



รายงานการปฏิบัติสหกิจศึกษา
ระบบรายงานความปลอดภัย โดยใช้KQL
(Security Report System by KQL)

โดย

นายห่อมนัฐ กำสุวรรณ

โครงการนี้เป็นส่วนหนึ่งของการปฏิบัติสหกิจศึกษาตามหลักสูตร
วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2565

รายงานการปฏิบัติสหกิจศึกษา
โครงการระบบรายงานความปลอดภัย โดยใช้KQL
(Security Report System by KQL)

โดย

นายห่อมนัฐ กำสุวรรณ

โครงการนี้เป็นส่วนหนึ่งของการปฏิบัติสหกิจศึกษาตามหลักสูตร
วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2565

มหาวิทยาลัยธรรมศาสตร์
คณะวิทยาศาสตร์และเทคโนโลยี

รายงานการปฏิบัติสหกิจศึกษา

ของ

นาย�้อมณัฐ กำสุวรรณ

เรื่อง

รายงานความปลอดภัย โดยใช้KQL

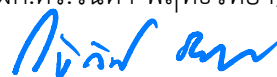
ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
เมื่อ วันที่ 14 ธันวาคม พ.ศ. 2565

อาจารย์ที่ปรึกษาสหกิจศึกษา



(ผศ.ดร.วนิดา พงษ์อิทธิยา)

อาจารย์ที่ปรึกษาร่วมสหกิจศึกษา



(ผศ. ดร.กชิตศ ชาญเขียว)

อาจารย์ที่ปรึกษาร่วมสหกิจศึกษา



(ผศ. ดร.กฤตคม ศรีจิรานนท์)

พนักงานที่ปรึกษา



(จิตราภรณ์ เอกเกษตรสิน)

Senior Technical Consultant

บทคัดย่อ

การรักษาความปลอดภัยของข้อมูลเป็นสิ่งที่มีความสำคัญในยุคสมัยที่ข้อมูลทุกอย่างเป็นสิ่งสำคัญความปลอดภัยในการเข้าถึงข้อมูลจึงเป็นเรื่องที่จำเป็นโดยเฉพาะในบริษัท หรือ องค์กรทางกรรมจำพัฒนาระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) โดยใช้แนวคิดจากระบบดีเฟนเดอร์365(Microsoft 365 Defender) ที่เป็นระบบรักษาความปลอดภัย โดยจะออกแบบมาในระบบรายงานความปลอดภัยที่ใช้ผ่านพาวเวอร์บีไอ (Microsoft Power BI) เป็นสื่อกลางในการจัดทำความสัมพันธ์ของข้อมูล บูรณาการเป็นกลุ่มข้อมูลที่ผ่านการตกผลึกและวิเคราะห์ในมิติต่าง ๆ เพื่อให้ง่ายต่อการนำเสนอและจัดทำรายงานในรูปแบบที่เข้าถึงและเข้าใจได้ง่าย (Dashboard) เพื่อใช้ในการสนับสนุนการตัดสินใจ วางแผนโต้ตอบ และวิเคราะห์แนวโน้มของความเสี่ยงต่างๆที่เกิดขึ้น ซึ่งมีความตอบโต้ภัยในการที่ผู้ดูแลระบบนั้นสามารถใช้งานได้จริง โดยมีการแสดงผลออกมา เช่น การตรวจสอบสถานะเครื่องที่ใช้ทำงาน, ตรวจสอบภัยคุกคาม, ตรวจสอบช่องโหว่ของผู้ใช้งาน, ตรวจสอบระบบป้องกันไวรัส, ตรวจสอบความเสี่ยงภายในระบบ, ตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ เป็นต้น เพื่อให้ผู้ใช้งานได้ใช้ข้อมูลในเชิงวิเคราะห์ สามารถมองเห็นภาพรวมของระบบรักษาความปลอดภัยได้

คำสำคัญ: ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender), ไมโครซอฟพาวเวอร์ออโต้เมท(Microsoft Power Automate), ไมโครซอฟพาวเวอร์บีไอ(Microsoft Power Bi), เคคิวแอล(KQL)

กิตติกรรมประกาศ

โครงการนี้สามารถลุล่วงไปได้ด้วยความกรุณาจากอาจารย์ ผศ.ดร.วนิดา พุทธิวิทยา อาจารย์ที่ปรึกษาร่วมสหกิจศึกษาอีกทั้ง 2 ท่านและพนักงานที่ปรึกษา คุณ จิตราภรณ์ เอกเกษตรสิน ที่ให้คำแนะนำ เสนอแนะ พร้อมทั้งแนะนำเครื่องมือในการใช้สร้างโครงการและการแก้ไขปรับปรุงข้อบกพร่องต่างๆ มาโดยตลอด จนโครงการนี้สามารถสำเร็จลุล่วงไปด้วยดี กระผมจึงขอกราบขอบพระคุณเป็นอย่างสูง

นาย น้อมณัฐ กำสุวรรณ

สารบัญ

บทคัดย่อ	3
กิตติกรรมประกาศ	4
สารบัญ	5
รายการสัญลักษณ์และคำย่อ	9
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของโครงการ	1
1.2 วัตถุประสงค์	1
1.3 ขอบเขตของโครงการ	2
1.3.1 ขอบเขตการพัฒนาของระบบ	2
1.3.2 ข้อจำกัดในการใช้งาน	2
1.4 ประโยชน์ของโครงการ	2
บทที่ 2 วรรณกรรม งาน และเทคโนโลยีที่เกี่ยวข้อง	3
2.1 แนวคิดทฤษฎีที่เกี่ยวข้อง	3
2.1.1 ระบบรักษาความปลอดภัยในคอมพิวเตอร์(Microsoft Security)	3
2.1.2 การดึงข้อมูลใช้ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface)	3
2.1.3 การออกแบบแอปพลิเคชัน (App design)	3
2.1.4 การคัดกรองข้อมูลจากฐานข้อมูล (Query)	3
2.2 ระบบงานปัจจุบัน /งานที่เกี่ยวข้อง	4
2.2.1 ระบบงานปัจจุบัน	4
2.2.2 ระบบงานในปัจจุบัน	8

	(6)
บทที่ 3 การดำเนินงาน	9
3.1 ภาพรวมของโครงการ	9
3.1.1 เป้าหมายโครงการที่ได้รับมอบหมายจากบริษัท	9
3.1.2 โครงสร้างสถาปัตยกรรมของระบบ	10
3.2 การวิเคราะห์ขอบเขตและความต้องการของระบบ	12
3.3 การออกแบบขั้นตอนการทำงานของระบบ	14
3.3.1 ลายละเอียดขั้นตอนแต่ละกรณีของระบบรายงานความปลอดภัย โดยใช้ เคคิวแอล (Security Report System by KQL)	14
3.3.2 กระบวนการทำงานแต่ละกรณีการใช้งานของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)	21
3.4 การออกแบบส่วนต่อประสานของระบบ	28
3.5 ประเด็นที่น่าสนใจและสิ่งที่ท้าทาย	48
บทที่ 4 ผลการดำเนินงาน	49
4.1 แผนการดำเนินงาน	49
4.2 ข้อเสนอแนะ/ปรับปรุงในอนาคต	51
4.3 ผลการดำเนินงาน	52
4.4 ผลการทดสอบ	53
4.4.1 ผลการสำรวจความพึงพอใจจากผู้ใช้งานแอปพลิเคชัน	54
บทที่ 5 สรุปผลการปฏิบัติสหกิจ	55
บรรณานุกรม	56
ภาคผนวก ภาคผนวก ก. งานอื่น ๆ เพิ่มเติม	58

สารบัญรูปภาพ

ภาพที่ 3.1 แผนภาพแสดงโครงสร้างสถาปัตยกรรมของระบบ	10
ภาพที่ 3.2 แผนภาพกรณีใช้งานของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)	12
ภาพที่ 3.3 แผนภาพแอคทีวิตี้ตรวจสอบสถานะเครื่องที่ใช้งาน	21
ภาพที่ 3.5 แผนภาพแอคทีวิตี้ตรวจสอบช่องโหว่ของผู้ใช้งาน	23
ภาพที่ 3.6 แผนภาพแอคทีวิตี้ตรวจสอบระบบป้องกันไวรัส	24
ภาพที่ 3.7 แผนภาพแอคทีวิตี้ตรวจสอบความเสี่ยงภายในระบบ	25
ภาพที่ 3.9 แผนภาพแอคทีวิตี้ตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ	27
ภาพที่ 3.10 หน้าการใช้งานหลัก	28
ภาพที่ 3.11 การจัดการอุปกรณ์(Device management)หน้าแสดงผลหลัก	29
ภาพที่ 3.12 รายงานทั้งหมดของการจัดการอุปกรณ์(Device management Full Report)	30
ภาพที่ 3.13 รายงานการป้องกันไวรัส(Antivirus Report) หน้าแสดงข้อมูลเบื้องต้น	31
ภาพที่ 3.14 รายงานการป้องกันไวรัส(Antivirus Report)หน้าแสดงข้อมูลหลัก	32
ภาพที่ 3.15 รายงานทั้งหมดของสถานะการป้องกัน(Signature Full Report)	33
ภาพที่ 3.16 รายงานทั้งหมดของการป้องกันไวรัส(Scan Antivirus Full Report)	34
ภาพที่ 3.17 รายงานการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) หน้าแสดงข้อมูลเบื้องต้น	35
ภาพที่ 3.18 รายงานการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) หน้าแสดงข้อมูลหลัก	36

