ใบงานที่ 1

Six Thinking Hats กับกรณีศึกษา

“ระบบทะเบียนกลางมหาวิทยาลัย”

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
   ระบบทะเบียนกลางมหาวิทยาลัย ได้แก่
   - ระบุ **Asset / Scope of protection** ของระบบทะเบียนกลาง
   - 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 ฯลฯ)

1. วัตถุประสงค์ของกิจกรรม (ต่อ)

2. ใช้กรอบ **Six Thinking Hats**
   เพื่อช่วยคิดอย่างเป็นระบบ จากหลายมุมมองทั้งเทคนิคและเชิงนโยบาย

3. ทำงานกลุ่มแบบหมุนเวียน
   แลกเปลี่ยนและต่อยอดแนวคิดจากกลุ่มอื่นได้อย่างมีเหตุผล

4. สรุปประเด็นเชิงวิชาการ
   และนำเสนอภาพรวมต่อชั้นเรียนภายในเวลาที่กำหนด

2. กรณีศึกษา

ระบบทะเบียนกลางในมุมมอง Cybersecurity

ให้ถือว่า **“ระบบทะเบียนกลางมหาวิทยาลัย”** เป็น
Critical Information System ระบบหนึ่งขององค์กร ซึ่งครอบคลุม

- **ข้อมูล (Data):**
  ประวัตินักศึกษา, รายวิชา, เกรด, Transcript, ตารางสอน,
  สถานะการลงทะเบียน, ข้อมูลการชำระเงิน
- **ผู้ใช้ (Users):**
  นักศึกษา, อาจารย์, เจ้าหน้าที่ทะเบียน, ผู้บริหาร,
  หน่วยงานอื่นที่ดึงข้อมูลไปใช้
- **บริการหลัก (Services):**
  ลงทะเบียน/เพิ่ม–ถอน, ดูเกรด, ออกรายงาน, ตรวจสอบสถานะ,
  เชื่อมต่อระบบอื่น ฯลฯ

2. กรณีศึกษา – กรอบคิดที่ต้องใช้

ให้นักศึกษานำกรอบคิดจากบทเรียนมาใช้ เช่น

- **CIA vs DAD**
  - ระบบทะเบียนกลางต้องปกป้องอะไร (CIA)
  - ผู้โจมตีอาจต้องการอะไร (DAD)
- **AAA**
  - การยืนยันตัวตน
  - การกำหนดสิทธิ์
  - การบันทึกการใช้งาน
- **Threat & Vulnerability**
  - ภัยคุกคามและช่องโหว่ที่น่ากังวล

2. กรอบคิดที่ต้องใช้ (ต่อ)

- **Cybersecurity Domains**
  - โดเมนใดบ้างที่เกี่ยวข้องกับการออกแบบ/ป้องกันระบบทะเบียนกลาง
- **Network Monitoring**
  - หากจะออกแบบระบบเฝ้าระวังเครือข่ายเพื่อคุ้มครองระบบทะเบียนกลาง
  - จะมองหาอะไรใน **traffic / log**

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 ของระบบทะเบียนกลาง
โต๊ะ 2	Red Hat	ความรู้สึก/ความกังวลของผู้ใช้/ผู้บริหาร เมื่อระบบไม่ปลอดภัยหรือใช้งานไม่ได้
โต๊ะ 3	Black Hat	ความเสี่ยง, ผลกระทบต่อ CIA, Threat–Vulnerability–Risk
	Yellow	

3. โครงสร้างการจัดกลุ่มและบทบาท (ต่อ)

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

3.2 บทบาทในแต่ละกลุ่ม

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

3.2 บทบาทในแต่ละกลุ่ม (ต่อ)

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

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

5. วิธีดำเนินกิจกรรมในแต่ละรอบ

รอบที่ 1 – เริ่มต้นที่หมวกของโต๊ะ (เวลา 8 นาที)

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

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

6. แนวทางคำถามของแต่ละหมวก

(เชื่อมกับ Cybersecurity)

