ภาคปฏิบัติ

CDIC2019 MASTERCLASS WORKSHOPS

ภาคปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 29 หัวข้อ

IT MANAGEMENT WORKSHOPS

สำหรับผู้บริหาร ผู้อำนวยการ ผู้จัดการ สายงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ

MW-01 Cybersecurity Compliance Gap Assessment

1 DAY การประเมินสถานภาพความพร้อมและดำเนินการตามข้อกฎหมาย พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์

- ภาพรวมข้อกำหนดตามกฎหมาย พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์
- ภาพรวมข้อกำหนดและสิ่งที่ต้องดำเนินการสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)
- เกณฑ์การประเมิน (Gap Assessment Criteria)
- แนวทางการประเมิน (Gap Assessment Approach)
- ข้อสรุปสำหรับการเตรียมความพร้อมและดำเนินการตามข้อกฎหมาย

MW-02 Cybersecurity Risk Assessment

1 DAY การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

- ภาพรวมข้อกำหนดตามมาตรฐานและแนวปฏิบัติสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- กรอบการบริหารจัดการความเสี่ยง บริบท และขอบเขตสำหรับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- กระบวนการประเมินความเสี่ยงและแนวทางการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- การระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และสรุปผลการประเมินความเสี่ยง
- การจัดทำแผนบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

MW-03 Cybersecurity Framework Implementation

2 DAYS การจัดทำและดำเนินการตามกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

- ภาพรวมกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework: CSF)
- CSF: Identify การระบุความเสี่ยง ประเมิน และจัดการความเสี่ยง
- CSF: Protect การจัดทำมาตรการและแนวปฏิบัติ
- CSF: Detect การตรวจสอบและเฝ้าระวัง
  - ตัวอย่าง Cybersecurity Monitoring
  - ตัวอย่าง Cyber Drill
  - ตัวอย่าง Cyber Threat Intelligence
  - ตัวอย่าง Cyber Range
  - ตัวอย่างกระบวนการ ระบบตรวจสอบและระบบเฝ้าระวัง
- CSF: Response การเผชิญเหตุและการตอบสนอง
  - ตัวอย่างแนวทางการจัดทำและดำเนินการแผนรับมือภัยคุกคามไซเบอร์ (Cybersecurity incident response plan)
- CSF: Recover การฟื้นฟูความเสียหาย
  - ตัวอย่างแนวทางการจัดทำและดำเนินการ Cyber Forensic and Investigation
  - ตัวอย่างแนวทางแผนกู้คืนระบบ

MW-04 Personal Data Protection (Privacy) Compliance Gap Assessment

1 DAY การประเมินสถานภาพความพร้อมและดำเนินการตามข้อกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

- ภาพรวมข้อกำหนดตามกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- ภาพรวมข้อกำหนดสำหรับผู้ควบคุมข้อมูลส่วนบุคคล (DP Controller)
- ภาพรวมข้อกำหนดสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล (DP Processor)
- ภาพรวมข้อกำหนดสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- เกณฑ์การประเมิน (Gap Assessment Criteria)
- แนวทางการประเมิน (Gap Assessment Approach)
- ข้อสรุปสำหรับการเตรียมความพร้อมและดำเนินการตามข้อกฎหมาย

MW-05 Privacy Impact Assessment (PIA)

1 DAY การประเมินผลกระทบต่อความเป็นส่วนตัว

- หลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Fundamental principle in privacy information)
- ภาพรวมของการประเมินผลกระทบต่อความเป็นส่วนตัว (Overview of PIA)
- มาตรฐานและแนวปฏิบัติสำหรับการประเมินผลกระทบต่อความเป็นส่วนตัว (International standards and leading practices)
- กระบวนการประเมินผลกระทบต่อความเป็นส่วนตัว (Process for conducting a PIA)
- รายงานผลการประเมินผลกระทบต่อความเป็นส่วนตัว (PIA report)

MW-06 Implementing ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management

1 DAY แนวทางดำเนินการตามมาตรฐานการบริหารจัดการข้อมูลส่วนบุคคล

- From ISMS to Privacy Information Management System (PIMS)
- Overview: Introduction
- PIMS-specific Requirements
  - Leadership
  - Planning
  - Support
  - Operation
  - Improvement
  - Performance evaluation
  - Context of the organization
- PIMS-specific Guidance (Information Security and Privacy)
- Guidance for PII Controllers
- Guidance for PII Processors
- Relationships to Other Related Standards
  - ISO/IEC 29100 Privacy Framework
  - ISO/IEC 27002 ISMS Controls
  - ISO/IEC 27001 ISMS Requirements
  - Mapping to ISO/IEC 27018 (Code of Practice for Protection of PII in Public Clouds Acting as PII Processors
  - Mapping to ISO/IEC 29151 (Code of Practice for PII Protection)
  - Mapping to the General Data Protection Regulation (GDPR)

