมตี ซึ่งจะเป็นความรู้สำคัญสำหรับการเพิ่มพูนความชำนาญด้านความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในการทำงานและการศึกษาเพิ่มเติมในหลักสูตรขั้นสูงอื่นๆ ต่อไป

#### เงื่อนไขการสมัครเข้าเรียน

เป็นผู้ได้รับใบประกาศนียบัตรการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐานจาก สกนช.

#### ขั้นตอนการเข้าเรียนด้วยตนเอง

1. เข้าระบบ THNCA e-Learning
2. เลือกหลักสูตรที่ต้องการ แล้วสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

เกณฑ์การผ่านและได้รับใบประกาศนียบัตรจาก สกนช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ทำข้อสอบวัดความรู้หลังเรียนได้คะแนนไม่น้อยกว่า 60%

### รายวิชาในหลักสูตร (จำนวนรวม 7 ชั่วโมง)

- บทที่ 1 บทนำเกี่ยวกับการป้องกันเครือข่ายระบบควบคุมเชิงอุตสาหกรรมและสกาตา  
(Introduction to ICS/SCADA Network Defense)
- บทที่ 2 โพรโตคอลที่ซีพี/ไอพี 101 (TCP/IP 101)
- บทที่ 3 ความรู้เบื้องต้นเกี่ยวกับการแฮ็ก (Introduction to Hacking)
- บทที่ 4 การจัดการช่องโหว่ (Vulnerability Management)
- บทที่ 5 กฎระเบียบและมาตรฐานด้านความปลอดภัยทางไซเบอร์  
(Standards and Regulations for Cybersecurity)
- บทที่ 6 การรักษาความปลอดภัยเครือข่ายระบบควบคุมเชิงอุตสาหกรรมและสกาตา  
(Securing the ICS/SCADA network)
- บทที่ 7 การเชื่อมต่อแอร์แกป (Bridging the Air Gap)
- บทที่ 8 ระบบตรวจจับการบุกรุก (IDS) และ ระบบป้องกันการบุกรุก (IPS)  
(Introduction to IDS and IPS)

*ผู้ที่เรียนผ่านหลักสูตรนี้แล้ว สามารถศึกษาและทำแบบฝึกหัดเพิ่มเติมผ่านระบบ MOOC เพื่อต่อยอดความรู้และความเชี่ยวชาญ*

## 6. Microsoft AI Skills For All

### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-learning จำนวน 1 ชั่วโมง 43 นาที

### คำอธิบายหลักสูตร

หลักสูตรนี้มุ่งเน้นการพัฒนาทักษะ AI ด้วย Microsoft Copilot และ Generative AI เพื่อเพิ่มประสิทธิภาพการทำงานในยุคดิจิทัล ผู้เรียนจะได้เรียนรู้การสร้างภาพและตัดต่อวิดีโออย่างมืออาชีพด้วย Clipchamp นอกจากนี้ หลักสูตรยังสอนเทคนิคการเล่าเรื่องและการแปลภาษาด้วย Copilot เพื่อการสื่อสารที่มีประสิทธิภาพ พร้อมรู้จักการใช้งาน Generative AI อย่างมีจริยธรรม รวมทั้งผู้เรียนจะได้ฝึกการสร้างบทบาทสมมติให้ AI และปรับแต่งข้อมูลที่ได้ให้เหมาะสมกับการใช้งานจริง รวมถึงใช้ AI ในการวางแผนธุรกิจ เช่น ธุรกิจท่องเที่ยว หลักสูตรนี้เสริมทักษะด้าน AI และช่วยให้ผู้เรียนปรับใช้เทคโนโลยีในสถานการณ์จริง เพิ่มความได้เปรียบในยุคดิจิทัล

### ขั้นตอนการเข้าเรียนด้วยตนเอง (หลักสูตรออนไลน์)

1. ลงทะเบียนเพื่อสมัครเป็นสมาชิกหรือเข้าระบบ THNCA e-Learning ที่ [www.thnca.or.th](http://www.thnca.or.th)
2. เลือกหลักสูตร Microsoft AI Skills For All (ออนไลน์) แล้วทำการสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน จำนวน 10 ข้อ
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน จำนวน 20 ข้อ
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม จำนวน 10 ข้อ
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

