

# ITD62-332 ความมั่นคงไซเบอร์

## *(Cybersecurity)*

ภาคการศึกษา 2/2568 — 3(2-2-5)

ผู้สอน: ผู้ช่วยศาสตราจารย์ ดร.ชนันท์ภรณ์ จันแดง

หลักสูตรรณวัตกรรมการสารสนเทศทางการแพทย์ / IT และนวัตกรรมดิจิทัล

# 1. รหัสและชื่อรายวิชา

ภาษาไทย: ITD62-332 ความมั่นคงไซเบอร์

ภาษาอังกฤษ: Cybersecurity

จำนวนหน่วยกิต: 3(2-2-5)

- บรรยาย 2 ชม.
- ปฏิบัติการ 2 ชม.
- ศึกษาค้นคว้า 5 ชม.

## 2. รายวิชาในหลักสูตร

อยู่ในหมวด  
โครงสร้างพื้นฐานของระบบ (System Infrastructure)  
สำหรับ 2 หลักสูตร

- นวัตกรรมสารสนเทศทางการแพทย์
- เทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

### 3. ผู้สอนและภาคที่เปิดสอน

ผู้ประสานงาน/ผู้สอน:

ผู้ช่วยศาสตราจารย์ ดร.ชนันท์ภรณ์ จันแดง

ภาคการศึกษา: 2

รายวิชาที่ต้องเรียนมาก่อน: ITD62-231 เทคโนโลยีอินเทอร์เน็ต

เรียนพร้อมกัน: ไม่มี

## 4. คำอธิบายรายวิชา

ศึกษาหลักการความมั่นคงไซเบอร์ ภัยคุกคาม ช่องโหว่ การวิเคราะห์ทราฟฟิกเครือข่าย การใช้เครื่องมือด้านความมั่นคงไซเบอร์ การจัดการบันทึกเหตุการณ์ การตรวจจับการบุกรุก รวมถึงการใช้เทคนิคปัญญาประดิษฐ์เพื่อตรวจจับความผิดปกติเชิงลึก มุ่งพัฒนาทักษะการคิดวิเคราะห์และจริยธรรมวิชาชีพด้านไซเบอร์

## 5. ผลการเรียนรู้ของรายวิชา (CLOs)

### ด้านความรู้

- CLO1: อธิบายหลักการพื้นฐานความมั่นคงไซเบอร์และภัยคุกคาม
- CLO2: อธิบายโปรโตคอลเครือข่ายและมาตรฐานความมั่นคงไซเบอร์

### ด้านทักษะ

- CLO3: วิเคราะห์กราฟฟิกระบบเครือข่ายและระบุพฤติกรรมผิดปกติ
- CLO4: ใช้ Wireshark, Suricata, Firewall, Log Tools
- CLO5: พัฒนา ML Model เพื่อตรวจจับมัลแวร์/ความผิดปกติ

### ด้านคุณธรรม

- CLO6: ปฏิบัติงานภายใต้กฎหมายและจริยธรรมไซเบอร์

## 6. แผนการสอน 12 สัปดาห์ (Integrated Plan)

Week	Full Topic Title	Lecture	Workshop / Lab	Assessment
1	Introduction to Cybersecurity and Fundamental Conceptual Frameworks	CIA/DAD Principles, Threat–Vulnerability, Security as Asset Protection	Analysis of real cyberattack scenarios	Quiz + Report
2	Network and Protocol Fundamentals: Architecture, Operations, and Vulnerability	IP, Subnetting, OSI/TCP-IP, Protocol Weaknesses	Packet Flow Analysis	Worksheet

## 7. วิธีประเมินผล

รายการประเมิน	สัดส่วน	รายละเอียด
แบบทดสอบ/แบบฝึกหัด	20%	ทฤษฎีและวิเคราะห์ภัยคุกคาม
งานปฏิบัติการ (Labs)	30%	Wireshark, IDS, ML Detection
งานวิเคราะห์/รายงาน	20%	Log Analysis, Attack Investigation
สอบกลางภาค	10%	ทฤษฎีความมั่นคงไซเบอร์
สอบปลายภาค	20%	Practical + Written



## 8. มาตรการจัดการเรียนรู้

- บรรยายเชิงวิเคราะห์
- ทดลองปฏิบัติการ
- วิเคราะห์เหตุการณ์จริง
- Workshop และ Coding Lab
- Case-based Learning
- Ethical Discussion

## 9. Learning Resources

- เอกสารประกอบการสอน
- Wireshark, Suricata, FastAPI, ReactJS
- Packet Tracer, Python (pandas, scikit-learn)
- ISO 27001, NIST 800-series
- CERT Incident Reports

