ใบงานที่ 1

Six Thinking Hats กับกรณีศึกษา

“ระบบเวชระเบียน ศูนย์การแพทย์ มหาวิทยาลัยวลัยลักษณ์”

รายวิชา: Introduction to Cybersecurity
หลังเรียน: Chapter 1 – Introduction to Cybersecurity
(CIA, DAD, AAA, Threat, Vulnerability, Cybersecurity Domains, Network Monitoring)

1. วัตถุประสงค์ของกิจกรรม

เมื่อจบกิจกรรมนี้ นักศึกษาควรสามารถ

1. นำความรู้จากบทที่ 1 มาประยุกต์ใช้กับกรณีศึกษา
   ระบบเวชระเบียน ศูนย์การแพทย์ มหาวิทยาลัยวลัยลักษณ์ ได้แก่
   - ระบุ **Asset / Scope of protection** ของระบบเวชระเบียน
   - ใช้กรอบ **CIA Triad – DAD Triad** วิเคราะห์ผลกระทบเชิงความมั่นคงปลอดภัย
   - อธิบายบทบาทของ **AAA Model** ในการควบคุมการเข้าถึงและการติดตามการใช้งาน
   - แยกแยะ **Threat / Vulnerability / Risk** ที่เกี่ยวข้อง
   - เชื่อมโยงกับ **Cybersecurity Domains** ที่เกี่ยวข้อง
     (เช่น Network Security, Information Security, GRC, Incident Response ฯลฯ)

1. วัตถุประสงค์ของกิจกรรม (ต่อ)

2. ใช้กรอบ **Six Thinking Hats**
   เพื่อช่วยคิดอย่างเป็นระบบ จากหลายมุมมองทั้งเทคนิค จริยธรรม และเชิงนโยบาย

3. ทำงานกลุ่มแบบหมุนเวียน
   แลกเปลี่ยนและต่อยอดแนวคิดจากกลุ่มอื่นได้อย่างมีเหตุผล

4. สรุปประเด็นเชิงวิชาการ
   และนำเสนอภาพรวมต่อชั้นเรียนภายในเวลาที่กำหนด

2. กรณีศึกษา

ระบบเวชระเบียนในมุมมอง Cybersecurity

ให้ถือว่า **“ระบบเวชระเบียน ศูนย์การแพทย์ มหาวิทยาลัยวลัยลักษณ์”**
เป็น **Critical Information System** ระบบหนึ่งขององค์กรด้านสาธารณสุข ซึ่งครอบคลุม

- **ข้อมูล (Data):**
  ข้อมูลระบุตัวตนผู้ป่วย, ประวัติการรักษา, การวินิจฉัยโรค, ผลตรวจห้องปฏิบัติการ, ภาพถ่ายทางการแพทย์, การสั่งยา, ประวัติการแพ้ยา, ข้อมูลนัดหมาย ฯลฯ
- **ผู้ใช้ (Users):**
  แพทย์, พยาบาล, เภสัชกร, เจ้าหน้าที่เวชระเบียน, บุคลากร IT, ผู้บริหารโรงพยาบาล, หน่วยงานภายนอกที่ได้รับอนุญาตให้เข้าถึงข้อมูล ฯลฯ

2. กรณีศึกษา – ขอบเขตระบบเวชระเบียน

- **บริการหลัก (Services):**
  - บันทึกและเรียกดูเวชระเบียนอิเล็กทรอนิกส์ (EMR/EHR)
  - การสั่งยาและการสั่งตรวจ (CPOE)
  - การนัดหมายและติดตามผู้ป่วย
  - การออกรายงานทางสถิติและคุณภาพบริการ
  - การแลกเปลี่ยนข้อมูลกับระบบอื่น (Lab, PACS, Billing ฯลฯ)

ให้นักศึกษานำกรอบคิดจากบทเรียนมาใช้ เช่น

- **CIA vs DAD:**
  - ระบบเวชระเบียนต้องปกป้องอะไร (CIA)
  - ผู้โจมตี/ผู้ไม่หวังดีอาจต้องการอะไร (DAD)

