



TESA AIoT

FOR SYSTEM
INTEGRATORS

TESA · FOR SYSTEM INTEGRATORS

2-DAY INTENSIVE PROGRAM · หลักสูตรฉบับ SI

TESA AIoT CYBERSECURITY GUIDELINE READINESS WORKSHOP

Turn NCSA-Aligned Security into a Competitive Advantage for System Integrators

เตรียมความพร้อมทีมของ System Integrator (เช่น PointIT) ให้ออกแบบ ส่งมอบ และดูแลโซลูชัน AIoT ที่ปลอดภัยตามแนวทางของ สกมช. (NCSA) — หลักสูตรเชิงลึก 2 วัน พร้อม Hands-on Lab (lab 80%)

💡 จุดขาย: เปลี่ยน **compliance** ให้เป็นรายได้ใหม่ และข้อได้เปรียบในการแข่งขันงาน

● ● **FREE** FOR SI PARTNERS ● **WORKSHOP + HANDS-ON LAB** ● **09:00-17:00** · ภาษาไทย

**SOLUTION
DELIVERY AT
SCALE**

ส่งมอบโซลูชัน AIoT
หลากหลายอุตสาหกรรม

**AIOT
CONVERGENCE**

อุปกรณ์เชื่อมต่อจำนวน
มหาศาลทุกโครงการ

**SECURE BY
DESIGN**

ฝังความปลอดภัยในทุก
งานที่ส่งมอบ

NCSA READINESS

พร้อมตอบแนวทาง
สกมช. ที่ลูกค้าร้องขอ

ทำไม SI จึงควรเตรียมความพร้อมตั้งแต่วันนี้

ความปลอดภัยกำลังกลายเป็นเงื่อนไขการประมูลและโอกาสสร้างรายได้ใหม่ — SI ที่พร้อมก่อนย่อมได้เปรียบทั้งการชนะงานและการตั้งราคา

01

ลูกค้าเริ่มกำหนดให้โซลูชันต้องสอดคล้องแนวทาง สกมช.
Compliance กำลังกลายเป็นข้อกำหนดใน TOR — พร้อมก่อนได้เปรียบตอนประมูล

02

เพิ่มบริการใหม่ด้านความปลอดภัยและ compliance
เปิดแหล่งรายได้และมาร์จิ้นใหม่จากบริการ value-added

03

สร้างความแตกต่างจากคู่แข่งด้วย Secure-by-Design
ส่งมอบโซลูชัน AIoT ที่ปลอดภัยตั้งแต่การออกแบบ ปิดดีลง่ายกว่า

04

ลดความเสี่ยงและความรับผิดชอบที่ส่งมอบ
due diligence และหลักฐานที่ส่งมอบช่วยจำกัดความรับผิด พร้อมยกระดับทักษะทีม

— PROGRAM AGENDA · โมดูล M0-M6

กำหนดการอบรม 2 วัน

จาก Policy & Business Readiness (วันแรก) สู่ Hands-on Delivery Assurance (วันสอง) — ทุกโมดูลจบด้วยหลักฐาน/เอกสารที่นำไปใช้กับลูกค้าได้จริง

DAY 1 Policy, Governance & Business Readiness	DAY 2 Hands-on Delivery Assurance
FOCUS: เข้าใจกติกา จัดตำแหน่งความรับผิด และเปลี่ยน compliance เป็นข้อได้เปรียบทางธุรกิจ	FOCUS: ตรวจสอบและรับประกันคุณภาพระบบที่ส่งมอบ พร้อมหลักฐานให้ลูกค้า (lab 80%)
01 Market & Threat Landscape for SI ภูมิทัศน์ตลาดและภัยคุกคาม AIoT (เคส Mirai)	01 Lab Setup & Solution Architecture Mapping ตั้ง lab + วาดสถาปัตยกรรมและ data flow ของระบบ
02 Law & SI Liability in the Supply Chain พ.ร.บ. ไซเบอร์ฯ · คอมพิวเตอร์ฯ · PDPA และความรับผิด	02 Acceptance Testing: Attack Surface ตรวจสอบพื้นผิวการโจมตี (port scan + hardening)
03 Frameworks & International Standards กรอบ 6 ประการ · ETSI 303 645 · ISO 27400 · IEC 62443	03 Verify Authentication & Password Hardening ตรวจสอบการยืนยันตัวตน/รหัสผ่านของอุปกรณ์
04 4-Level Model as Procurement Spec & Sales Tool ใช้ 4 ระดับเป็นสเปกจัดหาและเครื่องมือขาย	04 Verify Secure Communication & PDPA ตรวจสอบการเข้ารหัส TLS และ data flow ตาม PDPA
05 Role-Based Deep Dive (Bid · Architect · Delivery) เจาะลึกตามบทบาทธุรกิจในองค์กร SI	05 Supply Chain Assurance: SBOM & Vendor Verify สร้าง Solution SBOM + เทียบ CVE + ตรวจสอบ vendor
06 Business Cyber Drill: Delivered System as Botnet ซ้อมรับมือเมื่อระบบที่ส่งมอบถูกยึดเป็น botnet	06 Pre-delivery Security Assessment (VA / Fuzz) ประเมินความปลอดภัยก่อนส่งมอบ ระดับ 3-4
07 Company Compliance Roadmap วางแผนยกระดับความพร้อมของบริษัท	07 Handover & Compliance Evidence Pack จัดทำชุดหลักฐานส่งมอบให้ลูกค้า

