คู่มือการใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบสารสนเทศ

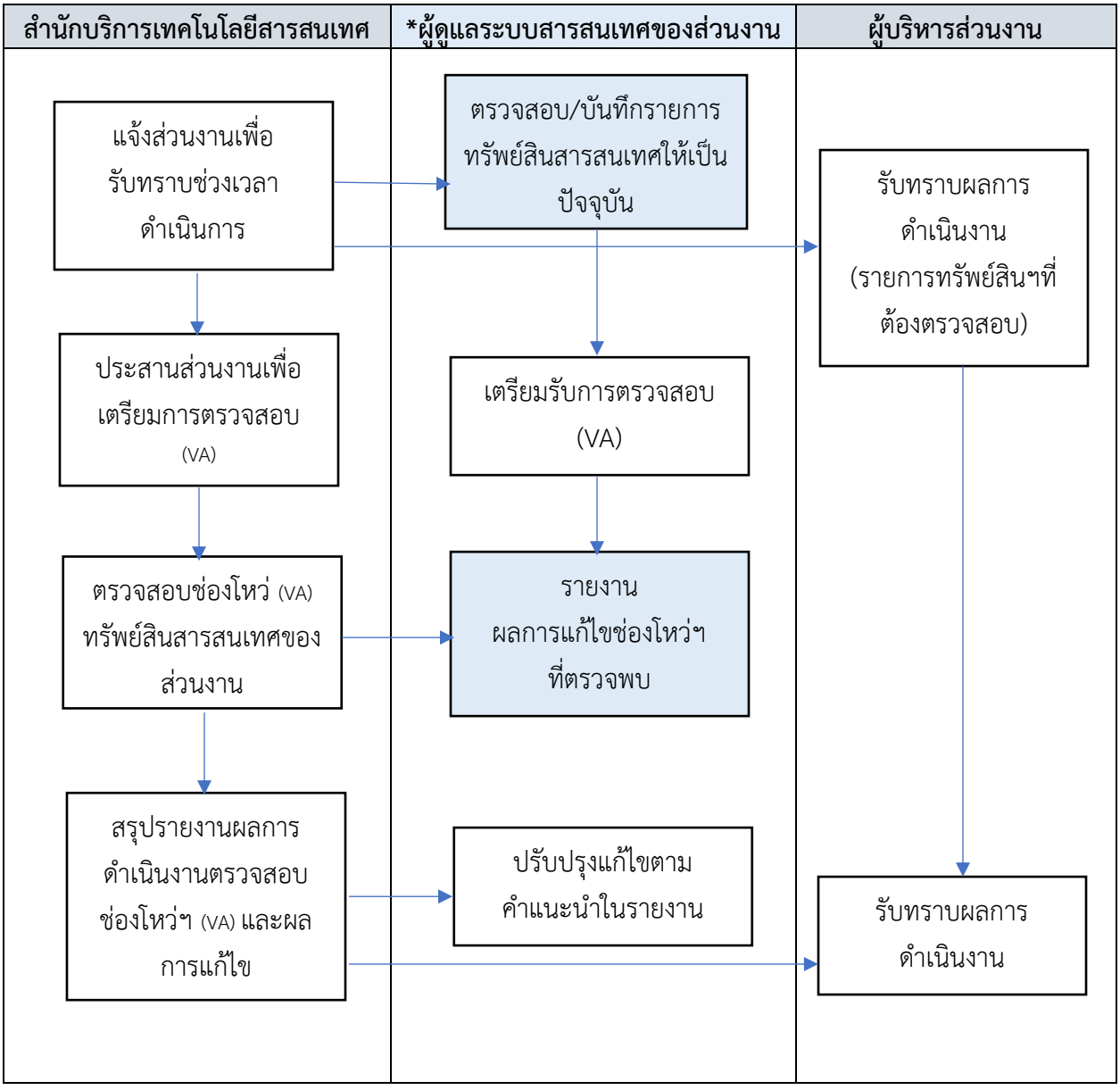
Vulnerability Tracking System

ฝ่ายความมั่นคงปลอดภัยไซเบอร์ สำนักบริการเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเชียงใหม่