2. กรอบคิดที่ต้องใช้กับระบบเวชระเบียน

- **AAA:**
  - การยืนยันตัวตน (Authentication) ของบุคลากรทางการแพทย์
  - การกำหนดสิทธิ์ (Authorization) แยกตามบทบาท (Role)
  - การบันทึกการใช้งาน (Accounting) เพื่อรองรับการตรวจสอบย้อนหลัง
- **Threat & Vulnerability:**
  - ภัยคุกคามและช่องโหว่ที่น่ากังวลต่อข้อมูลสุขภาพส่วนบุคคล (PHI)

2. กรอบคิดที่ต้องใช้กับระบบเวชระเบียน

- **Cybersecurity Domains:**
  - โดเมนใดบ้างที่เกี่ยวข้องกับการออกแบบ/ป้องกันระบบเวชระเบียน
- **Network Monitoring:**
  - หากจะออกแบบระบบเฝ้าระวังเครือข่ายเพื่อคุ้มครองระบบเวชระเบียน
  - จะมองหาอะไรใน **traffic / log** เป็นพิเศษ

3. โครงสร้างการจัดกลุ่มและบทบาท

3.1 การแบ่งกลุ่ม

- แบ่งนักศึกษาออกเป็น **6 กลุ่ม** จำนวนสมาชิกใกล้เคียงกัน
- แต่ละกลุ่มเริ่มต้นนั่งที่ “โต๊ะ/จุด” ซึ่งแทน **หมวกความคิด** ดังนี้

โต๊ะ/จุด	หมวก	มุมมองหลัก (เชื่อมกับ Cybersecurity)
โต๊ะ 1	White Hat	ข้อเท็จจริง, Asset, Scope, Data flow ของระบบเวชระเบียน
โต๊ะ 2	Red Hat	ความรู้สึก/ความกังวลของผู้ป่วย/บุคลากร/ผู้บริหาร เมื่อระบบไม่ปลอดภัยหรือใช้งานไม่ได้

3. โครงสร้างการจัดกลุ่มและบทบาท

โต๊ะ/จุด	หมวก	มุมมองหลัก (เชื่อมกับ Cybersecurity)
โต๊ะ 3	Black Hat	ความเสี่ยง, ผลกระทบต่อ CIA, Threat–Vulnerability–Risk
โต๊ะ 4	Yellow Hat	ประโยชน์/โอกาสของระบบเวชระเบียนที่ออกแบบด้าน security และ privacy ดี
โต๊ะ 5	Green Hat	แนวคิดสร้างสรรค์: AAA / Network Monitoring / นโยบายใหม่ด้านความลับข้อมูลสุขภาพ
โต๊ะ 6	Blue Hat	มองภาพรวม: เชื่อม CIA–DAD–AAA–Domains เป็นสถาปัตยกรรมความมั่นคงปลอดภัยของระบบเวชระเบียน

3. โครงสร้างการจัดกลุ่มและบทบาท (ต่อ)

> **สำคัญ:**
>
> - หมวกผูกกับ “โต๊ะ” ไม่ใช่กับตัวคน
> - นักศึกษาจะหมุนโต๊ะไปเรื่อย ๆ
> - แต่ “โจทย์และบทบาทของโต๊ะนั้น” ยังคงเดิม

3. โครงสร้างการจัดกลุ่มและบทบาท (ต่อ)

3.2 บทบาทในแต่ละกลุ่ม

- **หัวหน้า (Group Leader)**
  - ดูแลเวลาในกลุ่ม (ภายในรอบ)
  - เปิดโอกาสให้ทุกคนแสดงความเห็น
- **เลขา (Secretary)**
  - จดบันทึก “ประเด็นสำคัญ” ลงในกระดาษ/แบบฟอร์มของโต๊ะ
  - **เลขาจะเป็นคนเดียวที่ “ไม่หมุนโต๊ะ”**

3.2 บทบาทในแต่ละกลุ่ม (ต่อ)

