ภาคปฏิบัติ

CDIC2024 CYBERSECURITY WORKSHOPS

ภาคปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 41 หัวข้อ

DIGITAL AND CYBERSECURITY MANAGEMENT WORKSHOPS

หลักสูตรด้านการบริหารจัดการเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์

MW-01 | 1 DAY | Implementing AI Policy to Support Business Operations Effectively

หลักสูตรแนวทางการจัดทำนโยบายการใช้งาน AI มาช่วยสนับสนุนการดำเนินงานทางธุรกิจอย่างเหมาะสม

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

MW-02 | 1 DAY | Implementing AI System Impact Assessment and Risk Assessment for Artificial Intelligence Management System

หลักสูตรการประเมินผลกระทบและการประเมินความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน

- หลักการพื้นฐานของปัญญาประดิษฐ์
- มาตรฐานที่เกี่ยวข้องกับการประเมินผลกระทบ และการประเมินความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน
- แนวทางการบริหารความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน
- ความแตกต่างระหว่างการประเมินความเสี่ยงและการประเมินผลกระทบสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน และความเชื่อมโยงกับการประเมินผลกระทบอื่น ๆ เช่นการทำ DPIA
- หลักการ ขั้นตอน และแนวทางดำเนินการ สำหรับการประเมินผลกระทบสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน
- กรณีศึกษาสำหรับการประเมินผลกระทบ และการประเมินความเสี่ยงสำหรับการนำระบบปัญญาประดิษฐ์มาใช้งาน

MW-03 | 1 DAY | Implementing AI Management System Based on ISO/IEC 42001:2023

หลักสูตรการพัฒนาระบบบริหารจัดการเทคโนโลยีปัญญาประดิษฐ์ให้สอดคล้องกับมาตรฐานสากล ISO/IEC 42001:2023

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

MW-04 | 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-05 | 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
- การใช้มาตรการควบคุมทดแทนและมาตรการควบคุมที่ปรับแต่ง เพื่อให้การดำเนินงานสอดคล้องกับมาตรฐาน PCI DSS
- การเตรียมการเพื่อ Implement Controls ตามข้อกำหนดของ PCI DSS เวอร์ชัน 4.0.1 อย่างเต็มรูปแบบ

MW-06 | 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 ข้อบังคับเกี่ยวกับธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล
- ภาพรวมของแนวทางและแนวปฏิบัติที่ดีสำหรับการบริหารจัดการข้อมูลที่นำมาใช้ในการดำเนินการ
- แนวทางการบริหารจัดการข้อมูลในองค์กร

MW-07 | 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-08 | 1 DAY | Preparedness Guide for Cybersecurity Audit in Action (Alignment with Cybersecurity Compliance, Standards & Best Practices)

หลักสูตรแนวทางการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์สอดคล้องตามกฎหมายลำดับรองของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

- ภาพรวมการรักษาความมั่นคงปลอดภัยไซเบอร์และข้อกำหนดแนวทางการตรวจสอบ
- เกี่ยวกับการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
- หลักการและกระบวนการสำหรับการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
- การกำหนดวัตถุประสงค์และขอบเขตการตรวจสอบ
- การพิจารณาประเด็นความเสี่ยง ภัยคุกคาม และองค์ประกอบ
- แนวทางการตรวจสอบด้านกระบวนการและด้านเทคนิค
- การสรุปผลและการรายงานผลการตรวจสอบ

MW-09 — 1 DAY
Implementing Cybersecurity Control Baseline to Comply with Cybersecurity Act

หลักสูตรการจัดทำมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

- ทำความเข้าใจกฎหมายลำดับรองที่เกี่ยวข้องกับการจัดทำมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
- การจัดระดับผลกระทบของข้อมูลหรือสารสนเทศให้สอดคล้องกับกฎหมายลำดับรอง
- การประยุกต์ใช้แนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ

MW-10 — 1 DAY
Enhancing Organizational Integrity : The Role of Data Governance and Resilience in Establishing and Implementing Digital Trust

หลักสูตรกระบวนการสร้างความเชื่อมั่นทางดิจิทัลขององค์กร : การนำ Digital Trust Framework มาใช้จริงในองค์กร