MW-07 IoT Security Management

1 DAY การบริหารจัดการความมั่นคงปลอดภัยของ Internet of Things (IoT)

- IoT Challenges
- IoT Security Model
- IoT Privacy Consideration
- IoT Security Assessment Checklist
- IoT Service and Endpoint Ecosystem

MW-08 Introduction to PCI DSS Implementation

1 DAY การพัฒนามาตรฐานความปลอดภัยของข้อมูลสำหรับอุตสาหกรรมที่เกี่ยวข้องกับบัตรชำระเงิน

- The Purpose of the PCI DSS and the Requirement for Protection of Cardholder Data
  - PCI DSS Objectives and Intention
  - Related PCI Standards and Programmers
- Understand How PCI DSS Compliance is Enforced by the Payment Brands
  - Compliance Needs for Merchants and Service Providers
  - Explanation of the Different Levels
- Understand How Compliance Must be Reported by Merchants and Service Providers
  - Overview of the 12 Standard Requirements
  - Scoping and Applicability of the PCI DSS
  - Technical Implementation of the Requirements
  - Maintaining Compliance

MW-09 Social Media Intelligence Analysis and Investigation

1 DAY เทคนิคการวิเคราะห์ข้อมูลสื่อสังคมออนไลน์

- Twitter Investigation and Intelligence
- Uncover and Discover Email Id from Name and Domain
- Identify LinkedIn Profile by using on Open Source Advance Search Intelligence
- OSINT for Pinterest
- Reddit Forensics Investigation and accumulate actionable Intelligence
- Instagram Forensics, Investigation, and Reconnaissance
- Perform Facebook Investigation and Forensics with Zero Cost
- Case Studies

MW-10 Implementing Cybersecurity Incident Handling and Response

1 DAY การจัดการและตอบสนองอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

- Introduction
- Preparation
- Identification
- What to Check?
- Containment
- Eradication
- Recovery
- Lessons Learned
- Meet, Fix, and Share
- Validation and Monitoring
- Preparation of People and Policy
- Where Does Identification Occur?
- Deployment and Categorization
- Short-term and Long-term Actions
- Restoring and Improving Defenses
- Blue Team Building and Management

MW-11 GDPR, Cybersecurity Law & Data Protection Law Update

1 DAY ตามติดกฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และ GDPR

- Overview of the Future Trend of Regulatory Compliance and Upcoming Thailand IT-related & Digital Laws
- Understanding the Differentiation and Relationship of Laws
  - Electronics Transaction Laws
  - Cybersecurity Laws
  - Data Protection Laws
  - Computer Crime Laws
- Key Matters of Cybersecurity Laws
- Key Matters of Data Protection Laws
- Key Matters of GDPR and Data Protection Laws

MW-12 Building Cyber Resilience for the Enterprises Hands-on Workshop

1 DAY สร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยไซเบอร์ผ่านการปฏิบัติจริง

- Risk-based Standards and Best Practices for Cybersecurity
- Understanding Cybersecurity/Cyber Resilience vs. Business Continuity
- Establishing Cybersecurity Framework
- Cybersecurity Risk Management
- Cybersecurity Incident Response
- Cybersecurity and Cyber Resilience Review (CRR)

MW-13 Data Governance Framework and Guidelines

2 DAYS กรอบธรรมาภิบาลของข้อมูลและแนวทางดำเนินการ

- 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 Governance
  - Data Architecture
  - Data Quality
  - Documents and Content
  - Data Security
  - Data Modeling and Design
  - Data Storage and Operations
  - Reference and Master Data
  - Data Warehousing and Business Intelligence
  - Data Integration and Interoperability

SOFTWARE DEVELOPMENT WORKSHOPS

สำหรับนักพัฒนาซอฟต์แวร์ และโปรแกรมเมอร์

SW-01 How to Securing RESTful API

1 DAY การสร้าง RESTful API อย่างไรให้ปลอดภัยจากการโจมตีในโลกไซเบอร์

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

SW-02 Understanding DevSecOps Foundations

1 DAY พื้นฐานสำหรับผู้ที่ต้องการเข้าใจกระบวนการ DevSecOps ที่จะทำให้ Software มีความปลอดภัยสูงสุด

- Intro to DevSecOps
- Continuous Integration
- Docker and Deployment
- Continuous Deployment
- Automated Security Testing

