ภาคปฏิบัติ
CDIC2025 CYBERSECURITY WORKSHOPS
ภาคปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 38 หัวข้อ

DIGITAL AND CYBERSECURITY MANAGEMENT WORKSHOPS
หลักสูตรด้านการบริหารจัดการเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์

MW-01 — 1 DAY
Preparedness Guide for Cybersecurity Risk Assessment in Action (Alignment with Cybersecurity Compliance, Standards & Best Practices)

หลักสูตรแนวทางการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สอดคล้องตามกฎหมายลำดับรองของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

- ภาพรวมการรักษาความมั่นคงปลอดภัยไซเบอร์และข้อกำหนดแนวทางการประเมินความเสี่ยง
- กรอบการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- ข้อกำหนดอ้างอิงตามมาตรฐานและแนวปฏิบัติสำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- กรอบการดำเนินงานและกระบวนการสำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Management Framework and Process)
- การระบุปัจจัยเสี่ยง (Risk identification)
- การวิเคราะห์ความเสี่ยง (Risk analysis)
- การประเมินผลความเสี่ยง (Risk evaluation)
- การจัดการแผนตอบสนองความเสี่ยง (Risk treatment plan and Risk response)
- การติดตามผลและรายงานผล (Risk monitoring and reporting)

MW-02 — 1 DAY
Intensive One-Day Course in implementing New Version PCI DSS (Version 4.0.1)

หลักสูตรรวบรัดเพื่อดำเนินการตามข้อกำหนดเวอร์ชันใหม่ของมาตรฐานความมั่นคงปลอดภัยสำหรับบัตรเครดิต

- ภาพรวมเกี่ยวกับมาตรฐาน PCI DSS
- ระดับความสอดคล้องของ PCI DSS สำหรับองค์กรแต่ละประเภท
- เทคโนโลยีที่เกี่ยวข้องกับการดำเนินการให้สอดคล้องกับมาตรฐาน
- แนวทางการกำหนดขอบเขตของ PCI DSS
- ข้อกำหนดของ PCI DSS
- กำหนดการสำหรับการตรวจรับรอง PCI DSS เวอร์ชัน 4.0.1
- การเปลี่ยนแปลงระหว่าง PCI DSS เวอร์ชัน 4.0 และ เวอร์ชัน 4.0.1
- การใช้มาตรการควบคุมทดแทน และมาตรการควบคุมที่ปรับแต่ง เพื่อให้การดำเนินงานสอดคล้องกับมาตรฐาน PCI DSS
- การเตรียมการเพื่อ Implement controls ตามข้อกำหนดของ PCI DSS เวอร์ชัน 4.0.1 อย่างเต็มรูปแบบ

MW-03 — 1 DAY
Framework and Best Practices for Implementing Data Governance and Data Management in Organization for Comply with Related Law and Regulations

หลักสูตรแนวทางการบริหารจัดการข้อมูล และแนวปฏิบัติที่ดีสำหรับการบริหารจัดการข้อมูลสำหรับการพัฒนาธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลภายในองค์กร

- ความแตกต่างระหว่างธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล
- ภาพรวมของกฎหมาย ระเบียบ ข้อบังคับเกี่ยวกับภรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล
- ภาพรวมของแนวทางและแนวปฏิบัติที่ดีสำหรับการบริหารจัดการข้อมูลที่นำมาใช้ในการดำเนินการ
- แนวทางการบริหารจัดการข้อมูลในองค์กร

MW-04 — 2 DAYS
IT General Controls Audit (ITGC)

หลักสูตรการตรวจสอบเรื่องการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ

- หลักการและเหตุผล
- ความรู้พื้นฐานด้านคอมพิวเตอร์ที่จำเป็นสำหรับการตรวจสอบ ITGC
- แนวทางการตรวจสอบ ITGC
- นโยบายด้านการรักษาความปลอดภัยของระบบสารสนเทศ (IT Security Policy)
- โครงสร้างองค์กรและตำแหน่งงานของฝ่าย IT (IT Organization)
- การบริหารจัดการผู้ให้บริการภายนอกทางด้านเทคโนโลยีสารสนเทศ (IT Outsource Management)
- การพัฒนา จัดหาและบำรุงรักษาระบบสารสนเทศ (IT Change Management)
- การรักษาความปลอดภัยทางกายภาพ และมาตรการควบคุมสภาพแวดล้อม (Physical Access and Environmental Controls)
- การควบคุมการเข้าถึงระบบและข้อมูล (Logical Access Controls)
- การสำรองข้อมูล การกู้ข้อมูล การจัดลำดับงานและการจัดการกับปัญหา (IT Operation Controls)
- แผนรองรับสถานการณ์ฉุกเฉินทางด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan)
- Workshop (Case Study)

