ภาคปฏิบัติ

CDIC2020 MASTERCLASS WORKSHOPS

ภาคปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 35 หัวข้อ

IT TECHNICAL & PROFESSIONAL WORKSHOPS

สำหรับผู้จัดการและผู้ปฏิบัติงานด้านระบบเครือข่าย, ระบบปฏิบัติการ, เทคโนโลยีสารสนเทศ, ความมั่นคงปลอดภัยสารสนเทศและผู้สนใจด้านเทคนิคขั้นสูง

CLASSROOM ONLINE IS AVAILABLE

TW-01 3 DAYS

AWS Security
การใช้งาน AWS อย่างปลอดภัย

- Cloud Security Principles
- Indentity Access Management (IAM)
- AWS Networking
- Security Audit
- AWS Security Services

TW-02 3 DAYS

Azure Security
หลักสูตรอบรมการใช้งาน Azure อย่างปลอดภัย

- Cloud Security Principles
- Indentity Management
- Azure Networking
- Security Audit
- Azure Security Services

TW-03 2 DAYS

Artificial Intelligence for Cyber Security
พื้นฐานการสร้าง AI และใช้ AI เข้ามาช่วยแก้ปัญหาทางด้าน Security

- Artificial Intelligence (AI) Foundation
- Machine Learning
- Deep Learning
- Risk and Limitation

TW-04 2 DAYS

Basic Mobile Application Penetration Testing for Android
การทดสอบเจาะระบบปฏิบัติการแอนดรอยด์เบื้องต้น

- Android Device Architecture
- Unlocking, Rooting Mobile Devices
- Static Application Analysis
- Dynamic Application Analysis (Using Frida and Objection)
- Mobile Penetration Testing Based on OWASP Mobile Top10

TW-05 3 DAYS

Adaptive Network-based Infrastructure Attacking
เทคนิคและการทดสอบเจาะระบบเครือข่าย

- TCP/IP Basics
- The Art of Port Scanning
- Target Enumeration
- Brute-Forcing
- Metasploit Basics
- Hacking Recent Unix Vulnerabilities
- Hacking Databases
- Hacking Application Servers
- Hacking Third Party Applications (WordPress, Joomla, Drupal)
- Gaining Access Through Network Exploitation
- Gaining Access Through Social Engineering
- Windows Enumeration
- Hacking Recent Windows Vulnerabilities
- Client-Side Attack
- Post Exploitation: Dumping Secrets
- Hacking Windows Domains
- Effective Assessment Management
- External Network Footprinting
- Network Enumeration
- Vulnerability Identification
- Password Cracking
- Internal Network Attacks
- Gaining Situational Internal Awareness
- Escalation of Access
- Internal Lateral Movement
- Impact Demonstration

TW-06 2 DAYS

Wireless Hacking and Security Assessment
การโจมตีระบบและประเมินความเสี่ยงเครือข่ายไร้สาย

- Wireless Network and IEEE 802.11
- Network Interaction
- Aircrack-ng Essentials
- Cracking WEP with Various Methods
- Cracking WPA/WPA2
- Optimize the Cracking Tools
- Real World Attacking Techniques

TW-07 2 DAYS

Active Directory Attacks
การโจมตี Active Directory และแนวทางการป้องกัน

- Extensive AD Enumeration
- Active Directory Trust Mapping and Abuse
- Privilege Escalation (User Hunting, Delegation Issues and More)
- Kerberos Attacks and Defense (Golden, Silver Ticket, Kerberoast and More)
- Abusing Cross Forest Trust (Lateral Movement Across Forest, PrivEsc and More)
- Attacking Azure Integration and Components
- Abusing SQL Server Trust in AD (Command Execution, Trust Abuse, Lateral Movement)
- Credentials Replay Attacks (Over-PTH, Token Replay etc.)
- Persistence (WMI, GPO, ACLs and More)
- Defenses (JEA, PAW, LAPS, Deception, App Whitelisting, Advanced Threat Analytics etc.)
- Bypassing Defenses

