

การพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์

นายอนันต์ นามสุดโท

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์

นายอนันต์ นามสุดโท

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์

โดย นายอนันต์ นามสุดโท

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ

.....
คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

.....
ประธาน

(ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี)

.....
อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

.....
กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

ชื่อ : นายอนันต์ นามสุดโท

ชื่อการค้นคว้าอิสระ : การพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์

สาขาวิชา : การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์

ปีการศึกษา : 2568

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ เนื่องจากกระบวนการบริหารจัดการช่องโหว่ในปัจจุบันมักสิ้นสุดที่ขั้นตอนการสแกนและรายงานผล แต่ยังขาดเครื่องมือที่ช่วยติดตามและบริหารจัดการการแก้ไขอย่างเป็นระบบ ระบบที่พัฒนาขึ้นรองรับการนำเข้าข้อมูลผลการสแกนในรูปแบบ CSV จาก Rapid7 InsightVM เป็นกรณีศึกษา ครอบคลุมการจัดเก็บและแสดงข้อมูลช่องโหว่ การติดตามสถานะการดำเนินงาน การบันทึกแนวทางการแก้ไขหรือการยอมรับความเสี่ยงพร้อมบันทึกการตรวจสอบย้อนหลัง การแจ้งเตือนผู้เกี่ยวข้อง และการแสดงผลผ่าน Dashboard ตามบทบาทของผู้ใช้งาน ผู้วิจัยได้พัฒนาระบบต้นแบบและทดสอบการทำงานกับผู้ใช้งานจำนวน 30 คน ผลการวิจัยพบว่าระบบสามารถรองรับการทำงานหลักได้ครบถ้วนตามขอบเขตที่กำหนด และผลการประเมินความคิดเห็นของผู้ใช้งานด้านประโยชน์ต่อการบริหารจัดการช่องโหว่มีค่าเฉลี่ยรวมเท่ากับ 4.65 สะท้อนว่าระบบช่วยให้การติดตามและแก้ไขช่องโหว่เป็นไปอย่างมีแบบแผน ลดโอกาสการตกหล่นของรายการที่ต้องดำเนินการ และเพิ่มความสะดวกในการกำกับติดตามในองค์กร

(มีจำนวนทั้งสิ้น 76 หน้า)

คำสำคัญ : การบริหารจัดการช่องโหว่, ระบบติดตามช่องโหว่, การแก้ไขช่องโหว่, การยอมรับความเสี่ยง, Rapid7 InsightVM

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Anun Namsudtho

Independent Study Title : Development of a Cybersecurity Vulnerability Management and Remediation System

Major Field : Digital Network and Information Security Management
King Mongkut's University of Technology North Bangkok

Independent Study Advisor : Assistant Professor Dr. Nawaporn Wisitpongphan

Academic Year : 2025

ABSTRACT

This study aimed to develop a cybersecurity vulnerability management and remediation system. The study was motivated by the fact that current vulnerability management processes often end at the scanning and reporting stage, while still lacking a tool to systematically track and manage remediation activities. The developed system supports the import of scan results in CSV format from Rapid7 InsightVM as a case study. Its functions cover the storage and presentation of vulnerability data, remediation status tracking, the recording of remediation actions or risk acceptance decisions with audit trail support, notification of relevant stakeholders, and dashboard-based reporting according to user roles. The researcher developed a prototype system and tested it with 30 users. The results showed that the system was able to support all major functional requirements within the defined scope. In addition, the user evaluation of the system's usefulness for vulnerability management yielded an overall mean score of 4.65. These findings indicate that the system helps make vulnerability tracking and remediation more systematic, reduces the likelihood of overlooking items requiring action, and improves the convenience of organizational monitoring and oversight.

(Total 76 Pages)

Keywords: Vulnerability Management, Vulnerability Remediation, Vulnerability Tracking System, Risk Acceptance, Rapid7 InsightVM.

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาและการสนับสนุนจากหลายฝ่าย ผู้วิจัยขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ อาจารย์ที่ปรึกษา ที่ได้กรุณาให้คำปรึกษา ถ่ายทอดความรู้ ข้อเสนอแนะ และแนวทางอันเป็นประโยชน์ ตลอดจนสละเวลาอันมีค่าในการตรวจสอบและแก้ไข จนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จสมบูรณ์

ผู้วิจัยขอขอบพระคุณบริษัท บุญรอดบริวเวอรี่ จำกัด ที่ได้ให้การสนับสนุนทุนการศึกษาและค่าใช้จ่ายที่เกี่ยวข้อง อันเป็นปัจจัยสำคัญที่เอื้อให้ผู้วิจัยสามารถดำเนินการศึกษาและจัดทำงานวิจัยฉบับนี้จนสำเร็จลุล่วง

นอกจากนี้ ผู้วิจัยขอขอบพระคุณครอบครัว เพื่อนร่วมงาน และทุกท่านที่มิอาจกล่าวนามได้ครบถ้วน ณ ที่นี้ ที่ได้ให้ความช่วยเหลือ สนับสนุน และเป็นกำลังใจแก่ผู้วิจัยเสมอมา จนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงไปด้วยดี

อนันต์ นามสุดโท

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ข
บทคัดย่อภาษาอังกฤษ ..... ค
กิตติกรรมประกาศ ..... ง
สารบัญ ..... จ
สารบัญตาราง ..... ช
สารบัญรูปภาพ ..... ซ
บทที่ 1 บทนำ 1
1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ของการวิจัย 2
1.3 ขอบเขตของการวิจัย 3
1.4 ประโยชน์ที่คาดว่าจะได้รับ 4
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 6
2.1 แนวคิดและนิยามเกี่ยวกับช่องโหว่และการบริหารจัดการช่องโหว่ 6
2.2 วงจรชีวิตการจัดการช่องโหว่ (Vulnerability Management Lifecycle) 7
2.3 กรอบมาตรฐานและแนวปฏิบัติที่เกี่ยวข้องกับการบริหารจัดการช่องโหว่ 9
2.4 แนวคิดการให้คะแนนความรุนแรงของช่องโหว่ด้วย CVSS 9
2.5 แนวคิดการแก้ไขช่องโหว่ การจัดการแพตช์ และการยืนยันผล 10
2.6 แนวคิดการยอมรับความเสี่ยงและการตรวจสอบย้อนหลัง 11
2.7 แนวคิดการกำหนดบทบาทและสิทธิ์การเข้าถึง 11
2.8 แนวคิดการนำเข้าข้อมูลจากเครื่องมือสแกนและการทำข้อมูลให้เป็นมาตรฐาน 12
2.9 งานวิจัยที่เกี่ยวข้อง 13
บทที่ 3 วิธีการดำเนินงานวิจัย 16
3.1 การศึกษาและรวบรวมข้อมูล 16
3.2 การวิเคราะห์และออกแบบระบบ 18
3.3 การพัฒนาระบบ 31
3.4 การทดสอบระบบ 35
3.5 การนำระบบไปใช้งานจริง 36
3.6 การประเมินผลและวิเคราะห์ข้อมูล 36

3.7 การจัดทำเอกสารและรายงาน 39
บทที่ 4 ผลการดำเนินการวิจัย 40
4.1 ผลการพัฒนาระบบแต่ละโมดูล 40
4.2 ผลการทดลองใช้งานตามสถานการณ์ที่กำหนด 48
4.3 ผลการทดสอบความถูกต้องของระบบ 56
4.4 ผลการประเมินความคิดเห็นของผู้ใช้งานต่อระบบ 62
4.5 ข้อค้นพบจากการทดลองใช้งานระบบและการแสดงผลผ่าน Dashboard 65
บทที่ 5 สรุปผลและข้อเสนอแนะ 67
5.1 สรุปผลการวิจัย 67
5.2 อภิปรายผลการวิจัย 68
5.3 ข้อจำกัดของการวิจัย 70
5.4 ข้อเสนอแนะ 71
บรรณานุกรม 73
ประวัติผู้เขียน 76

พระจอมเกล้าพระนครเหนือ มหาวิทยาลัยเทคโนโลยี

สารบัญตาราง

หน้า

ตารางที่ 3-1 พจนานุกรมข้อมูลผู้ใช้งาน (users) 21
ตารางที่ 3-2 พจนานุกรมข้อมูลสินทรัพย์ (assets) 22
ตารางที่ 3-3 พจนานุกรมข้อมูลแคมเปญการประเมินช่องโหว่ (va_campaigns) 23
ตารางที่ 3-4 พจนานุกรมข้อมูลรอบการสแกน (va_scans) 23
ตารางที่ 3-5 พจนานุกรมข้อมูลช่องโหว่ (vulnerabilities) 24
ตารางที่ 3-6 พจนานุกรมข้อมูลรายงานผลการสแกน (scan_reports) 25
ตารางที่ 3-7 พจนานุกรมข้อมูลประวัติสถานะการแก้ไข (corrective_statuses) 26
ตารางที่ 3-8 พจนานุกรมข้อมูลเป้าหมายของรอบการสแกน (scan_targets) 26
ตารางที่ 3-9 พจนานุกรมข้อมูลตารางผู้ใช้งานที่เกี่ยวข้องกับรอบการสแกน (scan_users) 26
ตารางที่ 3-10 พจนานุกรมข้อมูลเกณฑ์ระดับความรุนแรง (severities) 27
ตารางที่ 3-11 พจนานุกรมข้อมูลแบบร่างอีเมล (email_templates) 28
ตารางที่ 3-12 สถานะการแก้ไขช่องโหว่ (Corrective Status) 32
ตารางที่ 3-13 ประเภทการดำเนินการแก้ไขช่องโหว่ (Corrective Action) 33
ตารางที่ 3-14 ประเภทการแจ้งเตือนทางอีเมล 33
ตารางที่ 3-15 บทบาทและสิทธิ์การเข้าถึงระบบ 34
ตารางที่ 4-1 ผลการทดสอบการนำเข้าข้อมูลจากไฟล์ CSV 57
ตารางที่ 4-2 ผลการทดสอบการจัดระดับความรุนแรง 58
ตารางที่ 4-3 ผลการทดสอบการควบคุมสิทธิ์ตามบทบาท 58
ตารางที่ 4-4 ผลการทดสอบระบบแจ้งเตือน 59
ตารางที่ 4-5 ผลการทดสอบความถูกต้องของ Dashboard และรายงาน 60
ตารางที่ 4-6 ผลการทดสอบการทำงานร่วมกันของระบบและประสิทธิภาพเบื้องต้น 61
ตารางที่ 4-7 ผลการประเมินด้านความง่ายในการใช้งานของระบบ 63
ตารางที่ 4-8 ผลการประเมินด้านประโยชน์ต่อการบริหารจัดการช่องโหว่ 63
ตารางที่ 4-9 ผลการประเมินด้านคุณภาพของข้อมูลและการแสดงผล 64
ตารางที่ 4-10 ผลการประเมินด้านประสิทธิภาพของระบบ 64
ตารางที่ 4-11 ผลการประเมินความพึงพอใจโดยรวม 65

สารบัญรูปภาพ

หน้า

ภาพที่ 3-1 แผนภาพความสัมพันธ์ระหว่างเอนทิตี (ER Diagram) ของระบบ 20
ภาพที่ 3-3 กระบวนการทำงานหลักของระบบ 29
ภาพที่ 3-4 โครงสร้างไฟล์ CSV ที่ส่งออกจาก Rapid7 InsightVM 31
ภาพที่ 4-1 หน้า Dashboard ภาพรวมของระบบ 41
ภาพที่ 4-2 หน้าจอแสดงรายการแคมเปญการประเมินช่องโหว่ 41
ภาพที่ 4-3 หน้าจอแสดงรายการรอบการสแกนภายใต้แคมเปญ 42
ภาพที่ 4-4 หน้าจอผลลัพธ์หลังการนำเข้าข้อมูล 42
ภาพที่ 4-5 หน้าจอรายการช่องโหว่ 43
ภาพที่ 4-6 หน้าจอรายละเอียดช่องโหว่ 44
ภาพที่ 4-7 หน้าจอบันทึกข้อมูล Corrective Action และสถานะการดำเนินการแก้ไข 44
ภาพที่ 4-8 หน้าจอแสดงรายละเอียดและลำดับเวลาการติดตาม Corrective Action 45
ภาพที่ 4-9 หน้าจอบันทึก Risk Acceptance 46
ภาพที่ 4-10 หน้าจอรายละเอียดหรือประวัติการยอมรับความเสี่ยง 46
ภาพที่ 4-11 หน้าจอจัดการ Email Template 47
ภาพที่ 4-12 หน้าจอกำหนดค่า Severity 47
ภาพที่ 4-13 หน้าจอกำหนดบทบาทและสิทธิ์การเข้าถึงของผู้ใช้งาน 48
ภาพที่ 4-14 หน้าจอสร้างรอบการสแกน 49
ภาพที่ 4-15 ตัวอย่างอีเมลแจ้งเตือนก่อนวันสแกน 49
ภาพที่ 4-16 หน้าจอรอบการสแกนหลังนำเข้ารายงานผลการสแกนและประมวลผลข้อมูล 50
ภาพที่ 4-17 ตัวอย่างอีเมลแจ้งเตือนเมื่อพบช่องโหว่ระดับรุนแรง 51
ภาพที่ 4-18 ตัวอย่างอีเมลแจ้งเตือนก่อนถึงกำหนดดำเนินการ 52
ภาพที่ 4-19 ตัวอย่างอีเมลแจ้งเตือนเมื่อถึงวันกำหนดดำเนินการ 52
ภาพที่ 4-20 ตัวอย่างอีเมลแจ้งเตือนเมื่อเกินกำหนดดำเนินการ 53
ภาพที่ 4-21 ตัวอย่างอีเมลแจ้งเตือนกรณีไม่มีการดำเนินการก่อนถึงวัน report date 7 วัน 54
ภาพที่ 4-22 หน้าจอแสดงรายการช่องโหว่ที่ยังมีสถานะ pending ก่อนถึงกำหนด report date 54
ภาพที่ 4-23 ตัวอย่างอีเมลแจ้งเตือนกรณีระบบเปลี่ยนรายการเข้าสู่เงื่อนไข Acceptance โดยอัตโนมัติ 55
ภาพที่ 4-24 หน้าจอแสดงประวัติการเปลี่ยนแปลงสถานะย้อนหลังของรายการช่องโหว่ 56

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานขององค์กร ภัยคุกคามทางไซเบอร์ก็มีความซับซ้อนและรุนแรงเพิ่มมากขึ้นอย่างต่อเนื่อง ตามรายงานของ National Vulnerability Database ในปี ค.ศ. 2024 มีการค้นพบช่องโหว่ความปลอดภัยใหม่มากกว่า 40,000 รายการ เพิ่มขึ้นร้อยละ 38 จากปีก่อนหน้า [1] ซึ่งสะท้อนให้เห็นถึงการขยายตัวของพื้นผิวการโจมตี (Attack Surface) ที่องค์กรต่างๆ ต้องเผชิญ หากช่องโหว่ความปลอดภัยเหล่านี้ไม่ได้รับการจัดการอย่างเหมาะสม ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากช่องโหว่ดังกล่าวในการโจมตีระบบสารสนเทศได้ ส่งผลให้เกิดความเสียหายทั้งทางด้านการเงิน ชื่อเสียง และความไว้วางใจจากผู้มีส่วนได้เสีย ตามรายงานของ IBM Security ปี ค.ศ. 2024 พบว่าร้อยละ 63 ของการเกิดเหตุการณ์ละเมิดข้อมูล (Data Breach) เกิดจากช่องโหว่ที่ยังไม่ได้รับการแก้ไข [2]

การบริหารจัดการช่องโหว่ (Vulnerability Management) จึงเป็นกระบวนการที่มีความสำคัญอย่างยิ่งต่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยทั่วไปแล้ว องค์กรต่างๆ ใช้เครื่องมือประเมินช่องโหว่ (Vulnerability Assessment Tools) เช่น Rapid7 InsightVM ในการสแกนและค้นหาช่องโหว่ภายในระบบของตน เครื่องมือเหล่านี้สามารถระบุช่องโหว่ได้อย่างมีประสิทธิภาพและให้คะแนนความรุนแรงตามระบบ Common Vulnerability Scoring System (CVSS) [3] อย่างไรก็ตาม เครื่องมือเหล่านี้มีข้อจำกัดสำคัญคือไม่มีระบบในการบริหารจัดการกระบวนการแก้ไขช่องโหว่แบบครบวงจร ตั้งแต่การติดตามสถานะการแก้ไข การแจ้งเตือนเจ้าของระบบ (System Owner) การบันทึกการยอมรับความเสี่ยง ไปจนถึงการตรวจสอบผลการแก้ไข

สำหรับองค์กรที่มีระบบสารสนเทศจำนวนมาก ปัญหาจะยิ่งทวีความซับซ้อนมากขึ้น เนื่องจากต้องทำการประเมินช่องโหว่ (Vulnerability Assessment) อย่างสม่ำเสมอ ซึ่งส่งผลให้มีช่องโหว่จำนวนมากที่ต้องติดตามและจัดการ การขาดระบบกลางในการบริหารจัดการทำให้เกิดปัญหาหลายประการ ได้แก่ ไม่สามารถติดตามได้ว่าช่องโหว่ใดได้รับการแก้ไขแล้ว ช่องโหว่ใดยังค้างอยู่ เจ้าของระบบไม่ทราบสถานะของระบบที่ตนรับผิดชอบ ไม่มีการแจ้งเตือนเมื่อใกล้ถึงกำหนดเวลาแก้ไข ไม่มีการบันทึกเหตุผลการยอมรับความเสี่ยงอย่างเป็นระบบ และไม่สามารถเปรียบเทียบผลการสแกนแต่ละครั้งเพื่อวิเคราะห์แนวโน้มได้

กรอบมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ เช่น NIST Cybersecurity Framework (CSF) เวอร์ชัน 2.0 [4] และ ISO/IEC 27001:2022 [5] ได้เน้นย้ำถึงความสำคัญของการบริหารจัดการช่องโหว่อย่างเป็นระบบ โดย NIST CSF กำหนดให้องค์กรต้องมีกระบวนการในการระบุ (Identify) ปกป้อง (Protect) ตรวจจับ (Detect) ตอบสนอง (Respond) และฟื้นฟู (Recover) จากภัยคุกคาม ในขณะที่ ISO 27001:2022 ภาคผนวก ก 8.8 กำหนดข้อกำหนดเฉพาะเกี่ยวกับการบริหารจัดการช่องโหว่ทางเทคนิค รวมถึงการระบุ ประเมิน และดำเนินการแก้ไขช่องโหว่อย่างทันท่วงที นอกจากนี้ มาตรฐาน PCI-DSS เวอร์ชัน 4.0 [6] ยังกำหนดให้ต้องทำการสแกนช่องโหว่ทุกไตรมาส และแก้ไขช่องโหว่ที่มีความรุนแรงสูง (Critical และ High) ภายในระยะเวลาที่กำหนด

แม้ว่าจะมีงานวิจัยและการพัฒนาระบบบริหารจัดการช่องโหว่มาก่อนหน้านี้ แต่ส่วนใหญ่มักเน้นไปที่การพัฒนาระบบที่ผูกติดกับเครื่องมือประเมินช่องโหว่เพียงตัวเดียว หรือเน้นเฉพาะการประเมินและจัดลำดับความสำคัญของช่องโหว่ โดยขาดระบบที่ครอบคลุมทั้งวงจรชีวิตของการแก้ไขช่องโหว่ (Vulnerability Lifecycle) ตั้งแต่การค้นพบไปจนถึงการตรวจสอบผล และที่สำคัญคือขาดความยืดหยุ่นในการรองรับข้อมูลจากเครื่องมือประเมินช่องโหว่หลากหลายประเภท ซึ่งเป็นความต้องการที่แท้จริงขององค์กรที่อาจต้องการใช้เครื่องมือหลายตัวร่วมกันหรือเปลี่ยนเครื่องมือในอนาคต

จากปัญหาและข้อจำกัดดังกล่าว การวิจัยนี้จึงมุ่งพัฒนาระบบบริหารจัดการช่องโหว่ความปลอดภัยสารสนเทศที่รองรับการนำเข้าข้อมูลผลการสแกนจากเครื่องมือ Rapid7 InsightVM ในรูปแบบไฟล์ CSV และสนับสนุนกระบวนการติดตามสถานะช่องโหว่ภายในองค์กรอย่างเป็นระบบ โดยระบบที่พัฒนาขึ้นครอบคลุมการนำเข้าข้อมูลผลการสแกน การจัดลำดับความสำคัญของช่องโหว่ การกำหนดและติดตามการดำเนินการแก้ไข การบันทึกการยอมรับความเสี่ยง การแจ้งเตือนผู้รับผิดชอบตามเงื่อนไขที่กำหนด และการแสดงผลข้อมูลผ่าน Dashboard ตามบทบาทของผู้ใช้งาน ทั้งนี้ ระบบดังกล่าวมีเป้าหมายเพื่อช่วยให้องค์กรสามารถติดตามและบริหารจัดการช่องโหว่ได้อย่างมีประสิทธิภาพมากขึ้น ลดความเสี่ยงจากการละเลยรายการช่องโหว่ และสนับสนุนการตรวจสอบย้อนหลังได้อย่างเป็นระบบ

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ ที่รองรับการนำเข้าข้อมูลผลการสแกนจากเครื่องมือประเมินช่องโหว่ในรูปแบบไฟล์ CSV โดยใช้ข้อมูลจาก Rapid7 InsightVM เป็นกรณีศึกษา

1.2.2 เพื่อออกแบบและพัฒนากลไกการติดตามสถานะช่องโหว่ การดำเนินการแก้ไข การยอมรับความเสี่ยง การแจ้งเตือนอัตโนมัติ และการแสดงผลผ่าน Dashboard และรายงานตามบทบาทของผู้ใช้งาน

1.2.3 เพื่อประเมินผลระบบที่พัฒนาขึ้นในด้านความถูกต้องของการทำงาน ความสามารถในการสนับสนุนกระบวนการบริหารจัดการช่องโหว่ และความคิดเห็นของผู้ใช้งานต่อระบบ

1.3 ขอบเขตของการวิจัย

1.3.1 เครื่องมือและเทคโนโลยีที่ใช้ในการพัฒนาระบบ

1.3.1.1 Laravel Framework สำหรับพัฒนาระบบด้วยภาษา PHP

1.3.1.2 Filament UI Framework สำหรับส่วนติดต่อผู้ใช้งาน (User Interface)

1.3.1.3 PostgreSQL สำหรับจัดเก็บฐานข้อมูล

1.3.1.4 Redis สำหรับรองรับ Queue และ Cache

1.3.1.5 Docker และ Docker Compose สำหรับสร้างแอปพลิเคชันในรูปแบบคอนเทนเนอร์ (Container)

1.3.2 ขอบเขตของข้อมูล

1.3.2.1 ข้อมูล Assets ที่อยู่ภายใต้การดูแลขององค์กร ครอบคลุมทั้ง Servers, Network Devices, Web Applications และ Databases

1.3.2.2 ข้อมูลช่องโหว่ที่มี Severity ระดับ Medium ขึ้นไป (Medium, High, Critical) ตามมาตรฐาน CVSS v3.1 [3]

1.3.2.3 ประวัติการแก้ไขช่องโหว่ย้อนหลังสำหรับการวิเคราะห์แนวโน้มและประเมินประสิทธิภาพ

1.3.2.4 ข้อมูลการยอมรับความเสี่ยง (Risk Acceptance) พร้อมเหตุผลประกอบและประวัติการดำเนินการที่เกี่ยวข้อง

1.3.3 ขอบเขตของ Vulnerability Lifecycle Management

1.3.3.1 Asset Inventory Management การดึงข้อมูล Assets จากระบบ Asset Inventory ที่มีอยู่และจัดการข้อมูลเจ้าของระบบ

1.3.3.2 Scan Scheduling & Notification การจัดรอบการสแกน การแจ้งเตือนเจ้าของระบบล่วงหน้าก่อนวันสแกน

1.3.3.3 Data Import & Processing การนำเข้าไฟล์ CSV จากเครื่องมือประเมินช่องโหว่ การแยกวิเคราะห์และทำให้ข้อมูลเป็นมาตรฐาน การตรวจจับช่องโหว่ใหม่และช่องโหว่ที่ถูกแก้ไขแล้ว

1.3.3.4 Risk Acceptance Management การบันทึกการยอมรับความเสี่ยง เหตุผลประกอบ และประวัติการดำเนินการเพื่อใช้ในการติดตามและตรวจสอบย้อนหลัง

1.3.3.5 Notification & Escalation การแจ้งเตือนอัตโนมัติเมื่อพบช่องโหว่ High/Critical การแจ้งเตือนติดตามความคืบหน้า

1.3.3.6 Reporting & Analytics Dashboard แสดงสถานะเรียลไทม์ การเปรียบเทียบผลระหว่างรอบการสแกน และการ Export รายงาน

1.3.4 ขอบเขตของกลุ่มผู้ใช้งานระบบ

1.3.4.1 System Owner สามารถดูข้อมูลเฉพาะระบบที่รับผิดชอบ ปรับปรุงสถานะการแก้ไข และบันทึก Risk Acceptance

1.3.4.2 Security Team สามารถดูข้อมูลทั้งหมด จัดการรอบการสแกน นำเข้าข้อมูล ติดตามสถานะการดำเนินการ และตรวจสอบข้อมูลการยอมรับความเสี่ยง

1.3.4.3 Auditor สามารถดู Audit Log Risk Acceptance Records และ Export รายงานเพื่อการตรวจสอบ

1.3.5 ขอบเขตของการประเมินผล

1.3.5.1 ประเมินความคิดเห็นของผู้ใช้งานต่อระบบด้วยแบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ (Likert Scale) จากผู้ใช้งานอย่างน้อย 30 คน ครอบคลุม System Owner, Security Team, Management และ Auditor

1.3.5.2 ทดสอบความถูกต้องของการนำเข้าและประมวลผลข้อมูลจาก CSV โดยเปรียบเทียบกับข้อมูลต้นทาง (Source Data) อย่างน้อย 100 รายการ

1.3.6 ข้อจำกัดของการวิจัย

1.3.6.1 ระบบในเฟสแรกรองรับเฉพาะการนำเข้าข้อมูลจาก Rapid7 InsightVM ในรูปแบบ CSV การรองรับเครื่องมือประเมินช่องโหว่อื่นจะเป็นการขยายผลในอนาคต

1.3.6.2 ไม่ครอบคลุมการทำ Vulnerability Scanning โดยตรง แต่เป็นการรับข้อมูลจากเครื่องมือประเมินช่องโหว่ที่มีอยู่แล้ว

1.3.6.3 การประเมินผลของระบบในงานวิจัยนี้อยู่ในขอบเขตของการทดลองใช้งานระบบต้นแบบและสถานการณ์ที่กำหนดในการวิจัย ยังไม่ได้มุ่งเน้นการติดตามผลการใช้งานจริงขององค์กรในระยะยาว

1.3.6.4 ไม่รวมถึงการพัฒนา Mobile Application สำหรับการใช้งานผ่านอุปกรณ์เคลื่อนที่

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ได้ระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ที่ช่วยสนับสนุนการนำเข้าข้อมูลผลการสแกน การติดตามสถานะการดำเนินการ การแจ้งเตือนผู้รับผิดชอบ การบันทึก

การยอมรับความเสี่ยง และการแสดงผลข้อมูลผ่าน Dashboard อย่างเป็นระบบ ซึ่งสามารถนำไปประยุกต์ใช้ในองค์กรได้

1.4.2 ช่วยเพิ่มความเป็นระบบและความต่อเนื่องในกระบวนการบริหารจัดการช่องโหว่ โดยเฉพาะการติดตามช่องโหว่ระดับ Critical และ High ทำให้ผู้เกี่ยวข้องสามารถตรวจสอบสถานะและดำเนินการได้สะดวกมากขึ้น และลดโอกาสการตกหล่นของรายการที่ต้องติดตาม

1.4.3 ช่วยเพิ่มความโปร่งใสและความรับผิดชอบในการบริหารจัดการช่องโหว่ เนื่องจากเจ้าของระบบและผู้ดูแลระบบ (System Owner/System Admin) ทีมรักษาความมั่นคงปลอดภัย (Security Team) และผู้ตรวจสอบ (Auditor) สามารถตรวจสอบข้อมูลตามบทบาทของตนเองได้ และมีประวัติการดำเนินการสำหรับใช้ตรวจสอบย้อนหลัง

1.4.4 เป็นแนวทางในการออกแบบและพัฒนาระบบบริหารจัดการช่องโหว่สำหรับองค์กรที่ต้องการปรับปรุงกระบวนการติดตามและแก้ไขช่องโหว่ และสามารถใช้เป็นพื้นฐานสำหรับการศึกษาหรือพัฒนาต่อยอดในอนาคต

พระจอมเกล้าพระนครเหนือ มหาวิทยาลัยเทคโนโลยี

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

บทนี้นำเสนอแนวคิด นิยาม และกรอบอ้างอิงที่เกี่ยวข้องกับช่องโหว่และการบริหารจัดการช่องโหว่ เพื่อใช้เป็นพื้นฐานในการพัฒนาระบบบริหารจัดการช่องโหว่ความปลอดภัยสารสนเทศที่รองรับการนำเข้าข้อมูลผลการสแกนจากเครื่องมือ Rapid7 InsightVM ในรูปแบบไฟล์ CSV โดยมุ่งเน้นการจัดลำดับความสำคัญของช่องโหว่ การติดตามการดำเนินการแก้ไขหรือการยอมรับความเสี่ยง การแจ้งเตือนผู้รับผิดชอบ และการแสดงผลข้อมูลเพื่อการกำกับติดตามในระดับองค์กร ทั้งนี้ เนื้อหาในบทนี้จะช่วยสนับสนุนการกำหนดข้อกำหนดของระบบและการออกแบบกระบวนการทำงานให้สอดคล้องกับหลักการและแนวปฏิบัติที่เป็นที่ยอมรับ

2.1 แนวคิดและนิยามเกี่ยวกับช่องโหว่และการบริหารจัดการช่องโหว่

ช่องโหว่ (Vulnerability) หมายถึง ความอ่อนแอในระบบสารสนเทศ ขั้นตอนด้านความมั่นคงปลอดภัย การควบคุมภายใน หรือการนำไปใช้งาน ที่อาจถูกใช้ประโยชน์ (exploited) หรือถูกกระตุ้น (triggered) โดยแหล่งคุกคาม จนนำไปสู่ความเสี่ยงด้านความมั่นคงปลอดภัยได้ แนวคิดนี้สะท้อนว่าช่องโหว่ไม่จำกัดเฉพาะข้อบกพร่องของซอฟต์แวร์เท่านั้น แต่รวมถึงความอ่อนแอจากกระบวนการการกำหนดค่าระบบ การควบคุมภายใน และการนำระบบไปใช้งานในบริบทจริงขององค์กร

แหล่งคุกคาม (Threat Source) หมายถึง เจตนาและวิธีการที่มุ่งใช้ประโยชน์จากช่องโหว่โดยตั้งใจ หรือสถานการณ์และวิธีการที่อาจกระตุ้นช่องโหว่โดยไม่ตั้งใจก็ได้ เมื่อพิจารณาร่วมกับนิยามของความเสี่ยง (Risk) ซึ่ง NIST อธิบายว่าเป็นมาตรวัดระดับที่สิ่งใดสิ่งหนึ่งถูกคุกคามโดยเหตุการณ์หรือสภาพการณ์ที่อาจเกิดขึ้น และโดยทั่วไปเป็นฟังก์ชันของผลกระทบด้านลบหากเหตุการณ์เกิดขึ้น และโอกาสการเกิดเหตุการณ์นั้น จะเห็นได้ว่าช่องโหว่เป็นองค์ประกอบสำคัญที่ทำให้ความเสี่ยงเกิดขึ้นได้จริง เพราะเป็นจุดที่แหล่งคุกคามสามารถใช้ประโยชน์หรือกระตุ้นให้เกิดผลกระทบต่อการดำเนินงานขององค์กร