### เกณฑ์การผ่านหลักสูตรเพื่อรับประกาศนียบัตรจาก สกมช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ผ่านการทดสอบวัดความรู้หลังเรียนได้คะแนนไม่ต่ำกว่าร้อยละ 60 (ไม่น้อยกว่า 12 คะแนน จากข้อสอบ 20 ข้อ)

### รายวิชาในหลักสูตร (จำนวนรวม 1 ชั่วโมง 10 นาที)

- บทที่ 1 บทนำ Copilot
- บทที่ 2 การสร้างรูปภาพด้วย Microsoft Copilot
- บทที่ 3 การใช้งาน Clipchamp เพื่อตัดต่อวิดีโอ
- บทที่ 4 เทคนิคการเล่าเรื่องและการสร้างข้อมูลตามความต้องการของแต่ละบุคคล
- บทที่ 5 การแปลภาษาด้วย Copilot
- บทที่ 6 Generative AI คืออะไร
- บทที่ 7 การเข้าใช้งาน Microsoft Copilot
- บทที่ 8 คำสั่งพื้นฐานใน Microsoft Copilot
- บทที่ 9 ข้อควรระวังในการใช้ Generative AI
- บทที่ 10 การสร้างบทบาทสมมติให้ Generative AI
- บทที่ 11 การกำหนดรูปแบบของข้อมูลผลลัพธ์
- บทที่ 12 การใช้ Generative AI ในการวางแผนธุรกิจ เช่น ธุรกิจท่องเที่ยว

## 7. Microsoft 365 Copilot

### รูปแบบการเรียนรู้

การเรียนออนไลน์ตามอัธยาศัย ผ่านระบบ e-learning จำนวน 1 ชั่วโมง 10 นาที

### คำอธิบายหลักสูตร

เป็นหลักสูตรพื้นฐานสำหรับผู้สนใจเรียนรู้เกี่ยวกับความสามารถของ Microsoft 365 Copilot ที่สามารถช่วยเพิ่มประสิทธิภาพการทำงานได้อย่างมาก ซึ่งครอบคลุมความรู้ในการใช้ Copilot ของโปรแกรมไมโครซอฟท์ต่างๆ ที่เป็นการช่วยเหลืออัตโนมัติ เช่น ช่วยในการสร้างเอกสาร สเปรดชีต และงานนำเสนอได้อย่างรวดเร็วและง่ายดาย โดยการแนะนำเนื้อหาและรูปแบบที่เหมาะสม สามารถช่วยจัดการอีเมล จัดการปฏิทินของคุณได้อย่างมีประสิทธิภาพ ช่วยสร้างสไลด์ที่น่าสนใจและเป็นมืออาชีพได้อย่างรวดเร็ว รวมทั้งช่วยให้การทำงานร่วมกันในทีมเป็นเรื่องง่ายขึ้น โดยการแนะนำวิธีการแบ่งปันและแก้ไขเอกสารร่วมกัน เป็นต้น

### ขั้นตอนการเข้าเรียนด้วยตนเอง (หลักสูตรออนไลน์)

1. ลงทะเบียนเพื่อสมัครเป็นสมาชิกหรือเข้าระบบ THNCA e-Learning ที่ [www.thnca.or.th](http://www.thnca.or.th)
2. เลือกหลักสูตร Microsoft 365 Copilot (ออนไลน์) แล้วทำการสมัครเรียน
3. ทำแบบทดสอบประเมินความรู้ก่อนเรียน จำนวน 10 ข้อ
4. เข้าเรียนบทเรียนที่ระบบเตรียมไว้ให้จนจบตามหลักสูตร
5. ทำแบบทดสอบวัดความรู้หลังการเรียน จำนวน 20 ข้อ
6. ทำแบบประเมินความพึงพอใจต่อหลักสูตรอบรม จำนวน 10 ข้อ
7. เมื่อผลสอบผ่านเกณฑ์ จะได้รับใบประกาศนียบัตรเป็นผู้สำเร็จการอบรมหลักสูตร

### เกณฑ์การผ่านหลักสูตรเพื่อรับประกาศนียบัตรจาก สกมช.

1. เข้าเรียนตามหลักสูตร e-learning ในระบบ
2. ผ่านการทดสอบวัดความรู้หลังเรียนได้คะแนนไม่ต่ำกว่าร้อยละ 60 (ไม่น้อยกว่า 12 คะแนน จากข้อสอบ 20 ข้อ)