TW-08 2 DAYS

Basic Web Application Penetration Testing
การทดสอบเจาะระบบผ่านเว็บแอพพลิเคชั่นเบื้องต้น

- Penetration Testing Process
- Introduction to Web Applications
- Cross Site Scripting
- SQL Injection
- Broken Access Control
- Other Attacks

TW-09 3 DAYS

All-In-One Cybersecurity
ครบเครื่องเรื่อง Cybersecurity ทั้งการโจมตีและการป้องกันทางไซเบอร์ที่นำไปปรับใช้ได้จริง

- Overview Cybersecurity Framework
- Risk Management
- Infrastructure Security
- Cloud Security
- Application Security
- Mobile Application Security
- IoT (Internet of Things) Security
- Incident Response and Handling

TW-10 3 DAYS

Cyber Attack Incident Responder for Technical
การเป็นหน่วยกู้ภัยทางไซเบอร์ภายในองค์กร

- Introduction of Cybersecurity Framework and Cyber Resilience
- Introduction of Incident Management
- Incident Handling Methodology
- Incident Response Preparation
- Incident Threats and Categories
- Workshop: Know your Enemy
- Incident Handling Case Study by Category
- Incident Handling Tools
- Workshop Incident Handling

TW-11 3 DAYS

How to be a Cyber Threat Hunter
การตรวจจับภัยคุกคามอย่างรวดเร็วด้วย Threat Intelligence

- Overview Threat Hunting
- How to Apply IOC for Host-Based Scanning
- Importing and Integrate IOC data from Threat Intelligent
- SCAP Protocol and Automate Vulnerability Detection
- Network-Based IOC (Indicator of Compromise)
- Log Management architecture design
- Microsoft Windows Event Log Analysis
- Network-Based Threat Hunting
- Threat Hunting Methodology
- Threat Exchange Source
- Threat Exchange Protocols
- Host-Based Threat Hunting
- IOC Scanner Tools
- Threat Data Feed
- Intelligent News Feed
- Malicious Code Activity

TW-12 3 DAYS

SOC Operation and Threat Analysis
ขั้นตอนการดำเนินงานในศูนย์เฝ้าระวังทางไซเบอร์ (SOC) และการวิเคราะห์ภัยคุกคามทางไซเบอร์

- Cybersecurity Threats
- Overview SOC (Security Operation Center)
- Incident Management Process
- Security Analyst Skills and Certification
- Intrusion Analysis & Incident Handling Techniques
- Use Case Development

TW-13 3 DAYS

R Programming for Data Science & Machine Learning
โปรแกรมภาษา R สำหรับ Data Science & Machine Learning

- Introduction to Data Science and Machine Learning
- Data Science Life Cycles
- Introduction to R Programming Language
- Introduction to Data Manipulation
- Introduction to Simple Data Analysis
- Data Visualization
- Introduction to Machine Learning with R
- Basic Data Science Methods and Machine Learning Fundamentals
- Intermediate Data Science Methods and Machine Learning Fundamentals
- Practical Predictive Analytics

TW-14 3 DAYS

Data Science & Big Data Analytics Software Development
การพัฒนาโปรแกรมสำหรับ Data Science และ การวิเคราะห์ Big Data

- Introduction to Big Data Analytics
- Introduction to Apache Hadoop
- Hadoop Essential Components
- Introduction to Parallel Distributed Computing with MapReduce
- Introduction to Apache Spark (high speed analytics platform)
- Introduction to Data Science & Machine Learning
- Introduction to Machine Learning with Apache Spark using MLlib

IT MANAGEMENT WORKSHOPS

สำหรับผู้บริหาร ผู้อำนวยการ ผู้จัดการ สายงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ

MW-01 1 DAY

IT-GRC Implementation Concepts in Practice for Digital Technology Enablers
ภาพรวมการนำมาตรฐานและแนวปฏิบัติที่ดีมาใช้สำหรับการบริหารจัดการด้านเทคโนโลยีดิจิทัล