ในทางปฏิบัติ จำเป็นต้องแยกความหมายของคำที่เกี่ยวข้องให้ชัดเจน กล่าวคือ การประเมินช่องโหว่ (Vulnerability Assessment) หมายถึง การตรวจสอบอย่างเป็นระบบของระบบสารสนเทศหรือผลิตภัณฑ์ เพื่อพิจารณาความเพียงพอของมาตรการความปลอดภัย ระบุข้อบกพร่องด้านความปลอดภัย ให้ข้อมูลเพื่อคาดการณ์ประสิทธิผลของมาตรการที่เสนอ และยืนยันความเพียงพอของมาตรการหลังการนำไปใช้ ขณะที่การสแกนช่องโหว่ (Vulnerability Scanning) เป็นเทคนิคที่ใช้เพื่อ

ระบุโฮสต์ คุณลักษณะของโฮสต์และช่องโหว่ที่เกี่ยวข้อง จึงอาจกล่าวได้ว่าการสแกนเป็นกิจกรรมเชิงเทคนิคที่เป็นส่วนหนึ่งของการประเมิน ขณะที่การประเมินมีขอบเขตกว้างกว่าและครอบคลุมการยืนยันผลหลังการนำมาตรการไปใช้ด้วย

การบริหารจัดการช่องโหว่ (Vulnerability Management) ในเชิงแนวปฏิบัติหมายถึงกระบวนการที่ดำเนินการอย่างต่อเนื่อง ตั้งแต่การค้นพบและรวบรวมข้อมูลช่องโหว่ การประเมินและจัดลำดับความสำคัญ การมอบหมายผู้รับผิดชอบ การดำเนินการแก้ไขหรือการกำหนดมาตรการลดความเสี่ยง การตรวจสอบยืนยันผล ตลอดจนการรายงานสถานะเพื่อการกำกับติดตาม ทั้งนี้ แนวปฏิบัติ CIS Controls v8 (Control 7: Continuous Vulnerability Management) ได้เน้นสาระสำคัญว่าองค์กรควรจัดทำแผนเพื่อประเมินและติดตามช่องโหว่อย่างต่อเนื่องบนสินทรัพย์ทั้งหมด เพื่อให้สามารถแก้ไขและลดช่วงเวลาแห่งโอกาสที่ผู้โจมตีจะใช้ประโยชน์จากช่องโหว่ได้

ในบริบทของการพัฒนาระบบบริหารจัดการกระบวนการแก้ไขช่องโหว่ความปลอดภัย ควรตระหนักถึงความแตกต่างระหว่าง ความรุนแรง (Severity) และความเสี่ยง (Risk) กล่าวคือ ความรุนแรงมักสะท้อนคุณลักษณะเชิงเทคนิคของช่องโหว่ที่วัดได้จากกรอบมาตรฐาน เช่น CVSS ขณะที่ความเสี่ยงเป็นการพิจารณาเชิงบริบทที่รวมทั้งโอกาสและผลกระทบตามคุณค่าของสินทรัพย์ ดังนั้นระบบจึงควรรองรับการจัดเก็บข้อมูลเพื่อสะท้อนบริบทขององค์กร เช่น ความสำคัญของสินทรัพย์ ผู้รับผิดชอบ ข้อจำกัดทางเทคนิค และหลักฐานการดำเนินการ เพื่อทำให้การตัดสินใจด้านการจัดลำดับและการกำกับติดตามมีความเหมาะสมและตรวจสอบได้

2.2 วงจรชีวิตการจัดการช่องโหว่ (Vulnerability Management Lifecycle)

วงจรชีวิตการจัดการช่องโหว่เป็นแนวคิดที่อธิบายการดำเนินงานด้านช่องโหว่ในลักษณะต่อเนื่องและเป็นวงรอบ โดยมีเป้าหมายให้การค้นพบช่องโหว่เชื่อมต่อไปสู่การแก้ไขและการยืนยันผลอย่างเป็นระบบ มิใช่สิ้นสุดที่การจัดทำรายงานผลการสแกนเพียงอย่างเดียว หลักการดังกล่าวสอดคล้องกับ CIS Controls (Control 7) ที่กำหนดให้มีการประเมินและติดตามช่องโหว่อย่างต่อเนื่องเพื่อสนับสนุนการแก้ไขและลดโอกาสการถูกโจมตี

เพื่อให้เกิดความชัดเจนในเชิงกระบวนการ วงจรชีวิตการจัดการช่องโหว่สามารถอธิบายเป็นลำดับกิจกรรมหลักที่เชื่อมโยงกัน ได้แก่ การกำหนดขอบเขตและการระบุสินทรัพย์ การสแกนและรวบรวมข้อมูล การวิเคราะห์และประเมินผล การจัดลำดับความสำคัญ การดำเนินการแก้ไขหรือการลดความเสี่ยง การตรวจสอบยืนยันผล และการรายงานเพื่อการปรับปรุงอย่างต่อเนื่อง

2.2.1 การกำหนดขอบเขตและการระบุสินทรัพย์ (Scope and Asset Identification) เป็นขั้นตอนการกำหนดขอบเขตของสินทรัพย์ที่ต้องประเมิน และระบุผู้เป็นเจ้าของหรือผู้รับผิดชอบให้ชัดเจน เพื่อให้การติดตามในภายหลังเป็นไปอย่างมีประสิทธิภาพ โดยครอบคลุมทั้งระบบเครือข่าย

เซิร์ฟเวอร์ แอปพลิเคชัน และบริการต่าง ๆ รวมถึงการกำหนดรอบการประเมินตามข้อจำกัดด้านทรัพยากรและระดับความเสี่ยงขององค์กร

2.2.2 การสแกนและรวบรวมข้อมูล (Scanning and Data Collection) เป็นขั้นตอนการใช้เทคนิคการสแกนช่องโหว่เพื่อระบุโฮสต์ คุณลักษณะของโฮสต์ และช่องโหว่ที่เกี่ยวข้อง โดยผลลัพธ์ที่ได้มักอยู่ในรูปแบบรายงานเชิงเทคนิคหรือไฟล์ข้อมูลที่สามารถส่งออกได้ ซึ่งเอื้อต่อการนำข้อมูลเข้าสู่ระบบกลางเพื่อใช้ในการติดตาม วิเคราะห์ และบริหารจัดการช่องโหว่ต่อไป

2.2.3 การวิเคราะห์และประเมินผล (Analysis and Assessment) เป็นการตีความผลการสแกนเพื่อทำความเข้าใจเงื่อนไขที่ทำให้เกิดช่องโหว่ ผลกระทบที่อาจเกิดขึ้น ความถูกต้องของการตรวจพบ และแนวทางการแก้ไขที่เหมาะสม ทั้งนี้แนวคิดการประเมินช่องโหว่ของ NIST เน้นว่ากระบวนการประเมินควรรวมถึงการยืนยันความเพียงพอของมาตรการหลังการนำไปใช้ ซึ่งสะท้อนหลักการสำคัญว่ากระบวนการต้องวนกลับมาทดสอบและยืนยัน ไม่ใช่เพียงสั่งแก้แล้วจบ

2.2.4 การจัดลำดับความสำคัญ (Prioritization) เป็นการตัดสินใจว่ารายการใดควรแก้ก่อนโดยใช้ข้อมูลความรุนแรงของช่องโหว่ประกอบ รวมถึงบริบทของสินทรัพย์ ความสำคัญต่อภารกิจ ความเชื่อมโยงกับระบบอื่น และข้อจำกัดในการแก้ไข เพื่อให้ทรัพยากรที่มีอยู่ถูกใช้ไปกับรายการที่สำคัญที่สุด

2.2.5 การดำเนินการแก้ไขหรือการลดความเสี่ยง (Remediation and Mitigation) เป็นขั้นตอนการดำเนินมาตรการเพื่อปิดช่องโหว่หรือทำให้ความเสี่ยงลดลง เช่น การติดตั้งแพตช์ การอัปเดตหรืออัปเกรด การปรับค่าการตั้งค่า และการใช้มาตรการควบคุมชดเชย รวมถึงการกำหนดกรอบเวลาและติดตามความคืบหน้าของการดำเนินงาน

2.2.6 ตรวจสอบยืนยันผล (Verification) เป็นการตรวจสอบว่ามาตรการที่ดำเนินการแล้วได้ผลจริง โดยอาจทำได้ด้วยการสแกนซ้ำ การตรวจสอบการตั้งค่าระบบ หรือการตรวจสอบหลักฐานจากผู้รับผิดชอบ ขั้นตอนนี้มีบทบาทสำคัญต่อความน่าเชื่อถือของระบบติดตามงาน เพราะทำให้สถานะปิดงาน มีหลักฐานรองรับและตรวจสอบได้

2.2.7 การรายงานและการปรับปรุงอย่างต่อเนื่อง (Reporting and Continuous Improvement) เป็นการสรุปสถานะ ผลการดำเนินการ และแนวโน้ม เพื่อสนับสนุนการกำกับติดตามและการปรับปรุงแผนการประเมินการแก้ไขในรอบถัดไป

วงจรชีวิตดังกล่าวทำให้การบริหารจัดการช่องโหว่กลายเป็นกระบวนการที่มีความต่อเนื่องและมีการปิดงานอย่างเป็นระบบ ซึ่งเป็นฐานแนวคิดสำคัญต่อการออกแบบระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ให้รองรับการทำงานจริง เช่น การจัดทำรอบการสแกน การนำเข้าไฟล์ผลสแกน การกำหนดสถานะงาน การแจ้งเตือนตามกำหนดเวลา และการเก็บหลักฐานเพื่อรองรับการตรวจสอบย้อนหลัง

2.3 กรอบมาตรฐานและแนวปฏิบัติที่เกี่ยวข้องกับการบริหารจัดการช่องโหว่

กรอบมาตรฐานและแนวปฏิบัติทำหน้าที่เป็นฐานอ้างอิงในการกำหนดแนวทางการบริหารความเสี่ยงและการควบคุมด้านความมั่นคงปลอดภัยให้มีความเป็นระบบ สื่อสารได้ และตรวจสอบได้ งานวิจัยนี้พิจารณากรอบอ้างอิงที่สัมพันธ์กับการบริหารจัดการช่องโหว่โดยตรง ดังนี้

NIST Cybersecurity Framework (CSF) 2.0 เป็นกรอบแนวทางที่ให้อนุกรมวิธานของผลลัพธ์ระดับสูง เพื่อให้องค์กรใช้ทำความเข้าใจ ประเมิน จัดลำดับ และสื่อสารความพยายามด้านความมั่นคงปลอดภัยไซเบอร์ โดยไม่ได้กำหนดวิธีการตายตัวในการบรรลุผลลัพธ์นั้น ด้วยเหตุนี้ CSF 2.0 จึงเหมาะสำหรับการใช้เป็นกรอบภาพรวมในระดับองค์กรเพื่อเชื่อมโยงงานด้านช่องโหว่เข้ากับการบริหารความเสี่ยง การกำกับดูแล และการรายงานต่อผู้บริหาร

CIS Controls v8 (Control 7) เป็นแนวปฏิบัติที่มุ่งให้หน่วยงานจัดทำแผนในการประเมินและติดตามช่องโหว่ของสินทรัพย์ทั้งหมดอย่างต่อเนื่องเพื่อการแก้ไขและลดช่วงเวลาแห่งโอกาสของผู้โจมตี กรอบดังกล่าวมีประโยชน์ในเชิงปฏิบัติการสำหรับการกำหนดความถี่การสแกน การกำหนดกระบวนการติดตาม การกำหนดกรอบเวลา และการติดตามผลการแก้ไขให้จบ

NIST SP 800-53 Rev. 5 ในหมวด RA-5 (Vulnerability Monitoring and Scanning) กำหนดแนวทางการควบคุมในระดับองค์กรสำหรับการติดตามและการสแกนช่องโหว่ โดยเน้นให้องค์กรดำเนินการตามความถี่และกระบวนการที่กำหนดไว้อย่างเหมาะสม พร้อมทั้งส่งเสริมการใช้เครื่องมือและเทคนิคที่สนับสนุนการทำงานร่วมกันระหว่างระบบ และการทำให้บางส่วนของกระบวนการบริหารจัดการช่องโหว่เป็นไปโดยอัตโนมัติภายใต้มาตรฐานที่เกี่ยวข้อง

NIST SP 800-40 Rev. 4 เป็นเอกสารแนวทางด้านการจัดการแพตช์ในระดับองค์กรที่อธิบายกระบวนการอย่างเป็นลำดับ ตั้งแต่การระบุ การจัดลำดับความสำคัญ การจัดหา การติดตั้ง และการตรวจสอบยืนยันผลของแพตช์ การอัปเดต หรือการอัปเกรดทั่วทั้งองค์กร แนวคิดดังกล่าวจึงเป็นพื้นฐานสำคัญของกระบวนการแก้ไขช่องโหว่และการยืนยันผล ซึ่งเป็นขั้นตอนหลักของวงจรชีวิตการบริหารจัดการช่องโหว่

2.4 แนวคิดการให้คะแนนความรุนแรงของช่องโหว่ด้วย CVSS

ในการสื่อสารระดับความรุนแรงของช่องโหว่ในทางปฏิบัติ มักอาศัย Common Vulnerability Scoring System (CVSS) ซึ่งเป็นกรอบมาตรฐานแบบเปิดที่ใช้สำหรับอธิบายลักษณะและระดับความรุนแรงของช่องโหว่ด้านซอฟต์แวร์ โดย CVSS v3.1 แบ่งชุดเมตริกออกเป็น 3 กลุ่ม ได้แก่ Base Metrics, Temporal Metrics และ Environmental Metrics

Base Metrics ใช้สะท้อนคุณลักษณะโดยเนื้อแท้ของช่องโหว่ ซึ่งโดยทั่วไปคงที่ไม่เปลี่ยนแปลงตามเวลาและสภาพแวดล้อมในการใช้งาน ส่วน Temporal Metrics ใช้สะท้อนปัจจัยที่สามารถ

เปลี่ยนแปลงได้ตามช่วงเวลา เช่น ความพร้อมของโค้ดโจมตี สถานะของการแก้ไข หรือระดับความเชื่อมั่นของข้อมูลที่เกี่ยวข้องกับช่องโหว่ ขณะที่ Environmental Metrics ใช้สะท้อนปัจจัยเฉพาะของสภาพแวดล้อมผู้ใช้งาน เช่น ความสำคัญของทรัพยากรสารสนเทศในองค์กร และเงื่อนไขแวดล้อมที่อาจส่งผลให้ระดับผลกระทบของช่องโหว่แตกต่างกันไปในแต่ละองค์กร

อย่างไรก็ตาม ในการนำคะแนน CVSS ไปประยุกต์ใช้ภายในระบบบริหารจัดการช่องโหว่ ผู้ใช้งานควรตระหนักว่า CVSS มีจุดมุ่งหมายเพื่อสื่อสาร “ความรุนแรง” (Severity) ในเชิงเทคนิค มิใช่ “ความเสี่ยง” (Risk) ในเชิงองค์กรโดยสมบูรณ์ เนื่องจากระดับความเสี่ยงที่แท้จริงยังขึ้นอยู่กับบริบทของสินทรัพย์ ผลกระทบต่อภารกิจหรือธุรกิจ สภาพแวดล้อมการใช้งานจริง ตลอดจนความสามารถและโอกาสของผู้ไม่หวังดีในการใช้ประโยชน์จากช่องโหว่นั้น ดังนั้น ระบบที่พัฒนาขึ้นควรเปิดให้สามารถกำหนดเกณฑ์ระดับความรุนแรงที่ต้องรายงาน (Reportable Severity) และเชื่อมโยงคะแนน CVSS เข้ากับบริบทของสินทรัพย์และผู้รับผิดชอบ เพื่อสนับสนุนการตัดสินใจและการจัดลำดับความสำคัญในการดำเนินงานได้อย่างเหมาะสม

2.5 แนวคิดการแก้ไขช่องโหว่ การจัดการแพตช์ และการยืนยันผล

การแก้ไขช่องโหว่ (Remediation) เป็นขั้นตอนสำคัญที่ทำให้การบริหารจัดการช่องโหว่เกิดผลในทางปฏิบัติ โดยแนวทางการแก้ไขอาจประกอบด้วยการติดตั้งแพตช์ การอัปเดตหรืออัปเกรดซอฟต์แวร์ การปรับค่าความมั่นคงปลอดภัย การปิดบริการที่ไม่จำเป็น หรือการเพิ่มมาตรการควบคุมชดเชยเพื่อลดความเสี่ยง

แนวทาง NIST SP 800-40 Rev. 4 ให้นิยามการจัดการแพตช์ในระดับองค์กรว่าเป็นกระบวนการที่ครอบคลุมการระบุ การจัดลำดับความสำคัญ การจัดหา การติดตั้ง และการตรวจสอบยืนยันผลของแพตช์ การอัปเดต และการอัปเกรดทั่วทั้งองค์กร ซึ่งสะท้อนว่าการจัดการแพตช์มิใช่เพียงการติดตั้งซอฟต์แวร์ แต่เป็นกระบวนการที่ต้องมีการวางแผน การประสานงาน และการควบคุมอย่างเหมาะสม เพื่อลดความเสี่ยงจากความผิดพลาดและลดผลกระทบต่อการให้บริการ

หัวใจสำคัญของการจัดการแพตช์และการแก้ไขช่องโหว่คือการยืนยันผล (Verification) เนื่องจากการเปลี่ยนสถานะว่าแก้ไขแล้วโดยไม่มีหลักฐานประกอบหรือไม่มีการตรวจสอบยืนยัน อาจทำให้ความเสี่ยงยังคงอยู่ หรือก่อให้เกิดผลกระทบจากการแก้ไขที่ไม่สมบูรณ์ แนวคิดนี้สอดคล้องกับนิยามของ Vulnerability Assessment ตามแนวทางของ NIST ที่ระบุถึงการยืนยันความเพียงพอของมาตรการหลังการนำไปใช้ ดังนั้น ในเชิงการพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ควรรองรับการบันทึกการดำเนินการแก้ไข เช่น วันที่ดำเนินการ ผู้ดำเนินการ แนวทางการแก้ไข การเปลี่ยนแปลงการตั้งค่า และแนบหลักฐานประกอบ รวมถึงรองรับการสแกนซ้ำเพื่อยืนยันผลเมื่อครบกำหนด

2.6 แนวคิดการยอมรับความเสี่ยงและการตรวจสอบย้อนหลัง

ในบางกรณี ช่องโหว่อาจไม่สามารถดำเนินการแก้ไขได้ทันที เช่น ยังไม่มีแพตช์ที่เหมาะสม การแก้ไขอาจส่งผลกระทบต่อการทำงานของระบบในระดับสูง หรือองค์กรมีข้อจำกัดด้านทรัพยากร ในสถานการณ์ดังกล่าว องค์กรจึงอาจพิจารณาแนวทางการตอบสนองต่อความเสี่ยง (Risk Response) ซึ่ง NIST อธิบายว่าเป็นกระบวนการตัดสินใจและการดำเนินการอย่างมีเจตนา ภายใต้ข้อมูลประกอบที่เพียงพอ เพื่อยอมรับ หลีกเลี่ยง บรรเทา แบ่งปัน หรือโอนย้ายความเสี่ยงที่ได้รับการระบุแล้ว ขณะเดียวกัน แนวคิดเรื่องความเสี่ยงที่ยอมรับได้ (Acceptable Risk) หมายถึง ระดับความเสี่ยงคงเหลือที่องค์กรสามารถยอมรับได้ ภายใต้เกณฑ์และขอบเขตการบริหารความเสี่ยงที่กำหนดไว้ รวมถึงระดับความทนทานต่อความเสี่ยง (Risk Tolerance) ขององค์กร

ดังนั้น การยอมรับความเสี่ยงจึงมิใช่การละเว้นการดำเนินการโดยปราศจากเหตุผล หากแต่เป็นการตัดสินใจเชิงบริหารภายใต้กรอบการจัดการความเสี่ยงที่ต้องมีข้อมูลรองรับอย่างเหมาะสม และต้องอยู่ภายใต้การกำกับติดตามอย่างต่อเนื่อง เพื่อป้องกันไม่ให้การยอมรับความเสี่ยงกลายเป็นการปล่อยค้างช่องโหว่โดยขาดหลักธรรมาภิบาล ทั้งนี้ ภายใต้กรอบการบริหารความเสี่ยง RMF ของ NIST SP 800-37 Rev.2 ได้ให้ความสำคัญกับการตัดสินใจด้านความเสี่ยงและการอนุญาตให้ระบบดำเนินงาน โดยเน้นความสม่ำเสมอ ความต่อเนื่อง และการติดตามอย่างต่อเนื่อง (Continuous Monitoring)

ด้วยเหตุนี้ ระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์จึงควรสนับสนุนการบันทึกการยอมรับความเสี่ยงในรูปแบบที่สามารถตรวจสอบย้อนหลังได้ โดยอย่างน้อยควรมีการบันทึกเหตุผลประกอบการยอมรับความเสี่ยง ขอบเขตหรือเงื่อนไขที่เกี่ยวข้อง และประวัติการเปลี่ยนแปลงข้อมูล (Audit Trail) เพื่อให้สามารถใช้เป็นข้อมูลอ้างอิงในการติดตาม ตรวจสอบ และทบทวนความเหมาะสมของการตัดสินใจในภายหลังได้อย่างเป็นระบบ

2.7 แนวคิดการกำหนดบทบาทและสิทธิ์การเข้าถึง

ระบบบริหารจัดการช่องโหว่เกี่ยวข้องกับผู้ใช้งานหลายบทบาท จึงจำเป็นต้องมีการควบคุมสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อรักษาความลับของข้อมูลเชิงเทคนิค ลดความเสี่ยงจากการเข้าถึงโดยไม่จำเป็น และสร้างความรับผิดชอบ (Accountability) ตามสายงาน

Role-Based Access Control (RBAC) เป็นแนวคิดการควบคุมการเข้าถึงที่กำหนดสิทธิ์ผ่านบทบาท โดยผูกการอนุญาต (Permissions) เข้ากับบทบาท แล้วมอบบทบาทให้ผู้ใช้ตามหน้าที่ความรับผิดชอบ วิธีนี้ทำให้การจัดการสิทธิ์เป็นระบบและสามารถขยายตัวรองรับจำนวนผู้ใช้ที่เพิ่มขึ้นได้อย่างมีประสิทธิภาพ การนำ RBAC มาประยุกต์ใช้กับระบบบริหารจัดการช่องโหว่ช่วยให้สามารถกำหนดขอบเขตการมองเห็นและการดำเนินการได้อย่างเหมาะสมตามบทบาท เช่น เจ้าของระบบ

มองเห็นเฉพาะรายการของตนเอง ขณะที่ผู้กำกับดูแลสามารถเห็นภาพรวมในระดับองค์กร ส่งผลให้การทำงานมีความปลอดภัย มีการแบ่งแยกหน้าที่ (Segregation of Duties) และสามารถตรวจสอบได้

2.8 แนวคิดการนำเข้าข้อมูลจากเครื่องมือสแกนและการทำข้อมูลให้เป็นมาตรฐาน

ระบบบริหารจัดการช่องโหว่ที่รองรับการทำงานจริงจำเป็นต้องจัดการข้อมูลจากหลายแหล่ง เช่น ผลจากเครื่องมือประเมินช่องโหว่ ข้อมูลสินทรัพย์จากระบบ Inventory และข้อมูลการดำเนินการแก้ไขจากผู้รับผิดชอบ การนำเข้าข้อมูลผลการสแกนจึงควรคำนึงถึงความถูกต้อง ความครบถ้วน ความสอดคล้อง และความสามารถในการเปรียบเทียบข้ามรอบเวลา โดยเฉพาะเมื่อองค์กรมีข้อจำกัดในการสแกนทั้งหมดในคราวเดียวและต้องแบ่งเป็นรอบ

ในทางปฏิบัติเครื่องมือสแกนช่องโหว่มักสนับสนุนการจัดทำรายงานและส่งออกข้อมูลในรูปแบบที่เครื่องอ่านได้เพื่อให้สามารถนำไปประมวลผลต่อ ตัวอย่างเช่น Rapid7 InsightVM รองรับการสร้างเทมเพลตส่งออก (export templates) โดยสามารถเลือกแอตทริบิวต์ของข้อมูลช่องโหว่ได้ และมีการสนับสนุนการส่งออกข้อมูลในรูปแบบ CSV ภายใต้เทมเพลตที่กำหนด เพื่อให้สามารถนำข้อมูลไปใช้งานต่อได้

อย่างไรก็ตาม เนื่องจากโครงสร้างข้อมูล ชื่อฟิลด์ การจัดกลุ่มระดับความรุนแรง และรายละเอียดเชิงเทคนิคของรายงานอาจแตกต่างกันตามเครื่องมือและตามรูปแบบเทมเพลต จึงมีความจำเป็นต้องทำข้อมูลให้เป็นมาตรฐาน (Standardization) เพื่อให้ระบบสามารถรวมข้อมูลจากหลายรอบการสแกน เปรียบเทียบแนวโน้ม และรายงานผลอย่างเป็นเอกภาพ โดย NIST SP 800-53 RA-5 ได้กล่าวถึงการใช้เครื่องมือหรือเทคนิคที่เอื้อต่อการทำงานร่วมกันและการทำให้อัตโนมัติบางส่วนของกระบวนการบริหารจัดการช่องโหว่โดยใช้มาตรฐานที่เหมาะสม อีกทั้ง NIST ได้พัฒนาแนวคิด SCAP (Security Content Automation Protocol) ซึ่งเป็นชุดสเปกแบบทำงานร่วมกัน (interoperable specifications) สำหรับการแสดงออก การแลกเปลี่ยน และการประมวลผลข้อมูลด้านการตั้งค่าความมั่นคงปลอดภัยและข้อมูลช่องโหว่ในรูปแบบมาตรฐาน เพื่อให้เกิดการทำงานอัตโนมัติและการรายงานที่สอดคล้องกันข้ามผลิตภัณฑ์และสภาพแวดล้อม

ดังนั้น ในการพัฒนาระบบระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์จึงควรกำหนดแบบจำลองข้อมูลกลาง (common data model) เพื่อจัดเก็บข้อมูลหลักได้แก่ ข้อมูลสินทรัพย์และตัวระบุ ข้อมูลช่องโหว่ ข้อมูลการตรวจพบที่ผูกกับรอบการสแกนและแหล่งที่มา ข้อมูลความรุนแรงและคะแนน ข้อมูลการดำเนินการและกำหนดเวลา ข้อมูลการยืนยันผล และประวัติการเปลี่ยนแปลง เป็นอย่างน้อย เพื่อให้ระบบสามารถรองรับการติดตาม การแจ้งเตือน และการรายงานเชิงเปรียบเทียบได้อย่างถูกต้อง ตรวจสอบได้ และนำไปใช้ประโยชน์ในเชิงบริหารจัดการได้จริง

2.9 งานวิจัยที่เกี่ยวข้อง

การบริหารจัดการช่องโหว่ความปลอดภัยเป็นกระบวนการที่มีความสำคัญอย่างยิ่งในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ งานวิจัยของ Walkowski และ Sujecki ได้นำเสนอโมเดลการบริหารจัดการช่องโหว่ที่ใช้ Common Vulnerability Scoring System (CVSS) เป็นพื้นฐานในการจัดลำดับความสำคัญ และเน้นย้ำถึงความสำคัญของการทำความเข้าใจบริบทขององค์กร [8] ผู้วิจัยชี้ให้เห็นว่าการใช้เพียงคะแนน CVSS อย่างเดียวไม่เพียงพอ เนื่องจากไม่ได้คำนึงถึงสภาพแวดล้อมเฉพาะขององค์กร วงจรชีวิตการจัดการช่องโหว่ (Vulnerability Management Lifecycle) โดยทั่วไปประกอบด้วยขั้นตอนหลัก ได้แก่ การระบุและประเมิน การจัดลำดับความสำคัญ การแก้ไขและลดความเสี่ยง การตรวจสอบและยืนยัน การรายงาน และการติดตามและปรับปรุง โดยหลักการสำคัญคือต้องเป็นกระบวนการต่อเนื่องและมีการปรับปรุงอย่างสม่ำเสมอ Mahouachi และคณะ [9] ได้ทำการสำรวจวิธีการตรวจจับช่องโหว่อย่างครอบคลุม และชี้ให้เห็นถึงปัญหาที่เกี่ยวข้องกับการจัดการฐานข้อมูลช่องโหว่ ซึ่งส่งผลต่อประสิทธิภาพของวิธีการระบุช่องโหว่บางประเภท นอกจากนี้ Shahzad และคณะ [10] ได้ทำการวิเคราะห์วงจรชีวิตของช่องโหว่ซอฟต์แวร์ในวงกว้าง โดยพบว่าระยะเวลาตั้งแต่การเปิดเผยช่องโหว่จนถึงการมีแพตช์ (Patch) มีความแตกต่างกันอย่างมากขึ้นอยู่กับผู้พัฒนาและประเภทของซอฟต์แวร์ การศึกษานี้เน้นย้ำถึงความสำคัญของการมีระบบติดตามช่องโหว่ที่มีประสิทธิภาพ

การจัดลำดับความสำคัญของช่องโหว่เป็นขั้นตอนที่มีความสำคัญอย่างยิ่งในกระบวนการบริหารจัดการช่องโหว่ เนื่องจากจำนวนช่องโหว่ที่ค้นพบในแต่ละปีมีจำนวนมหาศาล งานวิจัยของ Jacobs และคณะ แสดงให้เห็นว่าการใช้ Exploit Prediction Scoring System (EPSS) ร่วมกับ CVSS สามารถลดจำนวนช่องโหว่ที่ต้องแก้ไขได้อย่างมาก จากการศึกษาพบว่าหากจัดลำดับความสำคัญโดยใช้เฉพาะช่องโหว่ที่มีคะแนน CVSS ตั้งแต่ 7.0 ขึ้นไป จะต้องได้รับการแก้ไขประมาณร้อยละ 57 ของช่องโหว่ทั้งหมด แต่มีเพียงร้อยละ 2.3 เท่านั้นที่ถูกใช้ประโยชน์ในการโจมตี (Exploit) จริง ในขณะที่การใช้ EPSS threshold ที่ 10% จะแก้ไขเพียงร้อยละ 2.7 ของช่องโหว่ทั้งหมด แต่สามารถครอบคลุมช่องโหว่ที่ถูกใช้ประโยชน์ในการโจมตีได้ถึงร้อยละ 63 [11] ซึ่งแสดงให้เห็นถึงประสิทธิภาพของการใช้การเรียนรู้ของเครื่อง (Machine Learning) ในการทำนายความเสี่ยงของช่องโหว่ งานวิจัยของ Allodi และ Massacci นำเสนอผลการเปรียบเทียบความรุนแรงของช่องโหว่กับการถูกใช้ประโยชน์ในการโจมตีจริงโดยใช้การศึกษาเปรียบเทียบกรณีและกลุ่มควบคุม (Case-Control Studies) และพบว่าคะแนน CVSS มีความสัมพันธ์ต่ำกับความน่าจะเป็นที่ช่องโหว่จะถูกใช้ประโยชน์ในการโจมตี [12] ผู้วิจัยเสนอให้ใช้ปัจจัยอื่นร่วมด้วย เช่น ความพร้อมใช้งานของโปรแกรมหรือสคริปต์ที่ออกแบบมาเพื่อใช้ประโยชน์จากช่องโหว่ (Exploit Code) และมูลค่าของเป้าหมาย นอกจากนี้ Holm และคณะได้ทำการวิเคราะห์ตัวชี้วัดช่องโหว่ (Vulnerability Metrics) เชิงประจักษ์ในระดับ