ภาพที่ 3.19 ตัวอย่างหน้ารายงานแยกประเภทของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ (Attack surface reduction)	37
ภาพที่ 3.20 รายงานทั้งหมดของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ (Attack surface reduction)	38
ภาพที่ 3.21 รายงานความเสี่ยงที่เกิดช่องโหว่(Vulner Abilities)	39
ภาพที่ 3.22 รายงานทั้งหมดของความเสี่ยงที่เกิดช่องโหว่(Vulner Abilities Full Report)	40
ภาพที่ 3.23 รายงานความเสี่ยง(Risk Report)หน้าแสดงข้อมูลเบื้องต้น	41
ภาพที่ 3.24 รายงานความเสี่ยง(Risk Report)หน้าแสดงข้อมูล หน้าแสดงข้อมูลหลัก	42
ภาพที่ 3.25 รายงานทั้งหมดของความเสี่ยง(Risk Full Report)	43
ภาพที่ 3.26 รายงานการแจ้งเตือนภัยคุกคาม(Alert Report)หน้าแสดงข้อมูลเบื้องต้น	44
ภาพที่ 3.27 รายงานการแจ้งเตือนภัยคุกคาม(Alert Report)หน้าแสดงข้อมูลหลัก	45
ภาพที่ 3.28 รายงานทั้งหมดของการแจ้งเตือนภัยคุกคาม(Alert Full Report)	46
ภาพที่ 3.29 ระบบแจ้งเตือนความเสี่ยงไปยังอีเมล(Email)	47
ภาพที่ 3.30 อีเมล(Email)แจ้งเตือนถึงผู้ดูแลระบบ	47
ภาพที่ 3.31 รายงานการเก็ยคำสั่งของพาวเวอร์อโต้เมท(PowerAutomate Report)	48
ภาพที่ 4.1 ผลการดำเนินงานการเชื่อมต่อระหว่างผู้ใช้งานกับระบบ(User interface)	52
ภาพที่ 4.2 ผลการดำเนินงาน การเชื่อมต่อข้อมูลเข้ากับฐานข้อมูล	53

สารบัญตาราง

ตารางที่ 2.1 เปรียบเทียบความสามารถในการใช้งาน	8
ตารางที่ 3.1 แสดงรายละเอียด ผู้กระทำ(Actor) ใน อธิบายกรณี	13
ตารางที่ 3.2 แสดงรายละเอียดกรณีใช้งาน (Use Case) ต่างๆ	13
ตารางที่ 3.3 รายละเอียดกรณีการตรวจสอบสถานะเครื่องที่ใช้งาน	14
ตารางที่ 3.4 รายละเอียดกรณีการตรวจสอบภัยคุกคาม	15
ตารางที่ 3.6 รายละเอียดกรณีการตรวจสอบระบบป้องกันไวรัส	17
ตารางที่ 3.7 รายละเอียดกรณีการตรวจสอบความเสี่ยงภายในระบบ	18
ตารางที่ 3.8 รายละเอียดกรณีการแจ้งเตือนความเสี่ยงไปยังอีเมล(Email)และบันทึกลงระบบ	19
ตารางที่ 3 9 รายละเอียดกรณีการตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ	20
ตารางที่ 4.1 แผนการดำเนินงาน	49
ตารางที่ 4.1 แผนการดำเนินงาน(ต่อ)	50
ตารางที่ 4.1 แผนการดำเนินงาน(ต่อ)	51

รายการสัญลักษณ์และคำย่อ

สัญลักษณ์/คำย่อ

คำเต็ม/คำจำกัดความ

KQL

Kusto Query Language

Power Bi

Microsoft Power BI

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของโครงการ

การรักษาความปลอดภัยของข้อมูล เป็นสิ่งที่มีความสำคัญในยุคสมัยที่ข้อมูลทุกอย่างเป็นสิ่งสำคัญความปลอดภัยในการเข้าถึงข้อมูลจึงเป็นเรื่องที่จำเป็น ถ้ามองในมุมการทำงานภายในบริษัท การเสริมสร้างความแข็งแกร่งและป้องกันการถูกโจมตีบนช่องทางออนไลน์ถือว่าเป็นสิ่งที่ไม่ควรมองข้าม ซึ่งข้อมูลเหล่านั้นอาจเป็นข้อมูลที่ค่อนข้างละเอียดอ่อนไม่ว่าจะเป็นทรัพย์สินทางปัญญา, ข้อมูลทางการเงินข้อมูลส่วนบุคคลหรือข้อมูลประเทศอื่น ๆ ที่บุคคลอื่นสามารถเข้าถึงหรือเปิดเผยได้โดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อด้านลบกับองค์กรได้ เพราะองค์กรมักส่งข้อมูลที่มีความสำคัญข้ามเครือข่ายและอุปกรณ์ในการทำธุรกิจ ข้อมูลเหล่านั้นจึงควรได้รับการปกป้องโดยเฉพาะในยุคที่การโจมตีทางไซเบอร์นั้นมีความซับซ้อนมาก โดยเฉพาะถ้าเกิดการรั่วไหลอาจส่งผลกระทบต่อองค์กรอย่างร้ายแรงทั้งในแง่ค่าใช้จ่ายมหาศาลเพื่อแลกกับข้อมูลที่ถูกขโมยไป และที่สำคัญกว่านั้น คือ ชื่อเสียงด้านความปลอดภัย ซึ่งยากต่อการแก้ไขเพื่อให้ลูกค้าและผู้ให้บริการกลับมามั่นใจในองค์กรได้เหมือนเดิม แต่การที่จะรักษาความปลอดภัยของข้อมูลได้อย่างมีประสิทธิภาพนั้นจำเป็นต้องมีการตรวจสอบและการแจ้งเตือนเพื่อที่จะสามารถแก้ไขปัญหาได้ทันเวลาที่

ทางผู้จัดทำรายงานได้รับมอบหมายนั้นคือ การแสดงข้อมูลของระบบรักษาความปลอดภัยให้ได้ครบถ้วนมากขึ้น มีความหลากหลาย และชัดเจนมากกว่าตัวระบบเดิม โดยใช้ไม่จำกัดเทคโนโลยีที่เข้ามาแก้ไขปัญหาในครั้งนี้

จากความสำคัญที่กล่าวไปข้างต้นและสิ่งที่ได้รับมอบหมายจึงทำให้เกิดการพัฒนา ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) เป็นระบบที่ทำให้การตรวจสอบความปลอดภัยภายในองค์กรนั้นสามารถ ตรวจสอบได้อย่างละเอียดใช้งานได้ง่ายและมีการแจ้งเตือนภัยคุกคามของผู้ใช้งานไปยังผู้ดูแลระบบ

1.2 วัตถุประสงค์

โครงการนี้มีเป้าหมายเพื่อพัฒนาระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) โดยกำหนดวัตถุประสงค์ของโครงการดังต่อไปนี้

1. เพื่อศึกษาเกี่ยวกับความรู้เกี่ยวกับการรักษาความปลอดภัยของข้อมูล
2. เพื่อศึกษาการใช้ภาษา เคคิวแอล(KQL)

3. เพื่อศึกษาการออกแบบหน้านำเสนอข้อมูล(Dashboard) ที่ใช้ในการรายงานความปลอดภัย
4. เพื่อพัฒนาระบบแจ้งเตือนอัตโนมัติ เมื่อเกิดความเสี่ยงหรือภัยคุกคาม

1.3 ขอบเขตของโครงการ

ขอบเขตของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) จะถูกออกแบบมาใน พาวเวอร์บีโอแบบออนไลน์(Power Bi Online Report) เพราะเป็นรูปแบบที่ผู้ดูแลระบบหรือผู้ใช้งานนั้นสามารถใช้ได้ทั้งเว็บไซต์ คอมพิวเตอร์ และมือถือ นอกเหนือจากนั้นต้องรองรับการใช้งานของผู้ดูแลระบบหลายคน

1.3.1 ขอบเขตการพัฒนาของระบบ

1. มีการแสดงข้อมูลเกี่ยวกับความเสี่ยงและภัยคุกคามภายในระบบ
2. มีการแสดงสถานะการทำงานของระบบป้องกันไวรัส
3. มีการแสดงสถานะช่องโหว่และความไม่น่าเชื่อถือในการใช้งาน
4. มีส่วนที่เชื่อมต่อระหว่างผู้ใช้งานกับระบบ(UI) ที่ใช้งานได้ง่าย
5. มีการแจ้งเตือนความเสี่ยงไปยัง อีเมล(Email) ของผู้ดูแลระบบและส่งการแจ้งเตือนที่เกิดความเสี่ยงได้
6. มีการบันทึกการแจ้งเตือนและการกระทำที่ได้รับจาก อีเมล(Email)

1.3.2 ข้อจำกัดในการใช้งาน

1. การใช้งานระบบต้องเชื่อมต่ออินเทอร์เน็ตเพื่อได้รับข้อมูลที่เป็นปัจจุบันที่สุด
2. ระบบรองรับการใช้งานผ่านผลิตภัณฑ์ของพาวเวอร์บีโอ(Power Bi) เท่านั้น
3. สามารถแสดงผลได้ดีที่สุดบนเครื่องคอมพิวเตอร์

1.4 ประโยชน์ของโครงการ

1. ช่วยให้ผู้ดูแลระบบสามารถรับทราบสถานะความปลอดภัยได้
2. ช่วยให้ผู้ดูแลระบบสามารถรู้ภัยคุกคามแล้วสามารถป้องกันได้ทันเวลาที่
3. ช่วยเพิ่มความสะดวกสบายในการตรวจสอบข้อมูลของระบบรักษาความปลอดภัย
4. ช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์การจัดการใช้งานและการเข้าถึงของผู้ใช้งานผ่านระบบรายงานความปลอดภัย

บทที่ 2

วรรณกรรม งาน และเทคโนโลยีที่เกี่ยวข้อง

2.1 แนวคิดทฤษฎีที่เกี่ยวข้อง

2.1.1 ระบบรักษาความปลอดภัยในคอมพิวเตอร์(Microsoft Security)