- **ผู้นำเสนอ (Presenter)**
  - รับผิดชอบนำเสนอประเด็นสรุปของโต๊ะ (ร่วมกับเลขาและสมาชิกโต๊ะสุดท้าย)
- **สมาชิกอื่น ๆ**
  - ร่วมคิด แสดงความคิดเห็น ขยายความ
  - เชื่อมโยงกับเนื้อหาในบทที่ 1 และบริบทด้านการแพทย์

4. โครงสร้างเวลาและการหมุนเวียนกลุ่ม

4.1 รอบการคิด (หมุนเวียน 6 รอบ)

นักศึกษาจะทำงานเป็น “รอบ” ดังนี้

รอบ	เวลา (นาที)	การดำเนินการ
1	8 นาที	กลุ่มแรกคิดตาม Hat ของโต๊ะ
2	7 นาที	หมุนซ้าย + กลุ่มใหม่ต่อยอดจากบันทึกเดิม
3	6 นาที	หมุนซ้าย + ต่อยอด
4	5 นาที	หมุนซ้าย + ต่อยอด
5	4 นาที	หมุนซ้าย + ต่อยอด
6	3 นาที	หมุนซ้าย + ต่อยอด

4. โครงสร้างเวลา (ต่อ)

หลังจบรอบที่ 6

- ให้เวลาแต่ละโต๊ะ/กลุ่ม **สรุปประเด็น**
- นำเสนอ **กลุ่มละ ~5 นาที**
- เวลาที่เหลือ
  - อาจารย์สรุปและเชื่อมโยงกับแนวคิด Cybersecurity ทั้งบท
  - เน้นประเด็นด้าน **ข้อมูลสุขภาพ (PHI)** และความเป็นส่วนตัวของผู้ป่วย

5. วิธีดำเนินกิจกรรมในแต่ละรอบ

รอบที่ 1 – เริ่มต้นที่หมวกของโต๊ะ (เวลา 8 นาที)

1. สมาชิกกลุ่มอ่าน “แนวทางคำถามของหมวก” (ดูหัวข้อที่ 6)
2. ใช้ความรู้จากบทที่ 1 วิเคราะห์ **ระบบเวชระเบียน** ตามมุมมองของหมวกนั้น
3. เลขาจดบันทึก **แบบ bullet** สั้น กระชับ
    - ให้คนอื่นอ่านต่อได้
4. พยายามอ้างอิงคำศัพท์วิชาการ เช่น
    - CIA, DAD, AAA, Threat, Vulnerability, Domain, Monitoring, PHI

5. วิธีดำเนินกิจกรรม – การหมุนกลุ่ม

การหมุนกลุ่ม (ก่อนรอบที่ 2–6)

เมื่ออาจารย์ให้สัญญาณ **“เปลี่ยนรอบ”**

1. **เลขาอยู่กับที่** ไม่หมุนโต๊ะ
2. สมาชิกคนอื่น (รวมหัวหน้า/ผู้นำเสนอ)
    - ลุกและ **หมุนไปทางซ้าย 1 โต๊ะ**

5. วิธีดำเนินกิจกรรม – บทบาทของกลุ่มใหม่

3. สมาชิกกลุ่มใหม่ที่มาถึงโต๊ะ
    - ฟังเลขาอธิบายว่า
        - รอบก่อน ๆ คิดอะไรไว้แล้ว
        - มีประเด็นสำคัญอะไร
        - และคำถามไหนที่ยังค้าง

5. วิธีดำเนินกิจกรรม – บทบาทของกลุ่มใหม่

- จากนั้นใช้เวลาที่เหลือในรอบเพื่อ
  - เพิ่มตัวอย่างใหม่
  - ขยายความ
  - เชื่อมโยงกับแนวคิด Cybersecurity เพิ่มเติม
    - เช่น เดิมพูดถึง “เวชระเบียนหาย/เข้าไม่ได้”
    - ให้ลองเชื่อมเป็น **Availability**, Threat, Domain ที่เกี่ยว ฯลฯ