ระบบผ่านการโจมตีจริง และพบว่าหลายตัวชี้วัดที่ใช้กันอยู่ไม่สามารถทำนายความเสี่ยงได้แม่นยำในสภาพแวดล้อมจริง [13]

การพัฒนาระบบบริหารจัดการช่องโหว่ที่มีประสิทธิภาพเป็นหัวข้อที่ได้รับความสนใจอย่างมาก ในงานวิจัยทางวิชาการ Varela-Vaca และคณะได้พัฒนาระบบ AMADEUS ที่ใช้แบบจำลองคุณลักษณะ (Feature Models) ในการบริหารจัดการช่องโหว่ โดยเน้นการเชื่อมโยงข้อมูลจากหลายแหล่งแบบอัตโนมัติเพื่อใช้ในการวิเคราะห์ [14] งานวิจัยนี้แสดงให้เห็นถึงความสำคัญของการมีมาตรฐานแบบจำลองข้อมูล (Standardized Data Model) ที่สามารถรองรับข้อมูลจากแหล่งต่าง ๆ และเสนอแนวทางในการจัดการความซับซ้อนของข้อมูลช่องโหว่ที่มาจากหลากหลายเครื่องมือ Toprani และ Madisetti [15] ได้นำเสนอกระบวนการทำงานแบบเอเจนต์ของโมเดลภาษาขนาดใหญ่ (LLM Agentic Workflow) สำหรับการตรวจจับและแก้ไขช่องโหว่อัตโนมัติในโครงสร้างพื้นฐานแบบโค้ด (Infrastructure as Code : IaC) โดยใช้ Large Language Models (LLM) และการสร้าง Retrieval-Augmented Generation (RAG) ซึ่งบรรลุอัตราการตรวจจับร้อยละ 85 วิธีการนี้แสดงให้เห็นถึงแนวโน้มการใช้ปัญญาประดิษฐ์ (AI) และระบบอัตโนมัติในการบริหารจัดการช่องโหว่ที่กำลังได้รับความสนใจในปัจจุบัน นอกจากนี้ Goutam และ Tiwari ได้นำเสนอแนวทางในการประเมินช่องโหว่และการทดสอบการเจาะระบบเพื่อเพิ่มความปลอดภัยของเว็บแอปพลิเคชัน โดยเน้นการใช้เครื่องมืออัตโนมัติร่วมกับการทดสอบด้วยมือเพื่อเพิ่มความแม่นยำและลดผลบวกลวง (False Positives) [16]

การเชื่อมโยงระบบบริหารจัดการช่องโหว่กับเครื่องมือประเมินช่องโหว่ต่างๆ เป็นความท้าทายสำคัญ เนื่องจากแต่ละเครื่องมือมีรูปแบบข้อมูลและ API ที่แตกต่างกัน Rivera Pérez และคณะได้ทำการศึกษาแนวปฏิบัติในการบริหารจัดการช่องโหว่ของผู้ให้บริการที่เน้น IoT และพบว่าการขาดมาตรฐานในการรายงานช่องโหว่เป็นอุปสรรคสำคัญต่อการบริหารจัดการที่มีประสิทธิภาพ [17] ผู้วิจัยเสนอแนวทางในการปรับปรุงการสื่อสารระหว่างผู้ให้บริการและผู้ใช้งาน เพื่อให้การแก้ไขช่องโหว่เป็นไปอย่างรวดเร็วและมีประสิทธิภาพมากขึ้น งานวิจัยของ Rivera และคณะนำเสนอการประเมินช่องโหว่ในสถาบันการศึกษาระดับอุดมศึกษาจำนวน 272 แห่ง และพบว่ารายงานที่สร้างจากเครื่องมือสแกนมักทำให้เกิดภาระข้อมูลมากเกินไป (Information Overload) และไม่ได้ให้แนวทางการแก้ไขที่ชัดเจน [18] ทำให้สถาบันการศึกษาขาดความรู้ที่เหมาะสมในการปรับปรุงความมั่นคงปลอดภัย ผู้วิจัยได้พัฒนากลไกการรายงานอัตโนมัติที่ปรับปรุงแล้วเพื่อให้รายงานที่กระชับและสามารถนำไปปฏิบัติได้ ซึ่งช่วยลดเวลาในการวิเคราะห์และเพิ่มประสิทธิภาพในการแก้ไขช่องโหว่

การวิจัยด้านการป้องกันและบริหารจัดการช่องโหว่ยังมีอีกมากมาย เช่น Manadhata และ Wing ได้เสนอแนวคิดเรื่องตัวชี้วัดพื้นที่โจมตี (Attack Surface Metric) เพื่อวัดความเสี่ยงของระบบจากมุมมองของพื้นที่ที่สามารถถูกโจมตีได้ [19] แนวคิดนี้ช่วยให้สามารถประเมินความเสี่ยงของระบบ

ได้อย่างเป็นระบบและเป็นพื้นฐานสำหรับการออกแบบระบบบริหารจัดการช่องโหว่ที่มีประสิทธิภาพ Scarfone และ Mell [20] ได้จัดทำแนวทางปฏิบัติสำหรับการวางแผนการจัดการแพตช์ในองค์กร ซึ่งเน้นการบำรุงรักษาเชิงป้องกันสำหรับเทคโนโลยี แนวทางนี้ครอบคลุมตั้งแต่การระบุช่องโหว่ การประเมินความเสี่ยง การทดสอบแพตช์ไปจนถึงการติดตั้งและตรวจสอบผล ซึ่งสอดคล้องกับวัตถุประสงค์ของงานวิจัยนี้ที่ต้องการพัฒนาระบบครบวงจร นอกจากนี้ Jacobs และ Romanosky ได้นำเสนอวิธีการปรับปรุงการแก้ไขช่องโหว่ผ่านการทำนายการถูกใช้ประโยชน์ในการโจมตีที่ดี และพบว่าการใช้ข้อมูลภัยคุกคาม (Threat Intelligence) ร่วมกับข้อมูลช่องโหว่ สามารถเพิ่มประสิทธิภาพในการจัดลำดับความสำคัญของการแก้ไขช่องโหว่ได้อย่างมีนัยสำคัญ [21]

จากการทบทวนวรรณกรรมข้างต้น พบว่างานวิจัยที่ผ่านมาได้ให้ความสำคัญกับหลายมิติของการบริหารจัดการช่องโหว่ เช่น การจัดลำดับความสำคัญของช่องโหว่ การประยุกต์ใช้แบบจำลองข้อมูล การพัฒนาระบบอัตโนมัติ และการปรับปรุงรูปแบบการรายงานผล อย่างไรก็ตาม ยังพบช่องว่างในด้านการพัฒนาระบบต้นแบบที่รองรับการนำเข้าข้อมูลผลการสแกนจากไฟล์ CSV เพื่อนำมาใช้ติดตามกระบวนการดำเนินการภายในองค์กรอย่างเป็นระบบ โดยเฉพาะในส่วนของการติดตาม Corrective Action การบันทึก Risk Acceptance การแจ้งเตือนผู้รับผิดชอบ และการแสดงผลข้อมูลผ่าน Dashboard ตามบทบาทของผู้ใช้งาน งานวิจัยนี้จึงมุ่งพัฒนาระบบที่ตอบโจทย์ดังกล่าว เพื่อสนับสนุนการบริหารจัดการช่องโหว่ให้มีความต่อเนื่อง ตรวจสอบย้อนหลังได้ และเหมาะสมต่อการประยุกต์ใช้ในบริบทขององค์กร

บทที่ 3
วิธีการดำเนินงานวิจัย

บทนี้นำเสนอวิธีการดำเนินการวิจัยสำหรับการพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนกระบวนการบริหารจัดการช่องโหว่ความปลอดภัยสารสนเทศภายในองค์กร โดยอธิบายขั้นตอนการดำเนินการวิจัย 7 ขั้นตอน ได้แก่ การศึกษาและรวบรวมข้อมูล การวิเคราะห์และออกแบบระบบ การพัฒนาระบบ การทดสอบระบบ การทดลองใช้งานระบบต้นแบบ การประเมินผลและวิเคราะห์ข้อมูล และการจัดทำเอกสารและรายงาน ทั้งนี้กระบวนการดำเนินการวิจัยมุ่งเน้นการพัฒนาระบบที่รองรับการนำเข้าข้อมูลผลการสแกนจาก Rapid7 InsightVM ในรูปแบบไฟล์ CSV การติดตามการดำเนินการแก้ไข การบันทึกการยอมรับความเสี่ยง การแจ้งเตือน และการแสดงผลข้อมูลผ่าน Dashboard ตามบทบาทของผู้ใช้งาน

3.1 การศึกษาและรวบรวมข้อมูล

ขั้นตอนแรกของการวิจัยเป็นการศึกษาและรวบรวมข้อมูลที่เกี่ยวข้อง เพื่อใช้เป็นพื้นฐานในการกำหนดข้อกำหนดของระบบ (System Requirements) และเป็นแนวทางในการออกแบบระบบให้สอดคล้องกับมาตรฐานสากลและความต้องการของผู้ใช้งานจริง โดยมีรายละเอียดดังนี้

3.1.1 การศึกษากรอบมาตรฐานสากลด้านการบริหารจัดการช่องโหว่

ผู้วิจัยดำเนินการศึกษากรอบมาตรฐานสากลที่เกี่ยวข้องกับการบริหารจัดการช่องโหว่ เพื่อใช้เป็นแนวทางในการออกแบบกระบวนการทำงานของระบบ มาตรฐานที่ศึกษาประกอบด้วย NIST Cybersecurity Framework (CSF) 2.0 ซึ่งกำหนดกรอบการทำงานด้านการระบุ (Identify) ปกป้อง (Protect) ตรวจจับ (Detect) ตอบสนอง (Respond) และฟื้นฟู (Recover) จากภัยคุกคามทางไซเบอร์ โดยเฉพาะฟังก์ชัน Identify ที่ครอบคลุมการบริหารจัดการช่องโหว่ นอกจากนี้ยังศึกษา ISO/IEC 27001:2022 Annex A 8.8 ซึ่งกำหนดข้อกำหนดเฉพาะเกี่ยวกับการบริหารจัดการช่องโหว่ทางเทคนิค PCI-DSS v4.0 Requirement 11 ที่กำหนดให้ต้องสแกนช่องโหว่ทุกไตรมาสและแก้ไขช่องโหว่ที่มีความรุนแรงสูงภายในระยะเวลาที่กำหนด ตลอดจน CIS Controls v8 Control 7 ที่กำหนดให้มีการประเมินและติดตามช่องโหว่อย่างต่อเนื่อง

การศึกษากรอบมาตรฐานเหล่านี้ช่วยให้ผู้วิจัยสามารถกำหนดข้อกำหนดด้านกระบวนการ (Process Requirements) ได้อย่างครอบคลุม อาทิ เกณฑ์กำหนดระยะเวลาดำเนินการแก้ไขช่องโหว่

ตามระดับความรุนแรง ข้อกำหนดด้านบันทึกการตรวจสอบย้อนหลัง (Audit Trail) และรูปแบบการรายงานที่สอดคล้องกับมาตรฐาน ISO 27001 และ PCI-DSS

3.1.2 การทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง

ผู้วิจัยดำเนินการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องอย่างเป็นระบบ ครอบคลุมหัวข้อสำคัญ ได้แก่ ระบบบริหารจัดการช่องโหว่ (Vulnerability Management System) วงจรชีวิตการจัดการช่องโหว่ (Vulnerability Lifecycle Management) การจัดลำดับความสำคัญของช่องโหว่ตามระดับความรุนแรง การติดตามการดำเนินการแก้ไข การยอมรับความเสี่ยง และการแสดงผลข้อมูลเพื่อการติดตามและตัดสินใจ ทั้งนี้เพื่อศึกษาแนวปฏิบัติที่ดี ข้อจำกัด และช่องว่างของงานวิจัยที่ผ่านมา

ผลจากการทบทวนวรรณกรรมชี้ให้เห็นว่ายังคงมีช่องว่างในการพัฒนาระบบที่สามารถรองรับการนำเข้าข้อมูลผลการสแกนจากไฟล์ CSV เพื่อนำมาใช้ติดตามการดำเนินการภายในองค์กรอย่างเป็นระบบ โดยเฉพาะในส่วนของการติดตาม Corrective Action การบันทึก Risk Acceptance การแจ้งเตือนผู้รับผิดชอบ และการแสดงผลข้อมูลตามบทบาทของผู้ใช้งาน ซึ่งเป็นพื้นฐานสำคัญในการกำหนดขอบเขตและทิศทางของงานวิจัยนี้

3.1.3 การวิเคราะห์ข้อมูลย้อนหลังจากเครื่องมือประเมินช่องโหว่

ผู้วิจัยดำเนินการวิเคราะห์ข้อมูลผลการสแกนช่องโหว่ย้อนหลังจาก Rapid7 InsightVM ในรูปแบบไฟล์ CSV export เพื่อทำความเข้าใจโครงสร้างข้อมูล ฟิลด์ที่สำคัญ รูปแบบการจัดเก็บ และลักษณะของช่องโหว่ที่พบบ่อย การวิเคราะห์ครอบคลุมฟิลด์หลัก ได้แก่ รหัสช่องโหว่ (CVE ID) ที่อยู่ IP หรือชื่อโฮสต์ของสินทรัพย์ (Asset IP/Hostname) คะแนนความรุนแรง (CVSS Score) ระดับความรุนแรง (Severity) รายละเอียดช่องโหว่ (Description) แนวทางการแก้ไข (Solution) และวันที่ค้นพบ (Discovery Date)

ผลการวิเคราะห์ถูกนำไปใช้ในการออกแบบโครงสร้างข้อมูลมาตรฐาน (Standardized Data Schema) และกฎการทำให้ข้อมูลเป็นมาตรฐาน (Data Normalization Rules) ได้แก่ การจับคู่ระดับความรุนแรง (Severity Mapping) และการจัดหมวดหมู่ช่องโหว่ตามประเภท เช่น เว็บแอปพลิเคชัน ระบบปฏิบัติการ อุปกรณ์เครือข่าย และฐานข้อมูล

3.1.4 การสัมภาษณ์ผู้มีส่วนได้เสีย

ผู้วิจัยดำเนินการสัมภาษณ์เจ้าของระบบ (System Owner) และทีมรักษาความมั่นคงปลอดภัย (Security Team) โดยใช้วิธีการสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-structured Interview) เพื่อเก็บรวบรวมข้อกำหนดของระบบและปัญหาของกระบวนการปัจจุบัน ครอบคลุมประเด็นกระบวนการทำงานปัจจุบันในการจัดการช่องโหว่ ปัญหาและอุปสรรคที่พบ ความต้องการด้านการแจ้งเตือนและการรายงาน กระบวนการยอมรับความเสี่ยงที่ใช้อยู่ และความคาดหวังต่อระบบใหม่

ข้อมูลจากการสัมภาษณ์ถูกนำมาสังเคราะห์ร่วมกับผลการศึกษามาตรฐานและวรรณกรรม เพื่อกำหนดข้อกำหนดของระบบที่สอดคล้องกับความต้องการของผู้ใช้งานจริง

3.2 การวิเคราะห์และออกแบบระบบ

ขั้นตอนนี้เป็นการนำข้อมูลที่ได้จากขั้นตอนที่ 3.1 มาวิเคราะห์ความต้องการและออกแบบระบบในทุกมิติ ตั้งแต่สถาปัตยกรรม ฐานข้อมูล ส่วนต่อประสานผู้ใช้ จนถึงกระบวนการทำงานของระบบ โดยมีรายละเอียดดังนี้

3.2.1 การวิเคราะห์ความต้องการของระบบ

ผู้วิจัยดำเนินการวิเคราะห์ความต้องการของระบบโดยแบ่งเป็น 2 ส่วนหลัก ได้แก่ ข้อกำหนดเชิงหน้าที่ (Functional Requirements) ซึ่งกำหนดด้วยเทคนิคแผนภาพกรณีใช้งาน (Use Case Diagram) และเรื่องเล่าผู้ใช้งาน (User Stories) ครอบคลุมการทำงานหลัก 6 โมดูล ได้แก่ การจัดการสินทรัพย์ (Asset Management) การนำเข้าข้อมูล (Data Import) การติดตามช่องโหว่ (Vulnerability Tracking) การจัดการการยอมรับความเสี่ยง (Risk Acceptance) การแจ้งเตือน (Notification) และแดชบอร์ดและรายงาน (Dashboard and Reporting)

ส่วนข้อกำหนดเชิงคุณภาพ (Non-functional Requirements) ครอบคลุมด้านประสิทธิภาพ ได้แก่ ระบบต้องสามารถนำเข้าข้อมูลช่องโหว่ได้อย่างน้อย 5,000 รายการต่อครั้ง ด้านความมั่นคงปลอดภัย ได้แก่ ระบบต้องมีการควบคุมการเข้าถึงตามบทบาท (RBAC) และบันทึกการตรวจสอบย้อนหลัง (Audit Trail) ด้านความสามารถในการขยาย ได้แก่ โครงสร้างระบบออกแบบให้สามารถต่อยอดการรองรับข้อมูลจากเครื่องมืออื่นได้ในอนาคต และด้านความสะดวกในการใช้งาน ได้แก่ ผู้ใช้งานสามารถเรียนรู้การใช้งานได้ภายในเวลาไม่เกิน 30 นาที

3.2.2 การออกแบบสถาปัตยกรรมระบบและเทคโนโลยีที่ใช้

ผู้วิจัยออกแบบสถาปัตยกรรมระบบแบบ 3 ระดับ (3-tier Architecture) ประกอบด้วย ระดับการนำเสนอ (Presentation Layer) สำหรับส่วนแสดงผล ระดับแอปพลิเคชัน (Application Layer) สำหรับตรรกะทางธุรกิจ และระดับข้อมูล (Data Layer) สำหรับฐานข้อมูล โดยกำหนดชุดเทคโนโลยี (Technology Stack) ดังนี้

Laravel Framework เวอร์ชัน 12.30 ใช้สำหรับพัฒนาเว็บแอปพลิเคชันฝั่งเซิร์ฟเวอร์ (Backend) ด้วยภาษา PHP เนื่องจากมีระบบ ORM (Eloquent), ระบบ Queue, Task Scheduler และ Mail ในตัว ซึ่งเหมาะสมกับการพัฒนาระบบแจ้งเตือนอัตโนมัติและการประมวลผลงานเบื้องหลัง (Background Processing) นอกจากนี้ยังใช้ Laravel Gates และ Policies เป็นกลไกในการควบคุมสิทธิ์การเข้าถึง (RBAC)

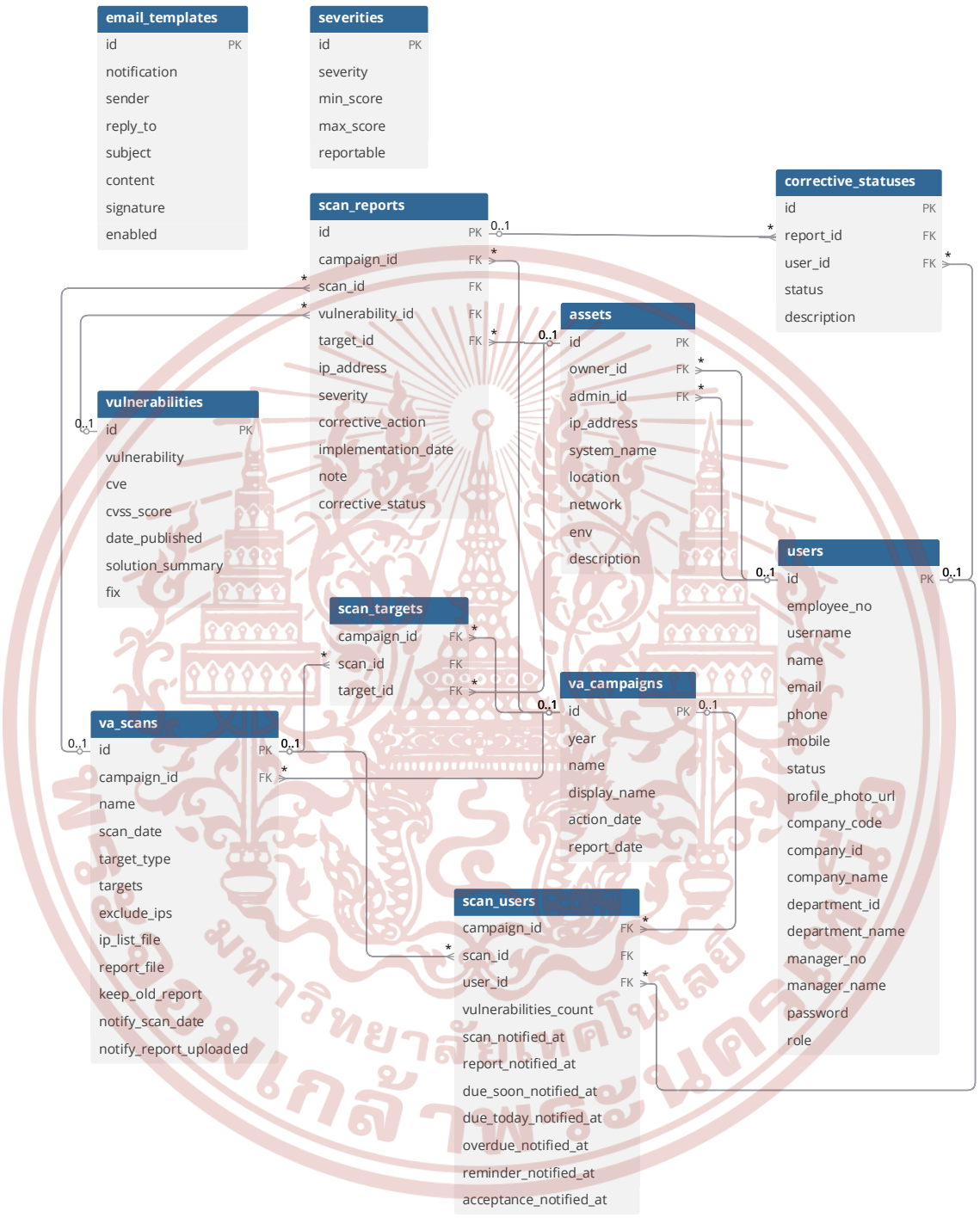
PostgreSQL เวอร์ชัน 17.8 ใช้สำหรับจัดเก็บข้อมูลช่องโหว่ สินทรัพย์ ประวัติการแก้ไข บันทึกการตรวจสอบ (Audit Log) และข้อมูลการตั้งค่าระบบ เนื่องจากรองรับ JSON data type ที่เหมาะสมกับข้อมูลช่องโหว่ที่มีโครงสร้างแตกต่างกันตามเครื่องมือประเมิน

Redis เวอร์ชัน 8.2 ใช้สำหรับจัดเก็บข้อมูลแคช (Cache) และจัดการคิวงาน (Queue) เพื่อเพิ่มประสิทธิภาพของระบบโดยเฉพาะการส่งอีเมลแจ้งเตือนจำนวนมากพร้อมกัน

Docker เวอร์ชัน 17.8 และ Docker Compose เวอร์ชัน 5.0.1 ใช้สำหรับบรรจุแอปพลิเคชัน (Containerization) เพื่อให้การปรับใช้งาน (Deployment) มีความสม่ำเสมอในทุกสภาพแวดล้อม

3.2.3 การออกแบบฐานข้อมูล

ผู้วิจัยออกแบบฐานข้อมูลเชิงสัมพันธ์ (Relational Database) บน PostgreSQL สำหรับรองรับการทำงานของระบบบริหารจัดการและติดตามช่องโหว่ โดยกำหนดเอนทิตีและความสัมพันธ์ของข้อมูลผ่านแผนภาพความสัมพันธ์ระหว่างเอนทิตี (Entity-Relationship Diagram: ERD) เพื่อให้โครงสร้างข้อมูลมีความถูกต้อง ลดความซ้ำซ้อน และสนับสนุนการเชื่อมโยงข้อมูลระหว่างผู้ใช้งาน สินทรัพย์ ผลการสแกน ช่องโหว่ และการดำเนินการแก้ไขได้อย่างมีประสิทธิภาพ ทั้งนี้ ในเล่มงานวิจัยจะแสดง ERD แบบย่อที่เน้นเฉพาะชื่อเอนทิตีและความสัมพันธ์หลัก เพื่อให้ผู้อ่านเข้าใจภาพรวมของฐานข้อมูลได้ชัดเจน



ภาพที่ 3-1 แผนภาพความสัมพันธ์ระหว่างเอนทิตี (ER Diagram) ของระบบ

ส่วนรายละเอียดระดับฟิลด์ของแต่ละตารางจะแสดงในตารางแสดงพจนานุกรมข้อมูล (Data Dictionary) ดังต่อไปนี้

ตารางที่ 3-1 แสดงตารางสำหรับจัดเก็บข้อมูลผู้ใช้งานระบบ ทั้งเจ้าของระบบ (System Owner) ผู้ดูแลระบบ (Administrator) และทีมรักษาความมั่นคงปลอดภัย โดยดึงข้อมูลพนักงานจากระบบบริหารทรัพยากรบุคคลขององค์กร

ตารางที่ 3-1 พจนานุกรมข้อมูลผู้ใช้งาน (users)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสผู้ใช้งาน (Primary Key)
employee_no	varchar(255)	Yes	NULL	รหัสพนักงาน
username	varchar(255)	Yes	NULL	ชื่อผู้ใช้สำหรับเข้าสู่ระบบ
first_name	varchar(255)	Yes	NULL	ชื่อ
last_name	varchar(255)	Yes	NULL	นามสกุล
name	varchar(255)	Yes	NULL	ชื่อ-นามสกุลแบบเต็ม
email	varchar(255)	Yes	NULL	อีเมล
phone	varchar(255)	Yes	NULL	เบอร์โทรศัพท์
mobile	varchar(255)	Yes	NULL	เบอร์มือถือ
status	varchar(255)	Yes	NULL	สถานะผู้ใช้งาน
profile_photo_url	varchar(255)	Yes	NULL	URL รูปโปรไฟล์
company_code	varchar(255)	Yes	NULL	รหัสบริษัท
company_id	varchar(255)	Yes	NULL	รหัสอ้างอิงบริษัท
company_name	varchar(255)	Yes	NULL	ชื่อบริษัท
business_unit_id	varchar(255)	Yes	NULL	รหัสหน่วยธุรกิจ
business_unit_name	varchar(255)	Yes	NULL	ชื่อหน่วยธุรกิจ
department_id	varchar(255)	Yes	NULL	รหัสแผนก
department_name	varchar(255)	Yes	NULL	ชื่อแผนก
manager_no	varchar(255)	Yes	NULL	รหัสผู้บังคับบัญชา
manager_name	varchar(255)	Yes	NULL	ชื่อผู้บังคับบัญชา

ตารางที่ 3-1 (ต่อ)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
email_verified_at	timestamp	Yes	NULL	วันที่ยืนยันอีเมล
password	varchar(255)	Yes	NULL	รหัสผ่าน (เข้ารหัสแบบ bcrypt)
role	varchar(255)	No	user	บทบาท (user, administrator)
remember_token	varchar(100)	Yes	NULL	โทเค็นจดจำการเข้าสู่ระบบ
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด

ตารางที่ 3-1 แสดงตารางสำหรับจัดเก็บข้อมูลสินทรัพย์สารสนเทศขององค์กร พร้อมระบุเจ้าของระบบและผู้ดูแลระบบที่รับผิดชอบ เพื่อใช้ในการจับคู่กับผลการสแกนช่องโหว่

ตารางที่ 3-2 พจนานุกรมข้อมูลสินทรัพย์ (assets)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสสินทรัพย์ (Primary Key)
owner_id	char(26)	Yes	NULL	รหัสเจ้าของระบบ (FK -> users)
admin_id	char(26)	Yes	NULL	รหัสผู้ดูแลระบบ (FK -> users)
ip_address	varchar(20)	No		ที่อยู่ IP ของสินทรัพย์
system_name	varchar(255)	Yes	NULL	ชื่อระบบ
location	varchar(255)	Yes	NULL	ที่ตั้ง
network	varchar(255)	Yes	NULL	เครือข่าย
env	varchar(255)	Yes	NULL	สภาพแวดล้อม
description	text	Yes	NULL	รายละเอียดเพิ่มเติม
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด
deleted_at	timestamp	Yes	NULL	วันที่ลบ (Soft Delete)

ตารางที่ 3-3 แสดงตารางสำหรับจัดเก็บข้อมูลแคมเปญการประเมินช่องโหว่ประจำปี โดยแต่ละแคมเปญกำหนดวันดำเนินการแก้ไขและวันส่งรายงาน

ตารางที่ 3-3 พจนานุกรมข้อมูลแคมเปญการประเมินช่องโหว่ (va_campaigns)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสแคมเปญ (Primary Key)
year	integer	No		ปี ค.ศ. ของแคมเปญ
name	varchar(255)	No		ชื่อแคมเปญ (ภายใน)
display_name	varchar(255)	No		ชื่อแคมเปญ (แสดงผล)
action_date	date	No		วันที่กำหนดดำเนินการแก้ไข
report_date	date	No		วันที่กำหนดส่งรายงาน
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด
deleted_at	timestamp	Yes	NULL	วันที่ลบ (Soft Delete)

ตารางที่ 3-4 แสดงตารางสำหรับจัดเก็บข้อมูลรอบการสแกนช่องโหว่ภายใต้แต่ละแคมเปญ รวมถึงเป้าหมายการสแกน ไฟล์รายงาน และการตั้งค่าการแจ้งเตือน

ตารางที่ 3-4 พจนานุกรมข้อมูลรอบการสแกน (va_scans)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสรอบการสแกน (Primary Key)
campaign_id	char(26)	No		รหัสแคมเปญ (FK -> va_campaigns)
name	varchar(255)	No		ชื่อรอบการสแกน
scan_date	date	No		วันที่สแกน
target_type	varchar(255)	No		ประเภทเป้าหมาย (network, ip)
targets	text	No	[ ]	รายการเป้าหมาย (JSON array)
exclude_ips	text	No	[ ]	รายการ IP ที่ยกเว้น (JSON array)

ตารางที่ 3-4 (ต่อ)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
ip_list_file	varchar(255)	Yes	NULL	ไฟล์รายการ IP
report_file	varchar(255)	Yes	NULL	ไฟล์รายงานผลสแกน (CSV)
keep_old_report	boolean	No	false	เก็บรายงานเก่าเมื่ออัปโหลดใหม่
notify_scan_date	boolean	No	false	แจ้งเตือนวันสแกนล่วงหน้า
notify_report _uploaded	boolean	No	false	แจ้งเตือนเมื่ออัปโหลดรายงาน
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด
deleted_at	timestamp	Yes	NULL	วันที่ลบ (Soft Delete)

ตารางที่ 3-5 แสดงตารางสำหรับจัดเก็บข้อมูลช่องโหว่ที่ค้นพบจากการสแกน รวมถึงรหัส CVE คะแนน CVSS และแนวทางการแก้ไข

ตารางที่ 3-5 พจนานุกรมข้อมูลช่องโหว่ (vulnerabilities)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสช่องโหว่ (Primary Key)
vulnerability	varchar(255)	No		ชื่อช่องโหว่
cve	varchar(20)	Yes	NULL	รหัส CVE
cvss_score	double precision	No		คะแนน CVSS
date_published	date	No		วันที่เผยแพร่
solution_summary	varchar(255)	Yes	NULL	สรุปแนวทางการแก้ไข
fix	text	Yes	NULL	รายละเอียดวิธีแก้ไข
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด

ตารางที่ 3-6 แสดงตารางสำหรับจัดเก็บข้อมูลผลการสแกนช่องโหว่ของแต่ละสินทรัพย์ในแต่ละรอบการสแกน โดยเชื่อมโยงกับตารางแคมเปญ รอบการสแกน ช่องโหว่ และสินทรัพย์ พร้อมบันทึกสถานะการแก้ไขและประเภทการดำเนินการ