ในปัจจุบันภัยคุกคามทางคอมพิวเตอร์มีการเติบโตขึ้นอย่างมีนัยสำคัญ ทั้งในแง่ปริมาณและความซับซ้อนของตัวภัยคุกคาม เนื่องจากเราไม่สามารถแยกแยะและจัดการภัยคุกคามได้ด้วยตัวเอง การใช้งานคอมพิวเตอร์จึงต้องการเครื่องมือช่วยดูแลความปลอดภัย ทางไมโครซอฟท์ก็ได้เล็งเห็นความต้องการในการดูแลรักษาความปลอดภัยที่เข้มข้น จึงได้ออกแบบระบบปฏิบัติการที่มาพร้อมกับความสามารถในการจัดการกับภัยคุกคามประเภทต่างๆ [8]

2.1.2 การดึงข้อมูลใช้ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface)

ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface: API) คือช่องทางการเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลจากระบบหนึ่งไปสู่ระบบอื่น ๆ ที่มีความสะดวก รวดเร็ว ปลอดภัย [1]

2.1.3 การออกแบบแอปพลิเคชัน (App design)

การออกแบบแอปพลิเคชัน คือ การออกแบบเพื่อตอบโจทย์การใช้งานของผู้ใช้ให้มากที่สุด สร้างความสอดคล้องกันระหว่างผู้ใช้และฟังก์ชันการใช้งาน ส่วนที่เชื่อมต่อระหว่างผู้ใช้งานกับระบบ(UI) จะต้องมีโครงสร้างการใช้งานและ แนวคิด(Concept) ที่ชัดเจน เพื่อให้ผู้ใช้การทั่วไบนั้นสามารถเข้าถึงได้ [2]

2.1.4 การคัดกรองข้อมูลจากฐานข้อมูล (Query)

การคัดกรองข้อมูลจากฐานข้อมูล คือ เป็นการกรองข้อมูลที่ต้องการจากฐานข้อมูลที่มีข้อมูลจำนวนมาก โดยคำสั่งที่ใช้ คือ เลือก(Select) ผลลัพธ์ที่ได้จากการคัดกรองข้อมูลจากฐานข้อมูล (Query) มีลักษณะข้อมูลเป็นตาราง ประกอบด้วย แถว(Column) และ แถว(Row) [3]

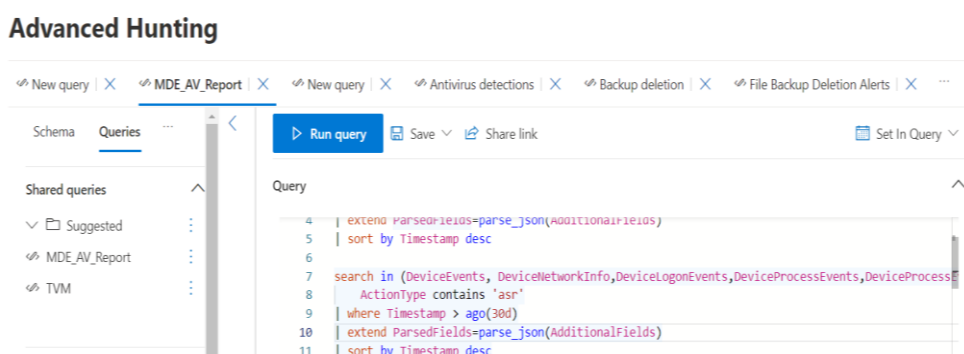
2.2 ระบบงานปัจจุบัน /งานที่เกี่ยวข้อง

2.2.1 ระบบงานปัจจุบัน

2.2.1.1 ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)

ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)เป็นโปรดักส์ที่ใช้ในการช่วยรักษาความปลอดภัยของผู้ใช้ด้วยการป้องกันการตรวจหาและการตอบสนองต่อภัยคุกคามที่ผสมรวมในปลายทาง อีเมล ข้อมูลประจำตัว แอปพลิเคชัน และข้อมูล [8]

(1)การตรวจสอบขั้นสูง(Advanced Hunting)



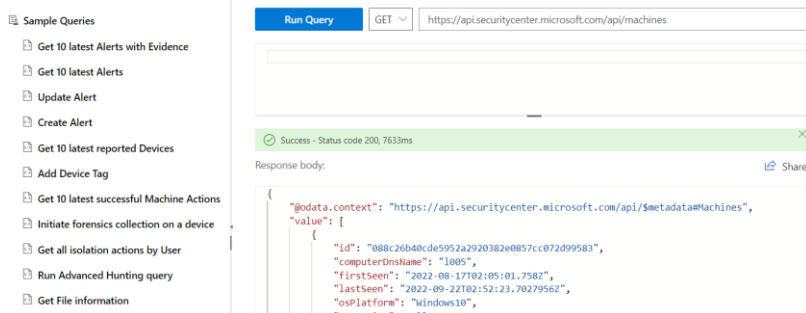
ภาพที่ 2.2 การตรวจสอบขั้นสูง(Advanced Hunting)

การตรวจสอบขั้นสูง(Advanced Hunting) เป็นเครื่องมือค้นหาภัยคุกคามตามวิธีที่ให้คุณสำรวจข้อมูลดิบได้นานถึง 30 วัน คุณสามารถตรวจสอบเหตุการณ์ในเครือข่ายของคุณในเชิงรุกเพื่อค้นหาตัวบ่งชี้และเตือนภัยคุกคาม การเข้าถึงข้อมูลที่ยืดหยุ่นช่วยให้สามารถค้นหาภัยคุกคามทั้งที่รู้จักและที่อาจเกิดขึ้นได้โดยไม่มีข้อจำกัด

(2) การตรวจสอบเอพีไอ(API Explorer)

API Explorer

Use the API explorer to test Microsoft Defender for Endpoint capabilities. Use the sample queries to get started.



ภาพที่ 2.3 การตรวจสอบเอพีไอ(API Explorer)

การตรวจสอบเอพีไอ(API Explorer) เป็นการดึงข้อมูลการเชื่อมต่อจากระบบหนึ่งไปสู่อีกระบบหนึ่ง(API) ทำให้ง่ายต่อการสร้างและดำเนินการค้นหา ทดสอบ และส่งคำขอสำหรับปลายทางดีเฟนเดอร์เอพีไอ(Defender for Endpoint API) ที่มีอยู่ ใช้การตรวจสอบเอพีไอ(API Explorer) เพื่อดำเนินการหรือค้นหาข้อมูลของระบบให้ออกมาในรูปแบบเจสัน(json) โดยใช้ โอดาต้า(OData) ในการดึงข้อมูลออกมาใช้โดยฟังก์ชันนี้มีอยู่ในตัว พาวเวอร์บีไอ(Power Bi)

2.2.1.2 ไมโครซอฟพาวเวอร์บีไอ(Microsoft Power Bi)

ไมโครซอฟพาวเวอร์บีไอ(Microsoft Power Bi)เป็นเครื่องมือในการวิเคราะห์ข้อมูล และสร้างรายงาน สร้าง หน้านำเสนอ(Dashboard) ได้อย่างน่าสนใจ ให้ผู้ใช้งานเพื่อประกอบการตัดสินใจ แบบรวมศูนย์ สามารถอัปเดต ได้อย่างทันที อีกทั้งยังสามารถดูได้จากทุกๆ อุปกรณ์ ทั้ง คอมพิวเตอร์,มือถือ,เว็บไซต์ ผู้ใช้สามารถทำ คลิกเพื่อดูข้อมูลในมุมมองที่ต้องการ เพื่อที่จะหาคำตอบ เพื่อตัดสินใจ ไมโครซอฟพาวเวอร์บีไอ(Microsoft Power Bi)สามารถเชื่อมต่อแหล่งข้อมูล (Data Source) ที่เป็นที่ยอมรับมากมาย เช่น เอ็กเซล(Excel), ฐานข้อมูล(Database), เว็บไซต์(Website), ไฟล์(File) ต่าง ๆ ด้วยหลักการของ ออกแบบครั้งเดียวแล้วดูได้จากทุกๆที่ ทุกๆเวลา(Design Once View Anywhere) [5]

(1)เครื่องมือแก้ไขขั้นสูง(Advanced Edlitor)



ภาพที่ 2.5 เครื่องมือแก้ไขขั้นสูง(Advanced Edlitor)

เครื่องมือแก้ไขขั้นสูง(Advanced Edlitor) เป็นการพาวเวอร์คิวรี(Power Query) ที่เราสร้างมานั้นจะมีฉากหลังคือภาษาเอ็ม(M language) ซึ่งแสดงผลได้เนื่องจาก ไมโครซอฟพาวเวอร์บีโอ(Microsoft Power Bi)ทำงานร่วมกันระหว่างเทคโนโลยี ไมโครซอฟ(Microsoft) ที่ได้ตีอยู่แล้ว ดังนั้น จึงสามารถใช้ข้อมูลทั้งหมดอย่างมีประสิทธิภาพ

โดย ภาษาเอ็ม(M language) เป็นภาษาสคริปต์ที่ทำงานในฉากเมื่อเราสร้างสูตรด้วย พาวเวอร์คิวรี(Power Query) ใน พาวเวอร์บีโอ(Power Bi) และ เอ็กเซล(Excel) มาจัดการทำให้ข้อมูลต่าง ๆ นั้น เพื่อเตรียมข้อมูลให้พร้อมที่จะนำไปใช้ในการวิเคราะห์ข้อมูลต่อไป โดยสามารถใช้คำสั่งการตรวจสอบขั้นสูง(Advanced Hunting) ใน ไมโครซอฟดีเฟนเดอร์365(Microsoft 365 Defender)มาเพื่อนำเสนอในพาวเวอร์บีโอ(Power Bi) ผ่าน M ภาษาเอ็ม(M language) ได้

2.2.1.3 เคคิวแอล(Kusto Query Language)