> เวลาในแต่ละรอบจะลดลง: 7 → 6 → 5 → 4 → 3 นาที
> รอบหลัง ๆ ต้องอ่านเร็ว คิดเร็ว และต่อยอดตรงประเด็นมากขึ้น

6. แนวทางคำถามของแต่ละหมวก

(เชื่อมกับ Cybersecurity & Healthcare)

ให้นักศึกษาใช้คำถามเหล่านี้เป็น “ตัวช่วยคิด” ในแต่ละโต๊ะ

6.1 White Hat

ข้อมูลและข้อเท็จจริงเชิง Cybersecurity

โฟกัส: **Asset, Scope, CIA baseline, Data flow** ของระบบเวชระเบียน

- ระบบเวชระเบียนมี **สินทรัพย์ (Assets)** อะไรบ้างที่ต้องปกป้อง?
    - ข้อมูลผู้ป่วย, ประวัติการรักษา, ผล Lab, ภาพถ่ายทางการแพทย์, ประวัติการแพ้ยา ฯลฯ
- ขอบเขตการปกป้อง (**Scope of protection**) คืออะไรบ้าง?
    - ระบบ EMR/EHR, ฐานข้อมูล, เครือข่ายโรงพยาบาล, อุปกรณ์ปลายทาง (PC/Tablet/Workstation ในหอผู้ป่วย)

6.1 White Hat (ต่อ)

- ถ้ามองในกรอบ **CIA Triad** –
  ระบบเวชระเบียนควรให้ความสำคัญกับ C / I / A ในประเด็นใดบ้างเป็นพิเศษ?
    - โดยเฉพาะ **Confidentiality** ของข้อมูลผู้ป่วย
- ข้อมูลใดบ้างที่ถ้ารั่วไหล / ถูกแก้ไข / ใช้งานไม่ได้
  จะกระทบต่อผู้ป่วย, บุคลากรทางการแพทย์ และศูนย์การแพทย์อย่างมีนัยสำคัญ?

6.2 Red Hat

ความรู้สึกและภาพลักษณ์เมื่อเกิดปัญหา Security

โฟกัส: **ความรู้สึกของ Stakeholders เมื่อ CIA ถูกคุกคาม**

- ถ้าข้อมูลเวชระเบียน (เช่น การวินิจฉัยโรค, ผล Lab, ประวัติการรักษา) ถูก **Disclosure หรือ Alteration**
  - ผู้ป่วยจะรู้สึกอย่างไร?
  - แพทย์/พยาบาลจะรู้สึกอย่างไร?
  - ผู้บริหาร/สังคมจะมองศูนย์การแพทย์อย่างไร?

6.2 Red Hat (ต่อ)

- ถ้าระบบเวชระเบียนเข้าใช้งานไม่ได้ช่วงเวลาสำคัญ
  (**Availability ถูกทำลาย** เช่น ตอนผ่าตัด/ฉุกเฉิน)
    - เกิดความเครียด กดดัน หรือความไม่เชื่อมั่นในระบบบริการทางการแพทย์แค่ไหน?
- มี “ความกังวลเชิงภาพลักษณ์” (Reputation)
  หรือ “ความไม่ยุติธรรม” ต่อผู้ป่วย
  ที่เกี่ยวข้องกับ **Integrity** ของข้อมูลหรือไม่?

6.3 Black Hat

ความเสี่ยง, DAD, Threat–Vulnerability–Risk

โฟกัส: **มุมมองผู้โจมตี + ช่องโหว่ + ความเสี่ยง**

- จากมุมมอง **DAD Triad (Disclosure / Alteration / Destruction)**
  - ผู้โจมตีหรือผู้ไม่หวังดีอาจต้องการทำอะไรกับระบบเวชระเบียน?
    - ขโมยข้อมูลผู้ป่วย
    - แก้ไขเวชระเบียน
    - ทำลายข้อมูลเพื่อทำให้บริการหยุดชะงัก