สารบัญ

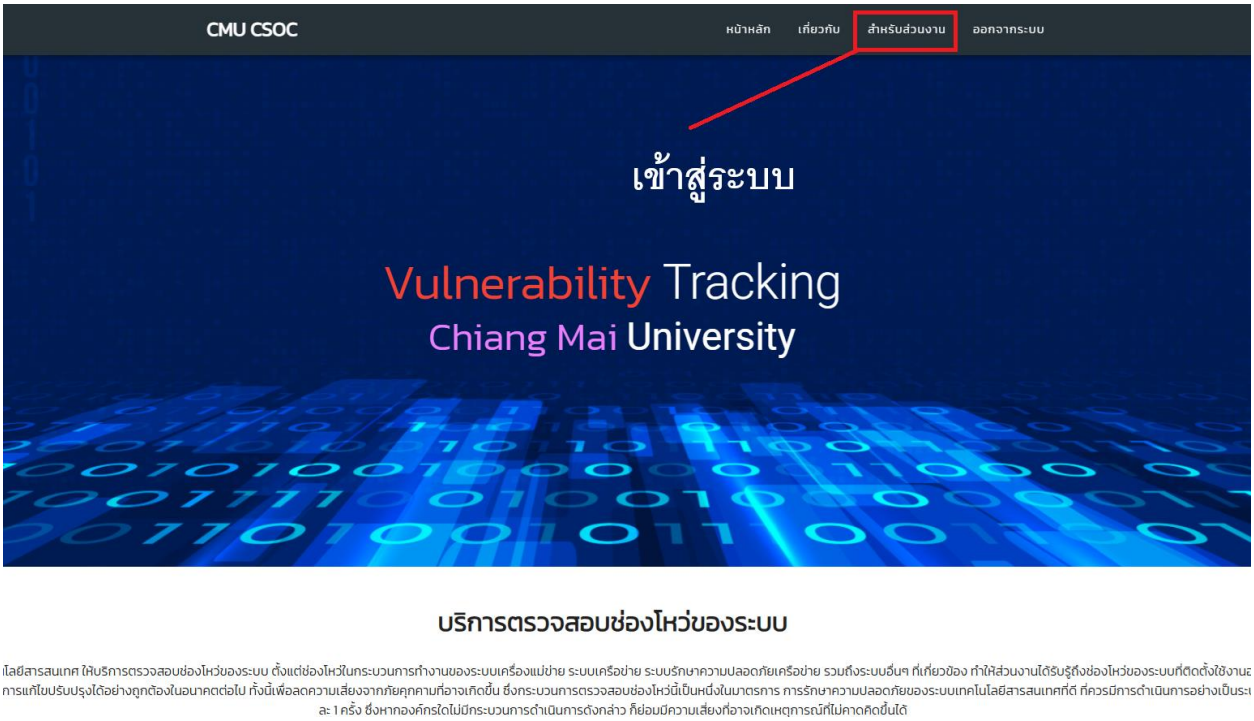
ขั้นตอนการใช้งานระบบ

ระบบติดตามการแก้ไขช่องโหว่ของระบบสารสนเทศ มหาวิทยาลัยเชียงใหม่ (CMU VTS) เป็นระบบติดตามการรายงานผลการดำเนินงานแก้ไขช่องโหว่ของระบบสารสนเทศของส่วนงาน หลังจากการตรวจสอบช่องโหว่ (VA) ประจำปีโดยสำนักบริการเทคโนโลยีสารสนเทศ โดยมีขั้นตอนการใช้งานที่ผู้ดูแลระบบสารสนเทศของส่วนงานต้องดำเนินการดังนี้ (กล่องสีฟ้า หมายถึง ดำเนินการในระบบ CMU VTS)



การเข้าสู่ระบบของส่วนงาน

เริ่มใช้งานระบบ CMU VTS ในรูปแบบ Web Application ผ่าน URL: https://vts.csd.itsc.cmu.ac.th และเข้าสู่ระบบด้วย IT Account ที่เมนู “สำหรับส่วนงาน” ดังภาพที่ 1

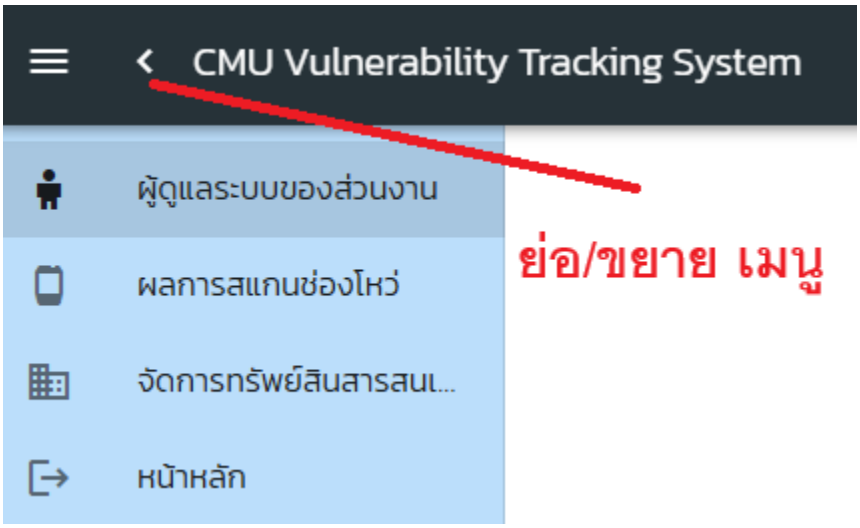


ภาพที่ 1 การคลิกเข้าสู่ระบบสำหรับส่วนงาน

หลังจากยืนยันตัวตนเข้าสู่ระบบเรียบร้อยแล้ว จะปรากฏเมนูจัดการข้อมูลด้านซ้ายมือ ประกอบด้วย