**รายวิชาในหลักสูตร (จำนวนรวม 1 ชั่วโมง 43 นาที)**

- บทที่ 1 Microsoft 365 Copilot ตอนที่ 1
- บทที่ 2 Microsoft 365 Copilot ตอนที่ 2
- บทที่ 3 Copilot introduction & Copilot Lab
- บทที่ 4 Microsoft Word Copilot
- บทที่ 5 Microsoft Teams Copilot
- บทที่ 6 Microsoft Outlook Copilot
- บทที่ 7 Microsoft Excel Copilot
- บทที่ 8 Microsoft 365 PowerPoint
- บทที่ 9 Microsoft Forms Copilot
- บทที่ 10 Microsoft 365 Whiteboard Copilot

# ขั้นตอนการสมัครสมาชิก THNCA e-Learning

ระบบการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์



1. เข้าเว็บไซต์  
www.thnca.or.th  
คลิก Login

2. คลิกปุ่ม  
“สมัครสมาชิก”

3. กรอกข้อมูลผู้ใช้งาน  
(ชื่อ-นามสกุล, อีเมล,  
รหัสผ่าน, ข้อมูลอื่น ๆ  
ตามที่ระบบกำหนด)

4. ตรวจสอบข้อมูล  
และกด  
สมัครสมาชิก

5. อ่านรายละเอียด  
เอกสารแสดงความ  
ยินยอม (Consent)  
จากนั้นกดปุ่ม “ยอมรับ”

6. เปิดอีเมล  
และคลิกลิงก์เพื่อ  
ยืนยันการสมัครสมาชิก

7. ลงทะเบียนใช้งาน  
Two-factor Authentication (2FA)  
โดยใช้แอปพลิเคชัน Authenticator  
ตามขั้นตอนที่ระบบแนะนำ

8. กรอกข้อมูล  
โปรไฟล์ผู้ใช้งาน  
ให้ครบถ้วน จากนั้น  
กดปุ่ม “ดำเนินการต่อ”

9. ยืนยันตัวตนผ่านแอปพลิเคชัน  
ThaID

10. เข้าสู่ระบบและ  
เริ่มเรียนได้ทันที

**หมายเหตุ:** เพื่อให้สามารถใช้งานระบบ THNCA e-Learning และ NCSA MOOC  
ร่วมกันได้อย่างสมบูรณ์ กรุณาใช้อีเมลเดียวกันในการสมัครทั้งสองระบบ

## ระบบ NCSA MOOC

MOOC เป็นแพลตฟอร์มเพื่อการเรียนรู้ด้าน Cybersecurity (Cybersecurity Practical Training Platform) ที่ถูกสร้างขึ้นเพื่อให้ทุกคนสามารถเข้าถึงและเรียนรู้เกี่ยวกับ Cybersecurity ได้อย่างเข้าใจง่ายและสนุก

ไปกับการเรียนรู้ โดยเน้นการเรียนรู้ในรูปแบบทฤษฎีและปฏิบัติ โดยให้ผู้ใช้งานค้นหาช่องโหว่ตามสถานการณ์หรือเหตุการณ์ที่สร้างขึ้น รวมทั้งได้ทดลองเจาะระบบด้วยตนเอง เพื่อให้ผู้ใช้งานได้รับประสบการณ์ที่ใกล้เคียงกับชีวิตจริงมากที่สุด ด้วยโจทย์และเนื้อหาขั้นสูงที่เหมาะสมกับบุคคลากรทางด้าน Cyber Security ที่ต้องการฝึกปฎิบัติมือให้มีความชำนาญมากขึ้น โดย MOOC Platform มีคุณสมบัติดังต่อไปนี้

- ระบบแล็บที่เต็มไปด้วยเนื้อหาเชิงปฏิบัติพร้อมกับเครื่องจำลองที่ถูกสร้างขึ้นสำหรับผู้ใช้งานแต่ละคน ให้สามารถใช้งานได้อย่างอิสระจากกัน การกระทำใด ๆ ภายในเครื่องจำลองของผู้ใช้งานนั้น ๆ จะไม่ส่งผลกระทบต่อเครื่องจำลองของผู้ใช้งานอื่น ๆ