6.3 Black Hat (ต่อ)

- ตัวอย่าง **Threat** ที่อาจเจอ เช่น
  - การเจาะระบบเพื่อดึงเวชระเบียนไปขายหรือแบล็กเมล์
  - การแก้ไขประวัติการแพ้ยา/โดสยา
  - การโจมตีให้ระบบล่มในห้องฉุกเฉิน
- ระบบเวชระเบียนอาจมี **Vulnerabilities** อะไรบ้าง? เช่น
  - ใช้ account ร่วมกัน, Password อ่อนแอ, ไม่มี MFA
  - เครื่องปลายทางในหอผู้ป่วยไม่ได้ล็อกหน้าจออัตโนมัติ
  - Patch/Update ระบบไม่ทันสมัย

6.3 Black Hat (ต่อ)

- เมื่อ Threat + Vulnerability รวมกันแล้ว
  กลายเป็น **Risk** อะไรที่ควรกังวลที่สุด?
    - เช่น เสี่ยงต่อการรักษาผิดพลาด, เสี่ยงต่อความเสียหายทางกฎหมาย, เสี่ยงต่อชื่อเสียงองค์กร

6.4 Yellow Hat

ด้านบวกและโอกาสจากการออกแบบระบบเวชระเบียนให้ Secure

โฟกัส: **โอกาสในการเสริม CIA / AAA / Monitoring และภาพรวมองค์กร**

- หากออกแบบระบบเวชระเบียนโดยคำนึงถึง **CIA + AAA** อย่างถูกต้อง
  - จะสร้างความเชื่อมั่นให้ผู้ป่วย/ญาติอย่างไร?
  - ช่วยให้บุคลากรทางการแพทย์ทำงานได้ปลอดภัยและมีประสิทธิภาพขึ้นอย่างไร?

6.4 Yellow Hat (ต่อ)

- ระบบที่มี **Accounting / Logging ดี** จะเป็นประโยชน์ต่อ
    - การทำ **Incident Response** และ **Forensics** เมื่อเกิดเหตุการณ์ละเมิดข้อมูลผู้ป่วย อย่างไร?
- มีโอกาสในการใช้ข้อมูลจากระบบเวชระเบียน ไปสนับสนุน **Governance, Risk, Compliance (GRC)** เช่น นโยบายการคุ้มครองข้อมูลสุขภาพ, การผ่านมาตรฐาน/การรับรองคุณภาพโรงพยาบาล อย่างไร?

6.5 Green Hat

ความคิดสร้างสรรค์ด้าน AAA และ Network Monitoring

โฟกัส: **มาตรการ/แนวทางใหม่ ๆ ที่ใช้ได้จริงในบริบทการแพทย์**

- จะออกแบบ **Authentication** อย่างไร
  ให้ปลอดภัยและไม่รบกวน workflow การรักษา?
    - เช่น Smart Card, MFA, Single Sign-On, Biometrics ในห้องฉุกเฉิน
- **Authorization** ที่ดีควรแยกสิทธิ์อย่างไรระหว่าง
    - แพทย์, พยาบาล, เภสัชกร, เจ้าหน้าที่เวชระเบียน, ผู้บริหาร ฯลฯ

6.5 Green Hat (ต่อ)

- จะใช้ **Accounting / Logging** แบบไหน
  ที่ช่วยให้ตรวจสอบเหตุการณ์ผิดปกติได้เร็วขึ้น?
    - เช่น Log การเข้าดูเวชระเบียนผู้ป่วยรายใดรายหนึ่งอย่างละเอียด
- ถ้าจะออกแบบ **Network Monitoring** เพื่อเฝ้าระวังระบบเวชระเบียน
    - จะเก็บ Log/Traffic อะไรบ้าง?
        - failed login ซ้ำ ๆ, การเข้าถึงเวชระเบียนจำนวนมากผิดปกติ, unusual outbound traffic ของข้อมูลเวชระเบียน ฯลฯ
    - จะตั้ง Alert Rule อย่างไรให้สอดคล้องกับ DAD?
        - เช่น ปริมาณการส่งออกข้อมูลผู้ป่วยจำนวนมากในเวลาสั้น ๆ = สงสัยว่าเป็น Disclosure