- ผู้ดูแลระบบของส่วนงาน
- ผลการสแกนช่องโหว่
- จัดการทรัพย์สินสารสนเทศ
- หน้าหลัก

ดังภาพที่ 2



ภาพที่ 2 เมนูจัดการข้อมูลสำหรับส่วนงาน หลังจากยืนยันตัวตนเข้าสู่ระบบแล้ว

การจัดการข้อมูล

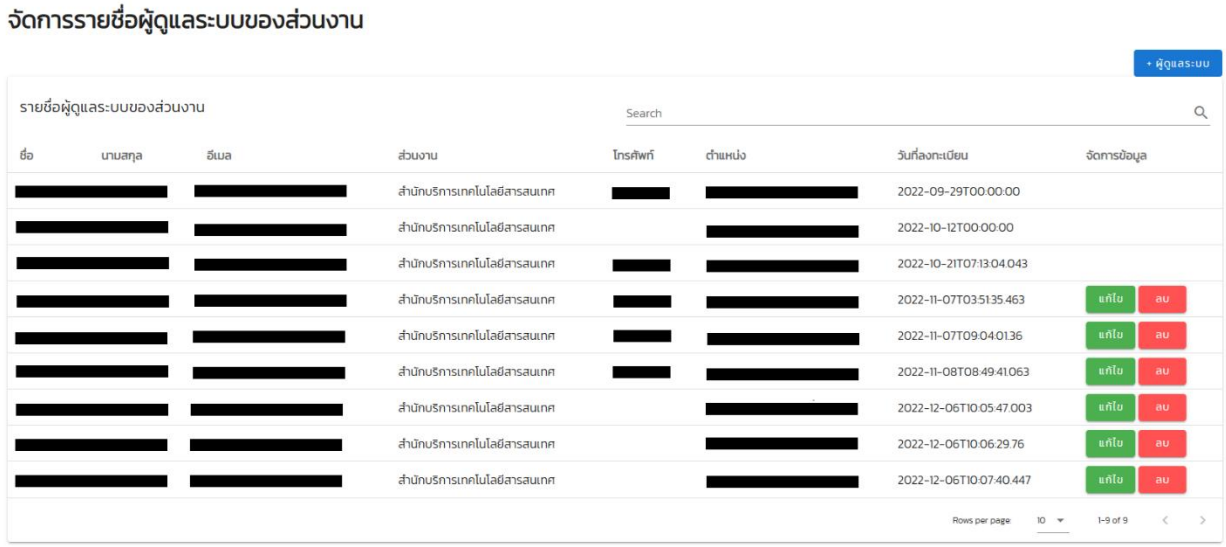
ผู้ดูแลระบบสารสนเทศของส่วนงาน สามารถจัดการข้อมูลในระบบ CMU VTS ได้ตามสิทธิของส่วนงานที่สังกัด ใน 3 หัวข้อหลัก ดังนี้

- การจัดการผู้ดูแลระบบของส่วนงาน
- ผลการตรวจสอบช่องโหว่และการรายงานผล
- จัดการทรัพย์สินสารสนเทศ

โดยมีลำดับขั้นตอนการดำเนินงานตามหัวข้อ “ขั้นตอนการใช้งานระบบ” อธิบายเมนูจัดการข้อมูลในแต่ละหัวข้อได้ดังนี้

- **การจัดการผู้ดูแลระบบของส่วนงาน**

  เป็นการจัดการรายชื่อผู้ดูแลระบบของส่วนงาน ผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงาน จะเป็นผู้มีสิทธิสูงสุดของส่วนงาน และสามารถเพิ่มรายชื่อผู้ดูแลระบบท่านอื่นภายหลังได้ แต่ผู้ที่ได้รับการเพิ่มจะสามารถดูรายงานผลการตรวจสอบช่องโหว่ได้เพียงอย่างเดียว ไม่สามารถรายงานผลการแก้ไขช่องโหว่ได้ เหมาะสำหรับผู้บริหาร หรือหัวหน้างาน ที่มีความประสงค์ดูข้อมูลในระบบ แต่การรายงาน จะเป็นหน้าที่ของผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงาน (ผู้ดูแลระบบหลัก) (* หากต้องการเพิ่มผู้ดูแลระบบหลัก สามารถแจ้งความประสงค์ผ่านหัวหน้าส่วนงานในรูปแบบบันทึกข้อความ) หน้าจอการจัดการรายชื่อผู้ดูแลระบบของส่วนงาน แสดงดังภาพที่ 3