ตารางที่ 3-6 พจนานุกรมข้อมูลรายงานผลการสแกน (scan_reports)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสรายงาน (Primary Key)
campaign_id	char(26)	No		รหัสแคมเปญ (FK -> va_campaigns)
scan_id	char(26)	No		รหัสรอบการสแกน (FK -> va_scans)
vulnerability_id	char(26)	No		รหัสช่องโหว่ (FK -> vulnerabilities)
target_id	char(26)	No		รหัสสินทรัพย์เป้าหมาย (FK -> assets)
ip_address	varchar(20)	No		ที่อยู่ IP ที่พบช่องโหว่
severity	varchar(255)	No		ระดับความรุนแรง (low, medium, high, critical)
corrective_action	varchar(255)	Yes	NULL	ประเภทการดำเนินการ (acceptance, patch)
Implementation_date	date	Yes	NULL	วันที่ดำเนินการแก้ไข
note	text	Yes	NULL	หมายเหตุการดำเนินการ
corrective_status	varchar(255)	No	finding	สถานะการแก้ไข (finding, pending, in_progress, completed)
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด

ตารางที่ 3-7 แสดงตารางสำหรับจัดเก็บประวัติการเปลี่ยนแปลงสถานะการแก้ไขช่องโหว่ เพื่อใช้เป็นบันทึกการตรวจสอบย้อนหลัง (Audit Trail)

ตารางที่ 3-7 พจนานุกรมข้อมูลประวัติสถานะการแก้ไข (corrective_statuses)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสประวัติสถานะ (Primary Key)
report_id	char(26)	No		รหัสรายงานที่เกี่ยวข้อง (FK -> scan_reports)
user_id	char(26)	Yes	NULL	รหัสผู้เปลี่ยนสถานะ (FK -> users)
status	varchar(255)	No	finding	สถานะ (finding, pending, in_progress, completed)
description	text	Yes	NULL	รายละเอียดการเปลี่ยนสถานะ
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด

ตารางที่ 3-8 แสดงตารางสำหรับจัดเก็บข้อมูลความสัมพันธ์แบบกลุ่มต่อกลุ่ม (Pivot Table) ระหว่างรอบการสแกนกับสินทรัพย์เป้าหมาย

ตารางที่ 3-8 พจนานุกรมข้อมูลเป้าหมายของรอบการสแกน (scan_targets)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
campaign_id	char(26)	No		รหัสแคมเปญ (PK, FK -> va_campaigns)
scan_id	char(26)	No		รหัสรอบการสแกน (PK, FK -> va_scans)
target_id	char(26)	No		รหัสสินทรัพย์เป้าหมาย (PK, FK -> assets)

ตารางที่ 3-9 แสดงตารางสำหรับจัดเก็บข้อมูลความสัมพันธ์ระหว่างรอบการสแกนกับผู้ใช้งาน (เจ้าของระบบ) พร้อมบันทึกจำนวนช่องโหว่และสถานะการแจ้งเตือนแต่ละประเภท

ตารางที่ 3-9 พจนานุกรมข้อมูลตารางผู้ใช้งานที่เกี่ยวข้องกับรอบการสแกน (scan_users)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
campaign_id	char(26)	No		รหัสแคมเปญ (PK, FK -> va_campaigns)

ตารางที่ 3-9 (ต่อ)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
scan_id	char(26)	No		รหัสรอบการสแกน (FK -> va_scans)
user_id	char(26)	No		รหัสผู้ใช้งาน (PK, FK -> users)
vulnerabilities_count	integer	No	0	จำนวนช่องโหว่ที่เกี่ยวข้อง
scan_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนวันสแกนล่วงหน้า
report_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนรายงานผลสแกน
due_soon_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนใกล้ครบกำหนดดำเนินการ
due_today_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนครบกำหนดดำเนินการวันนี้
overdue_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนเกินกำหนดดำเนินการ
reminder_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนติดตามผล
acceptance_notified_at	timestamp	Yes	NULL	วันที่แจ้งเตือนการยอมรับความเสี่ยง

ตารางที่ 3-10 แสดงตารางสำหรับจัดเก็บเกณฑ์การจำแนกระดับความรุนแรงของช่องโหว่ตามช่วงคะแนน CVSS พร้อมกำหนดว่าระดับใดต้องรายงาน

ตารางที่ 3-10 พจนานุกรมข้อมูลเกณฑ์ระดับความรุนแรง (severities)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสระดับความรุนแรง (Primary Key)
severity	varchar(255)	No		ระดับความรุนแรง (low, medium, high, critical)
min_score	decimal(8,1)	No		คะแนน CVSS ต่ำสุดของช่วง
max_score	decimal(8,1)	No		คะแนน CVSS สูงสุดของช่วง
reportable	boolean	No	false	ระดับ severity จะแสดงในรายงานหรือไม่
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ

ตารางที่ 3-10 (ต่อ)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด

ตารางที่ 3-11 แสดงตารางจัดเก็บแบบร่างอีเมลสำหรับการแจ้งเตือนแต่ละประเภท ให้ผู้ดูแลระบบสามารถปรับแต่งเนื้อหาอีเมลได้

ตารางที่ 3-11 พจนานุกรมข้อมูลแบบร่างอีเมล (email_templates)

Column	ชนิดข้อมูล	Null	ค่าเริ่มต้น	คำอธิบาย
id	char(26)	No		รหัสแม่แบบ (Primary Key)
notification	varchar(255)	No		ประเภทการแจ้งเตือน
sender	varchar(255)	Yes	NULL	อีเมลผู้ส่ง
reply_to	varchar(255)	Yes	NULL	อีเมลสำหรับตอบกลับ
subject	varchar(255)	Yes	NULL	หัวเรื่องอีเมล
content	text	Yes	NULL	เนื้อหาอีเมล (รองรับ HTML)
signature	text	Yes	NULL	ลายเซ็นอีเมล
enabled	boolean	No	true	เปิดใช้งานหรือไม่
created_at	timestamp	Yes	NULL	วันที่สร้างรายการ
updated_at	timestamp	Yes	NULL	วันที่แก้ไขล่าสุด

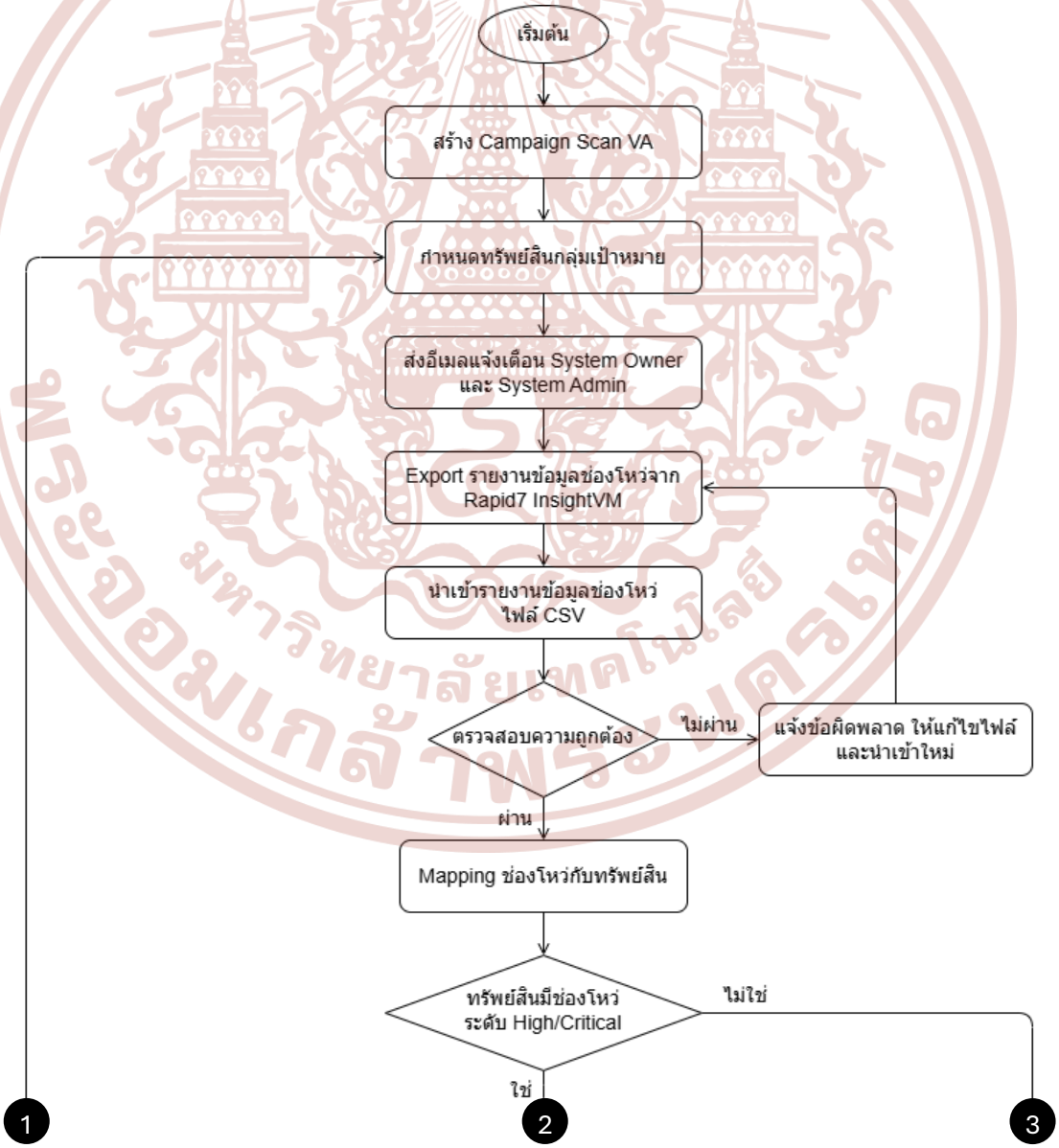
3.2.4 การออกแบบส่วนต่อประสานผู้ใช้

ผู้วิจัยออกแบบกระบวนการทำงานหลักของระบบโดยใช้แผนภาพการไหลของงาน แสดงขั้นตอนตั้งแต่การสร้างแคมเปญและรอบการสแกน การแจ้งเตือนเจ้าของระบบก่อนวันสแกน การนำเข้าผลการสแกนจากไฟล์ CSV การจับคู่ข้อมูลช่องโหว่กับสินทรัพย์ การแจ้งเตือนเมื่อพบช่องโหว่ระดับรุนแรง การกำหนดแนวทางการดำเนินการ และการติดตามสถานะของรายการช่องโหว่จนกว่ากระบวนการจะเสร็จสิ้น

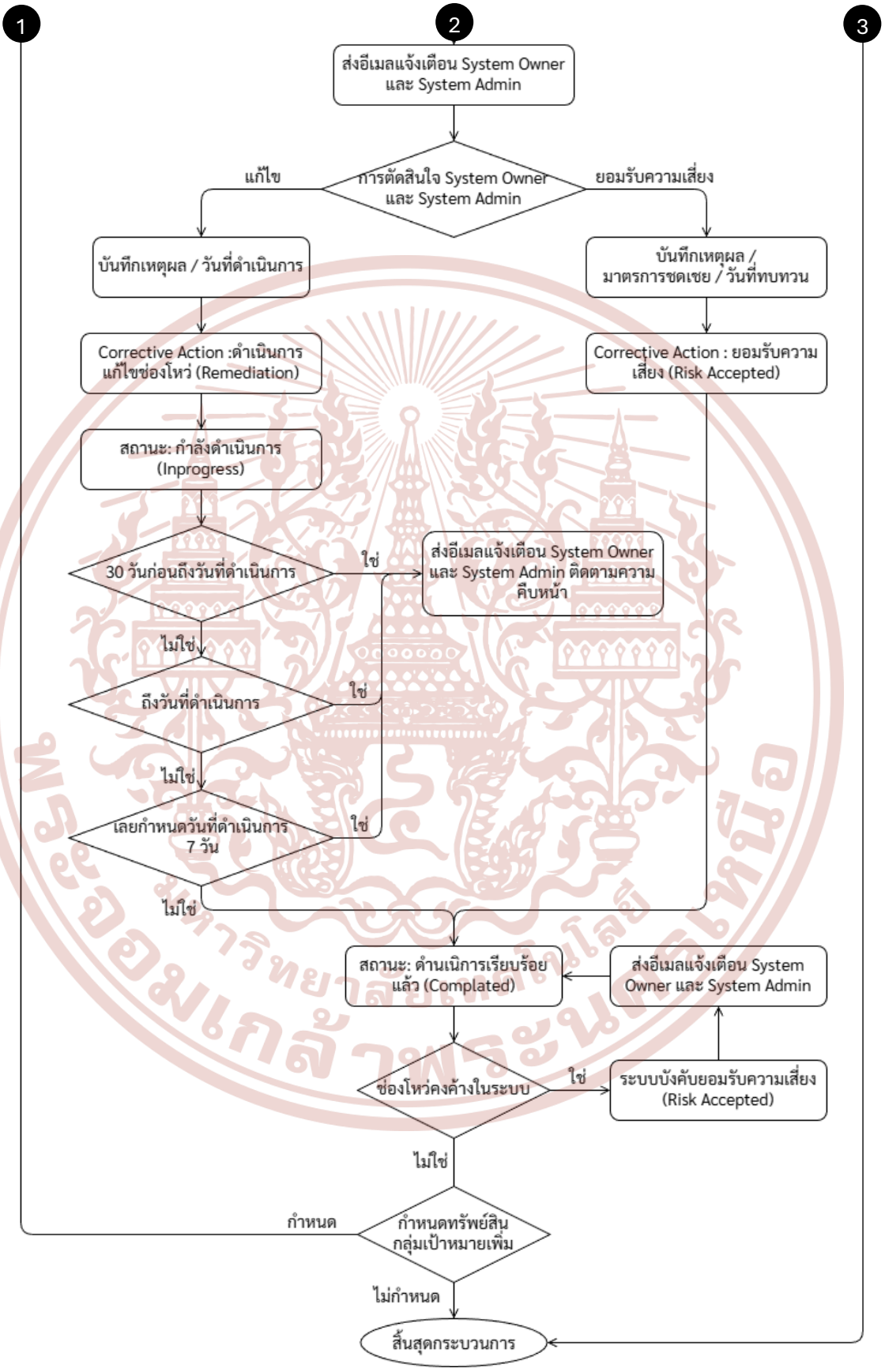
เมื่อทีมรักษาความมั่นคงปลอดภัยนำเข้าผลการสแกนเข้าสู่ระบบแล้ว ระบบจะตรวจสอบความถูกต้องของข้อมูลและประมวลผลรายการช่องโหว่ที่เกี่ยวข้อง จากนั้นเจ้าของระบบหรือผู้เกี่ยวข้อง

สามารถเลือกแนวทางการดำเนินการได้ 2 รูปแบบ ได้แก่ การดำเนินการแก้ไขช่องโหว่ (Patch/Remediation) หรือการยอมรับความเสี่ยง (Risk Acceptance) โดยกรณีเลือกดำเนินการแก้ไข ผู้ใช้งานจะระบุข้อมูลที่เกี่ยวข้องกับแผนการดำเนินการและอัปเดตสถานะผ่านระบบ ส่วนกรณีเลือกยอมรับความเสี่ยง ผู้ใช้งานจะต้องระบุเหตุผลประกอบเพื่อจัดเก็บเป็นหลักฐานในระบบ

สำหรับรายการที่ยังไม่มีการดำเนินการภายในระยะเวลาที่กำหนด ระบบจะส่งการแจ้งเตือนติดตามความคืบหน้าตามเงื่อนไขที่กำหนด หากพ้นกำหนดแล้วยังไม่มีการตอบสนองหรือไม่มีการอัปเดตสถานะผ่านระบบ ระบบจะบันทึกรายการดังกล่าวเป็นการยอมรับความเสี่ยงโดยอัตโนมัติ พร้อมจัดเก็บประวัติการแจ้งเตือนและการเปลี่ยนแปลงสถานะไว้ในระบบ เพื่อใช้เป็นข้อมูลอ้างอิงในการติดตามและตรวจสอบย้อนหลัง



ภาพที่ 3-2 กระบวนการทำงานหลักของระบบ


1
2
3
ส่งอีเมลแจ้งเตือน System Owner และ System Admin
การตัดสินใจ System Owner และ System Admin
แก้ไข
ยอมรับความเสี่ยง
บันทึกเหตุผล / วันที่ดำเนินการ
บันทึกเหตุผล / มาตรการชดเชย / วันที่ทบทวน
Corrective Action :ดำเนินการแก้ไขช่องโหว่ (Remediation)
Corrective Action : ยอมรับความเสี่ยง (Risk Accepted)
สถานะ: กำลังดำเนินการ (Inprogress)
30 วันก่อนถึงวันที่ดำเนินการ
ใช่
ส่งอีเมลแจ้งเตือน System Owner และ System Admin ติดตามความคืบหน้า
ไม่ใช่
ถึงวันที่ดำเนินการ
ใช่
ไม่ใช่
เลยกำหนดวันที่ดำเนินการ 7 วัน
ใช่
ไม่ใช่
สถานะ: ดำเนินการเรียบร้อยแล้ว (Complated)
ส่งอีเมลแจ้งเตือน System Owner และ System Admin
ช่องโหว่คงค้างในระบบ
ใช่
ระบบบังคับยอมรับความเสี่ยง (Risk Accepted)
ไม่ใช่
กำหนด
กำหนดทรัพย์สินกลุ่มเป้าหมายเพิ่ม
ไม่กำหนด
สิ้นสุดกระบวนการ

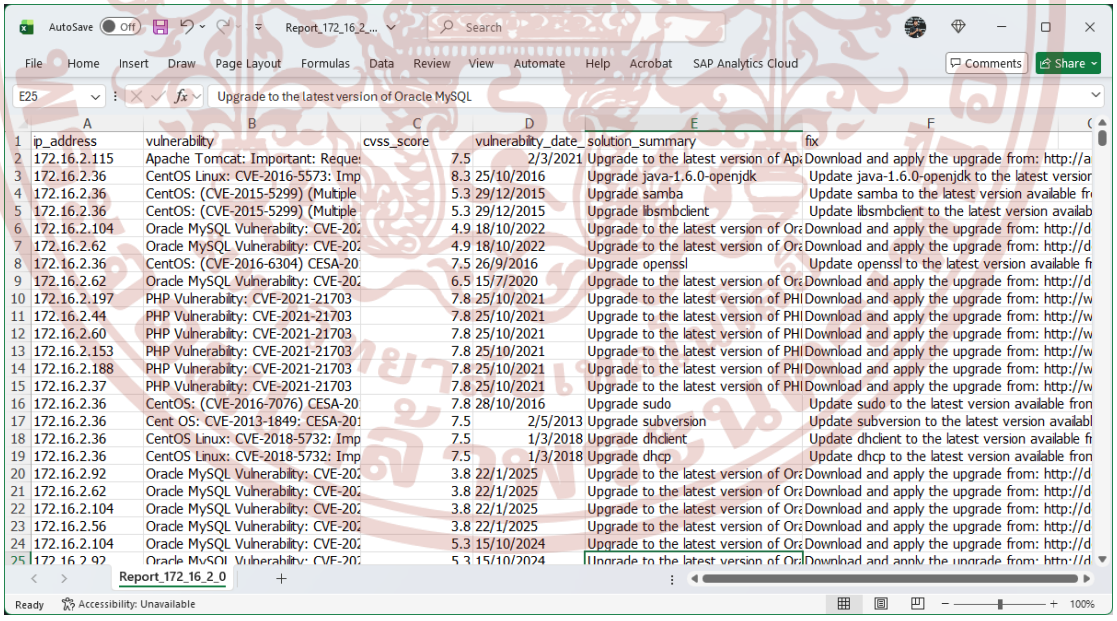
ภาพที่ 3-2 (ต่อ)

3.3 การพัฒนาระบบ

ขั้นตอนนี้เป็นการนำผลการออกแบบจากขั้นตอนที่ 3.2 มาดำเนินการพัฒนาระบบจริง โดยใช้แนวทางการพัฒนาแบบวนซ้ำ (Iterative Development) เพื่อให้สามารถรับข้อเสนอแนะและปรับปรุงระบบได้อย่างต่อเนื่อง การพัฒนาแบ่งออกเป็นโมดูลหลักดังนี้

3.3.1 การพัฒนาโมดูลจัดการสินทรัพย์ (Asset Management Module) สำหรับดึงข้อมูลสินทรัพย์จากระบบคลังสินทรัพย์ (Asset Inventory) ที่มีอยู่ขององค์กร จัดเก็บข้อมูลเจ้าของระบบและผู้รับผิดชอบ จัดการตารางสแกน (Scan Schedule) และส่งอีเมลแจ้งเตือนล่วงหน้าก่อนวันสแกนเพื่อให้เจ้าของระบบเตรียมความพร้อม

3.3.2 การพัฒนาโมดูลนำเข้าข้อมูล (Data Import Module) ซึ่งเป็นโมดูลหลักของระบบ ทำหน้าที่แยกวิเคราะห์ (Parse) ไฟล์ CSV จาก Rapid7 InsightVM ตรวจสอบความถูกต้องของข้อมูล (Data Validation) แปลงให้เป็นมาตรฐานตามโครงสร้างข้อมูลที่ออกแบบไว้ พร้อมทั้งจับคู่ข้อมูลช่องโหว่กับสินทรัพย์ในระบบ โมดูลนี้ออกแบบให้มีโครงสร้างที่สามารถต่อยอดเพื่อรองรับรูปแบบข้อมูลจากเครื่องมืออื่นได้ในอนาคต ตัวอย่างโครงสร้างไฟล์ CSV ที่ส่งออกจาก Rapid7 InsightVM แสดงดังภาพที่ 3-3



	A	B	C	D	E	F
1	ip_address	vulnerability	cvss_score	vulnerability_date_	solution_summary	fix
2	172.16.2.115	Apache Tomcat: Important: Reque	7.5	2/3/2021	Upgrade to the latest version of Ap	Download and apply the upgrade from: http://a
3	172.16.2.36	CentOS Linux: CVE-2016-5573: Imp	8.3	25/10/2016	Upgrade java-1.6.0-openjdk	Update java-1.6.0-openjdk to the latest versior
4	172.16.2.36	CentOS: (CVE-2015-5299) (Multiple	5.3	29/12/2015	Upgrade samba	Update samba to the latest version available fr
5	172.16.2.36	CentOS: (CVE-2015-5299) (Multiple	5.3	29/12/2015	Upgrade libsmbclient	Update libsmbclient to the latest version availab
6	172.16.2.104	Oracle MySQL Vulnerability: CVE-202	4.9	18/10/2022	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
7	172.16.2.62	Oracle MySQL Vulnerability: CVE-202	4.9	18/10/2022	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
8	172.16.2.36	CentOS: (CVE-2016-6304) CESA-20	7.5	26/9/2016	Upgrade openssl	Update openssl to the latest version available fi
9	172.16.2.62	Oracle MySQL Vulnerability: CVE-202	6.5	15/7/2020	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
10	172.16.2.197	PHP Vulnerability: CVE-2021-21703	7.8	25/10/2021	Upgrade to the latest version of PHI	Download and apply the upgrade from: http://w
11	172.16.2.44	PHP Vulnerability: CVE-2021-21703	7.8	25/10/2021	Upgrade to the latest version of PHI	Download and apply the upgrade from: http://w
12	172.16.2.60	PHP Vulnerability: CVE-2021-21703	7.8	25/10/2021	Upgrade to the latest version of PHI	Download and apply the upgrade from: http://w
13	172.16.2.153	PHP Vulnerability: CVE-2021-21703	7.8	25/10/2021	Upgrade to the latest version of PHI	Download and apply the upgrade from: http://w
14	172.16.2.188	PHP Vulnerability: CVE-2021-21703	7.8	25/10/2021	Upgrade to the latest version of PHI	Download and apply the upgrade from: http://w
15	172.16.2.37	PHP Vulnerability: CVE-2021-21703	7.8	25/10/2021	Upgrade to the latest version of PHI	Download and apply the upgrade from: http://w
16	172.16.2.36	CentOS: (CVE-2016-7076) CESA-20	7.8	28/10/2016	Upgrade sudo	Update sudo to the latest version available fron
17	172.16.2.36	Cent OS: CVE-2013-1849: CESA-201	7.5	2/5/2013	Upgrade subversion	Update subversion to the latest version availabl
18	172.16.2.36	CentOS Linux: CVE-2018-5732: Imp	7.5	1/3/2018	Upgrade dhclient	Update dhclient to the latest version available fi
19	172.16.2.36	CentOS Linux: CVE-2018-5732: Imp	7.5	1/3/2018	Upgrade dhcp	Update dhcp to the latest version available fron
20	172.16.2.92	Oracle MySQL Vulnerability: CVE-202	3.8	22/1/2025	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
21	172.16.2.62	Oracle MySQL Vulnerability: CVE-202	3.8	22/1/2025	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
22	172.16.2.104	Oracle MySQL Vulnerability: CVE-202	3.8	22/1/2025	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
23	172.16.2.56	Oracle MySQL Vulnerability: CVE-202	3.8	22/1/2025	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
24	172.16.2.104	Oracle MySQL Vulnerability: CVE-202	5.3	15/10/2024	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d
25	172.16.2.92	Oracle MySQL Vulnerability: CVE-202	5.3	15/10/2024	Upgrade to the latest version of Ora	Download and apply the upgrade from: http://d

ภาพที่ 3-3 โครงสร้างไฟล์ CSV ที่ส่งออกจาก Rapid7 InsightVM

3.3.3 การพัฒนาโมดูลติดตามช่องโหว่ (Vulnerability Tracking Module) สำหรับแสดงรายการช่องโหว่ตามสิทธิ์ของผู้ใช้งาน บันทึกประวัติการเปลี่ยนแปลงทุกรายการ และแสดง

รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข (Remediation Guidance) โดยจัดการสถานะการแก้ไขช่องโหว่ (Corrective Status) ตลอดวงจรชีวิต ดังแสดงในตารางที่ 3-12

ตารางที่ 3-12 สถานะการแก้ไขช่องโหว่ (Corrective Status)

สถานะ	ชื่อแสดงผล	คำอธิบาย
finding	พบช่องโหว่ (Finding)	สถานะเริ่มต้นเมื่อนำเข้าผลสแกน ช่องโหว่ยังไม่มีการดำเนินการใดๆ
pending	รอดำเนินการ (Pending)	เจ้าของระบบรับทราบช่องโหว่แล้ว อยู่ระหว่างวางแผนการแก้ไข
in_progress	กำลังดำเนินการ (In Progress)	อยู่ระหว่างดำเนินการแก้ไขช่องโหว่หรือติดตั้งแพตช์
completed	ดำเนินการเรียบร้อย (Completed)	ดำเนินการแก้ไขหรือยอมรับความเสี่ยงเรียบร้อยแล้ว

3.3.4 การพัฒนาโมดูลจัดการการยอมรับความเสี่ยง (Risk Acceptance Module) สำหรับรองรับการจัดการช่องโหว่ในกรณีที่ไม่สามารถดำเนินการแก้ไขได้ทันที โดยระบบเปิดให้ผู้ใช้งานเลือกประเภทการดำเนินการ (Corrective Action) ได้ 2 รูปแบบ ได้แก่ การแก้ไขช่องโหว่ (Patch/Remediation) และการยอมรับความเสี่ยง (Risk Acceptance)

ในกรณีที่ผู้ใช้งานเลือกการยอมรับความเสี่ยง ระบบจะรองรับการบันทึกเหตุผลหรือหมายเหตุประกอบ พร้อมจัดเก็บประวัติการดำเนินการที่เกี่ยวข้องไว้ในระบบ เพื่อใช้เป็นข้อมูลอ้างอิงสำหรับการติดตามและการตรวจสอบย้อนหลัง

นอกจากนี้ ระบบยังรองรับการบันทึกการยอมรับความเสี่ยงโดยอัตโนมัติตามเงื่อนไขของกระบวนการติดตามที่กำหนดไว้ในแคมเปญ กล่าวคือ หากรายการช่องโหว่ยังคงอยู่ในสถานะ pending และไม่มีการตอบสนองหรืออัปเดตสถานะภายในระยะเวลาที่กำหนด แม้ว่าระบบได้มีการแจ้งเตือนผู้รับผิดชอบแล้ว ระบบจะบันทึกรายการดังกล่าวให้เข้าสู่เงื่อนไข acceptance โดยอัตโนมัติ พร้อมจัดเก็บประวัติการแจ้งเตือนและการเปลี่ยนแปลงสถานะไว้ในระบบเพื่อรองรับการตรวจสอบย้อนหลัง

ตารางที่ 3-13 ประเภทการดำเนินการแก้ไขช่องโหว่ (Corrective Action)

ประเภท	ชื่อแสดงผล	คำอธิบาย
patch	แก้ไขช่องโหว่ (Patch/Remediation)	ดำเนินการแก้ไขช่องโหว่โดยการติดตั้งแพตช์ อัปเดตซอฟต์แวร์ หรือปรับค่าตั้งระบบ พร้อมบันทึกเหตุผลและวันที่ดำเนินการ
acceptance	ยอมรับความเสี่ยง (Risk Acceptance)	ยอมรับความเสี่ยงของช่องโหว่นั้น โดยผู้ใช้งานสามารถบันทึกเหตุผลประกอบผ่านระบบ หรือระบบสามารถบันทึกเข้าสู่เงื่อนไข acceptance โดยอัตโนมัติเมื่อไม่มีการดำเนินการภายในระยะเวลาที่กำหนด

3.3.5 พัฒนาโมดูลแจ้งเตือน (Notification Module) สำหรับส่งอีเมลแจ้งเตือนอัตโนมัติผ่านระบบคิวงาน (Queue) ของ Laravel เพื่อให้ส่งอีเมลจำนวนมากได้โดยไม่กระทบประสิทธิภาพของระบบ โดยผู้ดูแลระบบสามารถปรับแต่งเนื้อหาอีเมลแต่ละประเภทได้ผ่านหน้าจัดการแม่แบบอีเมล (Email Templates) ระบบรองรับการแจ้งเตือน 7 ประเภท ดังแสดงในตารางที่ 3-14

ตารางที่ 3-14 ประเภทการแจ้งเตือนทางอีเมล

ประเภทการแจ้งเตือน	เงื่อนไขการส่ง	ผู้รับ	คำอธิบาย
แจ้งเตือนวันสแกน (Scan Date)	ก่อนวันสแกนตามที่กำหนด	เจ้าของระบบและผู้ดูแลระบบ	แจ้งให้ทราบล่วงหน้าว่าจะมีการสแกนช่องโหว่ เพื่อเตรียมความพร้อมของระบบ
แจ้งเตือนรายงานผลสแกน (Report Uploaded)	เมื่ออัปโหลดไฟล์ CSV เสร็จ	เจ้าของระบบและผู้ดูแลระบบ	แจ้งผลการสแกนช่องโหว่พร้อมสรุปจำนวนช่องโหว่ที่พบ
แจ้งเตือนใกล้ครบกำหนด (Due Soon)	30 วันก่อนวันที่ดำเนินการ	เจ้าของระบบและผู้ดูแลระบบ	เตือนว่าใกล้ถึงกำหนดเวลาดำเนินการแก้ไขช่องโหว่
แจ้งเตือนครบกำหนดวันนี้ (Due Today)	วันที่ครบกำหนดดำเนินการ	เจ้าของระบบและผู้ดูแลระบบ	เตือนว่าวันนี้เป็นวันครบกำหนดดำเนินการ
แจ้งเตือนเกินกำหนด (Overdue)	เลยกำหนด 7 วัน	เจ้าของระบบและผู้ดูแลระบบ	เตือนว่าเลยกำหนดเวลาดำเนินการแล้ว ให้เร่งดำเนินการ
แจ้งเตือนติดตามผล (Reminder)	ตามช่วงเวลาที่กำหนด	เจ้าของระบบและผู้ดูแลระบบ	ติดตามความคืบหน้าการแก้ไขช่องโหว่ที่ยังค้างอยู่