- การกำกับดูแลด้านเทคโนโลยีดิจิทัล และแผนปฏิบัติการดิจิทัลขององค์กร (Digital Governance and Roadmap)
- การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation)
- การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)
- ธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)
- การบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)
- การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management)
- การบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management)

MW-02 1 DAY

Enabling IT Governance Standards for Digital Governance and Roadmap (ISO/IEC 38500 ITG Standards & Related Best Practices)
มาตรฐานการกำกับดูแลด้านเทคโนโลยีสารสนเทศและแนวทางขับเคลื่อนองค์กรในการกำกับดูแลด้านเทคโนโลยีดิจิทัล

- ข้อกำหนดของมาตรฐานการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (Standards)
- ต้นแบบการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (Model)
- หลักการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (Principles)
- หลักการด้านความรับผิดชอบ (Responsibilities)
- หลักการด้านยุทธศาสตร์ (Strategy)
- หลักการด้านการจัดหา (Acquisition)
- หลักการด้านผลดำเนินการ (Performance)
- หลักการด้านผลความสอดคล้องตามข้อกำหนด (Conformance)
- หลักการด้านการประพฤติปฏิบัติของบุคลากร (Human Behaviour)
- แนวปฏิบัติสำหรับกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศและองค์ประกอบ (Framework)
- แนวทางการกำหนดเกณฑ์และการประเมินผลลัพธ์ (ITG Beneficial Outcomes)
- แนวทางการประยุกต์ใช้มาตรฐานและดำเนินการ

MW-03 1 DAY

Enabling IT Governance Framework and Practices using COBIT for Digital Governance (COBIT 2019, Enterprise Governance of Information and Technology)
กรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติอ้างอิง COBIT สำหรับการกำกับดูแลด้านเทคโนโลยีดิจิทัล

- The COBIT Framework Overview
- COBIT 2019 Framework and Methodology
- COBIT 2019 Governance and Management Objectives
- COBIT 2019 Designing I&T Governance
- COBIT 2019 Implementation
- Principles, Framework and Practices for Digital Technology Enablers and IT Governance

MW-04 2 DAYS

Enabling Data Governance and Data Management Framework for Digital Governance
กรอบการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลสำหรับการกำกับดูแลด้านดิจิทัล

- Introduction
- Data Governance Fundamentals and Concept
- Data Management Fundamentals
- Data Definition
- Data Governance Structure
- Data Rule
- International Data Governance Framework
- Thailand Data Governance Framework Exercise
  #1 Data Governance Readiness Assessment
- Introduce DAMA DMBOK2
- Data Management Overview
  - Metadata
  - Data Integration and Interoperability
  - Data Architecture
  - Documents and Content
  - Data Security
  - Data Modeling and Design
  - Data Storage and Operations
  - Reference and Master Data
  - Data Governance
  - Data Warehousing and Business Intelligence
  - Data Quality
- Data Governance and Digital Governance
- Data Governance Maturity Model Assessment and Audit

MW-05 1 DAY

Enabling Information Security Risk Management for Information Security Management and Digital Technology Enablers
การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสำหรับเทคโนโลยีดิจิทัล

- Concepts of Information Security Risk Management and Digital Technology
- Related Standard and Best Practices for Information Security Risk Management
- Information Security Risk Management Framework and Process
- Identification of Risk Scenarios (Asset-base and Event-base)
- Identification of Assets, Vulnerabilities, Threats and related Risk Factors
- Information Security Risk Assessment (Identification, Analysis, Evaluation, Options, Risk Response)
- Information Security Risk Acceptance
- Information Security Risk Communication and Consultation, Monitoring and Review
- Integrated Risk Management for IT Risk, Data/Information Security Risk, Privacy Risk and Cybersecurity Risk

