



NT **AIoT**

NT x TESA
COLLABORATION

NT x TESA · OFFICIAL COLLABORATION

2-DAY INTENSIVE PROGRAM · หลักสูตรฉบับ NT

TESA **AIoT** CYBERSECURITY GUIDELINE READINESS WORKSHOP

Understanding Future AIoT Cybersecurity Requirements for Network Operators

เตรียมความพร้อมบุคลากร NT ให้เข้าใจแนวทาง AIoT Cybersecurity Guideline ของ สกมช. (NCSA) และประยุกต์ใช้กับโครงสร้างพื้นฐานและบริการขององค์กรได้อย่างมีประสิทธิภาพ — หลักสูตรเชิงลึก 2 วัน พร้อม Hands-on Lab

• • **FREE** FOR NT • **WORKSHOP + HANDS-ON LAB** • **09:00-16:30** · ภาษาไทย

**TELECOM
INFRASTRUCTURE**

โครงสร้างพื้นฐาน
โทรคมนาคมของ NT

**AIOT
CONVERGENCE**

อุปกรณ์ AIoT เชื่อมต่อ
จำนวนมหาศาล

**CYBER
RESILIENCE**

ลดความเสี่ยงและภัย
คุกคามไซเบอร์

NCSA READINESS

พร้อมรับแนวทาง
สกมช. ในอนาคต

ทำไมบุคลากร NT จึงควรเตรียมความพร้อม

โครงข่ายของ NT กำลังเชื่อมต่ออุปกรณ์ AIoT มากขึ้นทุกวัน การเตรียมพร้อมด้านความมั่นคงปลอดภัยตั้งแต่วันนี้จึงเป็นการลงทุนเชิงกลยุทธ์

01 Network Operator ที่ต้องรองรับการมาของ AIoT จำนวนมหาศาล
โครงสร้างพื้นฐานของ NT เชื่อมต่ออุปกรณ์ AIoT เพิ่มขึ้นต่อเนื่อง

02 ข้อกำหนดด้าน Cybersecurity ของ สกมช. ที่ต้องคำนึงในอนาคต
เข้าใจทิศทางการกำกับดูแลระดับชาติตั้งแต่เนิ่น ๆ

03 เตรียมพร้อมต่อความเสี่ยงจากภัยคุกคามไซเบอร์
ปกป้องบริการและข้อมูลสำคัญ ลดความเสี่ยงเชิงปฏิบัติการ

04 เสริมสร้างศักยภาพบุคลากรให้พร้อมรับเทคโนโลยีและภัยคุกคามใหม่
People readiness คือการลงทุนเชิงกลยุทธ์ระยะยาว

— PROGRAM AGENDA

กำหนดการอบรม 2 วัน

จากความเข้าใจภัยคุกคามและทิศทางของ สกมช. สู่มาตรการควบคุมเชิงปฏิบัติที่นำไปใช้ได้จริง

DAY 1
Understanding AIoT Cybersecurity

FOCUS: เข้าใจภัยคุกคาม ทิศทาง สกมช. และการประเมินความเสี่ยงของโครงสร้างพื้นฐาน

- | | |
|---|--|
| 01 AIoT Threat Landscape for Network Operators | เข้าใจภัยคุกคามที่เกิดขึ้นจริงในปัจจุบัน |
| 02 NCSA Direction & AIoT Cybersecurity Guideline | เข้าใจทิศทางระดับชาติของ สกมช. ในอนาคต |
| 03 Critical Information Infrastructure Protection | เข้าใจการปกป้องโครงสร้างพื้นฐานสำคัญ |
| 04 AIoT Risk Assessment & Management | เข้าใจวิธีประเมินและบริหารความเสี่ยง |
| 05 Cyber Drill Case Studies, Policy & Compliance | เข้าใจความรับผิดชอบด้านการกำกับดูแล |