ภาพที่ 3 หน้าจอการจัดการรายชื่อผู้ดูแลระบบของส่วนงาน

จากภาพที่ 3 รายชื่อผู้ดูแลระบบหลัก ที่ได้รับมอบหมายจากหัวหน้าส่วนงาน จะไม่สามารถแก้ไขหรือลบได้ (ต้องแจ้งทางสำนักบริการเทคโนโลยีสารสนเทศ) แต่ถ้าเป็นผู้ดูแลระบบสารสนเทศที่เพิ่มเติมภายหลังจึงจะสามารถเปลี่ยนแปลงแก้ไข/ลบข้อมูลได้ ส่วนการเพิ่มผู้ดูแลระบบสารสนเทศของส่วนงาน (ดูผลอย่างเดียว) สามารถทำได้ด้วยการคลิกปุ่ม 

และบันทึกข้อมูล ประกอบด้วย

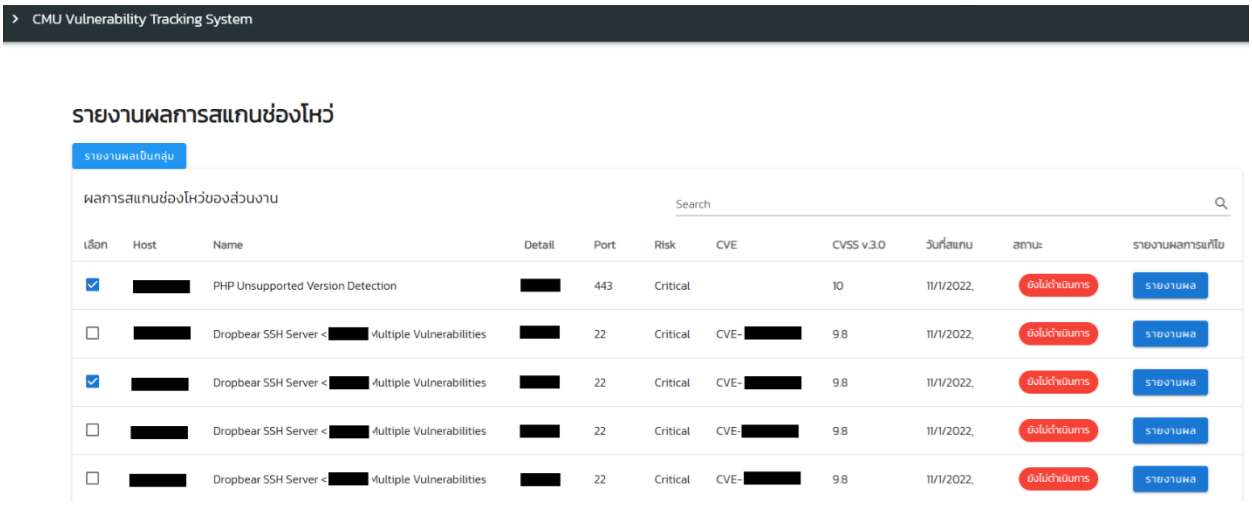
- ชื่อ – นามสกุล (* บังคับบันทึก)
- IT Account ในรูปแบบ name.surname@cmu.ac.th (* บังคับบันทึก)
- หมายเลขโทรศัพท์สำหรับติดต่อ (ไม่บังคับ)
- ตำแหน่ง (ไม่บังคับ)

ดังภาพที่ 4 หลังจากนั้นให้คลิกปุ่ม “บันทึกข้อมูล” รายชื่อจะถูกเพิ่มในหน้าจัดการผู้ดูแลระบบของส่วนงานทันที ถ้าหากไม่ต้องการบันทึก ให้คลิกปุ่ม “ปิดหน้าต่าง”

ภาพที่ 4 การเพิ่มผู้ดูแลระบบของส่วนงาน (* หมายถึง จำเป็นต้องระบุ)