6.5 Green Hat (ต่อ)

- มีแนวคิดเชิงนโยบาย/มาตรการเสริมอะไรที่
  “สร้างสรรค์แต่สมเหตุสมผล” เช่น
  - แจ้งเตือนเจ้าของเวชระเบียน (ผู้ป่วย) เมื่อมีการเข้าดูข้อมูลจากหน่วยงานภายนอก
  - Dashboard สำหรับผู้บริหารดูสถานะด้าน Cybersecurity ของระบบเวชระเบียน ฯลฯ

6.6 Blue Hat

การรวมภาพใหญ่ของ Cybersecurity สำหรับระบบเวชระเบียน

โฟกัส: **สถาปัตยกรรมและการเชื่อมโยงกรอบคิดทั้งหมด**

- ถ้าต้องอธิบาย “สถาปัตยกรรมด้าน Cybersecurity ของระบบเวชระเบียน”
  - CIA อยู่ตรงไหนบ้างในระบบ?
  - DAD ของผู้โจมตีจะชนกับกลไกป้องกันตรงไหน?
  - AAA ทำงานอย่างไรตั้งแต่ login จนถึงการออกจากระบบ?

6.6 Blue Hat (ต่อ)

- ระบบเวชระเบียนเกี่ยวข้องกับ **Cybersecurity Domains** ใดบ้าง? เช่น
    - Network Security / Application Security /Information Security (PHI Protection) /Incident Response & Forensics / GRC ฯลฯ
- ถ้าเกิดเหตุการณ์โจมตีจริง (เช่น ข้อมูลผู้ป่วยรั่วไหล/เวชระเบียนถูกแก้ไข)
    - ขั้นตอนของ **Incident Response** คร่าว ๆ ควรเป็นอย่างไร?
- ภาพรวมทั้งหมดนี้สนับสนุนอะไร
  ต่อเป้าหมายของศูนย์การแพทย์ในฐานะ
  องค์กรสาธารณสุขดิจิทัลที่มั่นคงปลอดภัย?

7. การสรุปและการนำเสนอ

หลังจบรอบที่ 6

1. สมาชิกที่อยู่ประจำโต๊ะในรอบสุดท้าย ร่วมกับเลขา
    - ทบทวนบันทึกจากทุกกลุ่มที่เคยผ่านโต๊ะนี้
    - จัดหมวดหมู่และเลือก “ประเด็นสำคัญ”
      ที่สะท้อนแนวคิด Cybersecurity ในบริบทเวชระเบียนอย่างชัดเจน
2. เตรียมการนำเสนอ (ประมาณ **5 นาที/โต๊ะ**)
    - ระบุหมวก/มุมมองของโต๊ะ
      (White / Red / Black / Yellow / Green / Blue)

7. การสรุปและการนำเสนอ (ต่อ)

- สรุปประเด็นหลักที่เกี่ยวกับ
  ระบบเวชระเบียน ศูนย์การแพทย์ มวล.
  โดยเชื่อมกับ

  CIA – DAD – AAA – Threat – Vulnerability – Domains – Monitoring

  เท่าที่เหมาะสมกับหมวกของตน

3. หลังการนำเสนอของทุกโต๊ะ
   - อาจารย์จะสรุปภาพรวมและเชื่อมโยงเข้ากับเนื้อหาบทที่ 1
   - อธิบายว่ากรอบคิดเหล่านี้สำคัญอย่างไรต่อการออกแบบ **Healthcare Information Systems** ที่มั่นคงปลอดภัย

8. แบบประเมิน (Rubric) – รวม 10 คะแนน

ด้านประเมิน	2 คะแนน	1 คะแนน	0 คะแนน
1. การประยุกต์แนวคิด Cybersecurity (CIA, DAD, AAA, Threat/Vuln/Risk, Domains)	เชื่อมโยงแนวคิดได้ชัดเจน ถูกต้อง และมีตัวอย่างระบุชัด (เช่น ระบุ CIA/DAD/AAA/Threat/Vuln/Risk หรือ Domains ที่เกี่ยวข้องกับระบบเวชระเบียนอย่างน้อย 2 เรื่องขึ้นไป)	นำแนวคิดมาใช้บ้าง แต่ยังไม่ครบ/ยังไม่ชัด (มีการอ้างถึงแต่ยังไม่ลึก หรือมีบางส่วนคลาดเคลื่อน)	แทบไม่เห็นการใช้แนวคิดจากบทเรียน หรือใช้ผิดอย่างมีนัยสำคัญ