- Enhancing the Digital Trust Model: Latest Updates from WEF and ISACA
- Strengthening Organizational Data Strategies: Core Principles of Governance and Resilience
- Navigating the Digital Landscape: Strategies for Mitigating 7 Critical Digital Risks
- Practical Steps for Implementing Effective Data Governance and Resilience in Your Organization

MW-11 — 1 DAY
Mastering Digital Risk: Strategies to Uncover and Manage Unseen Threats in Digital Business

หลักสูตรการจัดการความเสี่ยงทางดิจิทัล: กลยุทธ์ในการค้นหาและจัดการภัยคุกคามที่ซ่อนเร้นในธุรกิจดิจิทัล

- Understanding the 'Unknown Unknowns': Strategies for Revealing Hidden Risks in Digital Business
- Comprehensive Risk Management: Addressing Key Technology, Cybersecurity, Privacy, and Compliance Threats
- Leveraging Standards and Best Practices: A Guide to Industry-Recognized Frameworks for Risk Management
- Building an Integrated Digital Risk Management Framework: Processes and Best Practices
- Exploring the Spectrum of Digital Risks: Key Categories and Implications
- Actionable Risk Mitigation: Strategies to Safeguard and Strengthen Your Business

MW-12 — 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

MW-13 — 1 DAY
Preparedness Guide for Organizational Resilience and Business Continuity in Action (Alignment with Standards and Best Practices)

การพัฒนาและดำเนินการเกี่ยวกับความยืดหยุ่นขององค์กรและความต่อเนื่องทางธุรกิจตามมาตรฐานและแนวทางปฏิบัติที่ดี

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

IT PROFESSIONAL AND TECHNICAL WORKSHOPS
หลักสูตรด้านเทคนิคขั้นสูงและเทคโนโลยีสารสนเทศ

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

หลักสูตรเทคนิคและการทดสอบเจาะระบบเครือข่าย

- TCP/IP Fundamental
- The Art of Spoofing & Port Scanning
- Metasploit Basics
- Foot-printing & Enumeration Target
- Network Enumeration
- Post Exploitation: Dumping Secrets
- Gaining Access Through Network Exploitation
- Escalation of Access
- Client-Side Attack
- Social Engineering Attack
- Hacking Recent Linux Vulnerabilities
- Hacking Recent Windows Vulnerabilities
- Password Cracking & Brute-Forcing
- 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

หลักสูตรคู่มือสำหรับผู้เริ่มต้นในการเป็นผู้เชี่ยวชาญด้านความปลอดภัยระบบคลาวด์

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

TW-04 — 1 DAY
Advanced 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 — AWS Cloud Security Best Practices

3 DAYS

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 — Web Application Penetration Testing: Techniques and Tools

3 DAYS

หลักสูตรการทดสอบเจาะระบบผ่านเว็บแอปพลิเคชัน

- Penetration Testing Process
- Introduction to Web Applications
- OWASP TOP 10
- Cross Site Scripting
- SQL Injection
- Broken Access Control
- Other Attacks
- Broken Authentication

TW-07 — Mobile Application Penetration Testing: Techniques and Tools

2 DAYS

หลักสูตรการทดสอบเจาะระบบผ่านโมบายแอปพลิเคชัน

- 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

TW-08 — Active Directory Penetration Testing: Techniques and Tools

2 DAYS

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-09 — Scripting for Penetration Tester

2 DAYS

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-10 — Intelligence and Scenario-Based Penetration Testing

3 DAYS

หลักสูตรการทดสอบเจาะระบบเชิงสถานการณ์จริง

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

TW-11 — Threat Modeling in Action: Real World Applications

2 DAYS

หลักสูตรอบรมการสร้าง Threat Model เชิงปฏิบัติ

- Security Design Principles
- Threat Modeling Methodology
- Define Business and Technical Scope
- Application Decomposition
- Vulnerability and Weakness Analysis
- Risk Handling

TW-12 — Threat Intelligence Implementation and Analysis

2 DAYS

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 — Incident Response and Handling Techniques and Tools

2 DAYS

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 — Malware Analysis Techniques and Tools