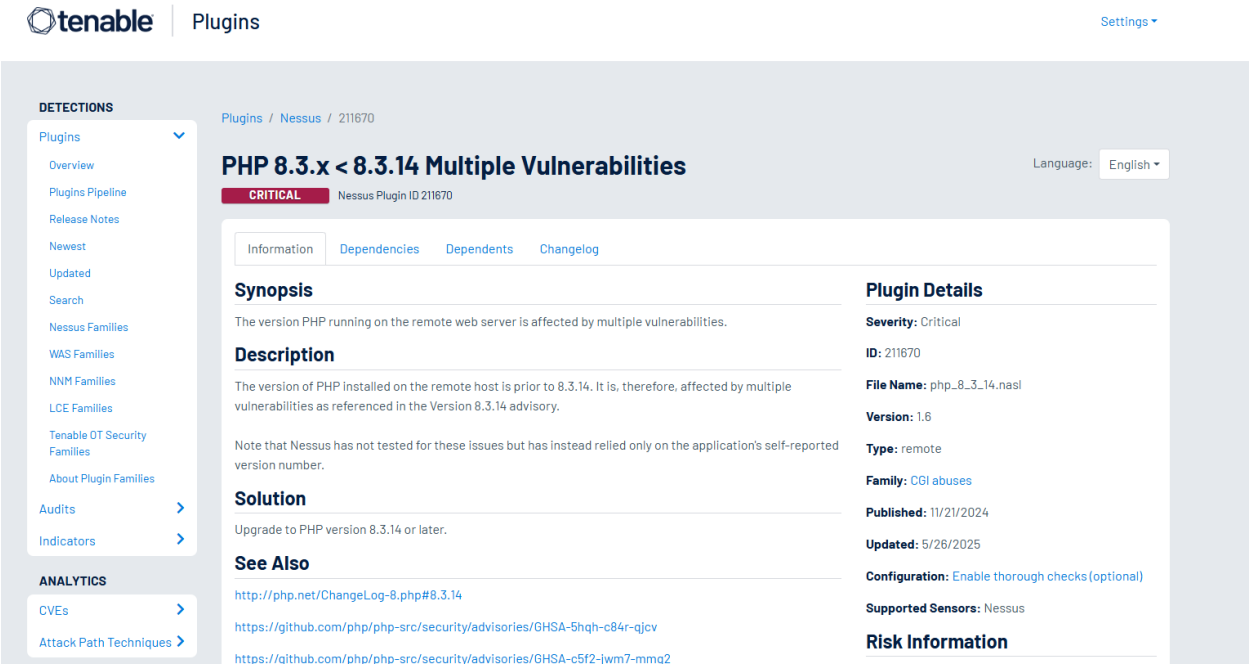
- **ผลการตรวจสอบช่องโหว่และการรายงานผล**
  ผู้ดูแลระบบสารสนเทศของส่วนงานสามารถดูผลการตรวจสอบช่องโหว่ (VA) ของทรัพย์สินสารสนเทศได้ที่เมนูนี้ รายงานผลการสแกนช่องโหว่ของส่วนงาน ประกอบด้วย ดังภาพที่ 5
  - **Host** หมายถึง ip หรือ domain ของทรัพย์สินสารสนเทศ
  - **Name** หมายถึง ชื่อของช่องโหว่ที่ตรวจพบ
  - **Detail** หมายถึง เลขรหัสของช่องโหว่ สามารถคลิกเพื่อเปิดเว็บแสดงรายละเอียดได้
  - **Port** หมายถึง Port ของ Host ที่ตรวจพบช่องโหว่

- **Risk** หมายถึง ระดับความเสี่ยงของช่องโหว่ ประกอบด้วย Critical, High, Medium, Low และ None (ให้ส่วนงานรายงานผลเฉพาะความเสี่ยงระดับ Critical เท่านั้น)
- **CVE** หมายถึง Common Vulnerabilities and Exposures ซึ่งเป็นระบบมาตรฐานที่ใช้ในการระบุและติดตามช่องโหว่
- **CVSS v.3.0** หมายถึง Common Vulnerability Scoring System เวอร์ชัน 3.0 ใช้ในการประเมินความรุนแรงของช่องโหว่ คะแนนตั้งแต่ 0.0 ถึง 10.0
- **วันที่สแกน** หมายถึง วันที่ทำการตรวจสอบช่องโหว่
- **สถานะ** หมายถึง สถานะการดำเนินการของการรายงานผลการแก้ไขช่องโหว่ ดังนี้
  - **ยังไม่ได้ดำเนินการ** หมายถึง ยังไม่มีการรายงานผลการดำเนินงานของส่วนงาน
  - **อยู่ระหว่างดำเนินการ** หมายถึง ส่วนงานรับทราบแล้ว และอยู่ในระหว่างการตรวจสอบแก้ไขปัญหา
  - **ดำเนินการแล้ว** หมายถึง ส่วนงานตรวจสอบและแก้ไขช่องโหว่แล้ว
- **รายงานผล** หมายถึง การคลิก เพื่อรายงานผลการดำเนินงาน และปรับปรุงสถานะของรายการช่องโหว่นั้น ๆ มีผลต่อคอลัมภ์สถานะ