- เนื้อหาที่อยู่ในภาษาไทยที่ถูกปรับมาให้เหมาะสมกับผู้เรียนรู้จากประสบการณ์ของผู้ออกแบบเนื้อหาใน MOOC นั้นประกอบด้วยเนื้อหาเกี่ยวกับ Cybersecurity 3 หัวข้อใหญ่ด้วยกัน

### 1. Basic Cybersecurity Lab – เรียนรู้เกี่ยวกับความรู้ทั่วไปของ Cybersecurity ดังนี้

Chapter 1 - Basic Cybersecurity Knowledge เรียนรู้เกี่ยวกับความรู้พื้นฐานเบื้องต้น

Chapter 2 - Basic Network เรียนรู้และทำความเข้าใจเนื้อหา network ทั่วไป

Chapter 3 - Wireless Network เรียนรู้เกี่ยวกับ Wireless Network

Chapter 4 - Cryptography เรียนรู้เกี่ยวกับความเข้าใจ Cryptography เบื้องต้น

### 2. Penetration Test – เรียนรู้เกี่ยวกับเนื้อหาที่เหมาะสมสำหรับ Penetration Test ดังนี้

Chapter 1 - Penetration Test เรียนรู้เกี่ยวกับ Penetration Test

Chapter 2 - Scanning เรียนรู้เกี่ยวกับ Scanning แบบต่าง ๆ

Chapter 3 - Linux Knowledge เรียนรู้เกี่ยวกับการใช้งาน Linux

Chapter 4 - Netcat เรียนรู้การใช้งาน Netcat

Chapter 5 - Cryptography Knowledge เรียนรู้เกี่ยวกับความเข้าใจ Cryptography เบื้องต้น

Chapter 6 - Network Security เรียนรู้เกี่ยวกับ network security

Chapter 7 - Web Security เรียนรู้เกี่ยวกับ web application security

Chapter 8 - Post Exploitation เรียนรู้เกี่ยวกับการโจมตีหลัง Exploit สำเร็จ

Chapter 9 - Reporting เรียนรู้เกี่ยวกับการเขียน Penetration test report

### 3. SOC (Security Operation Center) - Tier1 – เรียนรู้เนื้อหาที่เกี่ยวกับ SOC Level 1 ดังนี้

Chapter 1 - Basic Cybersecurity Knowledge เรียนรู้เกี่ยวกับความรู้พื้นฐานของ security

Chapter 2 - Incident Response Process เรียนรู้เกี่ยวกับ process ของ incident response

Chapter 2 - Linux Knowledge เรียนรู้เกี่ยวกับเนื้อหา Linux

Chapter 3 - OWASP Top10 2017 เรียนรู้เกี่ยวกับ OWASP Top10 2017

Chapter 4 - Network Analysis เรียนรู้เกี่ยวกับการวิเคราะห์ network packet

ผู้ที่ผ่านการเรียนในระบบ THNCA e-Learning มาแล้ว สามารถต่อยอดการเรียนรู้ได้ที่

<https://play.mooc.ncsa.or.th/>

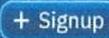
# ขั้นตอนการสมัครสมาชิก NCSA MOOC

1



เข้าเว็บไซต์  
<https://mooc.ncsa.or.th>

2



คลิก Signup

3



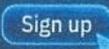
กรอกข้อมูลผู้ใช้งาน  
(แนะนำให้ใช้อีเมลเดียวกับ THNCA e-Learning)

4



เลือก I agree to Consent  
Agreement Form

5



กด Sign up

6



ยืนยันตัวตนผ่านอีเมล  
(เปิดใช้งานบัญชีผู้ใช้)

7



กรอกข้อมูลโปรไฟล์  
และกด Save

8



เข้าสู่ระบบ NCSA MOOC

9



ลงทะเบียน Two-factor Authentication (2FA)  
Scan QR Code ผ่าน Authenticator และกดยืนยัน

10



เลือกหลักสูตร  
และเริ่มฝึกปฏิบัติได้ทันที

หมายเหตุ: เพื่อให้สามารถใช้งานระบบ THNCA e-Learning และ NCSA MOOC  
ร่วมกันได้อย่างสมบูรณ์ กรุณาใช้อีเมลเดียวกันในการสมัครทั้งสองระบบ

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ  
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