เคคิวแอล(Kusto Query Language)เป็นภาษาคิวรีที่ปรับให้เหมาะสมและตัวเลือกการแสดงผลภาพของข้อมูลด้วยภาษาคัดลอกภาษาสอบถามเชิงโครงสร้าง (SQL) ที่เรียกว่า เคคิวแอล (Kusto Query Language) เพราะใช้สำหรับสืบค้นเท่านั้นและแตกต่างจาก ภาษาสอบถามเชิงโครงสร้าง (SQL) โดย เคคิวแอล (Kusto Query Language) ไม่สามารถอัปเดตหรือลบข้อมูลได้ [4]

2.2.1.4 ไมโครซอฟพาวเวอร์ออโตเมท(Microsoft Power Automate)

ไมโครซอฟพาวเวอร์ออโตเมท(Microsoft Power Automate)เป็นซอฟต์แวร์กลุ่ม ที่ช่วยให้ธุรกิจสร้างหุ่นยนต์มาทำงานในลักษณะงานซ้ำ ๆ รูปแบบเดิม ๆ แทนคน (robotic process automation) เป็น โปรแกรมที่ถูกออกแบบมาเพื่ออยู่ในระบบคลาวด์ตั้งแต่เริ่มต้น(Cloud-Native RPA) ใช้สำหรับสร้างและพัฒนาระบบอัตโนมัติ ด้วยเทคโนโลยีการออกแบบและพัฒนาเว็บไซต์หรือซอฟต์แวร์ออกมาได้รวดเร็วที่สุด ด้วยการเขียนโค้ดน้อยที่สุด (Low-Code Platform)ทำงานได้ดีกับไมโครซอฟ365(Microsoft 365) พร้อม เอพีไอ(API) และ การสร้างเอไอ(AI Builder)เป็นบริการระบบคลาวด์ที่เป็นประโยชน์และใช้งานง่ายสำหรับผู้ใช้ในสายงานธุรกิจ เพื่อสร้างเวิร์กโฟลว์ที่ทำให้งานและกระบวนการในธุรกิจที่ต้องใช้เวลามากเป็นแบบอัตโนมัติในแอปพลิเคชันและบริการต่างๆ [7]

2.2.1.5 โอดาต้า(OData)

โอดาต้า(โอดาต้า) หรือ โอเพ่นดาต้าโพรโทคอล(Open Data Protocol) คือ เป็นมาตรฐานโพรโทคอลสำหรับการสร้างและการใช้ข้อมูล แบบเปิดซึ่งช่วยให้สามารถสร้างและใช้งาน เอพีไอ(API) วัตถุประสงค์ของ โอดาต้า(OData) คือการจัดเตรียมโพรโทคอลเพื่อใช้งาน เร็ช(REST) หรือการจัดการการสื่อสารบนเครือข่ายที่ซับซ้อน(State Representational State Transfer)สำหรับการสร้างการแลกเปลี่ยนข้อมูล ระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย(Web Service) แบบเรียบง่าย โดยเรียกใช้ผ่านทางกำหนดประเภทของคำร้องขอ (HTTP Method)และส่งข้อมูลออกมาในรูปของ เอกซ์เอ็มแอลXML (XML) หรือ เอชทีทีพีHTTP (HTTP) และ เจสัน(JSON)เพื่อให้สามารถเข้าถึงข้อมูลจากโปรแกรมต่างๆของโอดาต้า (OData)[6]

2.2.2 ระบบงานในปัจจุบัน

2.2.2.1 ไมโครซอฟซีเคียวริตี้เซ็นเตอร์(Microsoft security center)

ไมโครซอฟซีเคียวริตี้เซ็นเตอร์(Microsoft security center)เป็นระบบแสดงข้อมูลของระบบรักษาความปลอดภัยเบื้องต้น ของ ไมโครซอฟดีเฟนเดอร์365(Microsoft 365 Defender) โดยที่จะแสดงแค่กราฟเท่านั้นไม่มีการแสดงข้อมูลในรูปแบบตารางจึงทำให้ข้อมูลนั้นมีจำนวนและรายละเอียดที่ไม่มาก [8]

ตารางที่ 2.1 เปรียบเทียบความสามารถในการใช้งาน

	ไมโครซอฟซีเคียวริตี้เซ็นเตอร์ (Microsoft security center)	ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)
ความสะดวกในการใช้งาน	ต้องมีสิทธิในระบบ ไมโครซอฟ ดีเฟนเดอร์365(Microsoft 365 Defender) ในถึงใช้งานได้	ไม่ต้องมีสิทธิในระบบ แค่ ได้รับงานยินยอมจากผู้สร้าง แทน สามารถใช้งานได้ง่ายไม่ว่าจะผ่านเว็บเบราว์เซอร์,แอป พลิเคชันมือถือ,โปรแกรม คอมพิวเตอร์
รายละเอียดของข้อมูลที่ได้	ได้กราฟแสดงข้อมูลแค่เบื้องต้น	มีการแสดงข้อมูลที่ละเอียด มากกว่าเพราะดึงข้อมูล โดยตรง

บทที่ 3

การดำเนินงาน

3.1 ภาพรวมของโครงการ

ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) เป็น ไมโครซอฟพาวเวอร์บีไอ(Microsoft Power Bi) ไว้สำหรับแสดงข้อมูลความปลอดภัย และแจ้งเตือนภัยคุกคามโดยมีระบบดังนี้

1. ระบบสามารถแสดงข้อมูลเกี่ยวกับสถานะเครื่องที่ใช้งานภายในระบบ
2. ระบบสามารถแสดงข้อมูลเกี่ยวกับภัยคุกคามภายในระบบ
3. ระบบสามารถแสดงข้อมูลเกี่ยวกับสถานะช่องโหว่ของผู้ใช้งานได้
4. ระบบสามารถแสดงข้อมูลเกี่ยวกับสถานะการทำงานของระบบป้องกันไวรัส และการใช้งานระบบสแกนไวรัสของผู้ใช้งาน
5. ระบบการแจ้งเตือนความเสี่ยงไปยัง อีเมล(Email) ของผู้ดูแลระบบและสิ่ง การเครื่องที่เกิดความเสี่ยงได้
6. ระบบสามารถแสดงข้อมูลเกี่ยวกับความเสี่ยงภายในระบบ
7. ระบบสามารถแสดงข้อมูลการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ

3.1.1 เป้าหมายโครงการที่ได้รับมอบหมายจากบริษัท

การศึกษาเรื่อง ความมั่นคงปลอดภัยทางไซเบอร์(Cyber security), คลังข้อมูล วิเคราะห์เชิงลึกด้านการโจมตีไซเบอร์(threat hunting) โดยศึกษาตัวงานพร้อมทั้งหา วิธีการที่ที่จะเข้ามาทำระบบแสดงผลช่วยให้การบริหารการดูแลภัยคุกคามมีประสิทธิภาพมากขึ้นทำความเข้าใจกับเคคิวแอล (Kusto Query Language) ในการดึงข้อมูลเพื่อสร้างหน้าแสดงผล ตลอดจนใช้เครื่องมืออย่างไมโครซอฟพาวเวอร์ออโตเมท(Microsoft Power Automate)ที่มี การเชื่อมต่อระบบมาสร้างระบบการแจ้งเตือนอัตโนมัติ เช่น หากพบความเสี่ยงเกิดขึ้นที่เครื่อง หากลักษณะเข้าข่ายระบบก็จะอีเมลแจ้งผู้ดูแลระบบให้ทราบ

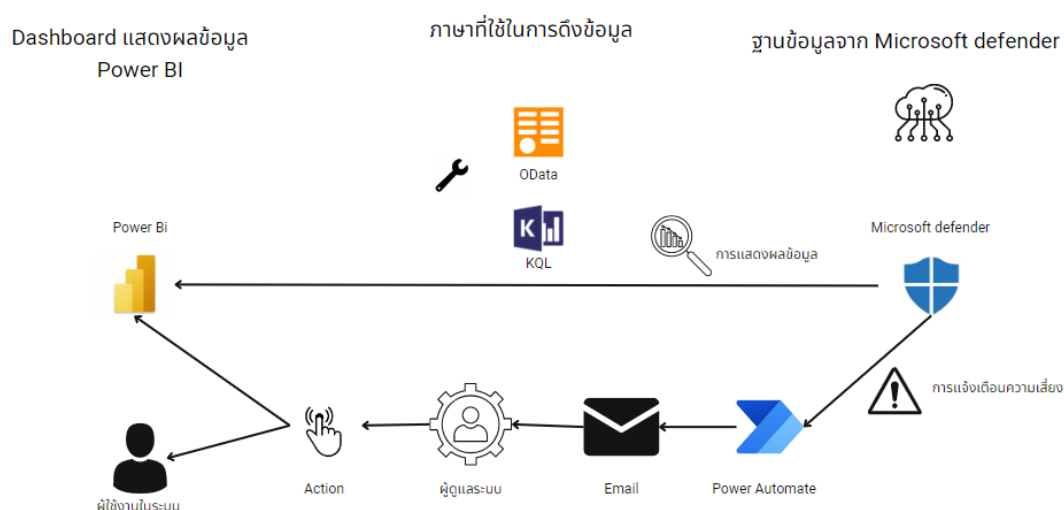
3.1.1.1 หัวข้อที่ได้การศึกษานอกเหนือจากที่ได้รับมอบหมาย

- (1) การใช้ไมโครซอฟพาวเวอร์บีไอ(Microsoft Power Bi)บันทึกคำสั่งเคคิวแอล (Kusto Query Language) ในการดึงข้อมูล
- (2) การใช้ โอดาต้า(Odata) ดึงข้อมูลของผู้ใช้งานมาใช้งานร่วมกับเคคิวแอล (Kusto Query Language)

3.1.1.2 การนำสิ่งที่ได้ศึกษามาวิเคราะห์โครงสร้างของระบบ

- (1) การนำข้อมูลที่ได้จากการใช้โอดาต้า(Odata)เป็นตัวกลางในการเก็บข้อมูลประจำเครื่องของผู้ใช้งานภายในระบบ
- (2) การที่ผู้ใช้งานนั้นสามารถใช้งานที่ได้จากการตั้งโดยเคคิวแอล (Kusto Query Language) และ โอดาต้า(Odata)โดยใช้แค่ไมโครซอฟฟาวเวอร์ บี้ไอ(Microsoft Power Bi)