โมเดล 4 ระดับ = เครื่องมือเชิงพาณิชย์

เลือกระดับให้ตรง “ความเสี่ยง × งบของลูกค้า” — ใช้เป็นสเปกจัดหา เกณฑ์คัด vendor และเครื่องมือขายไปพร้อมกัน

LEVEL 1 Baseline	LEVEL 2 Int'l Standard	LEVEL 3 Lifecycle / Supply Chain	LEVEL 4 Penetration Test
งานทั่วไป งบจำกัด — รหัสผ่าน · VDP · อัปเดต	มีข้อมูลส่วนบุคคล — TLS/WPA3 · secure parameters	ภาครัฐ / องค์กรใหญ่ — SBOM · CVSS · secure engineering	ความเสี่ยงสูง / CII — pentest & fuzz testing
मुख्य: ราคาเข้าถึงได้	मुख्य: จุดขายด้าน PDPA	मुख्य: value-added เพิ่มมาร์จิ้น	मुख्य: งานพรีเมียม ราคาสูงกว่า

อ้างอิงแนวทางความมั่นคงปลอดภัย AIoT ของ **สภมช.** — การกำหนด “ระดับขั้นต่ำที่ vendor ต้องผ่าน” คือ **procurement gate** ที่ปกป้องบริษัท และการเสนอระดับที่สูงขึ้นคือการขายที่ตั้งราคาได้

ตอบโจทย์ทุกบทบาทในองค์กร SI

ผู้บริหาร/ทีมขาย สถาปนิกโซลูชัน และวิศวกรเรียนร่วมกันได้ โดยแต่ละบทบาทได้เครื่องมือที่นำไปใช้กับงานจริง

EXECUTIVES & SALES LEADERS ผู้บริหารและทีมขาย	SOLUTION ARCHITECTS & PM สถาปนิกโซลูชันและ PM	ENGINEERS & IMPLEMENTATION วิศวกรและทีมติดตั้ง
Managing Director · Business/Sales Director · Account Manager	Solution Architect · Presales · Project Manager	Network · Security · Field · Support Engineers
- เห็นโอกาสรายได้ใหม่จากบริการความปลอดภัย - วางกลยุทธ์งานแบบ security-driven - สื่อสารคุณค่าด้าน compliance ให้ลูกค้า ได้รับ: มองเห็นโอกาสธุรกิจและวางตำแหน่งบริการความปลอดภัย	- ออกแบบโซลูชันแบบ secure-by-design - ใส่ security ลงในข้อเสนอและ BOQ - บริหารการส่งมอบตามมาตรฐาน ได้รับ: ออกแบบและเสนอโซลูชัน AIoT ที่ปลอดภัยและตอบ compliance	- ติดตั้งมาตรการควบคุมจริง - ตั้งค่าและดูแลระบบให้ปลอดภัย - ตอบสนองเหตุการณ์ให้ลูกค้า ได้รับ: ลงมือติดตั้งและดูแลมาตรการความปลอดภัย AIoT ให้ลูกค้า

สินทรัพย์ที่บริษัทได้กลับไป

ทุกอย่างเป็นแม่แบบ/เอกสารที่นำกลับไปใช้ซ้ำได้ทันทีในโครงการจริง — เปลี่ยนการอบรมให้เป็นสินทรัพย์ของบริษัท

VENDOR ASSESSMENT CHECKLIST

เกณฑ์คัดอุปกรณ์เข้า
โครงการอย่างมืออาชีพ

TOR / PROPOSAL SPEC LANGUAGE

ข้อความสเปกอ้างอิง
แนวทาง สกมช. สำหรับข้อ
เสนอ/สัญญา

COMPLIANCE EVIDENCE PACK + SBOM

แม่แบบส่งมอบ + Solution
SBOM ที่ใช้ซ้ำได้

COMPANY COMPLIANCE ROADMAP

แผนยกระดับความพร้อม
ของบริษัทที่นำไปทำต่อได้

— REGISTER NOW

สมัครเข้าร่วมอบรม

พาร์ทเนอร์ SI ไม่มีค่าใช้จ่ายใด ๆ (มูลค่ารวม 20,000 บาท/ท่าน) สนับสนุนเต็มจำนวนโดย TESA



สแกนเพื่อสมัครเข้าร่วมอบรม

REGISTER NOW

รายละเอียดหลักสูตร

DURATION

2 วัน

TIME

09:00 - 17:00

FORMAT

Workshop + Hands-on
Lab (lab 80%)

LANGUAGE

ภาษาไทย

TARGET GROUP

ผู้บริหาร · ทีมขาย ·
Architect · PM · วิศวกร
ของ SI

ค่าอบรม

ฟรีสำหรับพาร์ทเนอร์ SI

☎ 085-495-4294 ✉ contact@tesa.or.th 🌐 www.tesa.or.th