ตารางที่ 3-14 (ต่อ)

ประเภทการแจ้งเตือน	เงื่อนไขการส่ง	ผู้รับ	คำอธิบาย
แจ้งเตือนการยอมรับความเสี่ยง (Acceptance)	เมื่อมีการยอมรับความเสี่ยง	เจ้าของระบบและผู้ดูแลระบบ	แจ้งให้ทราบว่ามีการยอมรับความเสี่ยงสำหรับช่องโหว่

3.3.6 การพัฒนาแดชบอร์ด (Dashboard) และโมดูลรายงาน (Reporting Module) สำหรับแสดงสถานะช่องโหว่แบบเรียลไทม์ เปรียบเทียบผลระหว่างรอบการสแกน แสดงแนวโน้มการเกิดช่องโหว่ และส่งออกรายงานในรูปแบบ PDF และ Excel แดชบอร์ดแสดงข้อมูลตามบทบาทของผู้ใช้งาน โดยเจ้าของระบบเห็นเฉพาะระบบที่ตนรับผิดชอบ ส่วนทีมรักษาความมั่นคงปลอดภัย (Security Team) ผู้ตรวจสอบ (Auditor) และผู้บริหารที่กำกับดูแล เห็นภาพรวมขององค์กร

3.3.7 การพัฒนาระบบควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control: RBAC) โดยกำหนดบทบาทหลัก 3 บทบาท ได้แก่ เจ้าของระบบและผู้ดูแลระบบ (System Owner/System Admin) ทีมรักษาความมั่นคงปลอดภัย (Security Team) และผู้ตรวจสอบ (Auditor) แต่ละบทบาทมีสิทธิ์การเข้าถึงและการดำเนินการที่แตกต่างกันตามหน้าที่ความรับผิดชอบ

ตารางที่ 3-15 บทบาทและสิทธิ์การเข้าถึงระบบ

ฟังก์ชันการทำงาน	เจ้าของระบบและผู้ดูแลระบบ (System Owner/System Admin)	ทีมรักษาความมั่นคงปลอดภัย (Security Team)	ผู้ตรวจสอบ (Auditor)
ดูแดชบอร์ดภาพรวม	เฉพาะระบบที่รับผิดชอบ	ทั้งหมด	ทั้งหมด
ดูรายการช่องโหว่	เฉพาะระบบที่รับผิดชอบ	ทั้งหมด	ทั้งหมด
ดูประวัติการเปลี่ยนแปลง (Audit Trail)	เฉพาะระบบที่รับผิดชอบ	ทั้งหมด	ทั้งหมด
เปลี่ยนสถานะการแก้ไข	✓	✓	✗
บันทึกการยอมรับความเสี่ยง	✓	✓	✗
สร้าง/แก้ไขแคมเปญ	✗	✓	✗
นำเข้าไฟล์ CSV	✗	✓	✗

ตารางที่ 3-15 (ต่อ)

ฟังก์ชันการทำงาน	เจ้าของระบบและผู้ดูแลระบบ (System Owner/System Admin)	ทีมรักษาความมั่นคงปลอดภัย (Security Team)	ผู้ตรวจสอบ (Auditor)
จัดการสินทรัพย์	✗	✓	✗
จัดการผู้ใช้งาน	✗	✓	✗
จัดการรูปแบบอีเมล	✗	✓	✗
กำหนดเกณฑ์ระดับความรุนแรง	✗	✓	✗
ดูรายงานและส่งออก Excel	เฉพาะระบบที่รับผิดชอบ	✓	✓

3.4 การทดสอบระบบ

ขั้นตอนนี้เป็นการทดสอบระบบที่พัฒนาขึ้นอย่างรอบด้าน เพื่อให้มั่นใจว่าระบบทำงานได้ถูกต้องและตอบสนองความต้องการของผู้ใช้งาน โดยมีรายละเอียดดังนี้

3.4.1 การทดสอบการเชื่อมต่อระหว่างโมดูล (Integration Testing) สำหรับการทำงานร่วมกันระหว่างโมดูลต่างๆ โดยเฉพาะโมดูลนำเข้าไฟล์ CSV การเชื่อมต่อกับฐานข้อมูล และการแจ้งเตือนทางอีเมล โดยใช้ข้อมูลทดสอบ (Test Data) ที่ครอบคลุมทั้งข้อมูลปกติ ข้อมูลที่ไม่ถูกต้อง และข้อมูลขนาดใหญ่ เพื่อทดสอบการจัดการข้อผิดพลาดและประสิทธิภาพของระบบ

3.4.2 การทดสอบการยอมรับของผู้ใช้ (User Acceptance Testing: UAT) ดำเนินการกับกลุ่มผู้ใช้งานที่เกี่ยวข้อง ได้แก่ เจ้าของระบบและทีมรักษาความมั่นคงปลอดภัย เพื่อประเมินความสามารถในการใช้งาน ความถูกต้องของข้อมูล และความเหมาะสมของกระบวนการทำงานของระบบต้นแบบ ผลที่ได้จากการทดสอบถูกนำมาใช้ในการปรับปรุงระบบก่อนนำไปทดลองใช้งานตามสถานการณ์ที่กำหนดในการวิจัย

3.4.3 การทดสอบระบบแจ้งเตือนทางอีเมลทั้ง 7 ประเภทตามที่ออกแบบไว้ในตารางที่ 3-14 โดยจำลองสถานการณ์ต่างๆ ได้แก่ การแจ้งเตือนวันสแกนล่วงหน้า การแจ้งเตือนเมื่อพบช่องโหว่ระดับสูงหรือวิกฤต การแจ้งเตือนเมื่อใกล้ถึงกำหนดวันดำเนินการ การแจ้งเตือนเมื่อครบกำหนดวันดำเนินการ การแจ้งเตือนเมื่อเลยกำหนดวันดำเนินการ การแจ้งเตือนให้ดำเนินการ และการแจ้งเตือนยอมรับความเสี่ยงโดยอัตโนมัติ เพื่อตรวจสอบความถูกต้องของเนื้อหาอีเมล จังหวะการส่ง และรายชื่อผู้รับให้เป็นไปตามที่ออกแบบไว้

3.5 การนำระบบไปใช้งานจริง

ขั้นตอนนี้เป็นการนำระบบที่พัฒนาขึ้นไปทดลองใช้งานในสภาพแวดล้อมที่เตรียมไว้สำหรับการวิจัย เพื่อประเมินว่าระบบสามารถรองรับกระบวนการทำงานหลักได้ครบถ้วนตามที่ออกแบบไว้ โดยครอบคลุมการเตรียมระบบ การทดลองใช้งานโดยผู้เกี่ยวข้อง และการเก็บข้อมูลผลการทดลองเพื่อนำไปใช้ในการประเมินผลของงานวิจัย

3.5.1 การติดตั้งและเตรียมสภาพแวดล้อมสำหรับการทดลองใช้งานระบบ

ผู้วิจัยดำเนินการติดตั้งระบบต้นแบบในสภาพแวดล้อมที่พร้อมสำหรับการทดลองใช้งาน พร้อมกำหนดค่าที่จำเป็นสำหรับการทำงานของระบบ เช่น ฐานข้อมูล การตั้งค่าการส่งอีเมล และข้อมูลพื้นฐานที่เกี่ยวข้อง เพื่อให้ระบบสามารถรองรับการทดลองใช้งานตามสถานการณ์ที่กำหนดไว้ในการวิจัยได้อย่างถูกต้องและต่อเนื่อง

3.5.2 การทดลองใช้งานระบบโดยผู้เกี่ยวข้อง

ผู้วิจัยนำระบบไปทดลองใช้งานกับผู้เกี่ยวข้องในกระบวนการบริหารจัดการช่องโหว่ ได้แก่ System Owner, Security Team, Management และ Auditor โดยมีการอธิบายขั้นตอนการใช้งานและขอบเขตของการทดลอง เพื่อให้ผู้ใช้งานสามารถดำเนินการตามสถานการณ์ที่กำหนดได้อย่างถูกต้อง ทั้งนี้การทดลองใช้งานครอบคลุมกรณีสำคัญ เช่น การสร้างรอบการสแกน การนำเข้าข้อมูลผลการสแกน การบันทึก Corrective Action การบันทึก Risk Acceptance การแจ้งเตือน และการติดตามสถานะผ่าน Dashboard

3.5.3 การเก็บข้อมูลจากการทดลองใช้งานระบบ

ผู้วิจัยเก็บรวบรวมข้อมูลจากการทดลองใช้งานระบบในประเด็นที่เกี่ยวข้องกับการทำงานของระบบต้นแบบ ได้แก่ จำนวนรายการช่องโหว่ที่นำเข้าสู่ระบบ จำนวนรายการที่มีการกำหนด Corrective Action จำนวนรายการที่มีการบันทึก Risk Acceptance จำนวนการแจ้งเตือนที่ระบบส่งออก และข้อสังเกตหรือปัญหาที่พบระหว่างการทดลองใช้งาน เพื่อใช้ประกอบการพิจารณาความครบถ้วนและความเหมาะสมของระบบตามวัตถุประสงค์ของการวิจัย

3.6 การประเมินผลและวิเคราะห์ข้อมูล

ผู้วิจัยประเมินผลระบบที่พัฒนาขึ้นใน 2 ด้านหลัก ได้แก่ การประเมินความถูกต้องและความครบถ้วนของการทำงานของระบบ และการประเมินความคิดเห็นของผู้ใช้งานต่อระบบต้นแบบ จากนั้นนำข้อมูลที่ได้มาวิเคราะห์เพื่อสรุปผลว่าระบบสามารถสนับสนุนกระบวนการบริหารจัดการช่องโหว่ได้ตามขอบเขตที่กำหนดไว้เพียงใด

ในการประเมินความคิดเห็นของผู้ใช้งาน ผู้วิจัยใช้แบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ (Likert Scale) โดยแบบสอบถามดังกล่าวได้ผ่านการตรวจสอบความตรงเชิงเนื้อหาโดยผู้เชี่ยวชาญ

ก่อนนำไปใช้จริง ทั้งนี้ การตรวจสอบดังกล่าวใช้ดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ (IOC) เพื่อให้ข้อคำถามมีความเหมาะสมและสอดคล้องกับประเด็นที่ต้องการประเมิน

3.6.1 การประเมินความถูกต้องและความครบถ้วนของการทำงานของระบบ

ผู้วิจัยประเมินความถูกต้องและความครบถ้วนของการทำงานของระบบ โดยอาศัยผลจากการทดสอบการทำงานของโมดูลหลัก การทดลองใช้งานตามสถานการณ์ที่กำหนด และการตรวจสอบผลลัพธ์ที่ระบบแสดงออกมาเทียบกับข้อกำหนดของระบบที่ออกแบบไว้ การประเมินในส่วนนี้ครอบคลุมประเด็นสำคัญ ได้แก่ การนำเข้าข้อมูลจากไฟล์ CSV การจัดระดับความรุนแรงของช่องโหว่ การกำหนดและติดตาม Corrective Action การบันทึก Risk Acceptance การแจ้งเตือนทางอีเมล การควบคุมสิทธิ์ตามบทบาท และการแสดงผลผ่าน Dashboard

ผลการประเมินในส่วนนี้ใช้วิธีพิจารณาความถูกต้องของผลลัพธ์ที่ระบบประมวลผล ความครบถ้วนของข้อมูลที่บันทึกเข้าสู่ระบบ และความสอดคล้องของการทำงานกับกระบวนการที่กำหนดไว้ในการวิจัย เพื่อยืนยันว่าระบบสามารถรองรับการทำงานหลักได้อย่างเหมาะสมภายใต้ขอบเขตที่กำหนด

3.6.2 การประเมินความคิดเห็นของผู้ใช้งานต่อระบบ

ผู้วิจัยนำระบบไปทดลองใช้งานกับผู้เกี่ยวข้องในกระบวนการบริหารจัดการช่องโหว่ ได้แก่ System Owner, Security Team, Management และ Auditor โดยมีการอธิบายขั้นตอนการใช้งานและขอบเขตของการทดลอง เพื่อให้ผู้ใช้งานสามารถดำเนินการตามสถานการณ์ที่กำหนดได้อย่างถูกต้อง ทั้งนี้ การทดลองใช้งานครอบคลุมกรณีสำคัญ เช่น การสร้างรอบการสแกน การนำเข้าข้อมูลผลการสแกน การบันทึก Corrective Action การบันทึก Risk Acceptance การแจ้งเตือน และการติดตามสถานะผ่าน Dashboard

ภายหลังการทดลองใช้งาน ผู้วิจัยเก็บรวบรวมข้อมูลความคิดเห็นของผู้ใช้งานต่อระบบด้วยแบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ (Likert Scale) จากผู้ใช้งานจำนวน 30 คน โดยแบบสอบถามครอบคลุมประเด็นด้านความง่ายในการใช้งาน ความมีประโยชน์ของระบบ คุณภาพของข้อมูลและการแสดงผล ประสิทธิภาพของระบบ และความพึงพอใจโดยรวม เพื่อนำมาสะท้อนมุมมองของผู้ใช้งานต่อระบบต้นแบบที่พัฒนาขึ้น

แบบสอบถามดังกล่าวกำหนดระดับความคิดเห็นไว้ 5 ระดับ ได้แก่

ระดับ 5 หมายถึง เห็นด้วยมากที่สุด

ระดับ 4 หมายถึง เห็นด้วยมาก

ระดับ 3 หมายถึง เห็นด้วยปานกลาง

ระดับ 2 หมายถึง เห็นด้วยน้อย

ระดับ 1 หมายถึง เห็นด้วยน้อยที่สุด

3.6.3 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลในการวิจัยครั้งนี้ใช้สถิติเชิงพรรณนา เนื่องจากเป็นการประเมินผลการพัฒนาระบบต้นแบบและความคิดเห็นของผู้ใช้งานภายใต้ขอบเขตของการทดลองใช้งานระบบ โดยไม่มีการตั้งสมมติฐานเพื่อเปรียบเทียบความแตกต่างระหว่างกลุ่มตัวอย่าง

ข้อมูลทั่วไปของผู้ตอบแบบสอบถามวิเคราะห์โดยใช้ความถี่และร้อยละ เพื่ออธิบายลักษณะของผู้ตอบแบบสอบถามในแต่ละกลุ่ม ส่วนข้อมูลจากแบบสอบถามความคิดเห็นของผู้ใช้งานต่อระบบวิเคราะห์โดยใช้ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน เพื่อสรุประดับความคิดเห็นของผู้ใช้งานในแต่ละด้าน โดยมีรายละเอียดดังนี้

3.6.3.1 ค่าเฉลี่ย (Mean) ใช้สำหรับวิเคราะห์แนวโน้มโดยรวมของคะแนนที่ได้จากแบบสอบถาม โดยสามารถคำนวณได้จากสัมการที่ 3-1

$$\bar{X} = \sum \frac{X}{n} \tag{3-1}$$

โดยที่

X หมายถึง ค่าเฉลี่ยของคะแนน

X หมายถึง คะแนนของกลุ่มตัวอย่างแต่ละคน

n หมายถึง จำนวนกลุ่มตัวอย่าง

3.6.3.2 ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) ใช้สำหรับวัดการกระจายของคะแนนว่ามีความแตกต่างจากค่าเฉลี่ยมากน้อยเพียงใด โดยสามารถคำนวณได้จากสัมการที่ 3-2

$$S.D. = \sqrt{\frac{\sum(Xi - \bar{X})^2}{n - 1}} \tag{3-2}$$

โดยที่

SD หมายถึง ส่วนเบี่ยงเบนมาตรฐาน

Xi หมายถึง คะแนนของกลุ่มตัวอย่างคนที่ i

$\bar{X}$ หมายถึง ค่าเฉลี่ยของคะแนน

n หมายถึง จำนวนกลุ่มตัวอย่าง

สำหรับการแปลผลค่าเฉลี่ย ผู้วิจัยกำหนดเกณฑ์การแปลความหมายของคะแนนเฉลี่ย 5 ระดับ โดยอ้างอิงเกณฑ์การประเมินของ บุญชม ศรีสะอาด (2535: 100) ดังนี้

ค่าเฉลี่ย 4.51–5.00 หมายถึง ระดับมากที่สุด

ค่าเฉลี่ย 3.51–4.50 หมายถึง ระดับมาก

ค่าเฉลี่ย 2.51–3.50 หมายถึง ระดับปานกลาง

ค่าเฉลี่ย 1.51–2.50 หมายถึง ระดับน้อย

ค่าเฉลี่ย 1.00–1.50 หมายถึง ระดับน้อยที่สุด

3.7 การจัดทำเอกสารและรายงาน

ขั้นตอนสุดท้ายเป็นการจัดทำเอกสารประกอบการวิจัยอย่างครบถ้วน โดยมีรายละเอียดดังนี้

3.7.1 การจัดทำคู่มือการใช้งาน (User Manual) สำหรับผู้ใช้งานแต่ละบทบาท พร้อมภาพหน้าจอ (Screenshot) และขั้นตอนการใช้งานแบบทีละขั้นตอนในรูปแบบ PDF

3.7.2 การจัดทำเอกสารทางเทคนิค (Technical Documentation) ประกอบด้วย แผนภาพสถาปัตยกรรมระบบ (System Architecture Diagram) โครงร่างฐานข้อมูลในรูปแบบ ERD คู่มือการติดตั้ง (Installation Guide) และคู่มือการแก้ไขปัญหา (Troubleshooting Guide)

บทที่ 4
ผลการดำเนินการวิจัย

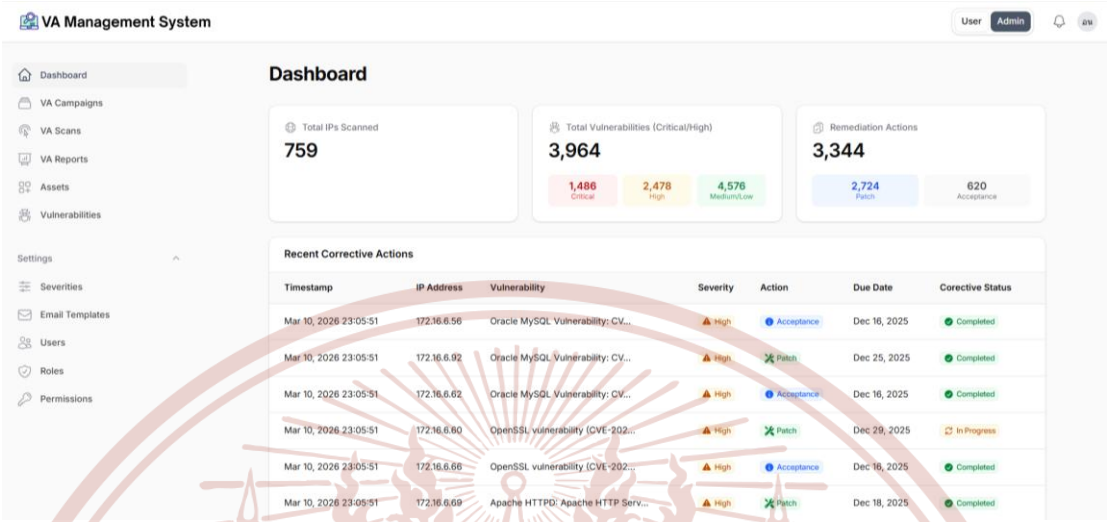
บทนี้นำเสนอผลการดำเนินการวิจัยจากการพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ ตามขอบเขตที่กำหนด โดยครอบคลุมผลการพัฒนาระบบในแต่ละโมดูล ผลการทดลองใช้งานตามสถานการณ์จริง ผลการทดสอบความถูกต้องของระบบ ผลการประเมินจากผู้ใช้หรือผู้เชี่ยวชาญ และข้อค้นพบจากข้อมูลที่แสดงผ่านระบบ Dashboard เพื่อแสดงให้เห็นว่าระบบที่พัฒนาขึ้นสามารถสนับสนุนกระบวนการบริหารจัดการช่องโหว่ได้อย่างเป็นระบบ และสอดคล้องกับวัตถุประสงค์ของการวิจัย

4.1 ผลการพัฒนาระบบแต่ละโมดูล

ผู้วิจัยได้พัฒนาระบบบริหารจัดการช่องโหว่ให้รองรับกระบวนการทำงานหลัก ตั้งแต่การกำหนดรอบการสแกน การนำเข้าผลการสแกนจากไฟล์ CSV การติดตามรายการช่องโหว่ การบันทึกการดำเนินการแก้ไข การบันทึกการยอมรับความเสี่ยง การแจ้งเตือนผู้รับผิดชอบ การกำหนดระดับความรุนแรง และการแสดงผลข้อมูลในรูปแบบ Dashboard ทั้งนี้ การนำเสนอในหัวข้อนี้แบ่งตามฟังก์ชันการทำงานหลัก 6 โมดูลที่กำหนดไว้ในข้อกำหนดเชิงหน้าที่ รวมถึงฟังก์ชันเสริมที่สนับสนุนการทำงานของโมดูลหลัก ได้แก่ การจัดการแคมเปญและรอบการสแกน การกำหนดระดับความรุนแรง และการควบคุมสิทธิ์ตามบทบาทผู้ใช้งาน โดยรายละเอียดผลการพัฒนาในแต่ละโมดูลมีดังนี้

4.1.1 โมดูล Dashboard

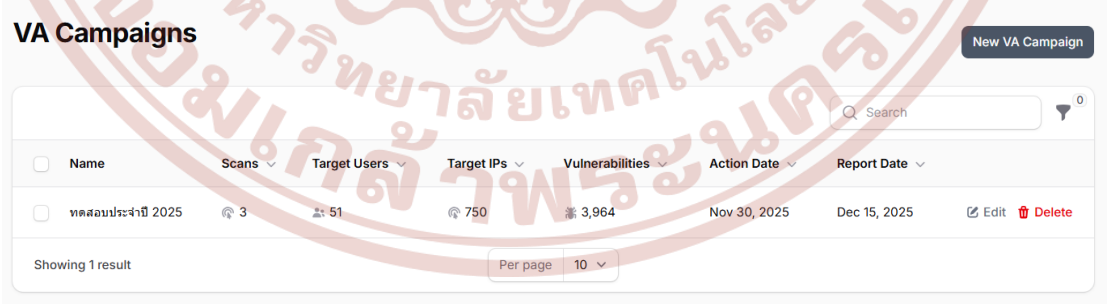
ระบบมีหน้าจอ Dashboard สำหรับแสดงภาพรวมข้อมูลสำคัญของการบริหารจัดการช่องโหว่ในหน้าจอเดียว โดยประกอบด้วยข้อมูลจำนวน IP ที่อยู่ในขอบเขตการสแกน จำนวนช่องโหว่ที่มีความรุนแรงระดับ Critical และ High สถานะของการดำเนินการแก้ไข และตารางแสดงรายการ Corrective Action ล่าสุด เพื่อช่วยให้ผู้ใช้งานติดตามสถานะของช่องโหว่ที่ต้องดำเนินการได้อย่างรวดเร็ว ทั้งนี้ข้อมูลที่แสดงบน Dashboard สามารถกำหนดให้สอดคล้องกับสิทธิ์ของผู้ใช้งานแต่ละบทบาทได้



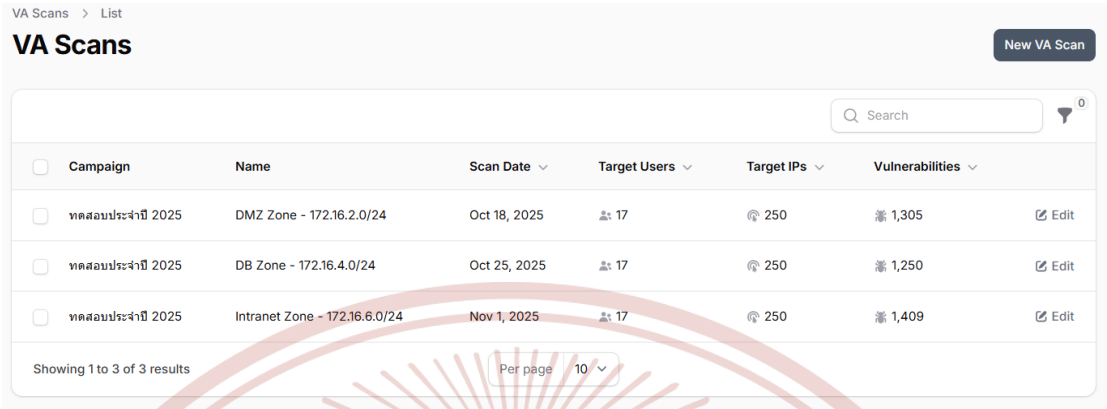
ภาพที่ 4-1 หน้า Dashboard ภาพรวมของระบบ

4.1.2 โมดูลจัดการแคมเปญและรอบการสแกน

ระบบรองรับการจัดการแคมเปญและรอบการสแกนเพื่อใช้กำหนดขอบเขตการดำเนินงานในแต่ละช่วงเวลา โดยผู้ดูแลระบบสามารถสร้างแคมเปญประจำปี กำหนดชื่อรอบการสแกน วันที่สแกน กลุ่มผู้ใช้งานเป้าหมาย ช่วงเครือข่ายหรือรายการ IP ที่ต้องการสแกน รวมถึงกำหนดวันดำเนินการและวันส่งรายงานได้ นอกจากนี้ระบบยังรองรับการตั้งค่าการแจ้งเตือนและการอัปโหลดไฟล์รายงานผลการสแกนในระดับรอบการสแกน ทำให้สามารถบริหารการประเมินช่องโหว่เป็นรอบและติดตามผลย้อนหลังได้อย่างเป็นระบบ



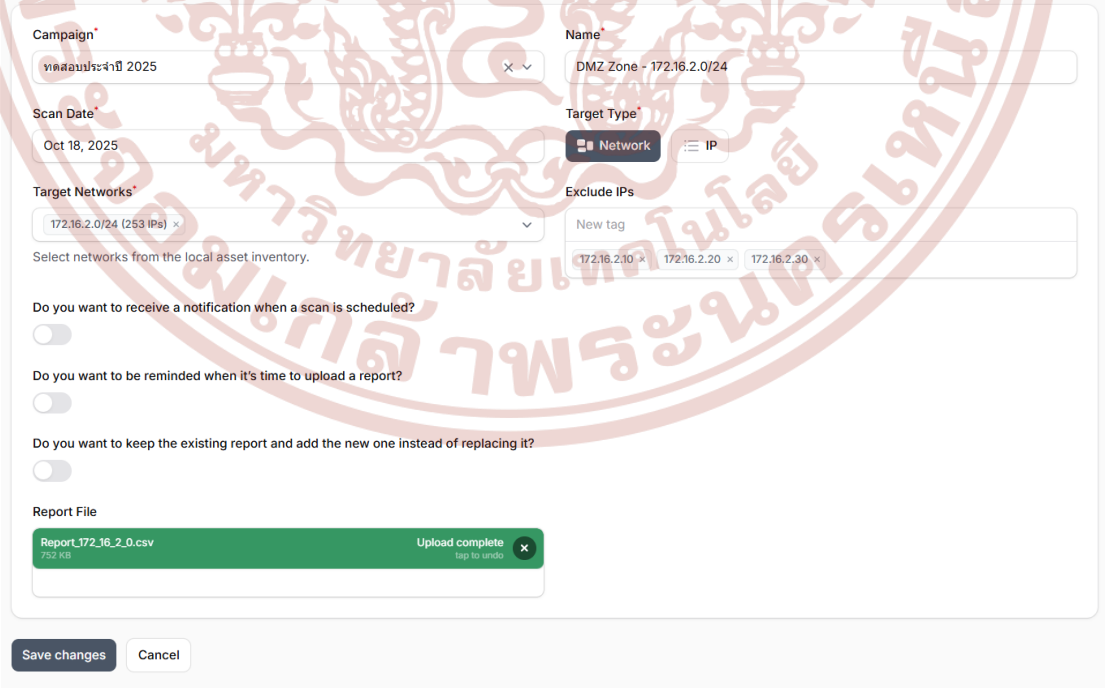
ภาพที่ 4-2 หน้าจอแสดงรายการแคมเปญการประเมินช่องโหว่



ภาพที่ 4-3 หน้าจอแสดงรายการรอบการสแกนภายใต้แคมเปญ

4.1.3 โมดูลนำเข้าข้อมูลผลการสแกนจากไฟล์ CSV

ระบบรองรับการนำเข้าข้อมูลผลการสแกนจากไฟล์ CSV ที่ส่งออกจากเครื่องมือ Rapid7 InsightVM โดยผู้ใช้งานสามารถอัปโหลดไฟล์รายงานผ่านหน้าจอรอบการสแกน จากนั้นระบบจะตรวจสอบรูปแบบข้อมูล แยกข้อมูลสำคัญของช่องโหว่ และบันทึกเข้าสู่ฐานข้อมูลตามโครงสร้างที่ออกแบบไว้ พร้อมทั้งเชื่อมโยงข้อมูลช่องโหว่กับสินทรัพย์ที่เกี่ยวข้องในระบบ กระบวนการดังกล่าวช่วยลดภาระการบันทึกข้อมูลแบบแมนนวลและทำให้ข้อมูลพร้อมต่อการติดตามในขั้นตอนถัดไป



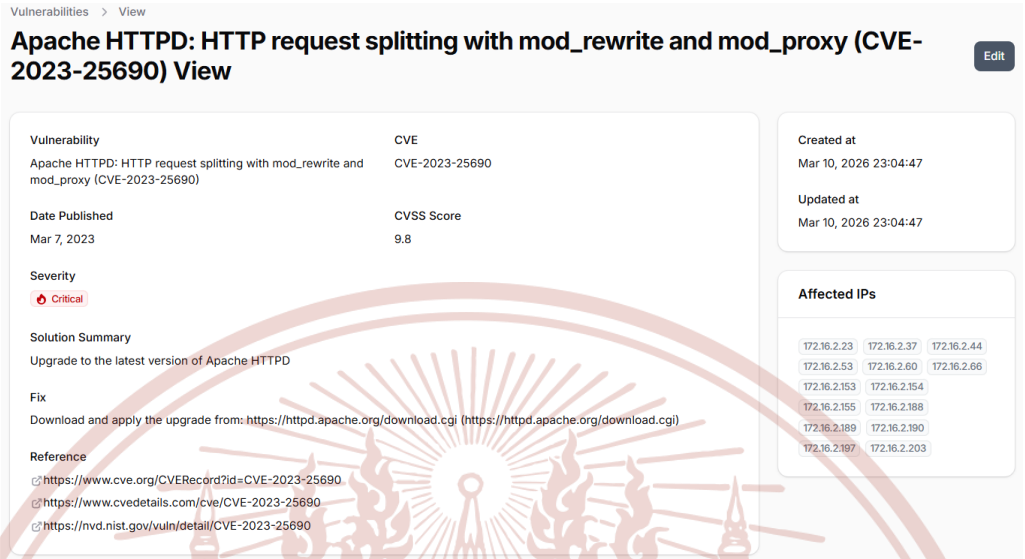
ภาพที่ 4-4 หน้าจอผลลัพธ์หลังการนำเข้าข้อมูล

4.1.4 โมดูลรายการช่องโหว่และรายละเอียดช่องโหว่

ระบบมีหน้าจอรายการช่องโหว่สำหรับแสดงข้อมูลช่องโหว่ที่ถูกนำเข้าสู่ระบบ โดยผู้ใช้งานสามารถค้นหา คัดกรอง และเรียงลำดับข้อมูลได้ตามเงื่อนไขที่สำคัญ เช่น รหัส CVE วันที่เผยแพร่ คะแนน CVSS ระดับความรุนแรง และจำนวนสินทรัพย์ที่ได้รับผลกระทบ เมื่อเลือกดูรายละเอียดของแต่ละรายการ ระบบจะแสดงข้อมูลเชิงลึกเพิ่มเติม เช่น ชื่อช่องโหว่ แนวทางการแก้ไข สรุปวิธีการแก้ไข แหล่งอ้างอิง และรายการ IP ที่ได้รับผลกระทบ เพื่อสนับสนุนการวิเคราะห์และการตัดสินใจเลือกแนวทางการจัดการที่เหมาะสม ทั้งนี้ผู้ใช้งานแต่ละบทบาทสามารถเข้าถึงข้อมูลได้ตามสิทธิ์ที่กำหนดในระบบ