3.1.2 โครงสร้างสถาปัตยกรรมของระบบ



ภาพที่ 3.1 แผนภาพแสดงโครงสร้างสถาปัตยกรรมของระบบ

ภาพที่ 3.1 แสดงแผนภาพแสดงโครงสร้างสถาปัตยกรรมของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)จากการวิเคราะห์โครงสร้างของระบบซึ่งแบ่งเป็น สถาปัตยกรรมแต่ละอย่างดังนี้

- 1.ผู้ดูแลระบบ คือ ผู้ที่ดูแลรักษาความปลอดภัยของระบบภายในองค์กรซึ่งสามารถสั่งการเครื่องของผู้ใช้งานได้
- 2.พาวเวอร์บีไอ(Power Bi) คือ เครื่องมือในการวิเคราะห์ข้อมูล สร้างรายงาน และสามารถดู Dashboard Reportได้
- 3.ไมโครซอฟฟาวเวอร์ออโต้เมท(Microsoft Power Automate)คือ เครื่องมือสำหรับเวิร์กโฟลว์ที่ทำให้งานและกระบวนการในแบบอัตโนมัติในแอปพลิเคชันและบริการต่างๆ

4. โอดาต้า(OData) คือ เครื่องมือสำหรับไว้ใช้แบบเปิดซึ่งช่วยให้สามารถสร้างและใช้งานข้อมูล API ได้

5. เคคิวแอล(KQL) คือ เครื่องมือสำหรับเป็นคิวรีที่ปรับให้เหมาะสมและตัวเลือกการแสดงผลของข้อมูลสำหรับสืบค้น

6. ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)คือ สำหรับช่วยรักษาความปลอดภัยของผู้ใช้ด้วยการป้องกันการตรวจหาและการตอบสนองต่อภัยคุกคามโดยมีการเบข้อมูลด้านความปลอดภัย

7. อีเมล(Email) คือข้อความของความเสี่ยงที่จะส่งตรงไปยังผู้ดูแลระบบโดยสามารถส่งการคำสั่งได้

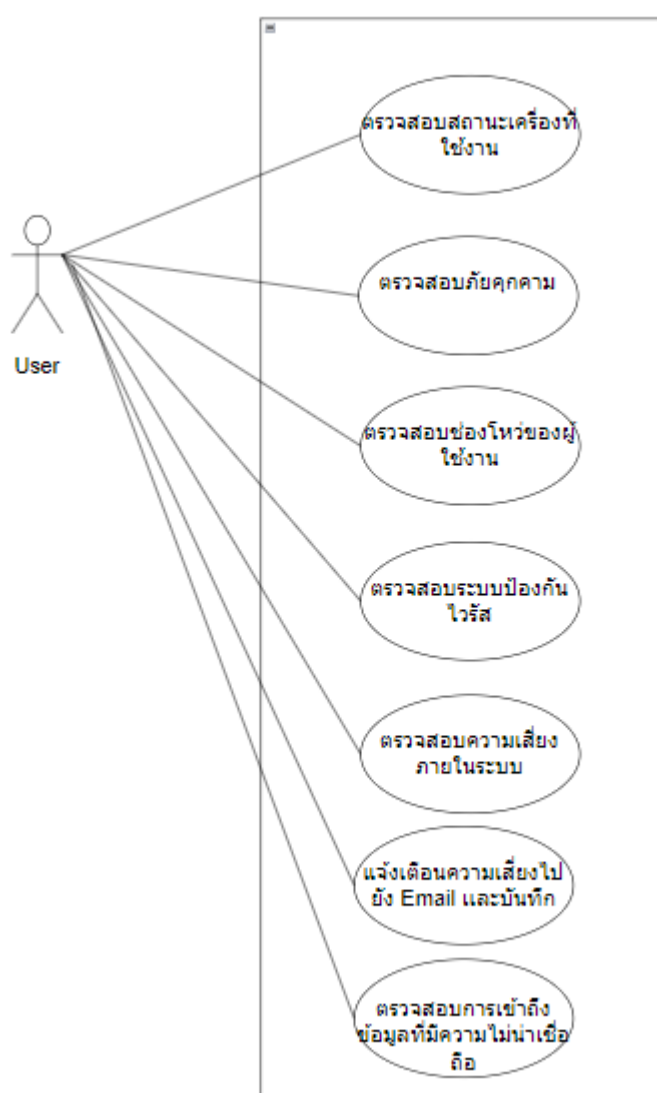
8. ผู้ใช้งานในระบบ คือ ผู้ใช้งานทั่วไปภายในองค์กรหรือบริษัทที่อยู่ในการดูแลของ Microsoft 365 Defender

ในการใช้งานผู้ดูแลระบบ นั้นจะใช้งาน ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)ผ่าน พาวเวอร์บีไอ(Power Bi)ไม่ว่าจะในรูปแบบเว็บ เบราวเซอร์,แอปพลิเคชันมือถือ,โปรแกรมคอมพิวเตอร์ โดย พาวเวอร์บีไอ(Power Bi)จะเก็บค่า เอพีไอ(API) จาก โอดาต้า(OData) และการใช้ เคคิวแอล(KQL) ดึงข้อมูลสืบค้นของ Microsoft 365 Defender และเมื่อเกิดภัยคุกคามก็จะทำการใช้ ไมโครซอฟพาวเวอร์ออโต้เมท(Microsoft Power Automate)ในการส่งการแจ้งเตือนไปยัง อีเมล(Email)ของผู้ดูแลระบบ โดยเมื่อมีการส่งการกับเครื่อง ผู้ใช้งานในระบบและคำสั่งที่ได้รับการแจ้งเตือนจะบันทึกผลเข้าสู่ พาวเวอร์บีไอ (Power Bi)

3.2 การวิเคราะห์ขอบเขตและความต้องการของระบบ

แสดงแผนภาพกรณีใช้งานของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) จากการวิเคราะห์ขอบเขตและความต้องการของระบบ

ในส่วนของผู้ใช้งาน นั้นสามารถใช้งานการตรวจสอบสถานะเครื่องที่ใช้งาน, ตรวจสอบภัยคุกคาม, ตรวจสอบช่องโหว่ของผู้ใช้งาน, ตรวจสอบระบบป้องกันไวรัส, ตรวจสอบความเสี่ยงภายในระบบ, แจ้งเตือนความเสี่ยงไปยัง Email และบันทึก, ตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ และ แจ้งเตือนความเสี่ยงไปยัง อีเมล(Email) และเข้าถึงข้อมูลอีเมล(Email)ที่บันทึกลงระบบ



ภาพที่ 3.2 แผนภาพกรณีใช้งานของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)

ตารางที่ 3.1 แสดงรายละเอียด ผู้กระทำ(Actor) ใน อธิบายกรณี
(Use Case Diagrams)

ผู้กระทำ	คำอธิบาย
ผู้ดูแลระบบ	ผู้ที่รับหน้าที่ในการดูแลระบบความปลอดภัยในองค์กร

ตารางที่ 3.2 แสดงรายละเอียดกรณีใช้งาน (Use Case) ต่าง ๆ

No.	อธิบายกรณี	ผู้กระทำ	คำอธิบาย
UC01	ตรวจสอบสถานะ เครื่องที่ใช้งาน	ผู้ดูแลระบบ	สามารถตรวจสอบสถานะของเครื่องที่ใช้ งานภายในระบบได้
UC02	ตรวจสอบภัย คุกคาม	ผู้ดูแลระบบ	สามารถตรวจสอบภัยคุกคามที่เกิดขึ้น ภายในระบบได้
UC03	ตรวจสอบช่องโหว่ ของผู้ใช้งาน	ผู้ดูแลระบบ	สามารถตรวจสอบช่องโหว่ของผู้ใช้งาน ได้
UC04	ตรวจสอบระบบ ป้องกันไวรัส	ผู้ดูแลระบบ	สามารถตรวจสอบระบบป้องกันไวรัสได้
UC05	ตรวจสอบความ เสี่ยงภายในระบบ	ผู้ดูแลระบบ	สามารถตรวจสอบความเสี่ยงภายใน ระบบได้
UC06	แจ้งเตือนความ เสี่ยงไปยัง Email และข้อมูลEmailที่ บันทึกลงReport	ผู้ดูแลระบบ	ได้รับแจ้งเตือนความเสี่ยงไปยัง Email และตรวจสอบบันทึกการแจ้งเตือนได้
UC07	ตรวจสอบการ เข้าถึงข้อมูลที่มี ความไม่น่าเชื่อถือ	ผู้ดูแลระบบ	สามารถตรวจสอบการเข้าถึงข้อมูลที่มี ความไม่น่าเชื่อถือได้

3.3 การออกแบบขั้นตอนการทำงานของระบบ

3.3.1 รายละเอียดขั้นตอนแต่ละกรณีของระบบรายงานความปลอดภัย โดยใช้
เคคิวแอล (Security Report System by KQL)

ตารางที่ 3.3 รายละเอียดกรณีการตรวจสอบสถานะเครื่องที่ใช้งาน

รหัสยูสเคส (Use case ID)	UC01
ชื่อยูสเคส (Use case Name)	ตรวจสอบสถานะเครื่องที่ใช้งาน
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถตรวจสอบสถานะของเครื่องที่ใช้งานภายในระบบได้
เงื่อนไขก่อนหน้า (Pre-Condition)	ต้องมีบัญชี พาวเวอร์บีไอ(Power Bi)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุญาตการเข้าถึง พาวเวอร์บีไอ(Power Bi)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 2. ผู้ดูแลระบบอยู่แสดงผลหลัก 3. ผู้ใช้เข้า การจัดการอุปกรณ์(Device management)เพื่อตรวจสอบสถานะเครื่องที่ใช้งาน
กระแสรอง (Alternative Flow)	<ol style="list-style-type: none"> 1. ถ้าผู้ดูแลต้องการดูข้อมูลละเอียดมากถึงสามารถกรดยางานทั้งหมด(Full Report)ได้