MW-05 — 1 DAY
Implementing Cybersecurity Control Baseline to comply with Cybersecurity Act

หลักสูตรการจัดทำมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์

- ทำความเข้าใจกฎหมายลำดับรองที่เกี่ยวข้องกับมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
- การจัดระดับผลกระทบของข้อมูลหรือสารสนเทศให้สอดคล้องกับกฎหมายลำดับรอง
- การประยุกต์ใช้แนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ

MW-06 — 1 DAY
Preparedness Guide for Organizational Resilience and Business Continuity in Action (Alignment with Standards and Best Practices)

หลักสูตรการพัฒนาและดำเนินการเกี่ยวกับความยืดหยุ่นขององค์กรและความต่อเนื่องทางธุรกิจตามมาตรฐานและแนวทางปฏิบัติที่ดี

- ภาพรวมทิศทางและแนวโน้มภัยคุกคาม ณ ปัจจุบัน
- กรอบแนวคิดการบริหารความต่อเนื่องทางธุรกิจและความยืดหยุ่นขององค์กรสำหรับรับมือกับสถานการณ์ต่าง ๆ ที่เกิดขึ้นกับองค์กร
- แนวทางการจัดทำแผนตอบสนองต่ออุบัติการณ์ที่ไม่คาดคิด
- แนวทางการจัดทำแผนความต่อเนื่องทางธุรกิจ
- แนวทางการฝึกซ้อมแผนตอบสนองต่ออุบัติการณ์และแผนความต่อเนื่องทางธุรกิจ

MW-07 — 1 DAY
Key Actions for Critical Service and Critical Information Infrastructure

หลักสูตรแนวปฏิบัติสำคัญที่ต้องดำเนินการสำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ ตามกฎหมายลำดับรองของกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์

- สาระสำคัญและภาพรวมการดำเนินการตามกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์
- สาระสำคัญและภาพรวมการดำเนินการสำหรับประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- สาระสำคัญและภาพรวมการดำเนินการสำหรับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- สาระสำคัญและภาพรวมการดำเนินการสำหรับภารกิจหรือการให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- สาระสำคัญและภาพรวมการดำเนินการแนวปฏิบัติพื้นฐาน (Security baseline) ตามลักษณะภัยคุกคามทางไซเบอร์ในแต่ละระดับ
- แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

www.cdicconference.com

AI MANAGEMENT SYSTEM & AI GUIDELINES FOR IMPLEMENTATION WORKSHOPS

หลักสูตรระบบบริหารจัดการ AI และแนวทางการประยุกต์ใช้งานอย่างเป็นรูปธรรม

AW-01 | 1 DAY | Implementing AI Policy to Support Business Operation Effectively

หลักสูตรแนวทางการจัดทำนโยบายการใช้งาน AI มาช่วยสนับสนุนการดำเนินงานทางธุรกิจอย่างเหมาะสม

- ภาพรวมมาตรฐานและแนวปฏิบัติที่ดีเกี่ยวกับการควบคุมการใช้งาน AI
- หลักการสำหรับควบคุมการใช้งาน AI
- ความเสี่ยงจากการใช้เทคโนโลยี AI ที่ควรพิจารณา และแนวทางควบคุมความเสี่ยง
- ภาพรวมของกฎหมาย ระเบียบ ข้อบังคับเกี่ยวกับการใช้งาน AI
- แนวทางการจัดทำนโยบาย AI

AW-02 | 1 DAY | Implementing AI System Impact Assessment and Risk Assessment for Artifitial Intellgence Management System

หลักสูตรการประเมินผลกระทบ และการประเมินความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน

- หลักการพื้นฐานของปัญญาประดิษฐ์
- มาตรฐานที่เกี่ยวข้องกับการประเมินผลกระทบ และการประเมินความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน
- แนวทางการบริหารความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน
- ความแตกต่างระหว่างการประเมินความเสี่ยง และการประเมินผลกระทบสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน และความเชื่อมโยงกับการประเมินผลกระทบอื่นๆ เช่นการทำ DPIA
- หลักการ ขั้นตอน และแนวทางดำเนินการ สำหรับการประเมินผลกระทบสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน
- กรณีศึกษาสำหรับการประเมินผลกระทบ และการประเมินความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน

AW-03 | 1 DAY | Implementing Artificial Intelligence Myanagement System based on ISO/IEC 42001:2023

หลักสูตรการพัฒนาระบบบริหารจัดการเทคโนโลยีปัญญาประดิษฐ์ให้สอดคล้องกับมาตรฐานสากล ISO/IEC 42001:2023