DAY 2
Practical Security Controls

FOCUS: ลงมือกับมาตรการควบคุมจริง ตั้งแต่การมองเห็นสินทรัพย์ถึงการตอบสนองเหตุ

- | | |
|--|---|
| 01 Asset Visibility & Inventory for AIoT | รู้ว่ามีสินทรัพย์อะไรในระบบบ้าง |
| 02 Device Identity & PKI Fundamentals | เข้าใจการสร้างความน่าเชื่อถือของอุปกรณ์ |
| 03 Secure Connectivity & Network Segmentation | ลดพื้นที่การโจมตีด้วยการแบ่งเครือข่าย |
| 04 Threat Detection, Monitoring & Incident Response | ตรวจจับและตอบสนองต่อภัยคุกคาม |
| 05 Case Studies & Best Practices | เรียนรู้จากกรณีศึกษาและตัวอย่างจริง |

— DESIGNED FOR EVERY ROLE

เนื้อหาเดียวที่ตอบโจทย์ทั้งองค์กร

ออกแบบให้ผู้บริหาร ผู้จัดการ และวิศวกรของ NT เรียนร่วมกันได้ โดยแต่ละบทบาทได้สิ่งที่ตรงกับงาน

EXECUTIVES & LEADERS ผู้บริหารและผู้นำ	MANAGERS & TEAM LEADERS ผู้จัดการและหัวหน้าทีม	ENGINEERS & OPERATIONS วิศวกรและทีมปฏิบัติการ
VP · SVP · Director · Department Head	Team Leader · Project Manager · Operations Manager	Network · Infrastructure · Operations · Security
- เข้าใจผลกระทบเชิงธุรกิจ - เข้าใจความรับผิดชอบด้านการกำกับดูแล - เตรียมทิศทางเชิงกลยุทธ์	- แปลงนโยบายสู่การปฏิบัติ - บริหารโครงการด้านความมั่นคงปลอดภัย - ประเมินความเสี่ยงเชิงปฏิบัติการ	- เข้าใจมาตรการควบคุมเชิงเทคนิค - นำแนวคิดไปประยุกต์ใช้จริง - เพิ่มความมั่นใจในการทำงาน
ได้รับ: เข้าใจทิศทาง Cybersecurity และผลกระทบต่อองค์กร	ได้รับ: แปลงนโยบายเป็นแผนการดำเนินงานที่ทำได้จริง	ได้รับ: เข้าใจมาตรการความมั่นคงปลอดภัย AIoT เชิงปฏิบัติ

— WHAT YOU WILL GET

สิ่งที่จะได้รับจากหลักสูตร

NCSA-ALIGNED KNOWLEDGE องค์ความรู้ที่สอดคล้องกับทิศทางของ สกมช.	PRACTICAL GUIDANCE FOR NT แนวทางปฏิบัติที่นำไปใช้กับ NT ได้จริง	AIoT RISK MITIGATION แนวคิดลดความเสี่ยง AIoT ที่ลงมือทำได้	TESA CERTIFICATE ใบรับรองการเข้าร่วมจาก TESA
---	---	--	--

— REGISTER NOW

สมัครเข้าร่วมอบรม

ผู้อบรม NT ไม่มีค่าใช้จ่ายใด ๆ (มูลค่ารวม 20,000 บาท/ท่าน) สนับสนุนเต็มจำนวนโดย TESA

 สแกนเพื่อสมัครเข้าร่วมอบรม REGISTER NOW	รายละเอียดหลักสูตร DURATION 2 วัน FORMAT Workshop + Hands-on Lab TARGET GROUP ผู้บริหาร · ผู้จัดการ · วิศวกร · ทีมปฏิบัติการ NT	TIME 09:00 - 16:30 LANGUAGE ภาษาไทย ค่าอบรม ฟรีสำหรับบุคลากร NT
	☎ 085-495-4294 ✉ contact@tesa.or.th 🌐 www.tesa.or.th	