ตารางที่ 3.4 รายละเอียดกรณีการตรวจสอบภัยคุกคาม

รหัสยูสเคส (Use case ID)	UC02
ชื่อยูสเคส (Use case Name)	ตรวจสอบภัยคุกคาม
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถตรวจสอบภัยคุกคามที่เกิดขึ้นภายในระบบได้
เงื่อนไขก่อนหน้า (Pre-Condition)	ต้องมีบัญชี พาวเวอร์บีไอ(Power Bi)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุญาตการเข้าถึง พาวเวอร์บีไอ(Power Bi)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 2. ผู้ดูแลระบบอยู่แสดงผลหลัก 3. ผู้ดูแลระบบเข้า รายงานการแจ้งเตือนภัยคุกคาม(Alert Report) เพื่อตรวจสอบสถานะภัยคุกคามเบื้องต้น 4. ผู้ดูแลระบบกดรายงาน(Report) เพื่อดูภัยคุกคามที่เกิดขึ้นภายในระบบ
กระแสรอง (Alternative Flow)	<ol style="list-style-type: none"> 1. ถ้าผู้ดูแลต้องการดูข้อมูลที่ละเอียดมากถึงสามารถกด รายงานทั้งหมด(Full Report)ได้

ตารางที่ 3.5 รายละเอียดกรณีการตรวจสอบช่องโหว่ของผู้ใช้งาน

รหัสยูสเคส (Use case ID)	UC03
ชื่อยูสเคส (Use case Name)	ตรวจสอบช่องโหว่ของผู้ใช้งาน
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถตรวจสอบช่องโหว่ของผู้ใช้งานได้
เงื่อนไขก่อนหน้า (Pre-Condition)	ต้องมีบัญชีพาวเวอร์บีไอ(Power Bi)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุญาตการเข้าถึงพาวเวอร์บีไอ(Power Bi)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 2. ผู้ดูแลระบบอยู่แสดงผลหลัก 3. ผู้ดูแลระบบเข้า ความเสี่ยงที่เกิดช่องโหว่(Vulner Abilities) เพื่อตรวจสอบสถานะภัยช่องโหว่เบื้องต้น 4. ผู้ดูแลระบบกดรายงาน(Report)เพื่อดูช่องโหว่ของผู้ใช้งานได้
กระแสรอง (Alternative Flow)	<ol style="list-style-type: none"> 1. ถ้าผู้ดูแลต้องการดูข้อมูลที่ละเอียดมากถึงสามารถกด รายงานทั้งหมด(Full Report)ได้

ตารางที่ 3.6 รายละเอียดกรณีการตรวจสอบระบบป้องกันไวรัส

รหัสยูสเคส (Use case ID)	UC04
ชื่อยูสเคส (Use case Name)	ตรวจสอบระบบป้องกันไวรัส
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถตรวจสอบตรวจสอบระบบป้องกันไวรัสได้
เงื่อนไขก่อนหน้า (Pre-Antivirus Report Condition)	ต้องมีบัญชีพาวเวอร์บีไอ(Power Bi)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุมัติการเข้าถึง พาวเวอร์บีไอ(Power Bi)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 2. ผู้ดูแลระบบอยู่แสดงผลหลัก 3. ผู้ดูแลระบบเข้า รายงานการป้องกันไวรัส(Antivirus Report) เพื่อตรวจสอบสถานะระบบป้องกันไวรัสเบื้องต้น 4. ผู้ดูแลระบบกดรายงาน(Report) เพื่อดูตรวจสอบระบบป้องกันไวรัสภายในระบบ
กระแสรอง (Alternative Flow)	<ol style="list-style-type: none"> 1 .ถ้าผู้ดูแลต้องการดูข้อมูลที่ละเอียดมากถึงสามารถกด รายงานทั้งหมด(Full Report) ได้ 2. ในรายงานทั้งหมด(Full Report) สามารถเลือกดูรายงาน ทั้งหมดของสถานะการป้องกัน(Signature Full Report) ที่เป็น การตรวจสอบเวอร์ชันของระบบป้องกันไวรัสได้

ตารางที่ 3.7 รายละเอียดกรณีการตรวจสอบความเสี่ยงภายในระบบ

รหัสยูสเคส (Use case ID)	UC05
ชื่อยูสเคส (Use case Name)	ตรวจสอบความเสี่ยงภายในระบบ
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถตรวจสอบความเสี่ยงภายในระบบได้
เงื่อนไขก่อนหน้า (Pre-Condition)	ต้องมีบัญชีพาวเวอร์บีไอ(Power Bi)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุญาตการเข้าถึงพาวเวอร์บีไอ(Power Bi)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 2. ผู้ดูแลระบบอยู่แสดงผลหลัก 3. ผู้ดูแลระบบเข้า รายงานความเสี่ยง(Risk Report) เพื่อตรวจสอบสถานะความเสี่ยงภายในระบบเบื้องต้น 4. ผู้ดูแลระบบกด รายงาน(Report)เพื่อดูตรวจสอบความเสี่ยงภายในระบบ
กระแสรอง (Alternative Flow)	<ol style="list-style-type: none"> 1. ถ้าผู้ดูแลต้องการดูข้อมูลที่ละเอียดมากถึงสามารถกด รายงานทั้งหมด(Full Report)ได้

ตารางที่ 3.8 รายละเอียดกรณีการแจ้งเตือนความเสี่ยงไปยังอีเมล(Email)และ
บันทึกลงระบบ

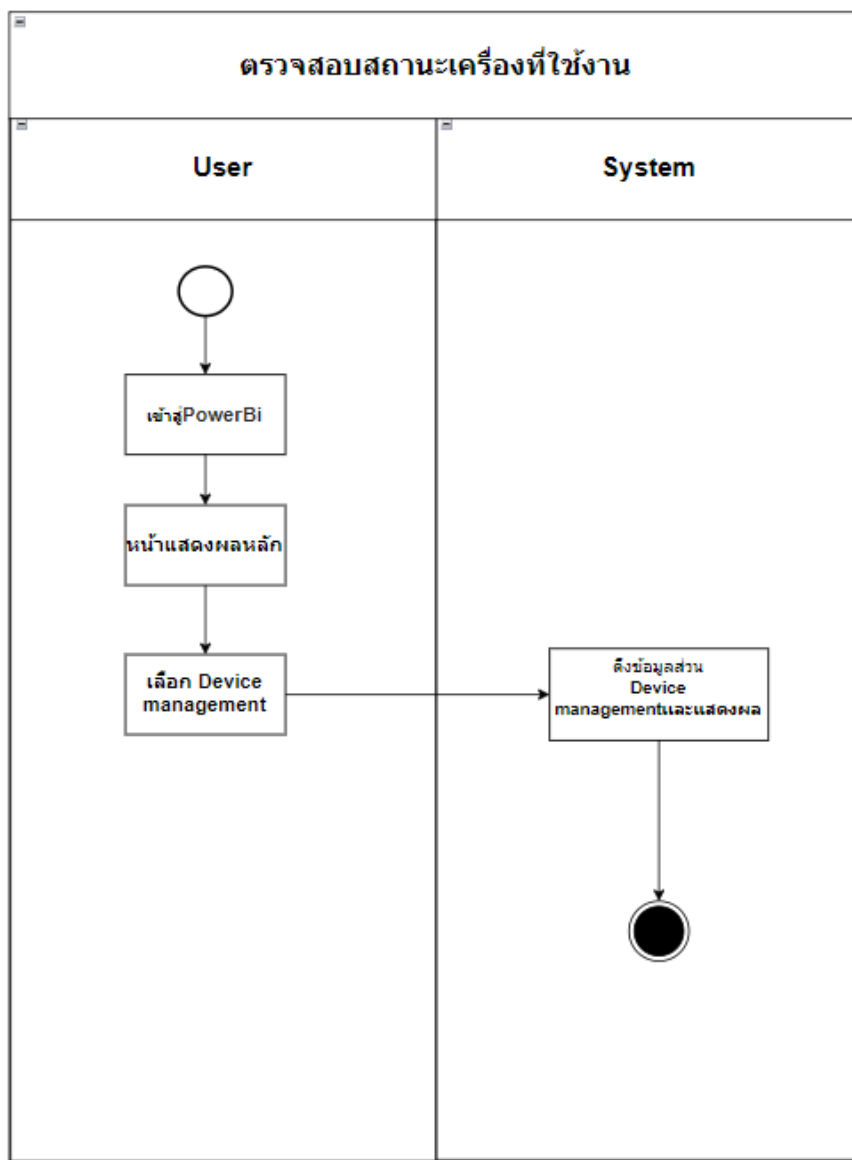
รหัสยูสเคส (Use case ID)	UC06
ชื่อยูสเคส (Use case Name)	แจ้งเตือนความเสี่ยงไปยังอีเมล(Email)และบันทึกลงระบบ
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถได้รับแจ้งเตือนความเสี่ยงไปอีเมล(Email)และบันทึกลงระบบ
เงื่อนไขก่อนหน้า (Pre-Condition)	ต้องมีบัญชี พาวเวอร์บีไอ(Power Bi) ต้องมีบัญชี พาวเวอร์ออโต้เมท(Power Automate)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุญาตการเข้าถึง พาวเวอร์บีไอ(Power Bi) ต้องทำการผูกอีเมล(Email)เข้ากับ พาวเวอร์ออโต้เมท(Power Automate)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. อีเมล(Email) แจ้งเตือนเมื่อเกิดความเสี่ยง 2. ผู้ดูแลระบบสั่งการเครื่องที่เกิดความเสี่ยงผ่าน อีเมล(Email) 3. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 4. ผู้ดูแลระบบอยู่แสดงผลหลัก 5. ผู้ดูแลระบบเข้า รายงานการสั่งการของพาวเวอร์ออโต้เมท(Power Automate Report)เพื่อตรวจสอบบันทึกการแจ้งเตือนและทำสั่งการ
กระแสรอง (Alternative Flow)	-