- ภาพรวมของเทคโนโลยีปัญญาประดิษฐ์
- มาตรฐานที่เกี่ยวข้องกับระบบบริหารจัดการเทคโนโลยีปัญญาประดิษฐ์
- รายละเอียดเกี่ยวกับการตรวจรับรองมาตรฐาน
- ข้อกำหนดหลักของมาตรฐาน ISO/IEC 42001
- มาตรการควบคุมสำหรับการบริหารจัดการเทคโนโลยีปัญญาประดิษฐ์ (AI Systems Controls)

MW-08 | 1 DAY | Leading Cybersecurity Governance: Transformative Strategies for Cyber Resilience Management Excellence

หลักสูตรการเป็นผู้นำด้านการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์และการเปลี่ยนผ่านสู่ความยั่งยืนทางไซเบอร์ขององค์กร

- Understanding Cybersecurity Governance: A Strategic Framework for Protecting Your Organization
- A Step-by-Step Guide to Building Robust Cybersecurity Governance
- Fostering a Culture of Cyber Resilience in Your Organization
- Defining Clear Roles and Responsibilities in Cybersecurity Governance
- Adopting a Holistic Approach to Cyber Risk Management
- From Vision to Reality: Translating Cybersecurity Strategy into Action
- Developing a Cybersecurity Program: Turning Strategy into Actionable Plans
- Measuring Cyber Resilience: The Role of a Cyber Resilience Dashboard
- Implement Cyber Resilience Platform
- Navigating Cybersecurity Transformation: Building and Following a Strategic Roadmap

AW-04 | 1 DAY | Generative AI for Cyber Investigation

หลักสูตรการใช้ Generative AI ในงาน Cyber Investigation

- ทำความรู้จักกับ Generative AI ในภาพรวม
- การเขียน Prompt สำหรับสั่งงาน Generative AI
- ทำความรู้จักกับ Generative AI ประเภทต่างๆ
- การประยุกต์ใช้ Generative AI ในงาน Cyber Investigation
- Use Case การใช้งาน Generative AI ที่น่าสนใจ
- ข้อจำกัด (Limitations) ของการใช้งาน Generative AI
- การประเมินความเสี่ยงของการนำ Generative AI มาประยุกต์ใช้ในองค์กร
- แนวโน้ม Generative AI ในอนาคต
- แหล่งข้อมูลสำหรับศึกษาต่อของ Generative AI
- Workshop Generative AI for Cyber Investigation
- แถม: การสืบค้นข้อมูลจากแหล่งข้อมูลเปิด(OSINT) สำหรับงาน Cyber Investigation

AW-05 | 1 DAY | Generative AI for Security Expert

หลักสูตรการใช้งาน Generative AI สำหรับ Security Expert

- AI Model for cyber security
- Prompt engineering
- Enhance detection engineering
- Improving log analytics
- Enhance network security monitoring

AW-06 | 1 DAY | Integrating Cybersecurity, AI & Quantum Risk into Enterprise Risk Management (ERM)

หลักสูตรการผสานความมั่นคงปลอดภัยไซเบอร์, AI และความเสี่ยงด้านควอนตัม สำหรับระบบการจัดการความเสี่ยงขององค์กร (ERM)

- The World Global Trends 2026-2030
- The Three Lines of Defense Model from 2013 to 2020
- Evolution of the Three Lines of Defence Model : From Risk Control to Value Creation
- Three Lines Model: Global & Thai Best Practices in Risk Governance
- The Three Musketeers : IT Governance Framework, Data Governance Framework & AI Governance Framework
- Cybersecurity Risk and ERM Alignment
- NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)
- Integration Challenges and Considerations
- Recommendations for Organizations
- The Revolution of AI and Quantum Computing
- Issues Regarding AI Usage in An Organization
- AI Firewall & AI Gateway
- Country Level Risk about the future of Thailand AI Sovereignty
- Key Takeaway

AW-07 | 1 DAY | Is AI a game changer ? Formulating AI strategy for the Enterprise

หลักสูตรการกำหนดกลยุทธ์ AI สำหรับองค์กร (AI เป็นตัวเปลี่ยนเกมจริงหรือ?)