ภาพที่ 5 รายงานผลการสแกนช่องโหว่ของส่วนงาน

สามารถดูรายละเอียดของช่องโหว่ได้จากคอลัมน์ “Detail” ด้วยการคลิก link ที่เลขรหัส เพื่อเปิดหน้าเว็บแสดงรายละเอียดของช่องโหว่ แสดงดังภาพที่ 6



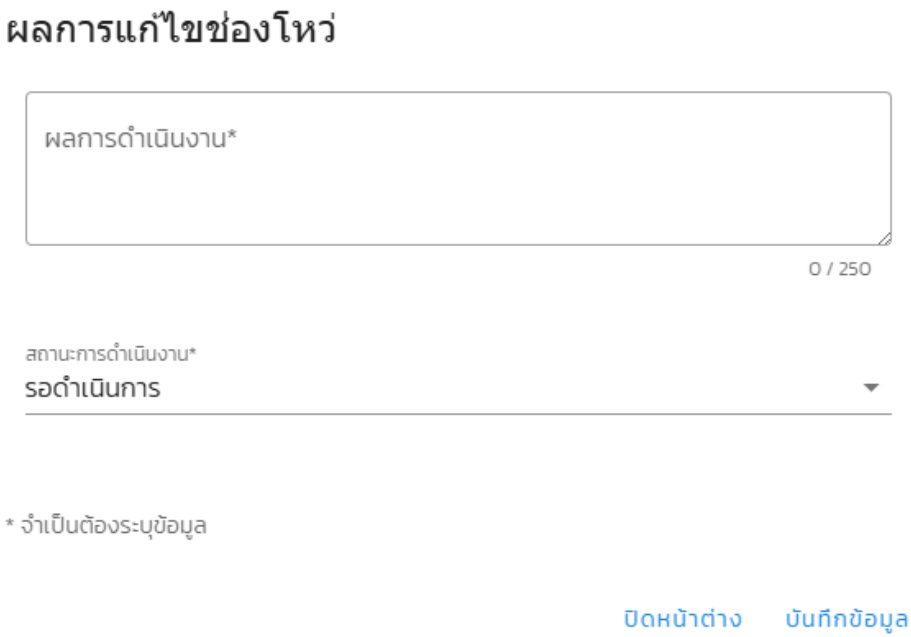
ภาพที่ 6 รายละเอียดของช่องโหว่ของแต่ละรายการทรัพย์สินสารสนเทศ อ้างอิงจากเลขรหัส

การรายงานผลการตรวจสอบแก้ไขช่องโหว่ สามารถทำได้ 2 วิธี คือ

- การรายงานผลทีละรายการ
- การรายงานผลเป็นกลุ่ม

<u>การรายงานผลทีละรายการ</u>

สามารถทำได้โดยการคลิกปุ่ม “รายงานผล” ด้านท้ายสุดของตาราง (ดูภาพที่ 5 ประกอบ) ของรายการที่ต้องการรายงานผลการแก้ไข จะปรากฏหน้าต่างการรายงานผลขึ้นมา ประกอบด้วย ผลการดำเนินงาน และสถานการณ์ดำเนินงาน (ดังภาพที่ 7) ให้บันทึกรายละเอียดเกี่ยวกับการดำเนินงาน (พอสังเขป) และสถานะปัจจุบัน หลังจากนั้นคลิกปุ่ม **“บันทึกข้อมูล”** (* แนะนำให้ท่านเปลี่ยนสถานะเป็น<u>อยู่ระหว่างดำเนินการ</u> หากท่านทราบผลการรายงานแล้ว และอยู่ในระหว่างการดำเนินการแก้ไข)