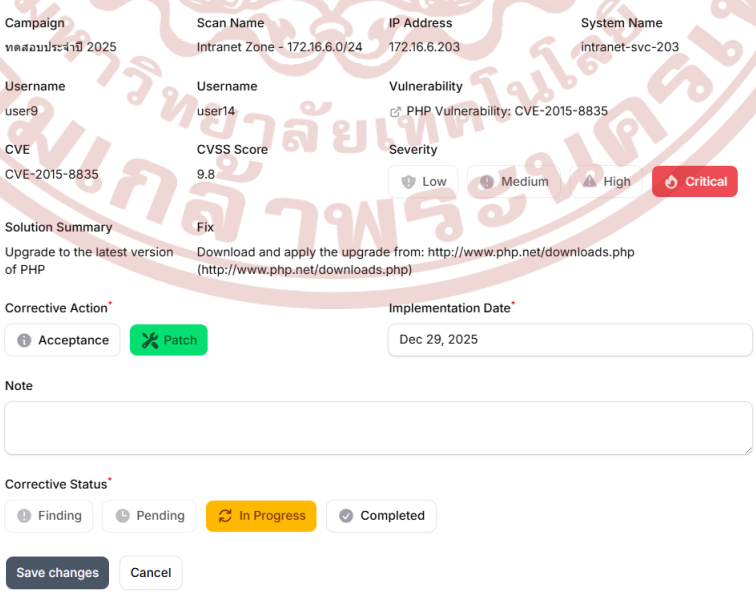
ภาพที่ 4-5 หน้าจอรายการช่องโหว่



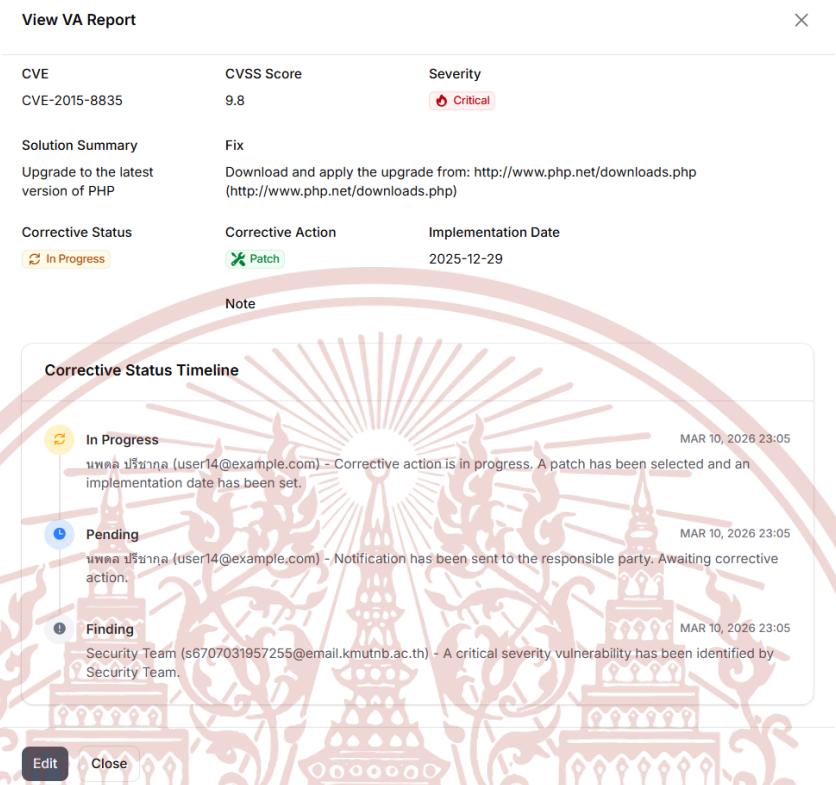
ภาพที่ 4-6 หน้าจอรายละเอียดช่องโหว่

4.1.5 โมดูล Corrective Action

ระบบรองรับการบันทึกและติดตามการดำเนินการแก้ไขช่องโหว่ในระดับรายรายการ โดยผู้รับผิดชอบสามารถเลือกประเภทการดำเนินการ กำหนดวันดำเนินการ บันทึกหมายเหตุ และอัปเดตสถานะการแก้ไขได้ตามลำดับขั้น ได้แก่ Finding, Pending, In Progress และ Completed นอกจากนี้ระบบยังแสดงประวัติการเปลี่ยนแปลงสถานะในรูปแบบลำดับเวลา (Timeline) เพื่อใช้ติดตามความคืบหน้าและตรวจสอบย้อนหลังได้อย่างเป็นระบบ



ภาพที่ 4-7 หน้าจอบันทึกข้อมูล Corrective Action และสถานะการดำเนินการแก้ไข

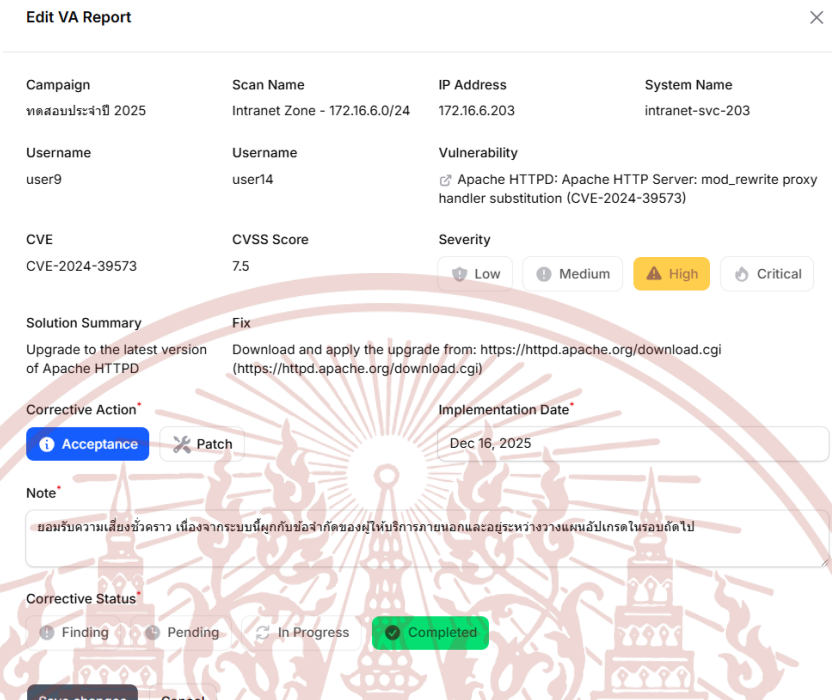


ภาพที่ 4-8 หน้าจอแสดงรายละเอียดและลำดับเวลาการติดตาม Corrective Action

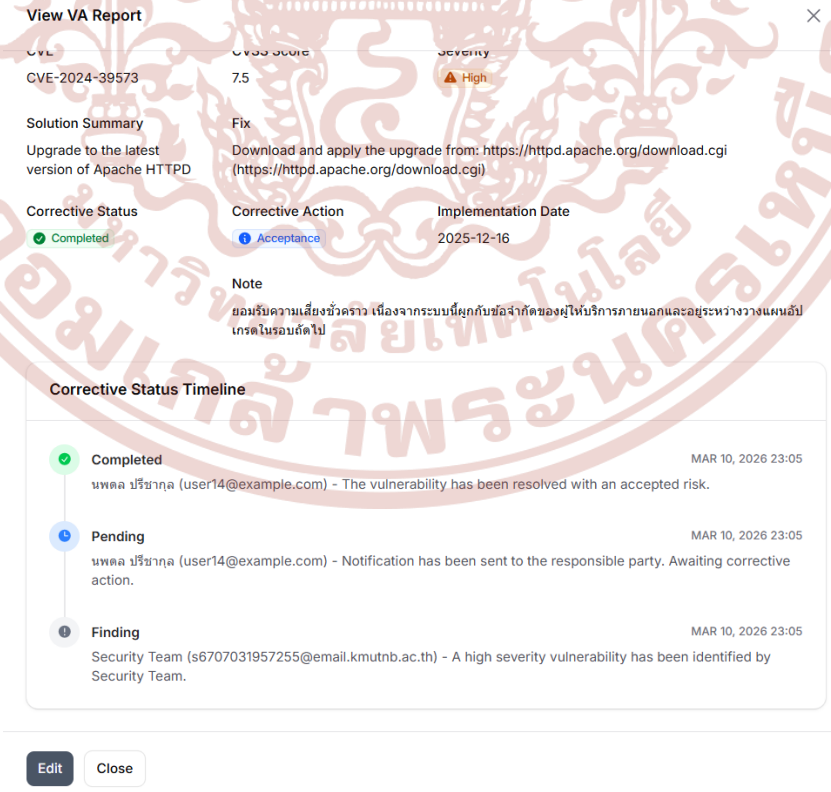
4.1.6 โมดูล Risk Acceptance

ระบบรองรับการยอมรับความเสี่ยงเป็นหนึ่งในรูปแบบของ Corrective Action สำหรับกรณีที่ยังไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ในทันที โดยผู้ใช้งานสามารถเลือกการดำเนินการแบบ Acceptance บันทึกเหตุผลหรือหมายเหตุประกอบ และตรวจสอบประวัติการเปลี่ยนแปลงย้อนหลังผ่านลำดับเวลาการติดตามได้

นอกจากนี้ ระบบยังรองรับการบันทึกการยอมรับความเสี่ยงโดยอัตโนมัติตามเงื่อนไขของแคมเปญ ในกรณีที่รายการช่องโหว่ยังคงอยู่ในสถานะ pending และไม่มีการดำเนินการภายในระยะเวลาที่กำหนด แม้ว่าระบบได้มีการแจ้งเตือนผู้รับผิดชอบแล้ว ระบบจะบันทึกรายการดังกล่าวเข้าสู่เงื่อนไข acceptance พร้อมจัดเก็บประวัติการแจ้งเตือนและการเปลี่ยนแปลงสถานะไว้ในระบบเพื่อรองรับการตรวจสอบย้อนหลัง



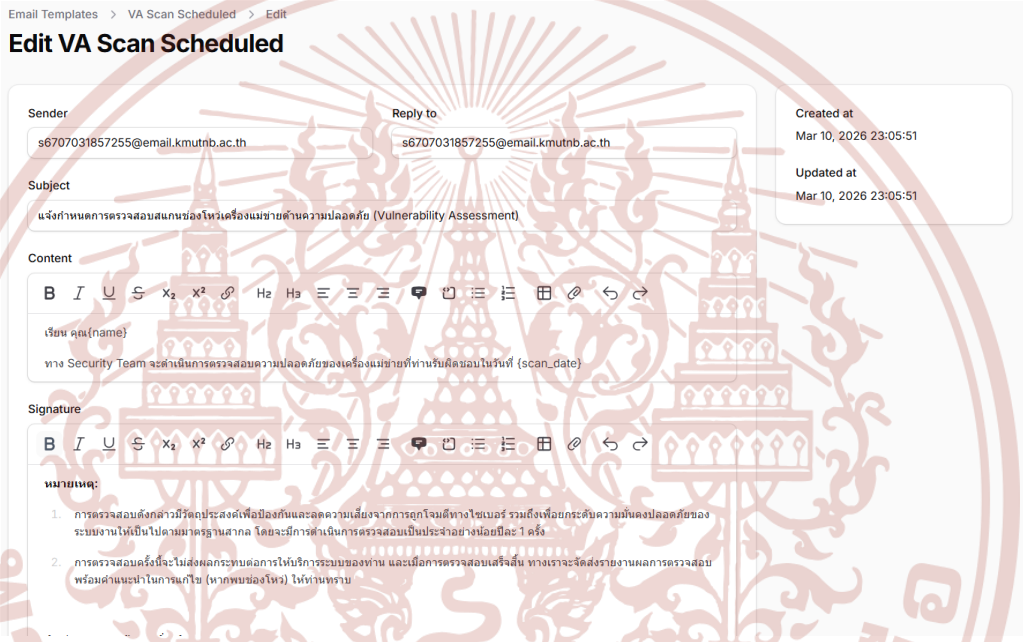
ภาพที่ 4-9 หน้าจอบันทึก Risk Acceptance



ภาพที่ 4-10 หน้าจอรายละเอียดหรือประวัติการยอมรับความเสี่ยง

4.1.7 โมดูล Notification และ Email Template

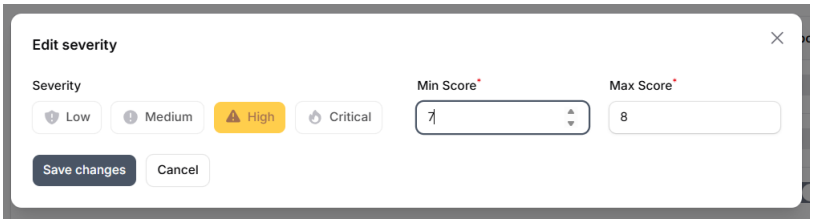
ระบบรองรับการจัดการแม่แบบอีเมลสำหรับการแจ้งเตือนในแต่ละเหตุการณ์ของกระบวนการบริหารจัดการช่องโหว่ โดยผู้ดูแลระบบสามารถกำหนดผู้ส่ง ผู้รับตอบกลับ หัวเรื่อง และเนื้อหาอีเมลได้ผ่านหน้าจอ Email Template เพื่อให้การสื่อสารกับผู้รับผิดชอบมีรูปแบบที่เป็นมาตรฐานและสามารถปรับแก้ได้ตามบริบทขององค์กร



ภาพที่ 4-11 หน้าจอจัดการ Email Template

4.1.8 โมดูลกำหนดระดับความรุนแรง

ระบบมีหน้าจอสำหรับกำหนดเกณฑ์ระดับความรุนแรงของช่องโหว่ โดยผู้ดูแลระบบสามารถปรับช่วงคะแนน CVSS ขั้นต่ำและสูงสุดของแต่ละระดับ เช่น Low, Medium, High และ Critical รวมถึงกำหนดได้ว่าระดับใดจะถือเป็นรายการที่ต้องรายงานหรือแจ้งเตือน (Reportable) เพื่อให้ระบบสามารถปรับใช้ตามนโยบายและเกณฑ์การบริหารความเสี่ยงขององค์กรได้อย่างยืดหยุ่น



ภาพที่ 4-12 หน้าจอกำหนดค่า Severity

4.1.9 การควบคุมสิทธิ์ตามบทบาทผู้ใช้งาน

ระบบรองรับการกำหนดบทบาทและสิทธิ์การเข้าถึงของผู้ใช้งานตามหน้าที่รับผิดชอบ โดยสามารถกำหนดสิทธิ์การเข้าถึงเมนูและฟังก์ชันต่าง ๆ ให้แตกต่างกันในแต่ละบทบาท ได้แก่ เจ้าของระบบและผู้ดูแลระบบ (System Owner/System Admin) ทีมรักษาความมั่นคงปลอดภัย (Security Team) และผู้ตรวจสอบ (Auditor) ทำให้ผู้ใช้งานแต่ละกลุ่มสามารถเข้าถึงเฉพาะข้อมูลและฟังก์ชันที่เกี่ยวข้องกับหน้าที่ของตน ซึ่งช่วยลดการเข้าถึงข้อมูลโดยไม่จำเป็น และสนับสนุนการควบคุมความปลอดภัยของข้อมูลตามแนวคิดการควบคุมสิทธิ์ตามบทบาทผู้ใช้งาน



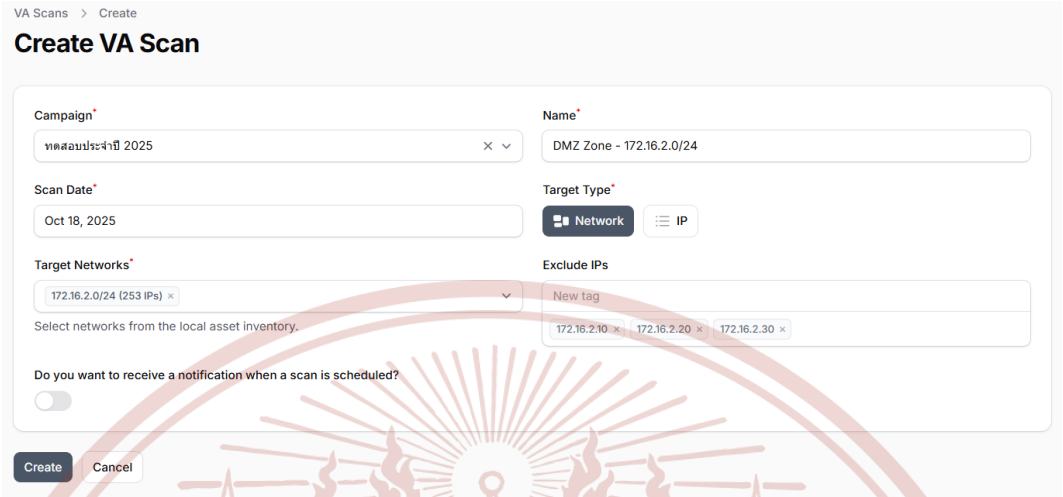
ภาพที่ 4-13 หน้าจอกำหนดบทบาทและสิทธิ์การเข้าถึงของผู้ใช้งาน

4.2 ผลการทดลองใช้งานตามสถานการณ์ที่กำหนด

เพื่อประเมินว่าระบบสามารถรองรับกระบวนการทำงานจริงได้ครบถ้วน ผู้วิจัยได้ทดลองใช้งานระบบตามสถานการณ์ที่กำหนดไว้ โดยอ้างอิงตามลำดับขั้นตอนของกระบวนการบริหารจัดการช่องโหว่ ตั้งแต่การสร้างรอบการสแกน การแจ้งเตือนผู้รับผิดชอบ การนำเข้าผลการสแกน การกำหนดแนวทางการจัดการช่องโหว่ การติดตามความคืบหน้าตามระยะเวลา และการปิดรอบการติดตามของรายการช่องโหว่ในระบบ

4.2.1 สถานการณ์การสร้างรอบการสแกนและแจ้งเตือนก่อนวันสแกน

ผู้ดูแลระบบสร้างรอบการสแกนใหม่โดยกำหนดแคมเปญ ชื่อรอบการสแกน วันสแกน ประเภทเป้าหมาย และช่วงเครือข่ายหรือรายการ IP ที่ต้องการตรวจสอบ จากนั้นระบบจะส่งอีเมลแจ้งเตือนไปยัง System Owner ที่เกี่ยวข้อง เพื่อแจ้งกำหนดการสแกนล่วงหน้าและเตรียมความพร้อมก่อนการดำเนินการจริง



ภาพที่ 4-14 หน้าจอสร้างรอบการสแกน



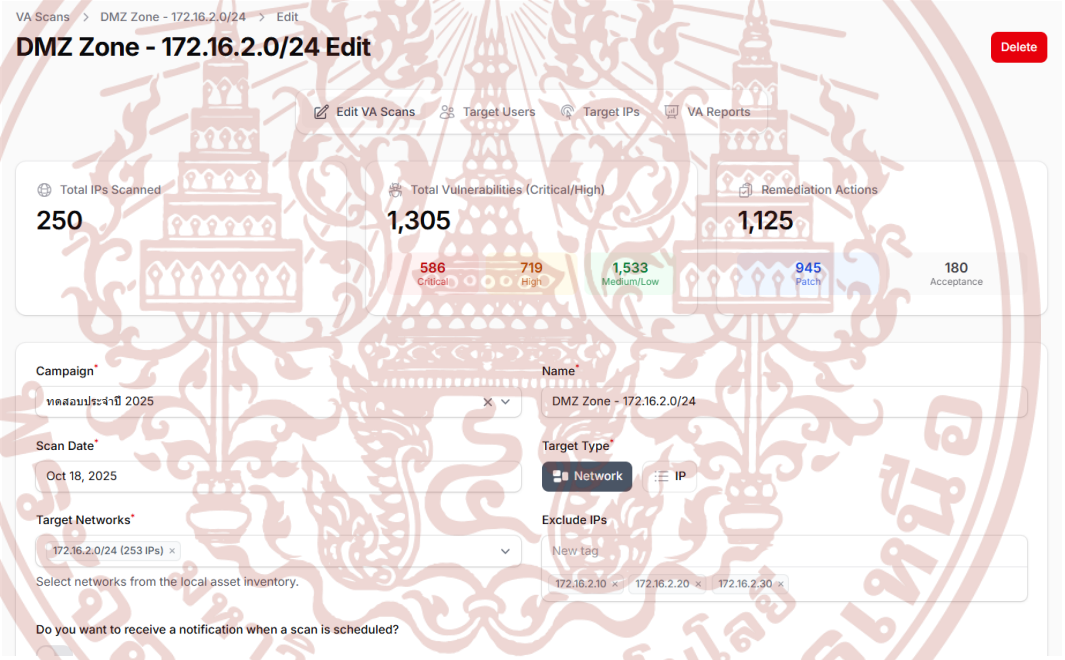
ภาพที่ 4-15 ตัวอย่างอีเมลแจ้งเตือนก่อนวันสแกน

ผลการทดลองใช้งานพบว่าระบบสามารถสร้างรอบการสแกนและส่งอีเมลแจ้งเตือนไปยังผู้รับผิดชอบได้ตามเงื่อนไขที่กำหนดไว้ ช่วยให้การวางแผนการประเมินช่องโหว่เป็นไปอย่างเป็นระบบและสามารถสื่อสารกับผู้เกี่ยวข้องได้ล่วงหน้า

4.2.2 สถานการณ์การนำเข้าผลการสแกนและแจ้งเตือนเมื่อพบช่องโหว่ระดับรุนแรง

ภายหลังการดำเนินการสแกน ผู้ดูแลระบบนำเข้าข้อมูลผลการสแกนจากไฟล์ CSV ที่ส่งออกจากเครื่องมือ Rapid7 InsightVM เข้าสู่ระบบ เมื่อระบบประมวลผลข้อมูลแล้ว รายการช่องโหว่จะถูกเชื่อมโยงกับรอบการสแกนและสินทรัพย์ที่เกี่ยวข้อง พร้อมทั้งแสดงข้อมูลสรุปของจำนวนสินทรัพย์ที่สแกน จำนวนช่องโหว่ที่ตรวจพบ และจำนวนแนวทางการดำเนินการที่เกี่ยวข้อง

ในกรณีที่ระบบตรวจพบช่องโหว่ที่มีระดับความรุนแรงเป็น Critical หรือ High และอยู่ในกลุ่มที่กำหนดให้เป็นรายการที่ต้องรายงาน (Reportable) ระบบจะส่งอีเมลแจ้งเตือนไปยังผู้รับผิดชอบเพื่อให้เข้ามาตรวจสอบรายละเอียดและดำเนินการต่อไปผ่านระบบ



ภาพที่ 4-16 หน้าจอรอบการสแกนหลังนำเข้ารายงานผลการสแกนและประมวลผลข้อมูล



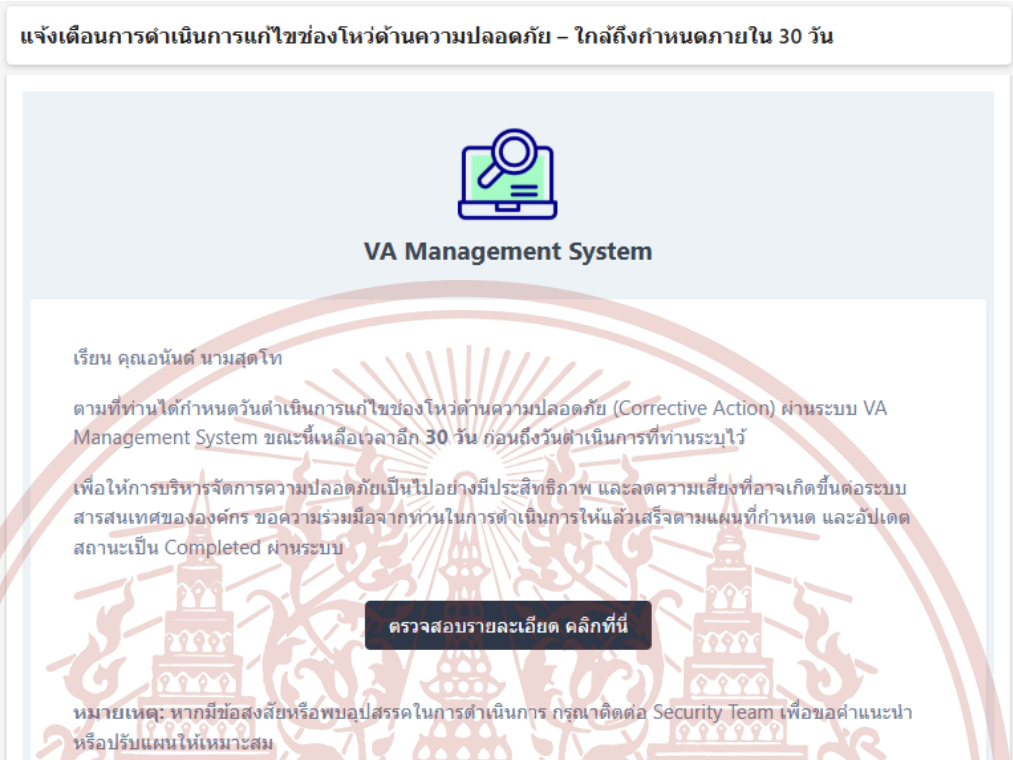
ภาพที่ 4-17 ตัวอย่างอีเมลแจ้งเตือนเมื่อพบช่องโหว่ระดับรุนแรง

ผลการทดลองใช้งานพบว่าระบบสามารถนำเข้าข้อมูลผลการสแกน ตรวจสอบระดับความรุนแรงของช่องโหว่ และส่งการแจ้งเตือนไปยังผู้รับผิดชอบได้ตามที่ออกแบบไว้

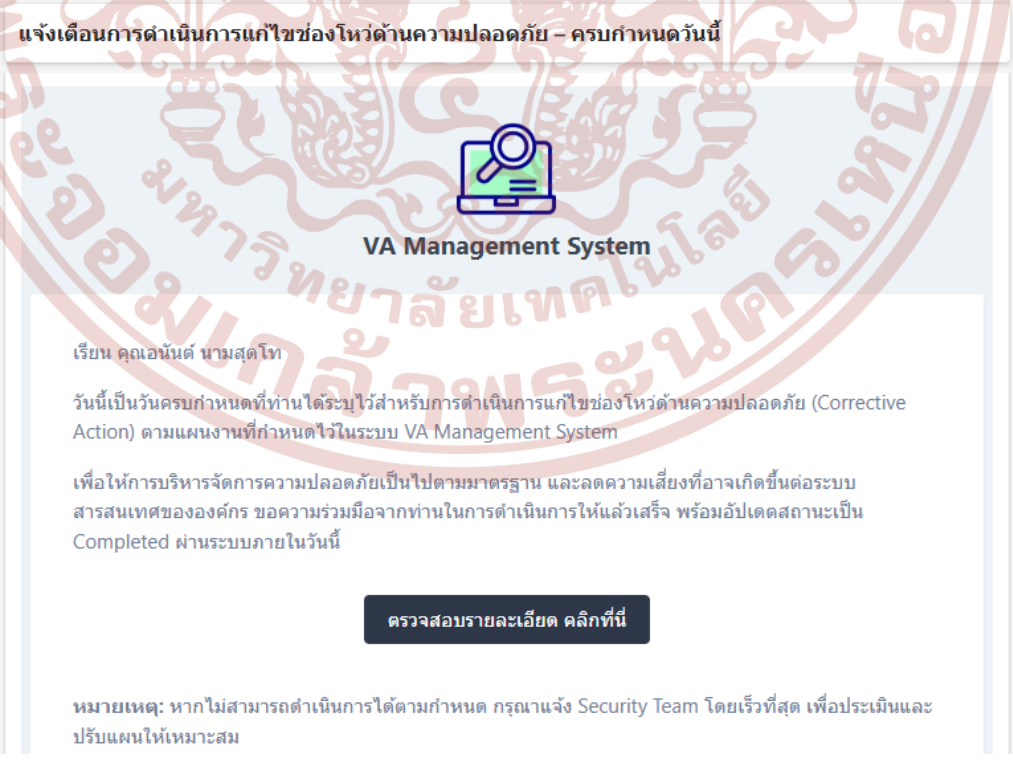
4.2.3 สถานการณ์การบันทึก Corrective Action และการติดตามตามกำหนดเวลา

ภายหลังผู้รับผิดชอบได้รับแจ้งเตือนและเข้ามากำหนดแนวทางการจัดการช่องโหว่ในระบบแล้ว ผู้รับผิดชอบสามารถเลือก Corrective Action ที่เหมาะสม เช่น การติดตั้ง Patch พร้อมระบุ Implementation Date เพื่อใช้เป็นกรอบเวลาสำหรับการติดตามความคืบหน้าในขั้นตอนถัดไป

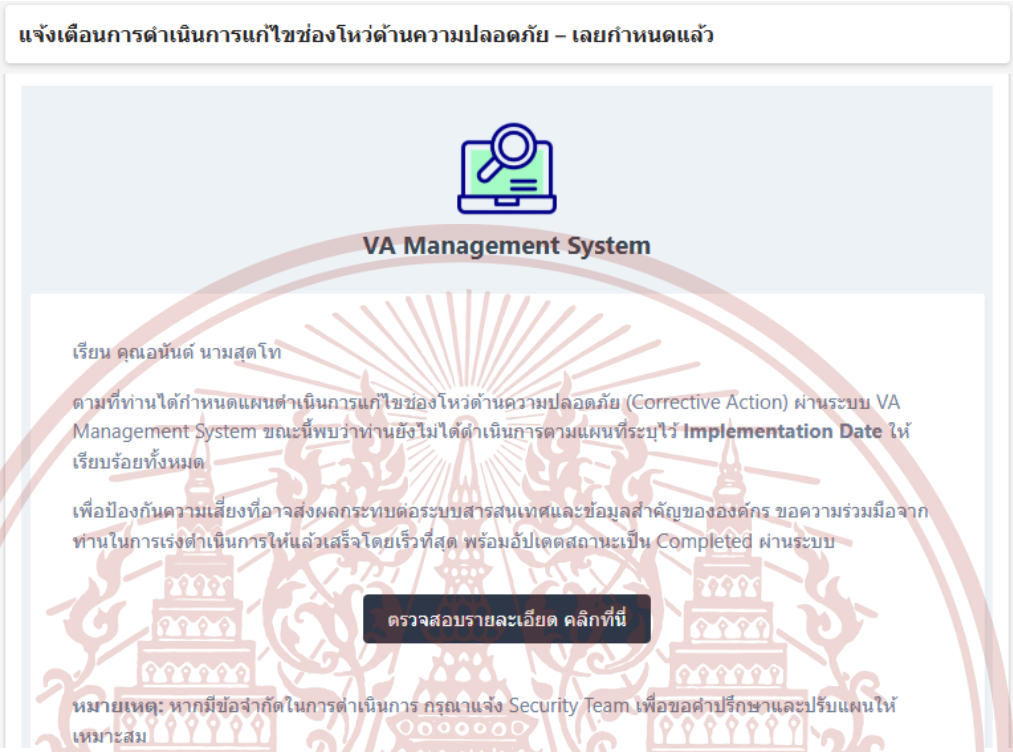
เมื่อมีการกำหนดแผนการดำเนินการแล้ว ระบบจะติดตามรายการดังกล่าวตามช่วงเวลาที่กำหนด โดยส่งอีเมลแจ้งเตือนก่อนถึงกำหนดดำเนินการ เมื่อถึงวันกำหนดดำเนินการ และเมื่อเกินกำหนดดำเนินการ เพื่อกระตุ้นให้ผู้รับผิดชอบดำเนินการแก้ไขและอัปเดตสถานะของรายการในระบบอย่างต่อเนื่อง