- Introduction & Context
  - The Big Question
  - Understanding AI in the Enterprise Context
- The Current AI Landscape
  - Market Trends & Adoption
  - AI Technology Overview
- Value Proposition of AI in Enterprises
  - Efficiency Gains
  - Innovation & Revenue Growth
  - Competitive Advantage
- Challenges & Risks
  - Organizational & Operational Risks
  - Ethical & Regulatory Considerations
  - Cybersecurity & AI Threats
- Case Studies & Real-World Impact
  - Success Stories
  - Lessons Learned from Failures
- Strategic Roadmap for AI in Enterprise
  - Readiness Assessment
  - Implementation Framework
  - Governance & Continuous Improvement
- Future Outlook
  - Emerging Technologies Complementing AI
  - What's Next for AI in Enterprises?
- Capstone Activity

PDPA AND DATA MANAGEMENT WORKSHOPS

หลักสูตรด้านการจัดการข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล

PW-01 — 1 DAY — Applying ISO/IEC 27701 (PIMS) for PDPA

หลักสูตรการนำข้อกำหนดมาตรฐานสากลมาประยุกต์ใช้กับการคุ้มครองข้อมูลส่วนบุคคล

- สถานะของ ISO/IEC 27701 เวอร์ชันล่าสุด และรายละเอียดการเปลี่ยนแปลง
- ภาพรวมมาตรฐานสากล ISO/IEC 27701 (PIMS) สำหรับการบริหารจัดการข้อมูลส่วนบุคคล
- ข้อกำหนดของมาตรฐาน ISO/IEC 27701 กับความสัมพันธ์มาตรฐาน ISO/IEC 27001:2022 (ISMS)
- แนวทางการนำมาตรฐาน ISO/IEC 27701 มาประยุกต์ใช้กับการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
- ข้อกำหนดด้านการบริหารจัดการข้อมูลส่วนบุคคล
- แนวทางดำเนินการและมาตรการควบคุมสำหรับผู้ควบคุมข้อมูลส่วนบุคคล
- แนวทางดำเนินการและมาตรการควบคุมสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล
- มาตรฐานและแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้องกับการบริหารจัดการข้อมูลส่วนบุคคล

PW-02 — 1 DAY — Implementing Data Security Controls for PDPA Compliance

หลักสูตรการจัดทำและดำเนินการมาตรการความมั่นคงปลอดภัยของข้อมูลในการปฏิบัติสอดคล้องตามกฎหมายลำดับรองของกฎหมายการคุ้มครองข้อมูลส่วนบุคคล

- มาตรการควบคุมสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- แนวทางดำเนินการมาตรการควบคุมด้านมาตรการเชิงองค์กร (Organizational)
- แนวทางดำเนินการมาตรการควบคุมด้านมาตรการเชิงเทคนิค (Technical)
- แนวทางดำเนินการมาตรการควบคุมด้านมาตรการทางกายภาพ (Physical)
- แนวทางดำเนินการมาตรการควบคุมด้านมาตรการบุคคล (People)
- การสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness)

PW-03 — 1 DAY — Integrating PDPA Data Protection and Data Governance Platform

หลักสูตรการบูรณาการแพลตฟอร์มด้านการคุ้มครองข้อมูลส่วนบุคคลกับการกำกับดูแลข้อมูล

- ภาพรวมเทคโนโลยี แพลตฟอร์ม องค์ประกอบ สำหรับการจัดการข้อมูลส่วนบุคคล
- การใช้แพลตฟอร์มในการบริหารจัดการ PDPA อย่างเป็นระบบ
- แนวทางการจัดการ Personal Data Inventory
- แนวทางการจัดการ Data Protection Impact Assessment (DPIA) and Risk Management
- แนวทางการจัดการ Consent Management System
- แนวทางการจัดการ Data Subject Right System
- แนวทางการจัดการ Executive Support System
- ความเชื่อมโยงของแพลตฟอร์มการจัดการข้อมูลส่วนบุคคลและแพลตฟอร์มการกำกับดูแลข้อมูล

SOFTWARE DEVELOPMENT AND PROGRAMMING WORKSHOPS

หลักสูตรด้านการพัฒนาระบบและซอฟต์แวร์

SW-01 — 3 DAYS — Microservices Architecture

หลักสูตรการออกแบบระบบให้เป็น Microservices

- Introduction to Microservices
- Design principles
- Design patterns
- Technology for microservices
- Distributed transaction
- Distributed tracing
- Data consistency
- Reporting patterns
- Securing your microservices
- Identity propagation
- Service to service authentication
- Logging and monitoring

SW-02 — 2 DAYS — How to Design Secure Software

หลักสูตรออกแบบ Software อย่างไรให้มีปลอดภัย

- Security Design Principles
- Define Business and Technical Scope
- Threat Modeling
- STRIDE
- PASTA
- OCTAVE
- Risk Handling

SW-03 — 3 DAYS — How to Securing Web API

หลักสูตรการสร้าง Web API อย่างไรให้ปลอดภัยจากการโจมตีในโลกไซเบอร์

- OWASP API Top 10
- GraphQL security
- gRPC security
- REST security
- Open API Specification
- Automated API security testing
- Cross-Origin Resource Sharing (CORS)
- JWT attack vectors
- Securing API with OAuth2
- OAuth2 security best practices
- Logging and monitoring