ตารางที่ 3.9 รายละเอียดกรณีการตรวจสอบการเข้าถึงข้อมูลที่มีความไม่
น่าเชื่อถือ

รหัสยูสเคส (Use case ID)	UC07
ชื่อยูสเคส (Use case Name)	ตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ
ผู้ใช้งาน (Actor)	ผู้ดูแลระบบ
คำอธิบาย (Description)	ผู้ดูแลระบบสามารถตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือได้
เงื่อนไขก่อนหน้า (Pre-Condition)	ต้องมีบัญชี พาวเวอร์บีไอ(Power Bi)
เงื่อนไขภายหลัง (Post-Condition)	ต้องได้รับสิทธิ์อนุญาตการเข้าถึง พาวเวอร์บีไอ(Power Bi)
กระแสหลัก (Basic Flow)	<ol style="list-style-type: none"> 1. ผู้ดูแลระบบเข้าสู่พาวเวอร์บีไอ(Power Bi) 2. ผู้ดูแลระบบอยู่แสดงผลหลัก 3. ผู้ดูแลระบบเข้า การเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) เพื่อตรวจสอบความไม่น่าเชื่อถือเบื้องต้น 4. ผู้ดูแลระบบกด รายงาน(Report) เพื่อดูความไม่น่าเชื่อถือที่เกิดขึ้นภายในระบบได้
กระแสรอง (Alternative Flow)	<ol style="list-style-type: none"> 1. ถ้าผู้ดูแลต้องการดูข้อมูลทีละเ็ดมากถึงสามารถกด รายงานทั้งหมด(Full Report) ได้ 2. ถ้าผู้ดูแลต้องการดูความไม่น่าเชื่อถือทั้ง 4 ที่มักเกิดขึ้นสามารถเข้ารายงาน(Report)ย่อยได้

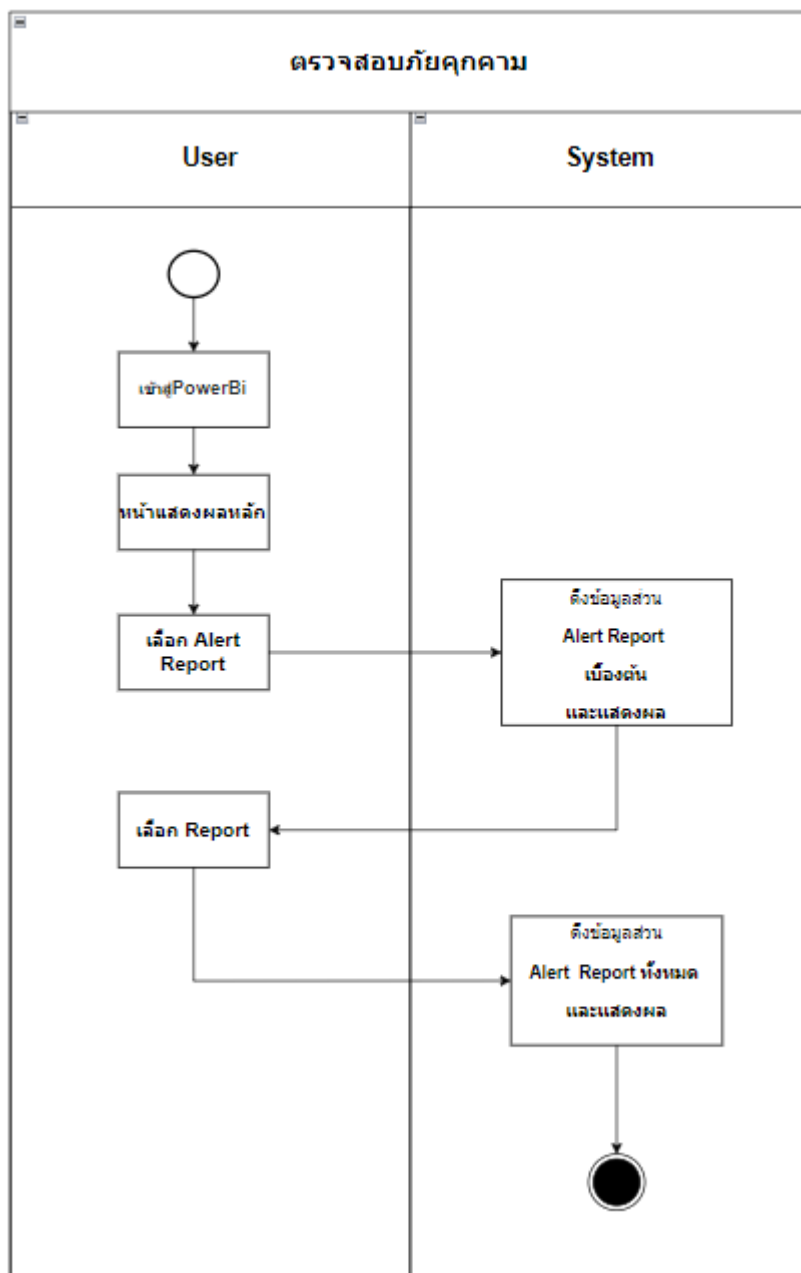
3.3.2 กระบวนการทำงานแต่ละกรณีการใช้งานของระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)

3.3.2.1 การตรวจสอบสถานะเครื่องที่ใช้งาน



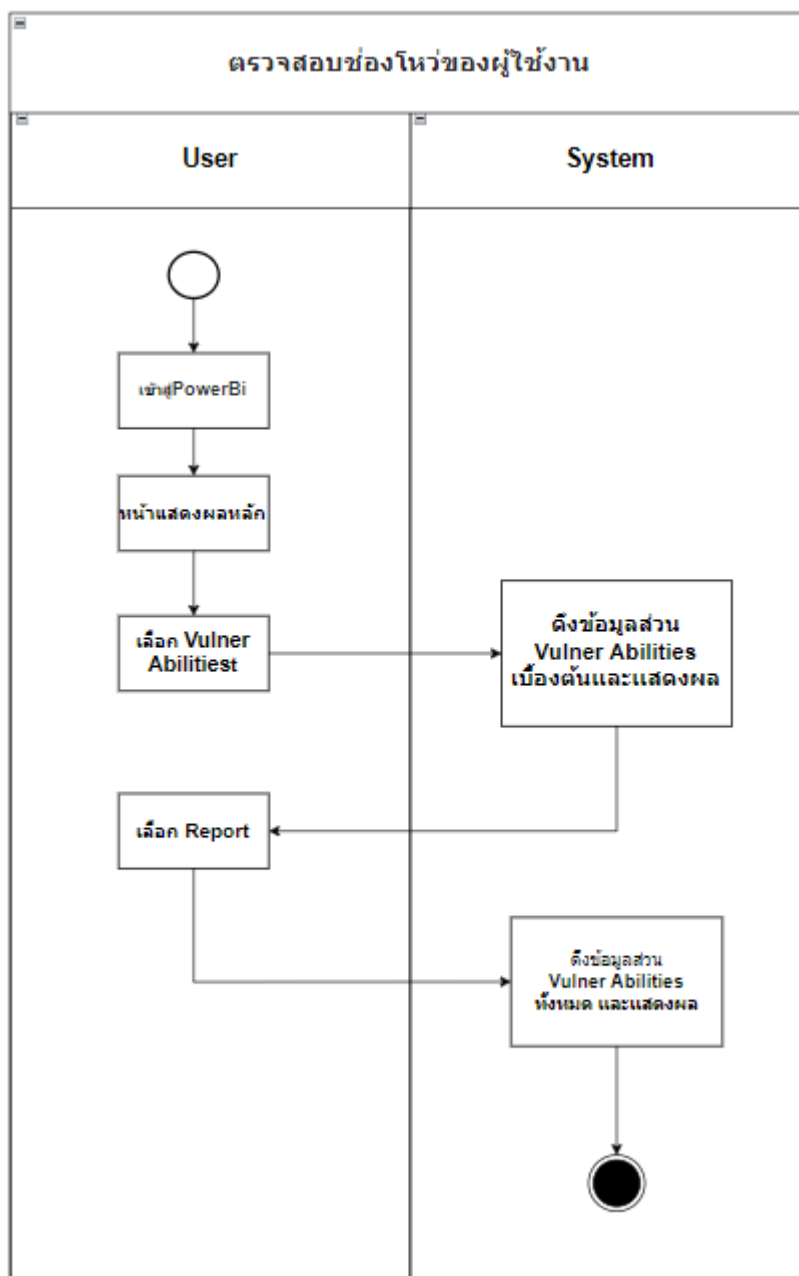
ภาพที่ 3.3 แผนภาพแอคทिवิตีตรวจสอบสถานะเครื่องที่ใช้งาน