ให้นักศึกษาใช้คำถามเหล่านี้เป็น “ตัวช่วยคิด” ในแต่ละโต๊ะ

6.1 White Hat

ข้อมูลและข้อเท็จจริงเชิง Cybersecurity

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

- ระบบทะเบียนกลางมี **สินทรัพย์ (Assets)** อะไรบ้างที่ต้องปกป้อง?
    - ข้อมูลนักศึกษา, เกรด, Transcript, ข้อมูลการเงิน ฯลฯ
- ขอบเขตการปกป้อง (**Scope of protection**) คืออะไรบ้าง?
    - ระบบบนเว็บ, ฐานข้อมูล, เครือข่ายภายใน, การเชื่อมต่ออินเทอร์เน็ต

6.1 White Hat (ต่อ)

- ถ้ามองในกรอบ **CIA Triad** –
  ระบบนี้ควรให้ความสำคัญกับ C / I / A ในประเด็นใดบ้างเป็นพิเศษ?
- ข้อมูลใดบ้างที่ถ้ารั่วไหล / ถูกแก้ไข / ใช้งานไม่ได้
  จะกระทบต่อมหาวิทยาลัยอย่างมีนัยสำคัญ?

6.2 Red Hat

ความรู้สึกและภาพลักษณ์เมื่อเกิดปัญหา Security

โฟกัส: **ความรู้สึกของ Stakeholders เมื่อ CIA ถูกคุกคาม**

- ถ้าข้อมูลทะเบียน (เช่น เกรด/Transcript)
  ถูก **Disclosure หรือ Alteration**
  - นักศึกษาจะรู้สึกอย่างไร?
  - อาจารย์/เจ้าหน้าที่จะรู้สึกอย่างไร?
  - ผู้ปกครอง/สังคมจะมองมหาวิทยาลัยอย่างไร?

6.2 Red Hat (ต่อ)

- ถ้าระบบลงทะเบียนล่มช่วงเวลาสำคัญ
  (**Availability ถูกทำลาย**)
    - เกิดความเครียด กดดัน หรือความไม่เชื่อมั่นในระบบแค่ไหน?
- มี “ความกังวลเชิงภาพลักษณ์” (Reputation)
  หรือ “ความไม่ยุติธรรม” ที่เกี่ยวข้องกับ
  Integrity ของข้อมูลหรือไม่?

6.3 Black Hat

ความเสี่ยง, DAD, Threat–Vulnerability–Risk

โฟกัส: **มุมมองผู้โจมตี + ช่องโหว่ + ความเสี่ยง**

- จากมุมมอง **DAD Triad (Disclosure / Alteration / Destruction)**
  - ผู้โจมตีอาจต้องการทำอะไรกับระบบทะเบียนกลาง?
- ตัวอย่าง **Threat** ที่อาจเจอ เช่น
  - การเจาะระบบเพื่อแก้ไขเกรด
  - การดึงข้อมูลส่วนตัวนักศึกษาออกไปขาย
  - การโจมตีให้ระบบล่มช่วงลงทะเบียน

6.3 Black Hat (ต่อ)

- ระบบอาจมี **Vulnerabilities** อะไรบ้าง? เช่น
  - Password อ่อนแอ, ไม่มี MFA
  - การตั้งสิทธิ์ในฐานข้อมูลไม่เหมาะสม
  - Patch/Update ไม่ทันสมัย
- เมื่อ Threat + Vulnerability รวมกันแล้ว กลายเป็น **Risk** อะไรที่ควรกังวลที่สุด?
  - ให้ยกตัวอย่างอย่างน้อย 1–2 รายการ

6.4 Yellow Hat

ด้านบวกและโอกาสจากการออกแบบระบบให้ Secure

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

- หากออกแบบระบบทะเบียนกลางโดยคำนึงถึง **CIA + AAA** อย่างถูกต้อง
  - จะสร้างความเชื่อมั่นให้นักศึกษา/อาจารย์อย่างไร?
  - ช่วยให้การทำงานของเจ้าหน้าที่ง่ายขึ้นอย่างไร?

6.4 Yellow Hat (ต่อ)

- ระบบที่มี **Accounting / Logging ดี** จะเป็นประโยชน์ต่อ
    - การทำ **Incident Response** และ **Forensics** อย่างไร?
- มีโอกาสในการใช้ข้อมูลจากระบบทะเบียนกลาง ไปสนับสนุน **Governance, Risk, Compliance (GRC)** ของมหาวิทยาลัยอย่างไร?