ภาคปฏิบัติ
CDIC2025 CYBERSECURITY WORKSHOPS
ภาคปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 38 หัวข้อ

IT PROFESSIONAL AND TECHNICAL WORKSHOPS
หลักสูตรด้านเทคนิคขั้นสูงและเทคโนโลยีสารสนเทศ

TW-01 — 3 DAYS — Adaptive Network-based Infrastructure Attacking
หลักสูตรเทคนิคและการทดสอบเจาะระบบเครือข่าย

- Network Layer & TCP/IP Fundamental
- Phase of Ethical Hacking
- The Art of Spoofing & Port Scanning
- The Art of Social Engineering & Metasploit Basic
- Target, Network & Windows Enumeration
- Post Exploitation: Credential Dumping
- Gaining Access Through Network Exploitation
- Escalation of Access
- Client-Side & Scripting Attack
- Hacking Recent Linux, Windows Vulnerabilities
- Password Cracking
- External Network Reconnaissance
- Hacking Application Servers
- Vulnerability Identification
- Internal Network Attacks
- Gaining Situational Internal Awareness
- Impact Demonstration
- Internal Lateral Movement

TW-02 — 3 DAYS — All-In-One Cybersecurity Mastering
หลักสูตรครบเครื่องเรื่อง Cybersecurity ทั้งการโจมตีและการป้องกันทางไซเบอร์ที่นำไปปรับใช้ได้จริง

- Overview Cybersecurity Framework
- Understanding Cyber Attack
- Risk Management
- Data Protection and Privacy
- Infrastructure Security
- Cloud Security
- Application Security
- Mobile Application Security
- Incident Response and Handling

TW-03 — 1 DAY — A Beginner's Guide to Becoming a Cloud Security Professional
หลักสูตรคู่มือสำหรับผู้เริ่มต้นการเป็นผู้เชี่ยวชาญด้านความปลอดภัยระบบคลาวด์

- Cloud Concepts, Architecture and Design
- Cloud Platform & Infrastructure Security
- Cloud Security Operations
- Cloud Data Security
- Cloud Application Security
- Cloud Security Operations

TW-04 — 1 DAY — Cloud Security
หลักสูตรอบรมการใช้งาน Cloud อย่างไรให้ปลอดภัย

- Cloud security principles
- Cloud security architecture
- SABSA conceptual analysis
- SABSA design
- Infrastructure-level cloud security
- Application-level cloud security
- Data-level cloud security
- Security as a services(SECaaS)

TW-05 — 3 DAYS — AWS Cloud Security Best Practices
หลักสูตรอบรมการใช้งาน AWS อย่างปลอดภัย

- Cloud security principles
- Shared responsibility model
- AWS Well Architecture Framework
- AWS security best practices
- Securing network on AWS
- Site-to-Site VPN
- Maintaining EC2 instance with AWS Inspector
- Securing application on AWS
- Securing data on AWS
- Security audit with AWS config and Trust advisor
- Cloud infrastructure analysis with scout suite
- Cloud infrastructure analysis with prowler
- Audit Infrastructure as Code(IoC) with tfsec

TW-06 — 1 DAY — Vulnerability Management
หลักสูตรการจัดการช่องโหว่ตั้งแต่การค้นหาไปจนถึงการป้องกัน

- Vulnerability Lifecycle
- Vulnerability Scanning
- Vulnerability Analysis
- Interpret and Prioritize Finding
- CVSS scoring

TW-07 — 3 DAYS — Securing Web Application
หลักสูตรการสร้าง Web Application อย่างไรให้ปลอดภัย

- OWASP Top 10 Risks
- Security Testing
- JacaScript Security
- API Security
- Secure in Deployment
- Modern Web Security Risks

TW-08 — 2 DAYS — Mobile Application Penetration Testing
หลักสูตรการทดสอบเจาะระบบผ่านโมบายแอพพลิเคชัน

- Introduction to Mobile Application Security
- OWASP MOBILE TOP 10
- Android Architectures
- Device and Data Security
- Network Traffic
- Reversing APKs
- Static Application Analysis
- Dynamic Application Analysis

www.cdicconference.com

TW-09 (2 DAYS) Active Directory Penetration Testing: Techniques and Tools

หลักสูตรเจาะลึกการทดสอบเจาะระบบใน Microsoft Active Directory

- Introduction to Active Directory Penetration Testing
- Active Directory Architecture and Components
- Setting Up the Testing Environment
- Enumeration and Information Gathering
- Exploiting Active Directory Vulnerabilities
- Advanced AD Attack Techniques
- Post-Exploitation Activities