MW-06 1 DAY

Enabling Availability Management, Incident Management, and Business Continuity Management for Digital Technology Enablers
การบริหารจัดการด้านความพร้อมใช้ เหตุขัดข้อง และความต่อเนื่องในการดำเนินการ สำหรับการบริหารจัดการเทคโนโลยีดิจิทัล

- Availability Management and Key Concepts for Digital Technology
- IT-related Incident & Security Incident Management
- Incident Response Management and Handling Guides
- Information Security Continuity and Aspects for Business Continuity Management
- Availability of Information Processing Facilities and Redundancies
- IT Contingency Planning, Disaster Recovery Planning and related Business Continuity Management
- Emergency Response and Related Procedures
- Business Continuity Planning and Review

MW-07 1 DAY

Lesson Learned and Practical Compliance Guide for PDPA Lawful Basis and Data Protection
แนวปฏิบัติและบทเรียนรู้สำหรับการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- ภาพรวมของกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)
- หลักการคุ้มครองข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ฐานการประมวลผลข้อมูลส่วนบุคคล
- ประเด็นด้านกฎหมายและแนวทางดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
- ประเด็นด้านกฎหมายและแนวทางดำเนินการของผู้ประมวลผลข้อมูลส่วนบุคคล
- ประเด็นด้านกฎหมายและแนวทางดำเนินการของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ประเด็นด้านกฎหมายกรณีการกระทำความผิดของนิติบุคคล
- การร้องเรียน ความรับผิดทางแพ่ง โทษอาญา โทษทางปกครอง

MW-08 1 DAY

Comply with PDPA Using ISO/IEC 27701
การนำ ISO/IEC 27701 ไปปฏิบัติเพื่อให้สอดคล้องต่อ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

- หลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานสากลและแนวปฏิบัติที่เกี่ยวข้อง
- เชื่อมโยงข้อกำหนดตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กับมาตรฐาน ISO/IEC 27701
- สิ่งที่ควรมีแต่หายไปจาก พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- แนวทางการนำ ISO/IEC 27701 ไปปฏิบัติ

MW-09 1 DAY

Practical Compliance Guide: Code of Practices for CII Cybersecurity Incident Response
การจัดทำประมวลแนวทางปฏิบัติสำหรับแผนการรับมือภัยคุกคามทางไซเบอร์

- ภาพรวมของกฎหมาย พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์
- ภาพรวมแนวทางการจัดทำประมวลแนวทางปฏิบัติสำหรับแผนการรับมือภัยคุกคามทางไซเบอร์
- แนวทางการนิยามภัยคุกคามทางไซเบอร์ ระดับไม่ร้ายแรง ระดับร้ายแรง ระดับวิกฤติ
- แนวทางการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์
- แนวทางการวางแผน ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- แนวทางการจัดสร้างทีมดำเนินการเพื่อรับมือภัยคุกคามทางไซเบอร์
- แนวทางการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์
- แนวทางการสื่อสาร และการรายงาน

MW-10 2 DAYS

Practical Compliance Guide: CII Cybersecurity Framework and Implementation
การจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- ภาพรวมกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์
- CSF: Identify การระบุความเสี่ยง ประเมิน และจัดการความเสี่ยง
- CSF: Protect การจัดทำมาตรการและแนวปฏิบัติ
- CSF: Detect การตรวจสอบและเฝ้าระวัง
- CSF: Response การเผชิญเหตุและการตอบสนอง
- CSF: Recover การฟื้นฟูความเสียหาย

MW-11 1 DAY

Practical Compliance Guide: CII Cyber Resilience Hands-on
การสร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยไซเบอร์ผ่านการปฏิบัติจริง

- ภาพรวมมาตรฐานและแนวปฏิบัติที่ดีสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์
- ภาพรวมแนวคิดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การรับมือภัยคุกคามทางไซเบอร์ และการรองรับความต่อเนื่องการดำเนินธุรกิจ
- การดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- การตอบสนองเหตุการณ์และภัยคุกคามทางไซเบอร์
- การดำเนินการด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Review: CRR)