ภาพที่ 7 หน้าต่างรายงานผลการแก้ไขช่องโหว่

การรายงานผลเป็นกลุ่ม

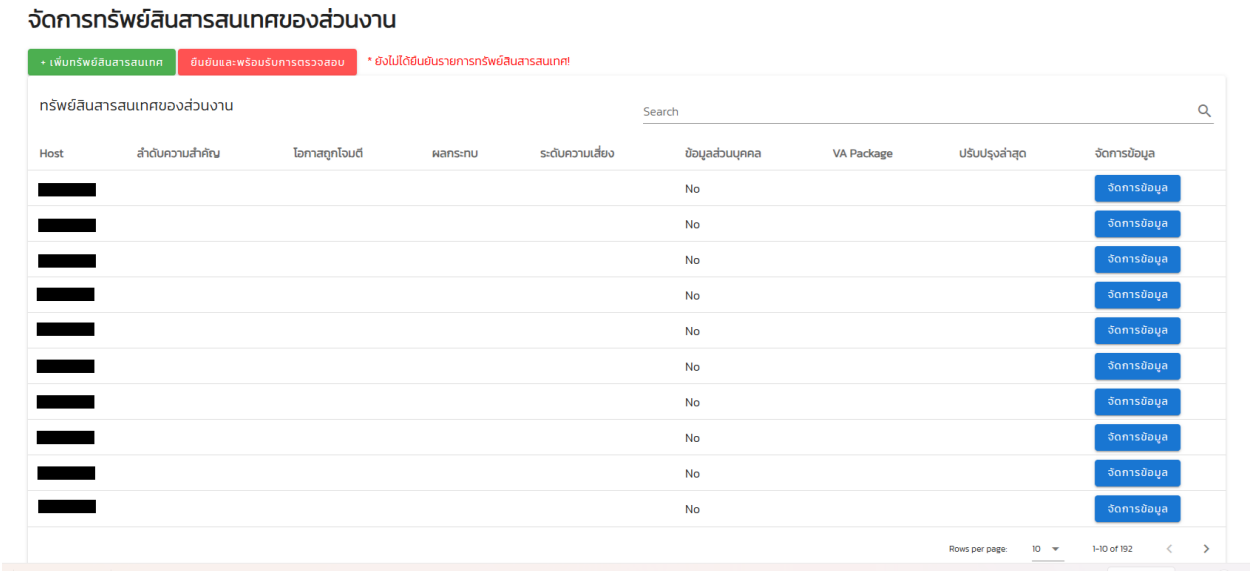
เป็นการรายงานผลการแก้ไขช่องโหว่เป็นกลุ่ม หรือการรายงานผลการแก้ไขช่องโหว่หัวข้อเดียวกันแต่แยก CVE หรือ Port เป็นต้น เป็นการรายงานหลาย ๆ รายการพร้อมกัน ด้วยการคลิกช่องสี่เหลี่ยมหน้ารายการที่ต้องการรายงาน (ดูภาพที่ 5 ประกอบ) หลังจากเลือกครบแล้ว ให้คลิกปุ่ม “รายงานผลเป็นกลุ่ม” จะปรากฏหน้าต่างผลการแก้ไขช่องโหว่ คล้ายกับการรายงานผลทีละรายการ แต่เป็นการรายงานที่มีผลกับทุกรายการที่เลือก ให้ระบุผลการดำเนินงานที่เกี่ยวข้อง พร้อมทั้งสถานะการดำเนินงาน และคลิกปุ่ม “บันทึกข้อมูล”

- **การจัดการทรัพย์สินสารสนเทศ**

รายการทรัพย์สินสารสนเทศของส่วนงาน ในที่นี้ หมายถึง ชื่อโดเมนของระบบสารสนเทศ หรือหมายเลขไอพีเครื่องแม่ข่าย (IP Address) ที่ติดตั้งระบบสารสนเทศที่ต้องการประเมินช่องโหว่ด้านความปลอดภัย โดยรายการต่าง ๆ เหล่านี้ต้องผ่านการประเมินผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ หรือ Business Impact Analysis (BIA) ซึ่งประกอบด้วย ลำดับความสำคัญ โอกาสถูกโจมตี (Likelihood) และผลกระทบ (Impact) ซึ่งจะถูกคำนวณให้เป็นระดับความเสี่ยง (Risk Score) ของ

แต่ละรายการทรัพย์สินสารสนเทศ (Asset) รายการทรัพย์สินสารสนเทศของส่วนงานที่ปรากฏในระบบมาจากการแจ้งตรวจสอบช่องโหว่ในปี 2567 และการประเมิน BIA ของส่วนงานประจำปี

ส่วนงานสามารถปรับปรุง หรือ เพิ่มข้อมูลให้เป็นปัจจุบันได้ โดยมีขั้นตอนดังต่อไปนี้ (ดูภาพที่ 8 ประกอบ)



ภาพที่ 8 การจัดการทรัพย์สินสารสนเทศของส่วนงาน

- การปรับปรุงรายการทรัพย์สินสารสนเทศ ด้วยการคลิกปุ่ม “จัดการข้อมูล” ท้ายรายการทรัพย์สินสารสนเทศนั้น ๆ หลังจากคลิกแล้วจะปรากฏหน้าต่างบันทึกข้อมูล ดังภาพที่ 9