TW-10 (2 DAYS) Scripting for Penetration Tester

หลักสูตรเขียนสคริปต์มือโปรสำหรับนักทดสอบเจาะระบบ

- Overview of popular scripting languages (Python, PowerShell, Bash)
- Setting Up the Environment
- Basic Scripting Techniques
- Python for Penetration Testing
- PowerShell for Penetration Testing
- Advanced Scripting Techniques
- Automating Penetration Testing Tasks
- Practical Applications of Scripting

TW-11 (3 DAYS) Intelligence and Scenario-Based Penetration Testing

หลักสูตรการทดสอบเจาะระบบเชิงสถานการณ์จริง

- Planning and Scoping Penetration Tests
- Advanced Attack Techniques
- Executing Penetration Tests
- Analysis, Reporting
- Post-Exploitation Analysis
- Reporting and Communication

TW-12 (2 DAYS) Threat Intelligence Implementation and Analysis

หลักสูตรการวิเคราะห์และใช้งานข้อมูลข่าวกรองภัยคุกคาม การป้องกันล่วงหน้าด้วยความรู้เชิงลึก

- Introduction to Threat Intelligence
- Setting Up the Threat Intelligence Program
- Threat Intelligence Tools and Platforms
- Data Collection and Processing
- Threat Intelligence Analysis
- Operationalizing Threat Intelligence
- Advanced Threat Intelligence Techniques

TW-13 (2 DAYS) Incident Response and Handling Techniques and Tools

หลักสูตรเทคนิคการตอบสนองและจัดการเหตุการณ์ พร้อมรับมือทุกภัยคุกคาม

- Introduction to Incident Response
- Incident Response Team (IRT) and Roles
- Preparation and Planning
- Identifying and Categorizing Incidents
- Incident Containment and Eradication
- Incident Recovery
- Post-Incident Activities

TW-14 (2 DAYS) Malware Analysis Techniques and Tools

หลักสูตรเทคนิคการวิเคราะห์มัลแวร์ในรูปแบบต่าง ๆ

- Introduction to Malware Analysis
- Setting Up the Analysis Environment
- Static Analysis Techniques
- Reverse Engineering Basics
- Dynamic Analysis Techniques
- Advanced Malware Analysis Techniques
- Memory Forensics

TW-15 (3 DAYS) SOC: Cybersecurity Threat Detection and Analysis: Techniques and Tools

หลักสูตรการตรวจจับภัยและวิเคราะห์ภัยคุกคามทางไซเบอร์

- Cybersecurity Threat and Attack Techniques
- Overview SOC (Security Operation Center)
  - What is SOC?
  - Type of SOC
  - SOC Service Catalog
  - SOC Roles and Responsibility
  - SOC Architecture
- Incident Management Process
- Security Analyst Skills and Certification
- Intrusion Analysis Techniques
  - Log Analysis Concept
  - Basic Splunk Indexes
  - Basic Splunk Search and Query
  - Workshop: Log Analysis to Cyber Security Threats by Incident Category
  - Network Traffic Analysis Tools
  - Analyze and Drilldown Threats
- Use Case Development

TW-16 (1 DAY) Python Data Analytics for Fraud Detection

หลักสูตรการใช้ Python ในงาน Data Analytics สำหรับการตรวจจับการทุจริต

- ความสำคัญของการทำ Fraud Detection ในองค์กร
- ทำความรู้จักกับ Python เบื้องต้น
- วิธีการ Setup Python ผ่าน Google Colab
- การเขียน Python ในลักษณะต่างๆ ขั้นพื้นฐาน
- ขั้นตอนการทำ Data Analytics for Fraud Detection
- การใช้งานเครื่องมือ (Library) Python ในงานวิเคราะห์ข้อมูล (Data Analytics)
- การทำความสะอาดข้อมูล (Data Cleaning) และแสดงข้อมูลเป็นรูปภาพ (Data Visualization) ด้วย Python
- Use Case Data analytics for Fraud Detection
- Workshop Python Data Analytics for Fraud Detection
- แถม: ตัวอย่างชุดข้อมูล (Dataset) สำหรับทำ Fraud Detection
- ใช้ Python ผ่าน Google Colab

TW-17 (3 DAYS) Machine Learning Security

หลักสูตรอบรมเกี่ยวกับความเสี่ยงบน Machine Learning ที่ต้องรู้จัก

- What is Machine Learning
- What is Generative AI
- What is Agentic AI
- Model Context Protocol(MCP)
- Securing MCP
- OWASP Machine Learning Top 10
- OWASP LLM Top 10
- AIOps
- MLOps
- GenAIOps
- AI data governance