MW-12 1 DAY

Digital Laws, Cybersecurity Act, Personal Data Protection Act and GDPR Update
ตามติดกฎหมายดิจิทัล กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และ GDPR

- ภาพรวมของกฎหมายดิจิทัล
- สถานะและสาระสำคัญของกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ ฉบับปรับปรุงและกฎหมายลำดับรอง
- สถานะและสาระสำคัญของกฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับปรับปรุงและกฎหมายลำดับรอง
- สถานะและสาระสำคัญของกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายลำดับรอง
- สถานะและสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง และ GDPR
- สถานะของการใช้บังคับกฎหมายดิจิทัลล่าสุดฉบับอื่น ๆ

MW-13 2 DAYS

IT General Controls Audit
การตรวจสอบเรื่องการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ

- หลักการและเหตุผล
- ความรู้พื้นฐานด้านคอมพิวเตอร์ที่จำเป็นสำหรับการตรวจสอบ ITGC
- Workshop (Case Study)
- แนวทางการตรวจสอบ ITGC
  - IT Security Policy
  - IT Change Management
  - IT Organization
  - Physical Access and Environmental Controls
  - Logical Access Controls
  - IT Operation Controls
  - BCP/DRP: Business Continuity Plan and Disaster Recovery Plan

SOFTWARE DEVELOPMENT WORKSHOPS
สำหรับนักพัฒนาซอฟต์แวร์ และโปรแกรมเมอร์

SW-01 1 DAY

How to Securing RESTful API
การสร้าง RESTful API อย่างไรให้ปลอดภัยจากการโจมตีในโลกไซเบอร์

- Cross-Origin Resource Sharing (CORS)
- Alternative for Securing API
- Best Practice for RESTful API
- JWT Authentication
- Perform Access Control

SW-02 1 DAY

Understanding DevSecOps Foundations
พื้นฐานสำหรับผู้ที่ต้องการเข้าใจกระบวนการ DevSecOps ที่จะทำให้ Software มีความปลอดภัยสูงสุด

- Introduction to DevOps
- Principles of DevOps
- Continuous Integration
- Continuous Deployment
- Automated Security Testing

SW-03 1 DAY

Security Requirement
การจัดการความต้องการด้าน security

- Requirement management
- Risk Rating
- Requirement gathering
- ASVS and MASVS

SW-04 1 DAY

Agile Application Security
การผลิตซอฟต์แวร์ที่มีความปลอดภัยด้วย Agile

- Introduction to Agile methodology
- How to inject security into Agile
- Security Requirements
- Vulnerabilities Management
- Code Review for Security

SW-05 2 DAYS

How to Secure your container
การรักษาความปลอดภัย Container

- OWASP Docker TOP10
- How to Secure your Container
- Setup Docker Private Registry
- Monitor Application Health
- How to Monitoring your Container
- Kubernetes Security

SW-06 3 DAYS

Automated Security Testing
การทดสอบความปลอดภัยแบบอัตโนมัติ

- Introduction to ASVA 4.0
- Automated Security Testing with Gauntlt
- Automated Security Testing with OWASP ZAP
- Manage Dependencies with Dependency Check

SW-07 2 DAYS

Effective Application Logging
การเก็บ Log อย่างไรให้มีประสิทธิภาพ

- How to Manage Application Log
- Elastic APM
- Configuring and Installing ELK Stack
- Elastic SEIM
- Querying and Analyzing

SW-08 3 DAYS

AI and Deep Learning with Python and TensorFlow
การเก็บ Log อย่างไรให้มีประสิทธิภาพ

- Introduction to TensorFlow
- Basic Components
- Tensor Operations
- Using Estimator
- TensorFlow Model Development Related Concepts
- Predictive Model Development with TensorFlow
- Introduction to Artificial Neural Network (ANN)
- Convolutional Neural Network (CNN)
- Image Recognition with Predictive Model
- CNN Network Variations