2 DAYS

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

ภาคปฏิบัติ

CDIC2024 CYBERSECURITY WORKSHOPS

ภาคปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 41 หัวข้อ

IT PROFESSIONAL AND TECHNICAL WORKSHOPS

หลักสูตรด้านเทคนิคขั้นสูงและเทคโนโลยีสารสนเทศ

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 (3 DAYS) Using IoT Platform and Build IoT Server to Suit the Organization

หลักสูตรการใช้งาน IoT Platform และการสร้าง IoT Server ให้เหมาะสมกับองค์กร

- เรียนรู้และเข้าใจโครงสร้างของระบบ Internet of Things
- การประยุกต์ใช้งาน Internet of Things ในแอปพลิเคชันต่าง ๆ
- ความแตกต่างระหว่างการใช้งาน IoT Platform และ IoT Server
- รู้จัก IoT Platform ในประเทศไทย และต่างประเทศ
- ความสำคัญของข้อมูลบนระบบ Internet of Things
- ความปลอดภัยในส่วนต่าง ๆของระบบ Internet of Things
- เรียนรู้องค์ประกอบต่าง ๆของระบบ Internet of Things
- ติดตั้งและตั้งค่า OS ให้เหมาะสมกับ IoT Server
- เรียนรู้การสร้าง และออกแบบ IoT Protocol บนระบบ IoT
- ทดสอบการรับข้อมูลผ่าน IoT Protocol จากอุปกรณ์ IoT
- เรียนรู้การสร้าง และออกแบบระบบ Data Collector
- เรียนรู้และเข้าใจโครงสร้างของ Database ในระบบ IoT
- ติดตั้ง ตั้งค่า และใช้งาน Database บน Server
- เรียนรู้การสร้าง Dashboard Application บน IoT Server
- เรียนรู้การสร้าง Notify Application บน IoT Server

TW-17 (1 DAY) Generative AI for Cyber Investigations: Techniques and Tools

หลักสูตรการใช้ Generative AI ในงาน Cyber Investigation

- ทำความรู้จักกับ Generative AI ในภาพรวม
- การเขียน Prompt สำหรับสั่งงาน Generative AI
- ทำความรู้จักกับ Generative AI ประเภทต่าง ๆ
- 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

TW-18 (1 DAY) Python Data Analytics for Fraud Detection: Techniques and Tools

หลักสูตรการใช้ Python ในงาน Data Analytics สำหรับการตรวจจับการทุจริต

- ความสำคัญของการทำ Fraud Detection ในองค์กร
- ทำความรู้จักกับ Python เบื้องต้น
- วิธีการ Setup Python ผ่าน Google Colab
- การเขียน Python ในลักษณะต่าง ๆ 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-19 (1 DAY) Fraud Detection using Machine Learning with Python

หลักสูตรการใช้ Machine Learning ในงาน Fraud Detection ด้วย Python

- ความสำคัญของการทำ Fraud Detection using Machine Learning ในองค์กร
- ทำความรู้จักกับ Python เบื้องต้น
- วิธีการ Setup Python ผ่าน Google Colab
- การเขียน Python ในลักษณะต่าง ๆ ขั้นพื้นฐาน
- ทำความรู้จัก Machine Learning
- ขั้นตอนการทำ Fraud Detection using Machine Learning
- การใช้งานเครื่องมือ (Library) Python ในงานวิเคราะห์ข้อมูล (Data Analytics) และงาน Machine Learning
- การทำความสะอาดข้อมูล (Data Cleaning) และแสดงข้อมูลเป็นรูปภาพ (Data Visualization) ด้วย Python
- การสร้าง Machine Learning Model สำหรับทำ Fraud Detection และการวัดผล Machine Learning Model
- Use Case Fraud Detection using Machine Learning
- Workshop Fraud Detection using Machine Learning with Python
- แถม: ตัวอย่างชุดข้อมูล (Dataset) สำหรับทำ Fraud Detection using Machine Learning with Python
- ใช้ Python ผ่าน Google Colab