CDIC2025 CONFERENCE THEME

เมื่อ 2 เทคโนโลยีแห่งอนาคต มุ่งสู่การเปลี่ยนโฉมหน้าความมั่นคงปลอดภัยไซเบอร์อย่างไม่เคยมีมาก่อน... Quantum Supremacy กำลังทลายขีดจำกัดการประมวลผล ทำให้มาตรฐานการเข้ารหัสมีความเสี่ยงสูงที่จะถูกเจาะทำลายได้ง่าย ๆ เป็นประวัติการณ์ ขณะที่ AGI ได้รับการพัฒนาความสามารถด้านการเรียนรู้ วางแผน และตัดสินใจได้เสมือนมนุษย์ เปิดโอกาสใหม่ในการเสริมสร้างระบบป้องกันภัยไซเบอร์ด้วย AI อัจฉริยะ โดยทั้ง 2 เทคโนโลยีดังกล่าวจะนำไปสู่การเกิดภัยคุกคามรูปแบบใหม่ที่ท้าทายในอนาคตอันใกล้นี้ CDIC2025 คือเวทีแห่งองค์ความรู้ที่สำคัญนำพาองค์กรของคุณให้เตรียมพร้อมสู่อนาคตไซเบอร์

ตั้งแต่การพัฒนา Post-Quantum Cryptography เพื่อรับมือภัยคุกคามใหม่ การเสริมความแข็งแกร่งของ SOC ผ่านระบบอัตโนมัติที่ขับเคลื่อนด้วย AGI และ Agentic AI การสร้าง Digital Trust ด้วย Generative AI และการวางกลยุทธ์รับมือกับ Cyber Warfare รูปแบบใหม่ที่ AI เป็นหัวใจหลักของการโจมตีและการป้องกัน พร้อมอัปเดตแนวทางกำกับดูแล AI จากปัญหา Hallucination สู่ Regulation ใหม่ ตลอดจนการเตรียมพร้อมรับกับกฎหมายไซเบอร์ในโลก Quantum และ AGI รวมถึงการสร้างความแข็งแกร่งด้าน Cyber Resilience ในระดับชาติ ร่วมขับเคลื่อนความมั่นคงดิจิทัลสู่อนาคตที่ยั่งยืน ยืดหยุ่น และเชื่อถือได้ พบกับสุดยอดผู้นำด้านความมั่นคงปลอดภัยไซเบอร์จากทั่วโลกในงาน CDIC 2025 ระหว่างวันที่ 26–27 พฤศจิกายน 2568 ณ Grand Hall ศูนย์นิทรรศการและการประชุมไบเทค กรุงเทพฯ

กลุ่มเป้าหมาย

- ผู้บริหารระดับสูง (CEO, COO, CRO)
- ผู้บริหารสารสนเทศระดับสูง (CIO, CTO, CDO)
- ผู้บริหารระบบความปลอดภัยข้อมูลระดับสูง (CSO, CISO)
- ผู้บริหารหรือผู้อำนวยการในสายงานไอทีและสารสนเทศ (Vice President, Assistant Vice President, IT Director, IT Manager)
- ผู้บริหารฝ่ายธุรกิจ ผู้บริหารฝ่ายดิจิทัล ผู้บริหารฝ่ายนวัตกรรม ผู้บริหารฝ่ายการตลาด (CBO, CDO, CIO, CMO)
- ผู้เชี่ยวชาญและที่ปรึกษาทางด้านระบบสารสนเทศและความปลอดภัยทางไซเบอร์ (IT Specialist, Cybersecurity Specialist, IT Consultant)
- บุคลากรด้านไอทีของหน่วยงานภาครัฐและเอกชน (IT Security Practitioner)
- ผู้ดูแลระบบเน็ตเวิร์กและระบบปฏิบัติการขององค์กร (Network & System Administrator)
- ผู้ตรวจสอบระบบสารสนเทศ (IT Auditor)
- ผู้พัฒนาซอฟต์แวร์ (Software Developer)
- บุคลากรในสายงานกฎหมาย (Law Enforcement)
- บุคลากรในสายงานกำกับดูแล (Compliance / IT Compliance)
- บุคลากรในสายงานบริหารความเสี่ยง (ERM / IT Risk)
- บุคลากรในสายงานนิติวิทยาศาสตร์คอมพิวเตอร์ (Cyber Cop / Digital Forensic Investigator)
- บุคลากรของผู้ให้บริการระบบเทคโนโลยี (IT Supplier, IT Outsourcing Provider)
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer / DPO)
- ผู้ปฏิบัติการ ผู้เชี่ยวชาญ และผู้ให้บริการด้านคลาวด์ (Cloud Administrator, Architect, Security Analyst, MSSP/MSP, Cloud Vendor)
- ผู้ปฏิบัติการ และผู้เชี่ยวชาญเทคโนโลยีควอนตัม (Data Engineer, Business Analyst, Quantum Technology Specialists)
- ประชาชนทั่วไปที่สนใจด้านความปลอดภัยข้อมูลคอมพิวเตอร์ (IT Smart Users)