ภาพที่ 4-18 ตัวอย่างอีเมลแจ้งเตือนก่อนถึงกำหนดดำเนินการ



ภาพที่ 4-19 ตัวอย่างอีเมลแจ้งเตือนเมื่อถึงวันกำหนดดำเนินการ



ภาพที่ 4-20 ตัวอย่างอีเมลแจ้งเตือนเมื่อเกินกำหนดดำเนินการ

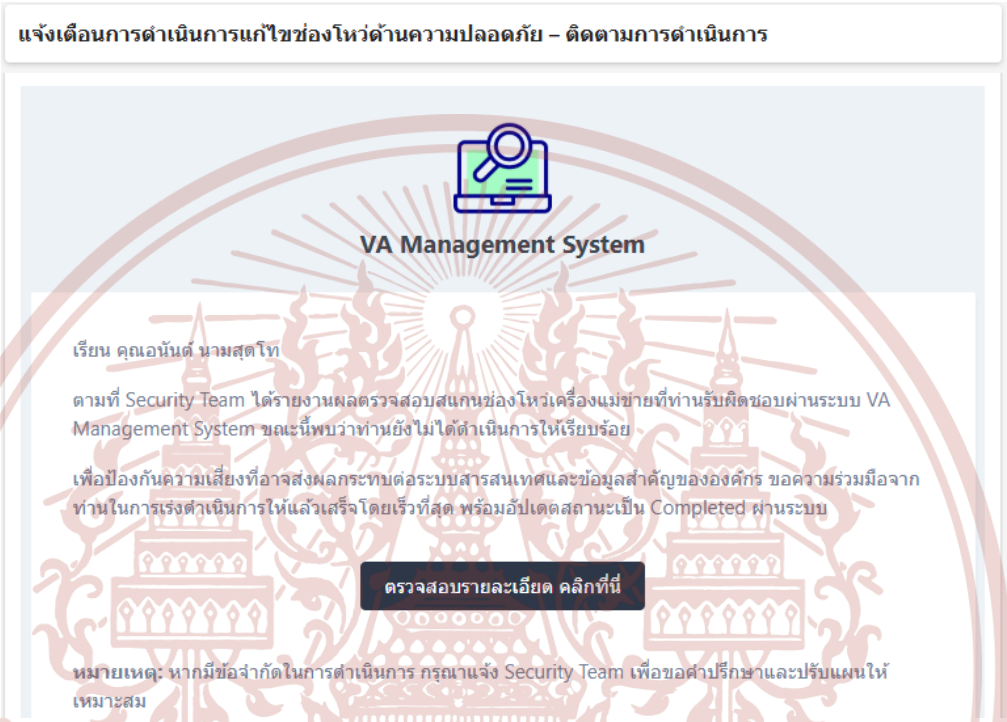
ผลการทดลองใช้งานพบว่าระบบสามารถติดตามสถานะของ Corrective Action ได้อย่างต่อเนื่อง และสามารถส่งอีเมลแจ้งเตือนตามช่วงเวลาที่กำหนดไว้ เพื่อสนับสนุนให้ผู้รับผิดชอบดำเนินการแก้ไขช่องโหว่ภายในระยะเวลาที่วางแผนไว้

4.2.4 สถานการณ์กรณีเจ้าของระบบไม่ดำเนินการภายในกำหนด และระบบบันทึกรายการเข้าสู่เงื่อนไข Acceptance โดยอัตโนมัติ

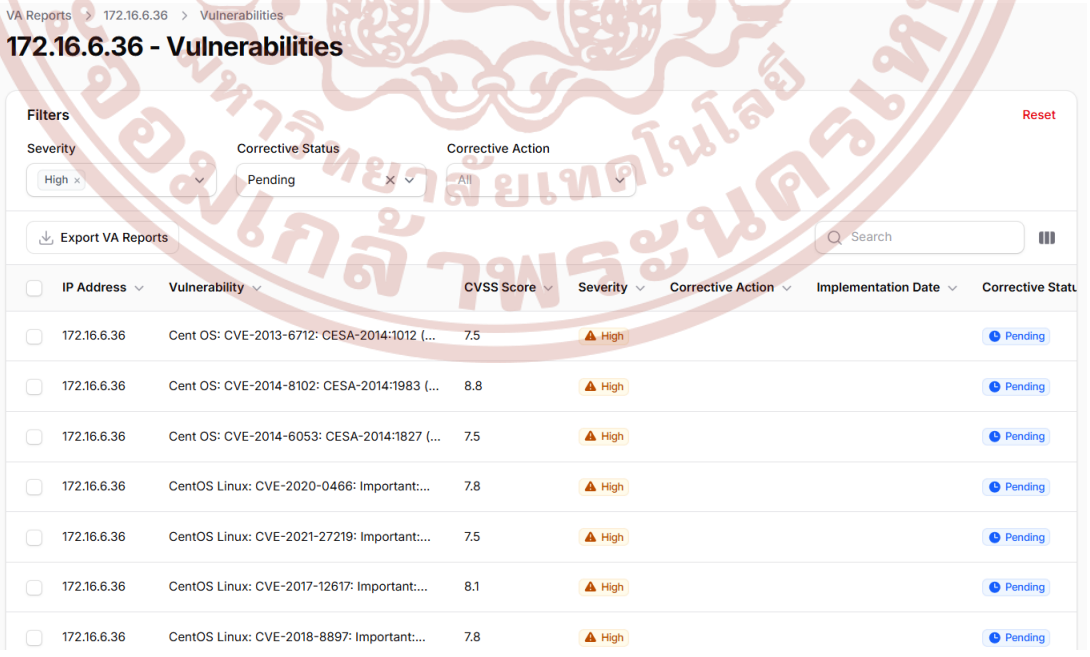
ในสถานการณ์นี้ ผู้วิจัยจำลองกรณีที่เจ้าของระบบไม่ได้ดำเนินการใด ๆ ต่อรายการช่องโหว่ภายในระยะเวลาที่กำหนด และรายการดังกล่าวยังคงอยู่ในสถานะ pending แม้ว่าระบบจะได้ส่งการแจ้งเตือนให้รับทราบก่อนหน้านี้แล้วก็ตาม เมื่อพ้นวัน report date ของแคมเปญและยังไม่มีการตอบสนองจากเจ้าของระบบ ระบบจะบันทึกรายการดังกล่าวเข้าสู่เงื่อนไข acceptance โดยอัตโนมัติตามกติกาการติดตามที่กำหนดไว้ในระบบ

ภายหลังการดำเนินการดังกล่าว ระบบจะเปลี่ยน corrective action เป็น acceptance และเปลี่ยน corrective status เป็น completed พร้อมบันทึกประวัติการแจ้งเตือนและการเปลี่ยนแปลงสถานะไว้ในระบบ เพื่อใช้ในการติดตามและตรวจสอบย้อนหลัง ผลการทดลองใช้งานพบว่าระบบ

สามารถดำเนินการตามเงื่อนไขนี้ได้อย่างถูกต้อง และช่วยลดโอกาสที่รายการช่องโหว่จะคงค้างอยู่ในระบบโดยไม่มีการอัปเดตสถานะ



ภาพที่ 4-21 ตัวอย่างอีเมลแจ้งเตือนกรณีไม่มีการดำเนินการก่อนถึงวัน report date 7 วัน



ภาพที่ 4-22 หน้าจอแสดงรายการช่องโหว่ที่ยังมีสถานะ pending ก่อนถึงกำหนด report date

เมื่อพ้นวัน report date แล้ว และเจ้าของระบบยังไม่มีการดำเนินการใด ๆ ต่อรายการช่องโหว่ดังกล่าว ระบบจะดำเนินการเปลี่ยนสถานะของรายการที่ยังคงเป็น pending ให้เข้าสู่เงื่อนไข acceptance โดยอัตโนมัติ ตามกติกาการปิดรอบการติดตามที่กำหนดไว้ในแคมเปญ ทั้งนี้ระบบจะเปลี่ยน corrective action เป็น acceptance และเปลี่ยน corrective status เป็น completed เพื่อให้รายการดังกล่าวมีสถานะสิ้นสุดในระบบอย่างชัดเจนและสามารถตรวจสอบย้อนหลังได้



ภาพที่ 4-23 ตัวอย่างอีเมลแจ้งเตือนกรณีระบบเปลี่ยนรายการเข้าสู่เงื่อนไข Acceptance โดยอัตโนมัติ

ทั้งนี้ รายการช่องโหว่ที่อยู่ในสถานะ in progress จะไม่เข้าสู่เงื่อนไขดังกล่าว เนื่องจากเจ้าของระบบได้เข้ามากำหนดแนวทางการดำเนินการและวันดำเนินการไว้แล้ว รายการประเภทนี้จะยังคงถูกติดตามภายใต้กลไกการแจ้งเตือนตามกำหนดเวลา ได้แก่ การแจ้งเตือนก่อนถึงกำหนดดำเนินการ การแจ้งเตือนเมื่อถึงกำหนดดำเนินการ และการแจ้งเตือนเมื่อเกินกำหนดดำเนินการ ตาม Implementation Date ที่ระบุไว้ในระบบ

นอกจากนี้ ระบบยังบันทึกประวัติการเปลี่ยนแปลงสถานะและการแจ้งเตือนในลักษณะลำดับเวลา เพื่อใช้ในการตรวจสอบย้อนหลัง โดยแสดงรายละเอียดสำคัญ เช่น สถานะของรายการก่อนและ

หลังการเปลี่ยนแปลง วันและเวลาที่เกิดเหตุการณ์ และข้อความอธิบายประกอบในแต่ละช่วงของกระบวนการ



ภาพที่ 4-24 หน้าจอแสดงประวัติการเปลี่ยนแปลงสถานะย้อนหลังของรายการช่องโหว่

ผลการทดลองใช้งานพบว่าระบบสามารถติดตามรายการที่ยังไม่มีการดำเนินการภายในระยะเวลาที่กำหนด และสามารถเปลี่ยนรายการเข้าสู่เงื่อนไข acceptance ตามกติกาที่กำหนดไว้ในแคมเปญได้อย่างถูกต้อง พร้อมทั้งบันทึกประวัติการเปลี่ยนแปลงเพื่อรองรับการตรวจสอบย้อนหลัง

4.3 ผลการทดสอบความถูกต้องของระบบ

ผู้วิจัยดำเนินการทดสอบระบบที่พัฒนาขึ้นเพื่อประเมินความถูกต้องของการทำงานตามข้อกำหนดเชิงหน้าที่และเงื่อนไขสำคัญของระบบ โดยครอบคลุมการนำเข้าข้อมูลจากไฟล์ CSV การจัดระดับความรุนแรงของช่องโหว่ การควบคุมสิทธิ์ตามบทบาท การแจ้งเตือนตามเงื่อนไขของระบบ การ

แสดงผลบน Dashboard และการทำงานร่วมกันของโมดูลหลัก ผลการทดสอบมีรายละเอียดดังต่อไปนี้

4.3.1 ผลการทดสอบการนำเข้าข้อมูล CSV

การทดสอบส่วนนี้มุ่งประเมินความถูกต้องของการอ่านข้อมูลจากไฟล์ CSV การตรวจสอบรูปแบบข้อมูล การแยกข้อมูลสำคัญของช่องโหว่ และการบันทึกข้อมูลเข้าสู่ฐานข้อมูล โดยผู้วิจัยได้เปรียบเทียบข้อมูลที่นำรเข้าสู่ระบบกับข้อมูลต้นทางจากไฟล์รายงานจำนวนอย่างน้อย 100 รายการ เพื่อยืนยันว่าค่าที่สำคัญ เช่น IP Address, ชื่อช่องโหว่, รหัส CVE, คะแนน CVSS และระดับความรุนแรง ถูกนำเข้าและประมวลผลได้อย่างถูกต้อง

ตารางที่ 4-1 ผลการทดสอบการนำเข้าข้อมูลจากไฟล์ CSV

ลำดับ	รายการทดสอบ	ข้อมูลทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
1	อัปโหลดไฟล์ CSV ที่มีรูปแบบถูกต้องและมีข้อมูลครบถ้วน	ไฟล์ CSV ที่ส่งออกจาก Rapid7 InsightVM จำนวน 100 รายการ	ระบบสามารถอ่านไฟล์ นำเข้าข้อมูล และบันทึกข้อมูลลงฐานข้อมูลได้ครบถ้วน	ผ่าน
2	อัปโหลดไฟล์ CSV ที่ข้อมูลบางฟิลด์สำคัญไม่ครบถ้วน	ไฟล์ CSV ที่ตัดค่าบางฟิลด์ เช่น IP Address หรือชื่อช่องโหว่ออกบางแถว	ระบบตรวจพบข้อมูลไม่สมบูรณ์และแจ้งข้อผิดพลาดก่อนบันทึก	ผ่าน
3	อัปโหลดไฟล์ที่ไม่ใช่รูปแบบ CSV	ไฟล์นามสกุล .txt และ .xlsx	ระบบปฏิเสธการนำเข้าและแจ้งให้ผู้ใช้เลือกไฟล์รูปแบบที่ถูกต้อง	ผ่าน
4	อัปโหลดไฟล์ที่มีข้อมูลซ้ำกับข้อมูลเดิมในรอบการสแกน	ไฟล์ CSV ที่มีรายการช่องโหว่ซ้ำกับข้อมูลที่นำเข้าไว้ก่อนแล้ว	ระบบจัดการข้อมูลซ้ำตามเงื่อนไขที่กำหนด และไม่ทำให้ข้อมูลในระบบผิดเพี้ยน	ผ่าน

4.3.2 ผลการทดสอบความถูกต้องของการจัดระดับความรุนแรง

การทดสอบส่วนนี้ใช้ตรวจสอบว่าระบบสามารถแปลผลคะแนน CVSS และจัดกลุ่มระดับความรุนแรงเป็น Critical, High, Medium และ Low ได้อย่างถูกต้องตามค่าที่ตั้งไว้ในระบบ โดยอ้างอิงตามช่วงคะแนนที่กำหนดในโมดูล Severity ซึ่งผู้ดูแลระบบสามารถปรับแต่งได้

ตารางที่ 4-2 ผลการทดสอบการจัดระดับความรุนแรง

ลำดับ	เงื่อนไขทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
1	คะแนน CVSS อยู่ในช่วง 9.0–10.0	ระบบจัดระดับเป็น Critical	ผ่าน
2	คะแนน CVSS อยู่ในช่วง 7.0–8.9	ระบบจัดระดับเป็น High	ผ่าน
3	คะแนน CVSS อยู่ในช่วง 4.0–6.9	ระบบจัดระดับเป็น Medium	ผ่าน
4	คะแนน CVSS อยู่ในช่วง 0.1–3.9	ระบบจัดระดับเป็น Low	ผ่าน

4.3.3 ผลการทดสอบการควบคุมสิทธิ์ตามบทบาท

การทดสอบส่วนนี้ใช้ตรวจสอบว่าผู้ใช้งานแต่ละบทบาทสามารถเข้าถึงข้อมูลและฟังก์ชันได้ตามสิทธิ์ที่กำหนดไว้ในระบบตามแนวคิด Role-Based Access Control โดยอ้างอิงบทบาทหลักของระบบ ได้แก่ Security Team, System Owner และ Auditor ซึ่งมีขอบเขตการเข้าถึงแตกต่างกันตามหน้าที่ความรับผิดชอบ

ตารางที่ 4-3 ผลการทดสอบการควบคุมสิทธิ์ตามบทบาท

ลำดับ	บทบาทผู้ใช้	เงื่อนไขทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
1	Security Team	เข้าสู่ระบบและเข้าถึงข้อมูลภาพรวมของ Dashboard รอบการสแกน รายงาน เมนูตั้งค่า และข้อมูลช่องโหว่ทั้งหมด	สามารถเข้าถึงข้อมูลและฟังก์ชันบริหารจัดการได้ครบถ้วน	ผ่าน
2	System Owner/System Admin	เข้าสู่ระบบและเข้าถึงเฉพาะรายการช่องโหว่ สินทรัพย์ และรายงานที่อยู่ในความรับผิดชอบของตนเอง	สามารถเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้องกับตนเอง	ผ่าน
3	Auditor	เข้าสู่ระบบเพื่อดูข้อมูลย้อนหลังและรายงานสำหรับการตรวจสอบ	สามารถเข้าถึงข้อมูลสำหรับตรวจสอบย้อนหลังและการออกรายงานได้ โดยไม่สามารถแก้ไขข้อมูลดำเนินการได้	ผ่าน

ตารางที่ 4-3 (ต่อ)

ลำดับ	บทบาทผู้ใช้	เงื่อนไขทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
4	System Owner/System Admin	พยายามเข้าถึงข้อมูลหรือเมนูที่ไม่อยู่ในความรับผิดชอบ	ระบบปฏิเสธการเข้าถึง	ผ่าน

4.3.4 ผลการทดสอบระบบแจ้งเตือน

การทดสอบส่วนนี้ใช้ตรวจสอบความถูกต้องของการแจ้งเตือนตามเงื่อนไขที่กำหนด ทั้งในด้านเหตุการณ์ที่กระตุ้นการแจ้งเตือน กลุ่มผู้รับ และผลลัพธ์ที่ระบบต้องแสดง โดยครอบคลุมกรณีการแจ้งก่อนวันสแกน การแจ้งเมื่อพบช่องโหว่ระดับรุนแรง การแจ้งติดตามตามกำหนดเวลา และการแจ้งเตือนเมื่อรายการเข้าสู่เงื่อนไข acceptance ตามกระบวนการของระบบ

ตารางที่ 4-4 ผลการทดสอบระบบแจ้งเตือน

ลำดับ	ประเภทการแจ้งเตือน	เงื่อนไขทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
1	แจ้งเตือนก่อนวันสแกน	สร้างรอบการสแกนและกำหนดให้มีการแจ้งเตือนก่อนถึงวันสแกน	ระบบส่งอีเมลแจ้งกำหนดการสแกนไปยังผู้เกี่ยวข้อง	ผ่าน
2	แจ้งเตือนเมื่อพบช่องโหว่ระดับรุนแรง	นำเข้าข้อมูลผลการสแกนและพบรายการระดับ Critical หรือ High ที่อยู่ในกลุ่ม Reportable	ระบบส่งอีเมลแจ้งเตือนไปยัง System Owner	ผ่าน
3	แจ้งเตือนก่อนถึงกำหนดดำเนินการ	ผู้รับผิดชอบกำหนด Implementation Date ไว้ล่วงหน้า และรายการยังไม่เสร็จสิ้น	ระบบส่งอีเมลแจ้งเตือนล่วงหน้าตามช่วงเวลาที่กำหนด	ผ่าน

ตารางที่ 4-4 (ต่อ)

ลำดับ	ประเภทการแจ้งเตือน	เงื่อนไขทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
4	แจ้งเตือนเมื่อถึงกำหนดและเมื่อเกินกำหนดดำเนินการ	รายการยังไม่ถูกอัปเดตเป็น Completed เมื่อถึงวันกำหนดและหลังพ้นกำหนด	ระบบส่งอีเมลแจ้งเตือนเมื่อถึงกำหนดและเมื่อเกินกำหนดดำเนินการ	ผ่าน
5	แจ้งเตือนกรณีรายการยังไม่มีการดำเนินการก่อนถึง Report Date	รายการช่องโหว่ยังคงอยู่ในสถานะ Pending และใกล้ถึงวัน Report Date ของแคมเปญ	ระบบส่งอีเมลเตือนให้ผู้รับผิดชอบเข้ามาดำเนินการในระบบ	ผ่าน
6	แจ้งเตือนกรณีระบบเปลี่ยนรายการเข้าสู่เงื่อนไข Acceptance โดยอัตโนมัติ	พ้นวัน Report Date แล้ว และรายการยังคงมีสถานะ Pending	ระบบเปลี่ยนสถานะตามกติกาที่กำหนดและส่งอีเมลแจ้งเตือนไปยังผู้เกี่ยวข้อง	ผ่าน

4.3.5 ผลการทดสอบความถูกต้องของ Dashboard และรายงาน

การทดสอบส่วนนี้ใช้ตรวจสอบว่าข้อมูลที่แสดงบนหน้าจอ Dashboard และรายงานต่าง ๆ สอดคล้องกับข้อมูลจริงที่ถูกจัดเก็บอยู่ในฐานข้อมูลและข้อมูลที่ประมวลผลจากผลการสแกน โดยเน้นค่าที่สำคัญต่อการติดตามสถานะช่องโหว่และการดำเนินการแก้ไข เช่น จำนวนช่องโหว่รวม จำนวนช่องโหว่ระดับรุนแรง สถานะ Corrective Action และข้อมูลที่แสดงต่อผู้ใช้แต่ละบทบาท

ตารางที่ 4-5 ผลการทดสอบความถูกต้องของ Dashboard และรายงาน

ลำดับ	รายการทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
1	จำนวนช่องโหว่รวมที่แสดงบน Dashboard	ค่าที่แสดงตรงกับข้อมูลจริงในฐานข้อมูลของรอบการสแกน	ผ่าน
2	จำนวนช่องโหว่ระดับ Critical และ High	ค่าที่แสดงสอดคล้องกับข้อมูลหลังการจัดระดับความรุนแรง	ผ่าน
3	สถานะ Corrective Action และ Corrective Status	แสดงผลตามข้อมูลล่าสุดที่ผู้ใช้หรือระบบบันทึกไว้	ผ่าน

ตารางที่ 4-5 (ต่อ)

ลำดับ	รายการทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
4	รายการล่าสุดที่ต้องติดตาม	แสดงข้อมูลล่าสุดของรายการที่เกี่ยวข้องได้ถูกต้อง	ผ่าน
5	การแสดงผลข้อมูลตามบทบาทผู้ใช้	ผู้ใช้แต่ละบทบาทเห็นข้อมูลบน Dashboard และรายงานแตกต่างกันตามสิทธิ์	ผ่าน

4.3.6 ผลการทดสอบการทำงานร่วมกันของระบบและประสิทธิภาพเบื้องต้น

การทดสอบส่วนนี้มุ่งตรวจสอบว่าระบบแต่ละโมดูลสามารถทำงานร่วมกันได้อย่างถูกต้อง ตั้งแต่การสร้างรอบการสแกน การนำเข้าข้อมูลผลการสแกน การประมวลผลระดับความรุนแรง การแจ้งเตือนผู้รับผิดชอบ การบันทึก Corrective Action หรือ Risk Acceptance ตลอดจนการแสดงผลบน Dashboard และการบันทึกประวัติการเปลี่ยนแปลง ทั้งนี้ยังครอบคลุมการทดสอบข้อมูลขนาดใหญ่ในระดับที่สอดคล้องกับข้อกำหนดเชิงคุณภาพของระบบ ซึ่งกำหนดให้ระบบรองรับการนำเข้าข้อมูลช่องโหว่อย่างน้อย 5,000 รายการต่อครั้ง

ตารางที่ 4-6 ผลการทดสอบการทำงานร่วมกันของระบบและประสิทธิภาพเบื้องต้น

ลำดับ	สถานการณ์ทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
1	สร้างรอบการสแกนและนำเข้าข้อมูลผลการสแกน	ข้อมูลจากไฟล์ CSV ถูกเชื่อมโยงกับรอบการสแกนและแสดงในรายการช่องโหว่ได้ถูกต้อง	ผ่าน
2	นำเข้าช่องโหว่ระดับ Critical หรือ High	ระบบประมวลผลระดับความรุนแรงและส่งแจ้งเตือนไปยังผู้รับผิดชอบได้ต่อเนื่อง	ผ่าน
3	ผู้รับผิดชอบกำหนด Patch หรือ Acceptance และอัปเดตสถานะ	ข้อมูลสถานะใหม่ถูกสะท้อนในหน้ารายละเอียด รายการติดตาม และ Dashboard	ผ่าน
4	รายการคงค้างจนพ้น Report Date	ระบบดำเนินการตามกติกาของแคมเปญ บันทึกการเปลี่ยนแปลงสถานะ และแจ้งเตือนผู้เกี่ยวข้อง	ผ่าน

ตารางที่ 4-6 (ต่อ)

ลำดับ	สถานการณ์ทดสอบ	ผลที่คาดหวัง	ผลการทดสอบ
5	นำเข้าข้อมูลจำนวนมาก	ระบบรองรับการนำเข้าข้อมูลจำนวนอย่างน้อย 5,000 รายการต่อครั้งโดยไม่เกิดความผิดพลาดในการประมวลผล	ผ่าน

สรุปผลการทดสอบโดยรวม พบว่าระบบที่พัฒนาขึ้นสามารถทำงานได้ถูกต้องตามขอบเขตที่กำหนดในประเด็นสำคัญ ได้แก่ การนำเข้าข้อมูลจากไฟล์ CSV การจัดระดับความรุนแรง การควบคุมสิทธิ์ตามบทบาท การแจ้งเตือนอัตโนมัติ การแสดงผลข้อมูลบน Dashboard และการทำงานร่วมกันของโมดูลหลักของระบบ ซึ่งสอดคล้องกับวัตถุประสงค์ของงานวิจัยที่มุ่งพัฒนาระบบบริหารจัดการช่องโหว่แบบครบวงจรที่รองรับการติดตาม การแจ้งเตือน และการตรวจสอบย้อนหลังได้อย่างเป็นระบบ

4.4 ผลการประเมินความคิดเห็นของผู้ใช้งานต่อระบบ

ภายหลังการพัฒนาระบบ ผู้วิจัยได้นำระบบไปทดลองใช้งานและประเมินความคิดเห็นของผู้ใช้งานต่อระบบ โดยใช้แบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ จากผู้ตอบแบบประเมินจำนวน 30 คน ครอบคลุมกลุ่ม System Owner, Security Team, Management และ Auditor จากนั้นนำข้อมูลมาวิเคราะห์ด้วยค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน เพื่อประเมินความคิดเห็นของผู้ใช้งานต่อระบบใน 5 ด้าน ได้แก่ ความง่ายในการใช้งาน ความมีประโยชน์ของระบบ คุณภาพของข้อมูลและการแสดงผล ประสิทธิภาพของระบบ และความพึงพอใจโดยรวม

ผลการประเมินในภาพรวมพบว่า ผู้ใช้งานมีความคิดเห็นต่อระบบอยู่ในระดับมากถึงมากที่สุด โดยด้านความง่ายในการใช้งานมีค่าเฉลี่ยรวม 4.58 ด้านความมีประโยชน์ของระบบมีค่าเฉลี่ยรวม 4.65 ด้านคุณภาพของข้อมูลและการแสดงผลมีค่าเฉลี่ยรวม 4.63 ด้านประสิทธิภาพของระบบมีค่าเฉลี่ยรวม 4.63 และด้านความพึงพอใจโดยรวมมีค่าเฉลี่ยรวม 4.80 ซึ่งสะท้อนว่าระบบที่พัฒนาขึ้นสามารถตอบสนองต่อการใช้งาน สนับสนุนการติดตามสถานะช่องโหว่ และมีความเหมาะสมต่อการนำไปประยุกต์ใช้ในองค์กรได้ในระดับที่น่าพอใจ

จากผลการประเมินดังกล่าว สามารถอธิบายแยกตามรายด้านได้ดังต่อไปนี้

4.4.1 ผลการประเมินด้านความง่ายในการใช้งานของระบบ

ผลการประเมินพบว่าผู้ใช้งานมีความคิดเห็นต่อระบบในด้านความง่ายในการใช้งานอยู่ในระดับมากที่สุด โดยเฉพาะในประเด็นด้านโครงสร้างเมนู การค้นหาและเข้าถึงข้อมูล รวมถึงความชัดเจนของ

หน้าจอและข้อความที่ใช้ในระบบ ซึ่งสะท้อนว่าผู้ใช้งานสามารถเรียนรู้และใช้งานระบบได้ไม่ซับซ้อน สอดคล้องกับข้อกำหนดเชิงคุณภาพที่กำหนดให้ผู้ใช้งานสามารถเรียนรู้การใช้งานได้ภายในเวลาอันเหมาะสม

ตารางที่ 4-7 ผลการประเมินด้านความง่ายในการใช้งานของระบบ

ด้านที่ประเมิน	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
โครงสร้างเมนูและลำดับขั้นตอนการใช้งานเข้าใจง่าย	4.40	0.61	มาก
การค้นหา คัดกรอง และเข้าถึงข้อมูลทำได้สะดวก	4.63	0.60	มากที่สุด
รูปแบบหน้าจอและข้อความที่ใช้ในระบบมีความชัดเจน	4.73	0.44	มากที่สุด
การกรอกข้อมูลในแบบฟอร์มต่าง ๆ ทำได้สะดวกและไม่ซับซ้อน	4.53	0.72	มากที่สุด

4.4.2 ผลการประเมินด้านความมีประโยชน์ของระบบ

ผลการประเมินพบว่าผู้ใช้งานมีความคิดเห็นต่อระบบในด้านความมีประโยชน์อยู่ในระดับมากที่สุด โดยเห็นว่าระบบช่วยให้การติดตามสถานะช่องโหว่และการดำเนินการแก้ไขเป็นไปอย่างมีระบบ ช่วยลดความตกหล่นของรายการที่ต้องดำเนินการ และสนับสนุนการตัดสินใจของผู้เกี่ยวข้องได้ดี ซึ่งสอดคล้องกับวัตถุประสงค์ของงานวิจัยที่มุ่งพัฒนาระบบบริหารจัดการช่องโหว่ที่ครอบคลุมการติดตาม การแจ้งเตือน และการบริหารจัดการความเสี่ยงอย่างเป็นระบบ

ตารางที่ 4-8 ผลการประเมินด้านประโยชน์ต่อการบริหารจัดการช่องโหว่

ด้านที่ประเมิน	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
ระบบช่วยให้ติดตามสถานะช่องโหว่ได้อย่างเป็นระบบ	4.83	0.37	มากที่สุด
ระบบช่วยลดการละเลยรายการช่องโหว่และช่วยลดเวลาที่ใช้ในการดำเนินการ	4.70	0.46	มากที่สุด
ระบบช่วยให้ตรวจสอบความคืบหน้าของการดำเนินการได้ชัดเจน	4.57	0.50	มากที่สุด
ระบบช่วยสนับสนุนการตัดสินใจของผู้เกี่ยวข้องได้อย่างถูกต้อง	4.50	0.62	มาก

4.4.3 ผลการประเมินด้านคุณภาพของข้อมูลและการแสดงผล

ผลการประเมินพบว่าผู้ใช้งานมีความคิดเห็นต่อระบบในด้านคุณภาพของข้อมูลและการแสดงผลอยู่ในระดับมากที่สุด โดยเฉพาะในประเด็นความถูกต้องของข้อมูล ความชัดเจนของ

Dashboard และความสะดวกในการตรวจสอบข้อมูลย้อนหลัง ซึ่งสะท้อนว่าระบบสามารถแสดงข้อมูลที่มีประโยชน์ต่อการติดตามช่องโหว่และการรายงานสถานะได้อย่างเหมาะสม สอดคล้องกับขอบเขตของระบบที่ครอบคลุม Dashboard, Reporting และการบันทึกประวัติการดำเนินการย้อนหลัง

ตารางที่ 4-9 ผลการประเมินด้านคุณภาพของข้อมูลและการแสดงผล

ด้านที่ประเมิน	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
ข้อมูลที่ระบบแสดงมีความถูกต้องและเป็นประโยชน์ต่อการติดตามช่องโหว่	4.73	0.51	มากที่สุด
Dashboard ช่วยให้เห็นภาพรวมของสถานะช่องโหว่และการดำเนินการได้ชัดเจน	4.53	0.56	มากที่สุด
ระบบช่วยให้ค้นหาข้อมูลย้อนหลังได้สะดวก	4.63	0.55	มากที่สุด
ระบบช่วยให้ตรวจสอบประวัติการดำเนินการย้อนหลังได้เหมาะสม	4.63	0.55	มากที่สุด