SW-03 How to Secure Your Container

1 DAY หลักสูตรการรักษาความปลอดภัยให้กับ Container

- OWASP Docker TOP 10
- How to secure your container
- Setup Docker private registry
- How to monitoring your container

SW-04 Automated Security Testing

2 DAYS หลักสูตรการทดสอบความปลอดภัยแบบอัตโนมัติ

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

SW-05 Agile Application Security

2 DAYS หลักสูตรการผลิตซอฟต์แวร์ที่มีความปลอดภัยด้วย Agile

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

IT AUDIT WORKSHOPS

สำหรับผู้ตรวจสอบระบบเทคโนยีสารสนเทศ

AW-01 IT Audit for Non-IT Auditor

1 DAY การตรวจสอบระบบเทคโนโลยีสารสนเทศสำหรับบุคลากรด้านไอทีและผู้สนใจทั่วไป

- บทบาทหน้าที่ของ IT Auditor (Role and Responsibilities of IT Audit)
- มาตรฐานสำหรับการทำงานของ IT Audit (IT Audit standards and Best practices)
- กระบวนการทำงานของ IT Audit (IT Audit process)
- ใบรับรองคุณวุฒิด้าน IT Audit และเส้นทางสายอาชีพ IT Audit (IT Audit certification and career path)

AW-02 IT General Controls Audit

2 DAYS การตรวจสอบเรื่องการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ

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

IT TECHNICAL & PROFESSIONAL WORKSHOPS

สำหรับผู้จัดการและผู้ปฏิบัติงานด้านระบบเครือข่าย ระบบปฏิบัติการ เทคโนโลยีสารสนเทศ
ความมั่นคงปลอดภัยสารสนเทศและผู้สนใจด้านเทคนิคขั้นสูง

TW-01 Introduction to Hacking Smart Contracts

1 DAY การตรวจสอบและแนวทางป้องกันการเจาะสมาร์ทคอนแทรค แพล็ตฟอร์ม

- Reentrancy
- Integer Underflows/Overflows
- Predictable Randomness
- Insecure Authorization
- Denial of Service
- Unchecked Low Level Function Calls
- Understanding and Constructing an ABI
- Identifying and Avoiding Client-Side Protections
- Code Reviewing Solidity Projects for Vulnerabilities
- Communicating with a Smart Contracts Directly Using a Tool Like MyEtherWallet
- Writing and Deploying Attack Contracts Written in Solidity on the Test Network

TW-02 Basic Mobile Application Penetration Testing for Android

2 DAYS การทดสอบเจาะระบบปฏิบัติการแอนดรอยด์เบื้องต้น

- Overview Architecture & Attack Vector
- Reversing APK
- Static Analysis
- Dynamic Analysis

TW-03 Basic Web Application Penetration Testing

2 DAYS การทดสอบเจาะระบบผ่านเว็บแอพพลิเคชั่นเบื้องต้น

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

TW-04 Internet of Things (IoT) Penetration Testing

2 DAYS การเจาะระบบอุปกรณ์ Internet of Things (IoT) ขั้นสูง

- Introduction to IoT
- Hardware Analysis
- Firmware Analysis
- Exploitation
- Mobile Application Hacking
- Radio Hacking

TW-05 Active Directory Attacks

2 DAYS 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-06 Adaptive Network-based Infrastructure Attacking

3 DAYS เทคนิคและการทดสอบเจาะระบบเครือข่าย

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

TW-07 Introduction to Data Science & Big Data Analytics Software Development

3 DAYS การพัฒนาโปรแกรมสำหรับ Data Science และ การวิเคราะห์ Big Data

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

TW-08 Introduction to Blockchain and Smart Contract Development with Ethereum

3 DAYS การพัฒนา Blockchain และ Smart Contract ด้วย Ethereum

- Introduction to Cryptocurrency & Blockchain Technology
- Introduction to Ethereum (Blockchain 2.0) Platform
- Basic of Ethereum Blockchain Development
- Smart Contract Programming with Solidity
- Smart contract Applications
- DApp Development with Truffle Framework

TW-09 Introduction to AI and Deep Learning with Python and TensorFlow

3 DAYS ทำความเข้าใจ AI และ Deep Learning ด้วย Python และ TensorFlow

- Introduction to TensorFlow
- Using Estimator
- Basic Components
- Tensor Operations
- CNN network variations
- Image recognition with predictive model
- TensorFlow model development related concepts
- Predictive model development with Tensorflow
- Introduction to Artificial Neural Network (ANN)
- Convolutional Neural Network (CNN)