วันเวลาและสถานที่จัดสัมมนา

- สัมมนา 2 วัน - การบรรยายและสาธิต (Conference 2 Days)
  - วันที่สัมมนา วันที่ 26–27 พฤศจิกายน 2568
  - เวลา 8:30-17:30 น.
  - สถานที่ ศูนย์นิทรรศการและการประชุมไบเทค (BITEC)
- ภาคปฏิบัติ - การสาธิตพร้อมฝึกปฏิบัติ
  - วันที่ปฏิบัติ รายละเอียดตามใบลงทะเบียน
  - เวลา 9:00-16:00 น.
  - สถานที่ โรงแรมระดับ 4 ดาวในกรุงเทพฯ

สิ่งที่ท่านจะได้รับเมื่อเข้าสัมมนา

- ของที่ระลึก
- กระเป๋าใส่เอกสาร
- อาหารกลางวันและอาหารว่าง
- ผู้เข้าสัมมนา 2 วัน จะได้รับวุฒิบัตรจาก
  - เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย (Software Park)
  - สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)
  - บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS Professional Center)

ประโยชน์จากการเข้าร่วมงาน CDIC2025

- **รับมือกับภัยคุกคามไซเบอร์ในยุค Quantum Supremacy**
  เรียนรู้การปรับตัวต่อยุคที่ Quantum Computing อาจทำลายมาตรฐานการเข้ารหัสที่ใช้อยู่ในปัจจุบัน พร้อมทำความเข้าใจแนวทางการพัฒนา Post-Quantum Cryptography เพื่อปกป้องข้อมูลสำคัญในระดับองค์กรและประเทศ
- **เสริมความแข็งแกร่งของ SOC ด้วย AGI และ Agentic AI**
  รับแนวคิดและเทคนิคการยกระดับการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยเทคโนโลยี AGI ที่สามารถวิเคราะห์เหตุการณ์ วางแผนรับมือและตอบโต้ภัยคุกคามได้อย่างมีประสิทธิภาพ
- **วางกลยุทธ์รับมือกับ Cyber Warfare รูปแบบใหม่**
  เข้าใจรูปแบบสงครามไซเบอร์ที่ใช้ AI เป็นแกนหลักของการโจมตีและป้องกันทั้งในภาครัฐและ Critical Infrastructure พร้อมรับมือกับความท้าทายด้านความมั่นคงปลอดภัยระดับประเทศ
- **สร้าง Digital Trust ด้วย Generative AI**
  เรียนรู้การประยุกต์ใช้ Generative AI และ AI ตัวแทน (Agentic AI) เพื่อเสริมสร้างความเชื่อมั่นทางดิจิทัล ทั้งในด้านการบริการภาครัฐ การเงิน การสื่อสาร และระบบอัตโนมัติ
- **เข้าใจปัญหา Hallucination และแนวทาง AI Regulation ล่าสุด**
  ติดตามทิศทางการกำกับดูแลปัญญาประดิษฐ์ ทั้งระดับไทยและสากล เช่น NIST AI RMF, EU AI Act, Thailand AI Governance เพื่อการใช้ AI อย่างรับผิดชอบ
- **เตรียมพร้อมรับมือกับกฎหมายไซเบอร์ยุคใหม่**
  อัปเดตกฎหมายและมาตรฐานสำคัญ เช่น พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act), พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA), แนวทางปฏิบัติตาม NIST CSF 2.0 เพื่อเพิ่มความมั่นคงในองค์กร
- **เชื่อมต่อเครือข่ายผู้เชี่ยวชาญระดับสูง**
  พบกับผู้นำจากหน่วยงานระดับประเทศและบริษัทเทคโนโลยีชั้นนำทั่วโลก เพื่อแลกเปลี่ยนมุมมอง ประสบการณ์ และร่วมสร้างเครือข่ายพันธมิตรความมั่นคงดิจิทัล
- **รับแรงบันดาลใจจากสุดยอดวิทยากรและนวัตกรรมล้ำยุค**
  สัมผัสการแสดงเทคโนโลยีแห่งอนาคตด้าน Cybersecurity, Quantum, AI และ Emerging Tech ผ่าน Live Show และนิทรรศการพิเศษ พร้อมข้อมูลเชิงลึกจากผู้เชี่ยวชาญ