4.4.4 ผลการประเมินด้านประสิทธิภาพของระบบ

ผลการประเมินพบว่าผู้ใช้งานมีความคิดเห็นต่อระบบในด้านประสิทธิภาพอยู่ในระดับมาก โดยเห็นว่าระบบตอบสนองต่อการใช้งานได้ในระดับที่เหมาะสม การเปลี่ยนหน้าจอและเรียกดูข้อมูลทำได้ต่อเนื่อง และผู้ใช้งานสามารถเรียนรู้วิธีใช้งานได้ภายในเวลาอันเหมาะสม ซึ่งสอดคล้องกับข้อกำหนดเชิงคุณภาพของระบบที่กำหนดให้รองรับการใช้งานได้อย่างมีประสิทธิภาพและเรียนรู้ได้ง่าย

ตารางที่ 4-10 ผลการประเมินด้านประสิทธิภาพของระบบ

ด้านที่ประเมิน	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
ระบบตอบสนองต่อการใช้งานได้รวดเร็วในระดับที่เหมาะสม	4.73	0.44	มากที่สุด
การเปิดดูข้อมูลหรือเปลี่ยนหน้าจอทำได้ต่อเนื่องไม่ซับซ้อน	4.67	0.54	มากที่สุด
ผู้ใช้งานสามารถเรียนรู้การใช้งานระบบได้ภายในเวลาอันเหมาะสม	4.50	0.62	มาก

4.4.5 ผลการประเมินความพึงพอใจโดยรวม

ผลการประเมินพบว่าผู้ใช้งานมีความพึงพอใจต่อระบบโดยรวมอยู่ในระดับมากที่สุด และเห็นว่าระบบมีความเหมาะสมต่อการนำไปใช้งานจริงในองค์กร เนื่องจากสามารถสนับสนุนกระบวนการบริหารจัดการช่องโหว่ได้อย่างเป็นระบบ ครอบคลุมทั้งการติดตามสถานะ การแจ้งเตือน การบันทึกการดำเนินการ และการตรวจสอบย้อนหลังตามบทบาทของผู้ใช้งาน

ตารางที่ 4-11 ผลการประเมินความพึงพอใจโดยรวม

ด้านที่ประเมิน	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
ระบบมีความเหมาะสมต่อการนำไปใช้งานจริงในองค์กร	4.87	0.34	มากที่สุด
โดยภาพรวม ระบบสามารถสนับสนุนกระบวนการบริหารจัดการช่องโหว่ได้อย่างมีประสิทธิภาพ	4.80	0.40	มากที่สุด
ผู้ใช้งานมีความพึงพอใจต่อระบบที่พัฒนาขึ้นโดยรวม	4.73	0.44	มากที่สุด

แม้ว่าผลการประเมินความคิดเห็นของผู้ใช้งานจะอยู่ในระดับมากถึงมากที่สุดในทุกด้าน แต่ผลดังกล่าวควรตีความภายใต้ขอบเขตของการวิจัย เนื่องจากเป็นการประเมินระบบต้นแบบจากผู้ใช้งานที่เกี่ยวข้องกับกระบวนการทำงานของระบบโดยตรง และอยู่ในบริบทของการทดลองใช้งานตามขอบเขตที่กำหนด จึงอาจมีแนวโน้มของการให้คะแนนเชิงบวกได้บ้าง อย่างไรก็ตาม ผู้วิจัยมิได้ใช้ผลการประเมินดังกล่าวเพื่อสรุปว่าระบบก่อให้เกิดประสิทธิผลเชิงองค์กรในระยะยาว แต่ใช้เพื่อสะท้อนความเหมาะสม การยอมรับ และศักยภาพของระบบในการสนับสนุนกระบวนการบริหารจัดการช่องโหว่ในระดับต้นแบบ

4.5 ข้อค้นพบจากการทดลองใช้งานระบบและการแสดงผลผ่าน Dashboard

จากการทดลองใช้งานระบบด้วยข้อมูลที่นำเข้าสู่ระบบและสถานการณ์ที่กำหนด พบว่าระบบสามารถแสดงข้อมูลสำคัญที่เกี่ยวข้องกับการติดตามสถานะช่องโหว่ได้อย่างเป็นระบบผ่านหน้าจอ Dashboard โดยผู้ใช้งานสามารถมองเห็นข้อมูลสรุปของจำนวนช่องโหว่ระดับรุนแรง สถานะของ Corrective Action รายการที่ยังคงค้างดำเนินการ และข้อมูลที่เกี่ยวข้องกับการยอมรับความเสี่ยงได้ภายในหน้าจอเดียว

ข้อค้นพบสำคัญคือ Dashboard ช่วยให้ผู้ใช้งานติดตามงานได้สะดวกขึ้น ทั้งในด้านการเปรียบเทียบข้อมูลระหว่างรอบการสแกน การระบุรายการช่องโหว่ระดับ Critical และ High ที่ควรเร่งดำเนินการ และการตรวจสอบสถานะของรายการที่ยังไม่มีการอัปเดต ทั้งนี้ ข้อค้นพบดังกล่าว

สะท้อนศักยภาพของระบบต้นแบบในด้านการแสดงผลและการสนับสนุนการติดตาม มากกว่าการสรุปผลเชิงปริมาณจากการใช้งานจริงขององค์กรในระยะยาว

นอกจากนี้ การแสดงผลผ่าน Dashboard ยังสะท้อนให้เห็นศักยภาพของระบบในการสนับสนุนการเปรียบเทียบข้อมูลระหว่างรอบการสแกน และการติดตามความเปลี่ยนแปลงของสถานะช่องโหว่ในภาพรวม ซึ่งเป็นประโยชน์ต่อการตรวจสอบความต่อเนื่องของกระบวนการบริหารจัดการช่องโหว่และการวางแผนติดตามงานในรอบถัดไป อีกทั้งระบบยังรองรับการแสดงผลตามบทบาทของผู้ใช้งาน ทำให้เจ้าของระบบสามารถเห็นเฉพาะข้อมูลในความรับผิดชอบของตน ขณะที่ทีมรักษาความมั่นคงปลอดภัย (Security Team) ผู้ตรวจสอบ (Auditor) และผู้บริหารที่กำกับดูแล สามารถเห็นภาพรวมในระดับที่กว้างกว่าได้ตามสิทธิ์ที่กำหนดไว้ในระบบ ทั้งนี้ ข้อค้นพบในส่วนนี้เป็นผลจากการพิจารณาศักยภาพของระบบผ่านข้อมูลที่นำเข้าสู่ระบบและผลการทดลองใช้งานตามสถานการณ์ที่กำหนดในการวิจัย มิได้มุ่งวัดผลเชิงปริมาณจากการใช้งานจริงขององค์กรในลักษณะกรณีศึกษาเฉพาะแห่ง แต่สะท้อนให้เห็นว่าระบบที่พัฒนาขึ้นสามารถสนับสนุนการแสดงผลข้อมูล การติดตามสถานะ และการรับรู้ข้อมูลสำคัญของกระบวนการบริหารจัดการช่องโหว่ได้ตามวัตถุประสงค์ของการวิจัย

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 5
สรุปผลและข้อเสนอแนะ

บทนี้นำเสนอการสรุปผลการวิจัย อภิปรายผลจากการพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ ข้อจำกัดของการวิจัย และข้อเสนอแนะสำหรับการนำระบบไปประยุกต์ใช้และการศึกษาต่อยอดในอนาคต โดยอาศัยผลการดำเนินงานที่นำเสนอในบทที่ 4 เป็นหลัก ซึ่งครอบคลุมผลการพัฒนาระบบ ผลการทดสอบความถูกต้องของระบบ ผลการประเมินความคิดเห็นของผู้ใช้งาน และข้อค้นพบจากการทดลองใช้งานระบบและการแสดงผลผ่าน Dashboard

5.1 สรุปผลการวิจัย

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับสนับสนุนกระบวนการบริหารจัดการช่องโหว่ภายในองค์กร โดยใช้ข้อมูลผลการสแกนจากเครื่องมือ Rapid7 InsightVM ในรูปแบบไฟล์ CSV เป็นกรณีศึกษา ระบบที่พัฒนาขึ้นมุ่งรองรับการนำเข้าข้อมูลผลการสแกน การติดตามสถานะการดำเนินการแก้ไขช่องโหว่ การบันทึกการยอมรับความเสี่ยง การแจ้งเตือนผู้รับผิดชอบ และการแสดงผลข้อมูลผ่าน Dashboard ตามบทบาทของผู้ใช้งาน ผู้วิจัยได้ดำเนินการศึกษาข้อมูลและแนวคิดที่เกี่ยวข้อง วิเคราะห์ความต้องการของระบบ ออกแบบโครงสร้างการทำงานและฐานข้อมูล พัฒนาระบบต้นแบบ และประเมินผลการทำงานของระบบตามขอบเขตที่กำหนดไว้

ผลการวิจัยแสดงให้เห็นว่า ระบบที่พัฒนาขึ้นสามารถรองรับการทำงานหลักของกระบวนการบริหารจัดการช่องโหว่ได้สอดคล้องกับวัตถุประสงค์ของการวิจัย โดยครอบคลุมการจัดการรอบการสแกน การนำเข้าข้อมูลผลการสแกนจากไฟล์ CSV การจัดเก็บและแสดงรายการช่องโหว่ การบันทึก Corrective Action การบันทึก Risk Acceptance การแจ้งเตือนทางอีเมล การกำหนดระดับความรุนแรง และการควบคุมสิทธิ์ตามบทบาทของผู้ใช้งาน นอกจากนี้ ระบบยังสามารถแสดงผลข้อมูลในรูปแบบ Dashboard เพื่อช่วยสรุปภาพรวมของสถานะช่องโหว่และการดำเนินการที่เกี่ยวข้อง ทำให้ผู้ใช้งานสามารถติดตามข้อมูลที่อยู่ในความรับผิดชอบของตนได้สะดวกและเป็นระบบมากขึ้น ภายใต้ขอบเขตของระบบที่พัฒนาขึ้นในการวิจัยครั้งนี้

ในด้านการทดสอบความถูกต้องของระบบ ผลการทดสอบพบว่าระบบสามารถทำงานได้ตามเงื่อนไขสำคัญที่กำหนดไว้ เช่น การนำเข้าข้อมูลจากไฟล์ CSV การประมวลผลข้อมูลช่องโหว่ การจัดระดับความรุนแรง การควบคุมสิทธิ์การเข้าถึงข้อมูล การแจ้งเตือนตามเงื่อนไข และการแสดงผลข้อมูลผ่าน Dashboard และรายงาน ผลดังกล่าวสะท้อนว่าระบบต้นแบบที่พัฒนาขึ้นสามารถรองรับขั้นตอนสำคัญของกระบวนการติดตามและบริหารจัดการช่องโหว่ภายในองค์กรได้ในระดับที่สอดคล้องกับวัตถุประสงค์ของการวิจัย อีกทั้งยังช่วยให้ข้อมูลที่เกี่ยวข้องกับช่องโหว่ถูกรวบรวมไว้ในระบบเดียว ซึ่งเอื้อต่อการติดตามความคืบหน้าของการดำเนินการ การตรวจสอบสถานะของรายการที่ค้างอยู่ และการตรวจสอบย้อนหลังในกรณีที่จำเป็น

สำหรับผลการประเมินความคิดเห็นของผู้ใช้งานจากกลุ่มตัวอย่างจำนวน 30 คน พบว่าผู้ใช้งานมีความคิดเห็นต่อระบบอยู่ในระดับมากถึงมากที่สุดในทุกด้านที่ประเมิน โดยด้านความง่ายในการใช้งานมีค่าเฉลี่ยรวม 4.58 ด้านความมีประโยชน์ของระบบมีค่าเฉลี่ยรวม 4.65 ด้านคุณภาพของข้อมูลและการแสดงผลมีค่าเฉลี่ยรวม 4.63 ด้านประสิทธิภาพของระบบมีค่าเฉลี่ยรวม 4.63 และด้านความพึงพอใจโดยรวมมีค่าเฉลี่ยรวม 4.80 ผลการประเมินดังกล่าวสะท้อนว่าผู้ใช้งานมีมุมมองเชิงบวกต่อระบบทั้งในด้านการใช้งานและการสนับสนุนกระบวนการทำงาน โดยเฉพาะในส่วนของการติดตามสถานะช่องโหว่ การตรวจสอบความคืบหน้าของการดำเนินการ และการเข้าถึงข้อมูลที่เกี่ยวข้องผ่าน Dashboard อย่างไรก็ตาม ผลการประเมินดังกล่าวเป็นผลที่ได้จากการทดลองใช้ระบบภายใต้ขอบเขตของการวิจัย จึงควรพิจารณาตามบริบทของการศึกษานี้

โดยสรุป ระบบที่พัฒนาขึ้นสามารถรองรับการทำงานหลักที่เกี่ยวข้องกับกระบวนการบริหารจัดการช่องโหว่ภายในองค์กรได้สอดคล้องกับวัตถุประสงค์ของการวิจัย ทั้งในด้านการนำเข้าข้อมูล การติดตามสถานะ การบันทึกการดำเนินการ การแจ้งเตือน และการแสดงผลข้อมูลเพื่อสนับสนุนการติดตามและกำกับดูแลในภาพรวม ผลการวิจัยจึงแสดงให้เห็นว่าระบบที่พัฒนาขึ้นสามารถใช้เป็นแนวทางในการสนับสนุนกระบวนการบริหารจัดการช่องโหว่ภายในองค์กร และสามารถนำไปต่อยอดหรือปรับใช้ให้เหมาะสมกับบริบทขององค์กรในอนาคตได้

5.2 อภิปรายผลการวิจัย

การอภิปรายผลจากการวิจัยครั้งนี้แสดงให้เห็นว่า ระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นสามารถสนับสนุนกระบวนการบริหารจัดการช่องโหว่ภายใน

องค์กรได้ในหลายด้าน โดยเฉพาะในประเด็นที่เกี่ยวข้องกับการรวบรวมข้อมูล การติดตามสถานะการดำเนินการ และการแจ้งเตือนผู้รับผิดชอบ ระบบที่พัฒนาขึ้นช่วยเชื่อมโยงข้อมูลผลการสแกนจากเครื่องมือภายนอกเข้ากับกระบวนการติดตามภายในองค์กร ทำให้การจัดการช่องโหว่มีลำดับขั้นที่ชัดเจนมากขึ้น ตั้งแต่การนำเข้าข้อมูล การกำหนดแนวทางการดำเนินการ การติดตามสถานะ ไปจนถึงการตรวจสอบย้อนหลังผ่านระบบเดียว ซึ่งสอดคล้องกับแนวคิดเรื่องวงจรชีวิตการจัดการช่องโหว่และแนวทางการพัฒนาระบบที่ควรรองรับข้อมูลกลาง การติดตาม การแจ้งเตือน และการรายงานเชิงเปรียบเทียบอย่างเป็นระบบ

ผลการทดสอบระบบที่เป็นไปตามขอบเขตในประเด็นสำคัญสะท้อนว่า การออกแบบระบบโดยคำนึงถึงกระบวนการทำงานจริงขององค์กรมีส่วนช่วยให้ระบบสามารถรองรับงานที่เกี่ยวข้องกับการบริหารจัดการช่องโหว่ได้อย่างเหมาะสม โดยเฉพาะการนำเข้าข้อมูลจากไฟล์ CSV การควบคุมสิทธิ์การเข้าถึงข้อมูล และการบันทึกประวัติการดำเนินการย้อนหลัง ประเด็นเหล่านี้มีความสำคัญต่อการใช้งาน เนื่องจากการติดตามช่องโหว่ไม่ได้เกี่ยวข้องเฉพาะการรับข้อมูลจากเครื่องมือสแกนเท่านั้น แต่ยังครอบคลุมถึงความรับผิดชอบของผู้เกี่ยวข้อง การตรวจสอบสถานะ และการใช้ข้อมูลเพื่อการกำกับติดตามภายในองค์กรด้วย

ในด้านความคิดเห็นของผู้ใช้งาน ผลการประเมินที่อยู่ในระดับมากถึงมากที่สุดสะท้อนว่าระบบที่พัฒนาขึ้นได้รับการยอมรับในระดับที่ดี ทั้งในด้านการใช้งาน ความมีประโยชน์ของระบบ และความเหมาะสมของข้อมูลที่แสดงผ่านหน้าจอระบบและ Dashboard ผลดังกล่าวบ่งชี้ว่าแนวทางการออกแบบระบบที่มุ่งให้ผู้ใช้งานแต่ละบทบาทเข้าถึงข้อมูลที่จำเป็นต่อหน้าที่ของตนเอง มีส่วนช่วยให้การใช้งานระบบเป็นไปอย่างสะดวกและลดความซ้ำซ้อนในการติดตามข้อมูล อย่างไรก็ตาม ผลการประเมินดังกล่าวเป็นผลที่ได้จากการทดลองใช้ระบบภายใต้ขอบเขตของการวิจัย จึงควรพิจารณาตามบริบทของการศึกษานี้

อีกประเด็นหนึ่งที่พบจากการวิจัยคือ การแสดงผลผ่าน Dashboard มีส่วนช่วยให้ผู้ใช้งานรับรู้สถานะของช่องโหว่และการดำเนินการได้ชัดเจนยิ่งขึ้น เนื่องจากสามารถสรุปข้อมูลสำคัญให้อยู่ในรูปแบบที่เข้าใจได้ง่ายและใช้ติดตามงานได้สะดวก ข้อค้นพบนี้สอดคล้องกับแนวคิดด้าน Reporting and Continuous Improvement ที่ให้ความสำคัญกับการสรุปสถานะ ผลการดำเนินการ และแนวโน้ม เพื่อใช้ประกอบการกำกับติดตามและการปรับปรุงการดำเนินงานในรอบถัดไป อย่างไรก็ตาม

ผลที่ได้ในส่วนนี้ยังสะท้อนการทำงานของระบบภายใต้เงื่อนไขและข้อมูลที่กำหนดไว้ในการวิจัย มากกว่าการสรุปผลเชิงประสิทธิผลของการใช้งานจริงในระยะยาวขององค์กร

เมื่อพิจารณาโดยรวม ผลการวิจัยชี้ให้เห็นว่า การพัฒนาระบบที่ออกแบบให้สอดคล้องกับบริบทของการทำงานจริง เช่น การกำหนดบทบาทผู้ใช้งาน การจัดการข้อมูลจากหลายขั้นตอนของกระบวนการ และการรองรับทั้ง Corrective Action และ Risk Acceptance สามารถช่วยเพิ่มความเป็นระบบของกระบวนการบริหารจัดการช่องโหว่ได้ตามขอบเขตที่กำหนดในการวิจัย แม้ว่าระบบที่พัฒนาขึ้นจะยังมีข้อจำกัดบางประการ แต่ผลการวิจัยก็สะท้อนถึงความเป็นไปได้ในการนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการติดตามรายการช่องโหว่ การลดโอกาสการตกหล่น และการตรวจสอบย้อนหลังภายในองค์กรได้ในระดับหนึ่ง

5.3 ข้อจำกัดของการวิจัย

แม้งานวิจัยนี้จะสามารถพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ที่รองรับกระบวนการบริหารจัดการช่องโหว่ได้ตามวัตถุประสงค์หลักที่กำหนดไว้ แต่ยังมีข้อจำกัดบางประการที่ควรพิจารณา ประการแรก ระบบในระยะนี้ยังรองรับการนำเข้าข้อมูลผลการสแกนจากเครื่องมือ Rapid7 InsightVM ในรูปแบบไฟล์ CSV เป็นหลัก และยังไม่ได้ครอบคลุมการเชื่อมต่อกับเครื่องมือประเมินช่องโหว่อื่นโดยตรง ดังนั้น หากนำไปใช้ในองค์กรที่มีเครื่องมือประเมินหลายประเภท อาจต้องมีการพัฒนาเพิ่มเติมในส่วนของการเชื่อมต่อและแปลงข้อมูลให้รองรับรูปแบบที่หลากหลายมากขึ้น

ประการที่สอง งานวิจัยนี้มุ่งเน้นการพัฒนาระบบสำหรับการติดตามและบริหารจัดการช่องโหว่ภายหลังการสแกน จึงไม่ได้ครอบคลุมกระบวนการทำ Vulnerability Scanning โดยตรง กล่าวคือ ระบบทำหน้าที่รับข้อมูลจากเครื่องมือภายนอกที่มีอยู่แล้ว และนำข้อมูลดังกล่าวมาสนับสนุนการติดตาม การแจ้งเตือน การยอมรับความเสี่ยง และการรายงานผล ดังนั้น ความถูกต้องและความสมบูรณ์ของข้อมูลต้นทางยังคงขึ้นอยู่กับคุณภาพของผลการสแกนจากเครื่องมือภายนอกด้วย นอกจากนี้ การประเมินผลของระบบในงานวิจัยนี้อยู่ในขอบเขตของการทดลองใช้งานระบบต้นแบบและสถานการณ์ที่กำหนดในการวิจัย ยังไม่ได้มุ่งเน้นการติดตามผลการใช้งานจริงขององค์กรในระยะยาว จึงควรระมัดระวังในการตีความผลในเชิงประสิทธิผลระดับองค์กรโดยตรง

ประการที่สาม งานวิจัยนี้พัฒนาระบบในรูปแบบเว็บแอปพลิเคชันเป็นหลัก และยังไม่ได้ครอบคลุมการใช้งานผ่านอุปกรณ์เคลื่อนที่ในลักษณะ Mobile Application ซึ่งอาจเป็นข้อจำกัดในกรณีที่องค์กรต้องการให้ผู้ใช้งานบางบทบาทติดตามหรืออัปเดตสถานะผ่านอุปกรณ์พกพาโดยตรง อย่างไรก็ตาม ข้อจำกัดดังกล่าวสามารถใช้เป็นแนวทางสำหรับการพัฒนาต่อยอดในอนาคตได้

5.4 ข้อเสนอแนะ

5.4.1 ข้อเสนอแนะในการนำระบบไปประยุกต์ใช้

ในการนำระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ไปประยุกต์ใช้ในองค์กร ควรกำหนดบทบาทและสิทธิ์ของผู้ใช้งานให้ชัดเจนตั้งแต่ต้น โดยเฉพาะบทบาทของเจ้าของระบบและผู้ดูแลระบบ (System Owner/System Admin) ทีมรักษาความมั่นคงปลอดภัย (Security Team) และผู้ตรวจสอบ (Auditor) เพื่อให้การเข้าถึงข้อมูลและการดำเนินการในระบบสอดคล้องกับหน้าที่ความรับผิดชอบ นอกจากนี้ องค์กรควรกำหนดเกณฑ์ระดับความรุนแรง รูปแบบการแจ้งเตือน และเงื่อนไขการติดตามให้เหมาะสมกับนโยบายและกระบวนการทำงานของตนเอง รวมถึงควรเตรียมความพร้อมของข้อมูลต้นทาง เช่น ข้อมูลสินทรัพย์ ข้อมูลเจ้าของระบบ และรูปแบบไฟล์ผลการสแกนให้มีความถูกต้องและเป็นปัจจุบัน เพื่อให้ระบบสามารถติดตามสถานะช่องโหว่และแสดงผลข้อมูลได้อย่างมีประสิทธิภาพ

อีกประเด็นที่ควรให้ความสำคัญคือ การกำหนดกระบวนการทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานด้านความมั่นคงปลอดภัย เจ้าของระบบ และผู้ตรวจสอบภายใน เพื่อให้ข้อมูลในระบบไม่เป็นเพียงข้อมูลที่ถูกบันทึกไว้ แต่สามารถนำไปใช้ติดตาม กำกับ และตัดสินใจได้จริง องค์กรควรส่งเสริมให้มีการอัปเดตสถานะการดำเนินการอย่างสม่ำเสมอ การบันทึกเหตุผลของการยอมรับความเสี่ยงอย่างชัดเจน และการตรวจสอบข้อมูลย้อนหลังเป็นระยะ เพื่อให้ระบบสามารถสนับสนุนกระบวนการบริหารจัดการช่องโหว่ได้อย่างต่อเนื่องและเกิดประโยชน์สูงสุด

5.4.2 ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

สำหรับการวิจัยในอนาคต ควรขยายขอบเขตของระบบให้รองรับการนำเข้าหรือเชื่อมต่อข้อมูลจากเครื่องมือประเมินช่องโหว่หลายประเภทมากขึ้น เช่น Tenable Nessus หรือ OpenVAS รวมถึงพัฒนาโครงสร้างข้อมูลกลางที่สามารถรองรับข้อมูลจากหลายแหล่งได้อย่างยืดหยุ่น เพื่อเพิ่มศักยภาพของระบบในการใช้งานจริงในองค์กรที่มีสภาพแวดล้อมซับซ้อนมากขึ้น นอกจากนี้ อาจพัฒนากลไก

การจัดลำดับความสำคัญของช่องโหว่ให้คำนึงถึงบริบทขององค์กรเพิ่มเติม นอกเหนือจากระดับความรุนแรงเชิงเทคนิค เพื่อให้การตัดสินใจด้านการแก้ไขและติดตามมีความเหมาะสมยิ่งขึ้น โดยอาจพิจารณานำ Exploit Prediction Scoring System (EPSS) มาใช้ร่วมกับ CVSS เพื่อเพิ่มความแม่นยำในการระบุช่องโหว่ที่มีความเสี่ยงสูงต่อการถูกใช้ประโยชน์ในการโจมตีจริง ดังที่ได้กล่าวถึงในบทที่ 2

ในด้านการศึกษาต่อยอด ควรมีการทดลองใช้งานจริงในองค์กรเป็นระยะเวลาต่อเนื่อง เพื่อประเมินผลกระทบของระบบต่อกระบวนการทำงานในมิติที่ลึกขึ้น เช่น ความต่อเนื่องของการติดตามงาน การลดจำนวนรายการคงค้าง การลดการตกหล่นของช่องโหว่ และประสิทธิผลของการแจ้งเตือนต่อการดำเนินการของผู้รับผิดชอบ รวมถึงอาจขยายการพัฒนาไปสู่การใช้งานผ่านอุปกรณ์เคลื่อนที่และการสร้างรายงานเชิงวิเคราะห์ที่หลากหลายมากขึ้น เพื่อเพิ่มความสะดวกและความยืดหยุ่นในการใช้งานระบบในสภาพแวดล้อมจริง

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บรรณานุกรม

1. National Vulnerability Database, “NVD - Statistics,” NIST National Vulnerability Database. Accessed: Oct. 16, 2025. [Online]. Available: https://nvd.nist.gov/vuln/search/statistics
2. IBM and Ponemon Institute, “Cost of a Data Breach Report 2024,” IBM, Armonk, NY, July 2024. [Online]. Available: https://www.ibm.com/reports/data-breach
3. FIRST.Org, Inc., Common Vulnerability Scoring System v3.1: Specification Document, June 2019. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document
4. National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
5. International Organization for Standardization and International Electrotechnical Commission, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO/IEC 27001:2022, Geneva, Switzerland., Oct. 2022. [Online]. Available: https://www.iso.org/standard/82875.html
6. PCI Security Standards Council, “Payment Card Industry Data Security Standard: Requirements and Testing Procedures,” PCI Security Standards Council, Wakefield, MA, 4.0, Mar. 2022. [Online]. Available: https://www.pcisecuritystandards.org
7. Center for Internet Security, “CIS Controls Version 8,” Center for Internet Security (CIS), v8, May 2021. [Online]. Available: https://www.cisecurity.org/controls/v8/
8. M. Walkowski, J. Oko, and S. Sujecki, “Vulnerability Management Models Using a Common Vulnerability Scoring System,” Appl. Sci., vol. 11, no. 18, p. 8735, Sept. 2021, doi: 10.3390/app11188735.

9. K. Bennouk, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, A. Z. Faroukhi, and D. Mahouachi, “A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies,” J. Cybersecurity Priv., vol. 4, no. 4, pp. 853–908, Oct. 2024, doi: 10.3390/jcp4040040.
10. M. Shahzad, M. Z. Shafiq, and A. X. Liu, “A large scale exploratory analysis of software vulnerability life cycles,” in 2012 34th International Conference on Software Engineering (ICSE), Zurich, Switzerland: IEEE, June 2012, pp. 771–781. doi: 10.1109/ICSE.2012.6227141.
11. J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, and M. Roytman, “Exploit Prediction Scoring System (EPSS),” Digit. Threats Res. Pract., vol. 2, no. 3, pp. 1–17, Sept. 2021, doi: 10.1145/3436242.
12. L. Allodi and F. Massacci, “Comparing Vulnerability Severity and Exploits Using Case-Control Studies,” ACM Trans. Inf. Syst. Secur., vol. 17, no. 1, pp. 1–20, Aug. 2014, doi: 10.1145/2630069.
13. H. Holm, M. Ekstedt, and D. Andersson, “Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 825–837, Nov. 2012, doi: 10.1109/TDSC.2012.66.
14. Á. J. Varela-Vaca, D. Borrego, M. T. Gómez-López, R. M. Gasca, and A. G. Márquez, “Feature models to boost the vulnerability management process,” J. Syst. Softw., vol. 195, p. 111541, Jan. 2023, doi: 10.1016/j.jss.2022.111541.
15. D. Toprani and V. K. Madisetti, “LLM Agentic Workflow for Automated Vulnerability Detection and Remediation in Infrastructure-as-Code,” IEEE Access, vol. 13, pp. 69175–69181, 2025, doi: 10.1109/ACCESS.2025.3560911.
16. Goutam and V. Tiwari, “Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application,” in 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India: IEEE, Nov. 2019, pp. 601–605. doi: 10.1109/ISCON47742.2019.9036175.

17. S. R. Pérez, M. Van Eeten, and C. H. Gañán, “Patchy Performance? Uncovering the Vulnerability Management Practices of IoT-Centric Vendors,” in 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA: IEEE, May 2024, pp. 1198–1216. doi: 10.1109/SP54263.2024.00154.
18. C. R. Harrell, M. Patton, H. Chen, and S. Samtani, “Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions,” in 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL: IEEE, Nov. 2018, pp. 148–153. doi: 10.1109/ISI.2018.8587380.
19. P. K. Manadhata and J. M. Wing, “An Attack Surface Metric,” IEEE Trans. Softw. Eng., vol. 37, no. 3, pp. 371–386, May 2011, doi: 10.1109/TSE.2010.60.
20. M. Souppaya and K. Scarfone, “Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology,” National Institute of Standards and Technology, Nov. 2021. doi: 10.6028/NIST.SP.800-40r4.
21. J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, “Improving vulnerability remediation through better exploit prediction,” J. Cybersecurity, vol. 6, no. 1, p. tyaa015, Jan. 2020, doi: 10.1093/cybsec/tyaa015.

ประวัติผู้เขียน

ชื่อ	นายอนันต์ นามสุดโท
ชื่อการค้นคว้าอิสระ	การพัฒนาระบบบริหารจัดการและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์
สาขาวิชา	การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ประวัติ	เกิดเมื่อวันที่ 16 พฤษภาคม 2536 ปัจจุบันอายุ 33 ปี โดยเกิดที่จังหวัดยโสธร เข้าศึกษาระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการคอมพิวเตอร์ ที่มหาวิทยาลัยราชภัฏอุบลราชธานีจนสำเร็จการศึกษาในปีการศึกษา 2557 และเข้าศึกษาต่อระดับปริญญาโท สาขาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ในด้านการทำงาน พ.ศ. 2558 ถึงปัจจุบัน ตำแหน่ง IT Security 1 บริษัท บุญรอดบริวเวอรี่ จำกัด