ภาพที่ 9 การบันทึก/ปรับปรุงข้อมูลทรัพย์สินสารสนเทศ

มีขั้นตอนการบันทึก/ปรับปรุงรายการทรัพย์สินสารสนเทศ ดังนี้

- ระบุลำดับความสำคัญของทรัพย์สินสารสนเทศ (ระดับ 1 – 5) โดย 5 หมายถึง สำคัญที่สุด
- ระบุโอกาสถูกโจมตีทางไซเบอร์ของทรัพย์สินสารสนเทศ (ระดับ 1 – 5) โดย 5 หมายถึง มากที่สุด
- ระบุผลกระทบจากการถูกโจมตีของทรัพย์สินสารสนเทศนั้น ๆ ต่อการดำเนินงานที่เกี่ยวข้อง (ระดับ 1 – 5) โดย 5 หมายถึง มีผลกระทบสูงสุด
- ระดับความเสี่ยง (โอกาสถูกโจมตี x ผลกระทบ) จะถูกคำนวณอัตโนมัติ หากมีระดับคะแนนตั้งแต่ 15 ขึ้นไป ตัวเลือกของ VA Package จะถูกกำหนดเป็น Credential Scan โดยอัตโนมัติ
- ระบุว่าทรัพย์สินสารสนเทศนั้น ๆ มีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล หรือไม่ (Yes/No) หากมีทรัพย์สินสารสนเทศมีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล ตัวเลือกของ VA Package จะถูกกำหนดเป็น Credential Scan โดยอัตโนมัติ
- VA Package เป็นการเลือกประเภทของการตรวจสอบช่องโหว่ทรัพย์สินสารสนเทศ มีให้เลือก 3 ประเภท ได้แก่
    - Basic Scan เป็นการตรวจสอบจากมุมมองภายนอกโดยไม่ต้องอนุญาตอะไรเพิ่มเติม
    - Open Firewall Scan เป็นการตรวจสอบช่องโหว่ในมุมมองที่เสมือนเชื่อมต่อภายในระบบเครือข่ายของส่วนงาน
    - Credential Scan เป็นการตรวจสอบช่องโหว่ในเชิงลึก เหมาะกับทรัพย์สินสารสนเทศที่มีความสำคัญสูงมาก และทรัพย์สินสารสนเทศที่มีข้อมูลส่วนบุคคล

เมื่อกำหนดค่าทุกรายการเสร็จสิ้นแล้ว ให้คลิกปุ่ม “บันทึกข้อมูล” หรือ “ปิดหน้าต่าง” หากต้องการยกเลิกการบันทึก/ปรับปรุงข้อมูล

- การลบรายการทรัพย์สินสารสนเทศ หรือ ไม่ประสงค์จะตรวจสอบช่องโหว่ของรายการสารสนเทศนั้น ๆ ให้ทำการแจ้งความประสงค์ด้วยการ คลิกเลือกกล่องสี่เหลี่ยม “ไม่ต้องการสแกนช่องโหว่” ก่อนการบันทึกข้อมูล จะเป็นการลบรายการดังกล่าว ดังภาพที่ 10

ภาพที่ 10 การแจ้งลบรายการทรัพย์สินสารสนเทศนั้น ๆ (อ้างอิงจากภาพที่ 9)

- การเพิ่มรายการทรัพย์สินสารสนเทศ จากหน้าจอในภาพที่ 8 คลิกปุ่ม 

เพื่อเพิ่มรายการทรัพย์สินสารสนเทศ จะปรากฏหน้าต่างเพิ่มข้อมูลดังภาพที่ 11

ภาพที่ 11 การเพิ่มรายการทรัพย์สินสารสนเทศ

รายละเอียดของการบันทึกข้อมูล อยู่ในหัวข้อการปรับปรุงรายการทรัพย์สินสารสนเทศ หน้า 10

- การยืนยันรายการทรัพย์สินสารสนเทศ หลังจากการเพิ่ม แก้ไข/ปรับปรุงรายการทรัพย์สินสารสนเทศของส่วนงานเสร็จสิ้นแล้ว ต้องทำการยืนยันเพื่อแจ้งความประสงค์ตรวจสอบช่องโหว่ด้วยการคลิกปุ่ม 

หลังจาก**ยืนยัน**แล้ว จะไม่สามารถแก้ไขข้อมูลได้ หากต้องการแก้ไขข้อมูลหลังจากยืนยันแล้ว ให้แจ้งความประสงค์ได้ที่อีเมล security@cmu.ac.th

หากท่านมีคำถาม หรือข้อเสนอแนะใด ๆ นอกเหนือจากคู่มือฉบับนี้ สามารถติดต่อสอบถามได้ที่อีเมล security@cmu.ac.th ฝ่ายความมั่นคงปลอดภัยไซเบอร์ สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่