TW-20 (1 DAY) Top 10 Machine Learning Security Risks

หลักสูตรอบรมเกี่ยวกับความเสี่ยงบน Machine Learning ที่ต้องรู้จัก

- Input Manipulation Attack
- Data Poisoning Attack
- Model Inversion Attack
- Membership Inference Attack
- Model Theft
- AI Supply Chain Attacks
- Transfer Learning Attack
- Model Skewing
- Output Integrity Attack
- Model Poisoning

PDPA AND DATA MANAGEMENT WORKSHOPS

หลักสูตรด้านการจัดการข้อมูลและ
การคุ้มครองข้อมูลส่วนบุคคล

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 — 3 DAYS — Secure CI/CD Pipeline

หลักสูตรเครื่องมือที่ต้องใช้ในการทำ Continuous Delivery

- Secure Software Development Life Cycle (SSDLC)
- Principles of DevOps
- Continuous Integration
- Continuous Deployment
- Modern CI/CD Pipeline
- Managing test Results
- Automated Security Testing with Newman
- Automated Security Testing with OWASP ZAP
- Manage Dependencies with Dependency Check
- Continuous Compliance with Chef Inspec

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

SW-04 — 2 DAYS — Automated Security Testing

หลักสูตรอบรมการทดสอบความปลอดภัยแบบอัตโนมัติ

- Introduction to ASVS 4.0
- Static Application Security Testing with SonarQube
- Dynamic Analysis Security Testing with Postman
- Dynamic Analysis Security Testing with OWASP ZAP
- Software Bill of Material(SBOM)
- Generating SBOM with Syft
- Vulnerability Scanning with Grype

TW-21 — 1 DAY — Addressing the Challenges of Generative AI: Uncovering Risks and Developing Effective Mitigation Strategies

หลักสูตรจัดการกับด้านมืดของ Generative AI: เปิดความเสี่ยงและพัฒนากลยุทธ์ในการแก้ไขปัญหาอย่างมีประสิทธิภาพ

- Exploring Generative AI: From Creative Applications to Future Impacts
- Navigating the Ethical and Societal Implications of Generative AI
- Ensuring Fairness in AI: Tackling Bias and Promoting Equity
- Addressing Misinformation and Privacy Concerns in Generative AI
- Implementing Responsible AI Practices: Mitigation Strategies and Regulatory Considerations

CDIC2024 SPONSORS

ROYAL CROWN

Microsoft
Bitdefender
EC-Council
Building A Culture Of Security
iCms Cyber Solution
YIP IN TSOI
nForce Secure
CLAROTY

DIAMOND

THALES
Building a future we can all trust
Netone
CISCO
netka
ManageEngine
SecureD
MAYASEVEN
HACK THINGS
imperva
a Thales company

PLATINUM

Bangkok Systems
SONICWALL
OffSec
The Path to a Secure Future
TÜVNORD
getGn
TECHNOLOGY
SOSECURE
PARASOFT
Automated Software Testing
BMSP bmsp.tech
Akamai
Managed / Provided by BMSP bmsp.tech
Akamai
securonix
Hitachi Vantara
securonix
Managed / Provided by BMSP bmsp.tech
FUSION ADVANTEC

GOLD

AXGATE
Security and Beyond
CompTIA
TKC
IPPS
IP PAYMENT SOLUTIONS
CYFIRMA
DECODING THREATS
MM7
Multimedia Technology

SILVER

MST
Magic Software Thailand
IT Solutions to Improve Your Efficiency
FAST
Fraud Analytic & Automated Solution Technology
Protecting Trust, Preventing Fraud
NTT-TX
iDoperation
Simplify Management of Privileged Access
PRO ONE
AMICABLE BRIDGE
netskope
IIJ Global
BUREAU VERITAS
weborion
by cloudsine
wizlynx group
Your Cyber Security Partner worldwide
SILVERFORT
V-KEY
STRONGER WITH V-OS

PARTNER

NCSA สกมช
pdpc สคส.
TPQI
สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย
The Institute of Internal Auditors of Thailand
AiSP
Association of Information Security Professionals
INTELLIGENCE DATA ANALYTIC
CYBERTRON
CYNIUS
CYBERTECH & CONSULTING
XCION

CO-HOST

สวทช NSTDA
SOFTWARE PARK THAILAND
ISACA
Bangkok Chapter
ACIS
TISA
CIO
Thai CIO Association
ISC2