6.5 Green Hat

ความคิดสร้างสรรค์ด้าน AAA และ Network Monitoring

โฟกัส: **มาตรการ/แนวทางใหม่ ๆ ที่ใช้ได้จริงตามหลัก Cybersecurity**

- จะออกแบบ **Authentication** อย่างไร
  ให้ปลอดภัยและเหมาะกับนักศึกษา/บุคลากร?
    - เช่น MFA, Single Sign-On, Student ID + App
- **Authorization** ที่ดีควรแยกสิทธิ์อย่างไรระหว่าง
    - นักศึกษา / อาจารย์ / เจ้าหน้าที่ทะเบียน / ผู้บริหาร

6.5 Green Hat (ต่อ)

- จะใช้ **Accounting / Logging** แบบไหน
  ที่ช่วยให้ตรวจสอบเหตุการณ์ผิดปกติได้เร็วขึ้น?
- ถ้าจะออกแบบ **Network Monitoring** เพื่อเฝ้าระวังระบบทะเบียนกลาง
  - จะเก็บ Log/Traffic อะไรบ้าง?
    - เช่น failed login, suspicious query, unusual outbound traffic
  - จะตั้ง Alert Rule แบบใดให้สอดคล้องกับ DAD?
    - เช่น การไหลออกของข้อมูลจำนวนมาก = สงสัยว่าเป็น Disclosure

6.5 Green Hat (ต่อ)

- มีแนวคิดเชิงนโยบาย/มาตรการเสริมอะไรที่
  “สร้างสรรค์แต่สมเหตุสมผล” เช่น
  - แจ้งเตือนผ่านแอปเมื่อมีการเปลี่ยนแปลงข้อมูลสำคัญ
  - Dashboard ความมั่นคงปลอดภัยสำหรับผู้บริหาร ฯลฯ

6.6 Blue Hat

การรวมภาพใหญ่ของ Cybersecurity สำหรับระบบทะเบียนกลาง

โฟกัส: **สถาปัตยกรรมและการเชื่อมโยงกรอบคิดทั้งหมด**

- ถ้าต้องอธิบาย “สถาปัตยกรรมด้าน Cybersecurity ของระบบทะเบียนกลาง”
  - CIA อยู่ตรงไหนบ้างในระบบ?
  - DAD ของผู้โจมตีจะชนกับกลไกป้องกันตรงไหน?
  - AAA ทำงานอย่างไรในกระบวนการเข้าใช้ระบบ?

6.6 Blue Hat (ต่อ)

- ระบบทะเบียนกลางเกี่ยวข้องกับ **Cybersecurity Domains** ใดบ้าง? เช่น
  - Network Security
  - Application Security
  - Information Security
  - Incident Response & Forensics
  - GRC ฯลฯ
- ถ้าเกิดเหตุการณ์โจมตีจริง (เช่น แก้ไขเกรด/ดึงข้อมูลนักศึกษาออก)
  - ขั้นตอนของ **Incident Response** คร่าว ๆ ควรเป็นอย่างไร?
- ภาพรวมทั้งหมดนี้สนับสนุนอะไร ต่อเป้าหมายของมหาวิทยาลัยในฐานะองค์กรดิจิทัลที่มั่นคงปลอดภัย?

7. การสรุปและการนำเสนอ

หลังจบรอบที่ 6

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

7. การสรุปและการนำเสนอ (ต่อ)

- สรุปประเด็นหลักที่เกี่ยวกับระบบทะเบียนกลาง
  โดยเชื่อมกับ

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

  เท่าที่เหมาะสมกับหมวกของตน

3. หลังการนำเสนอของทุกโต๊ะ
   - อาจารย์จะสรุปภาพรวมและเชื่อมโยงเข้ากับเนื้อหาบทที่ 1
   - อธิบายว่ากรอบคิดเหล่านี้สำคัญอย่างไรต่อการออกแบบระบบจริง
   - และต่อยอดไปสู่การออกแบบ **network monitoring system**

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 ที่เกี่ยวข้องอย่างน้อย 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 เชื่อมโยงกับบริบทมหาวิทยาลัย	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” ไม่ใช่แค่ผู้ใช้ระบบ
- เชื่อมทุกประเด็นกลับไปที่
  CIA – DAD – AAA – Threat/Vuln/Risk – Domains – Monitoring
- ให้ความสำคัญทั้ง **ความถูกต้องทางวิชาการ**
  และ **การทำงานร่วมกันในทีม**