8. แบบประเมิน (Rubric) – ต่อ

ด้านประเมิน	2 คะแนน	1 คะแนน	0 คะแนน
2. คุณภาพการวิเคราะห์กรณีศึกษา	วิเคราะห์ปัญหา/ผลกระทบ/สาเหตุได้เป็นระบบ มีเหตุผลรองรับชัดเจน เชื่อมโยงกับบริบทศูนย์การแพทย์และผู้ป่วย	มีการวิเคราะห์ แต่ยังตื้น/กระโดดสรุป เหตุผลยังไม่ชัด หรือหลงไปที่รายละเอียดไม่สำคัญ	วิเคราะห์ผิวเผิน สรุปแบบท่องจำ หรือไม่สอดคล้องกับโจทย์
3. การใช้กรอบ Six Thinking Hats	เนื้อหาที่สรุปสอดคล้องกับหมวกของโต๊ะอย่างชัดเจน มีการต่อยอดจากกลุ่มก่อนหน้า (ไม่ใช่เขียนซ้ำ)	มีใช้กรอบ Six Hats แต่ยังปน/หลุดบทบาทบางส่วน หรือยังไม่ค่อยต่อยอดจากสิ่งที่กลุ่มก่อนหน้าเขียน	ไม่สนใจกรอบหมวก / เขียนแบบทั่วไป ไม่สอดคล้องกับบทบาทของโต๊ะ

8. แบบประเมิน (Rubric) – ต่อ

ด้านประเมิน	2 คะแนน	1 คะแนน	0 คะแนน
4. การสังเคราะห์และการนำเสนอ	สรุปประเด็นได้ชัดเจน กระชับ เป็นลำดับ (ปัญหา → วิเคราะห์ → ข้อเสนอด้าน security) นำเสนอภายในเวลาที่กำหนด ใช้ศัพท์วิชาการเหมาะสม	มีการสรุปและนำเสนอ แต่ลำดับยังไม่ชัด/เยิ่นเย้อ หรือเลยเวลาเล็กน้อย ใช้ศัพท์วิชาการปนภาษาพูดมาก	นำเสนอไม่ชัดเจน สรุปประเด็นไม่ได้/อ่านจากกระดาษอย่างเดียว จัดเวลาไม่เหมาะสม
5. การทำงานเป็นทีมและมีส่วนร่วม	เห็นการแบ่งบทบาทชัดเจน สมาชิกส่วนใหญ่มีส่วนร่วม อภิปราย/ถามตอบ แลกเปลี่ยนกันจริง	แบ่งบทบาทแล้ว แต่การมีส่วนร่วมกระจุกตัวบางคน คนอื่นค่อนข้างเงียบ	ไม่เห็นความร่วมมือเป็นทีม ทำงานเหมือนคนเดียว/สองคน ที่เหลือไม่เกี่ยวข้อง

หมายเหตุสำหรับนักศึกษา

- ใช้กิจกรรมนี้เป็นโอกาสทดลอง
  “คิดแบบนัก Cybersecurity ในบริบทการแพทย์”
- เชื่อมทุกประเด็นกลับไปที่
  CIA – DAD – AAA – Threat/Vuln/Risk – Domains – Monitoring
- ให้ความสำคัญทั้ง **ความถูกต้องทางวิชาการ**
  และ **จริยธรรมในการจัดการข้อมูลสุขภาพของผู้ป่วย**
- ฝึกการทำงานเป็นทีม และการสื่อสารเชิงวิชาชีพในสภาพแวดล้อมด้านสาธารณสุขดิจิทัล