3.3.2.2 การตรวจสอบภัยคุกคาม



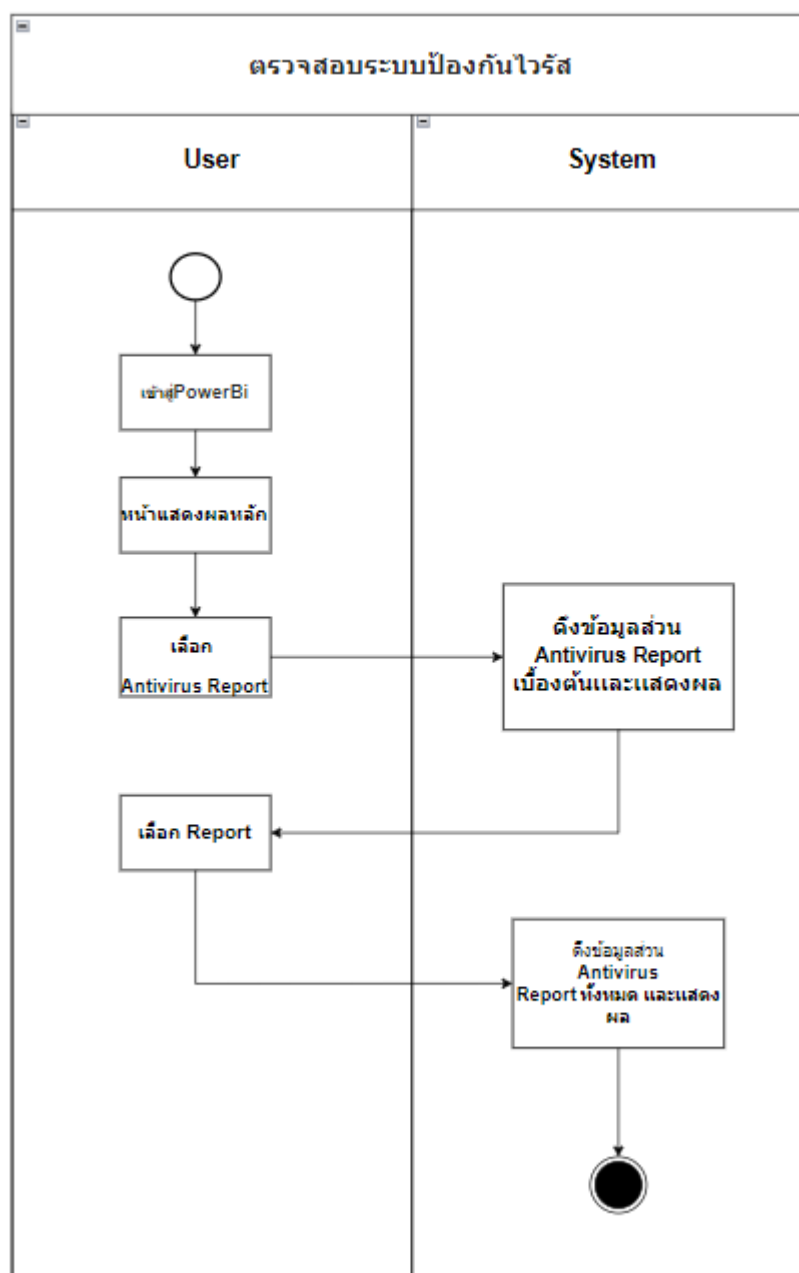
ภาพที่ 3.4 แผนภาพแอคทีวิตีตรวจสอบภัยคุกคาม

3.3.2.3 การตรวจสอบช่องโหว่ของผู้ใช้งาน



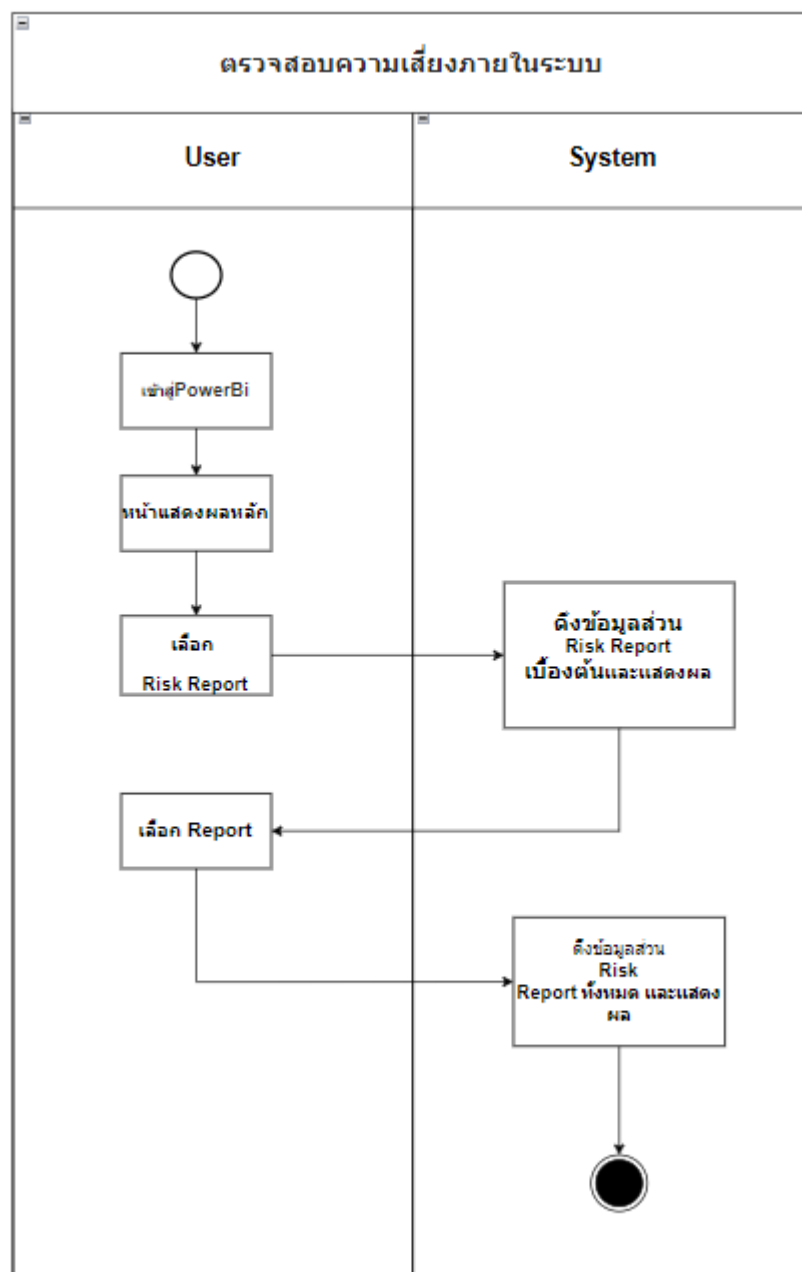
ภาพที่ 3.5 แผนภาพแอคทีวิตีตรวจสอบช่องโหว่ของผู้ใช้งาน

3.3.2.4 การตรวจสอบระบบป้องกันไวรัส



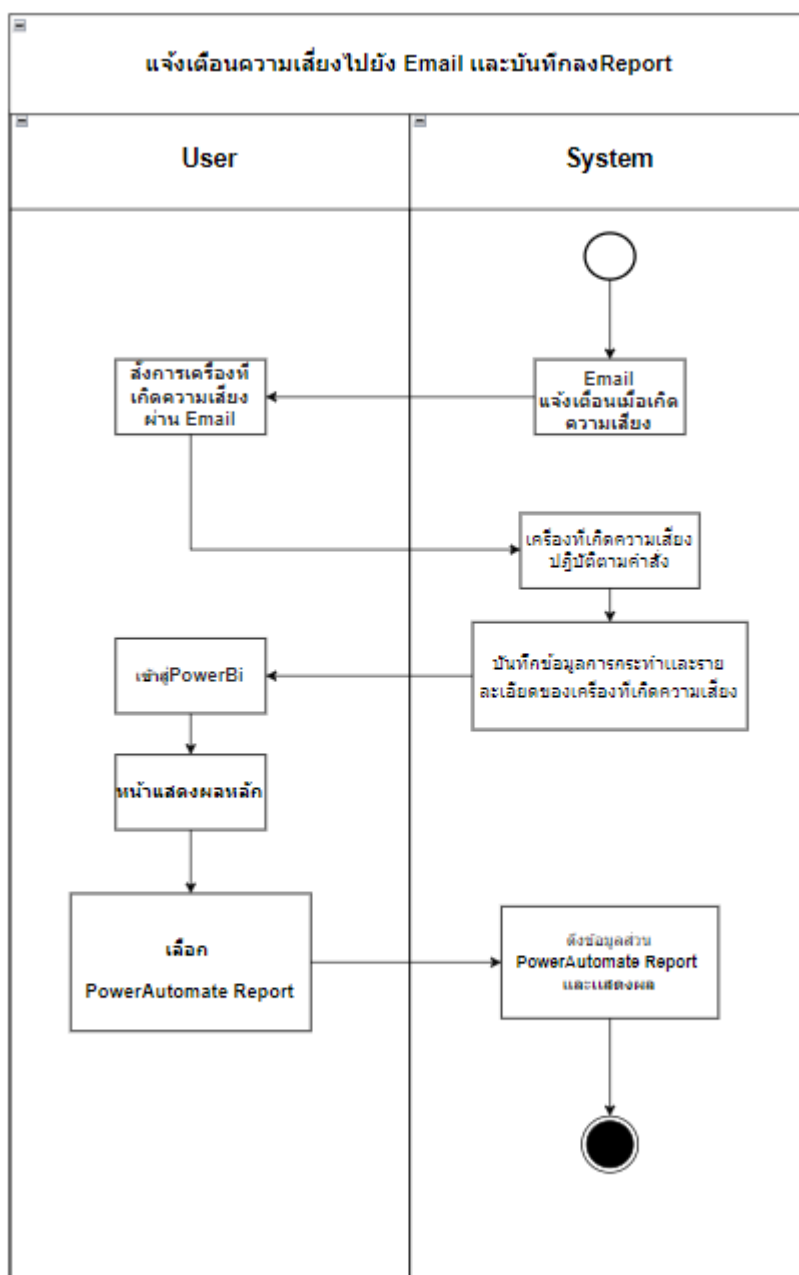
ภาพที่ 3.6 แผนภาพแอคทีวิตีตรวจสอบระบบป้องกันไวรัส

3.3.2.5 การตรวจสอบความเสี่ยงภายในระบบ



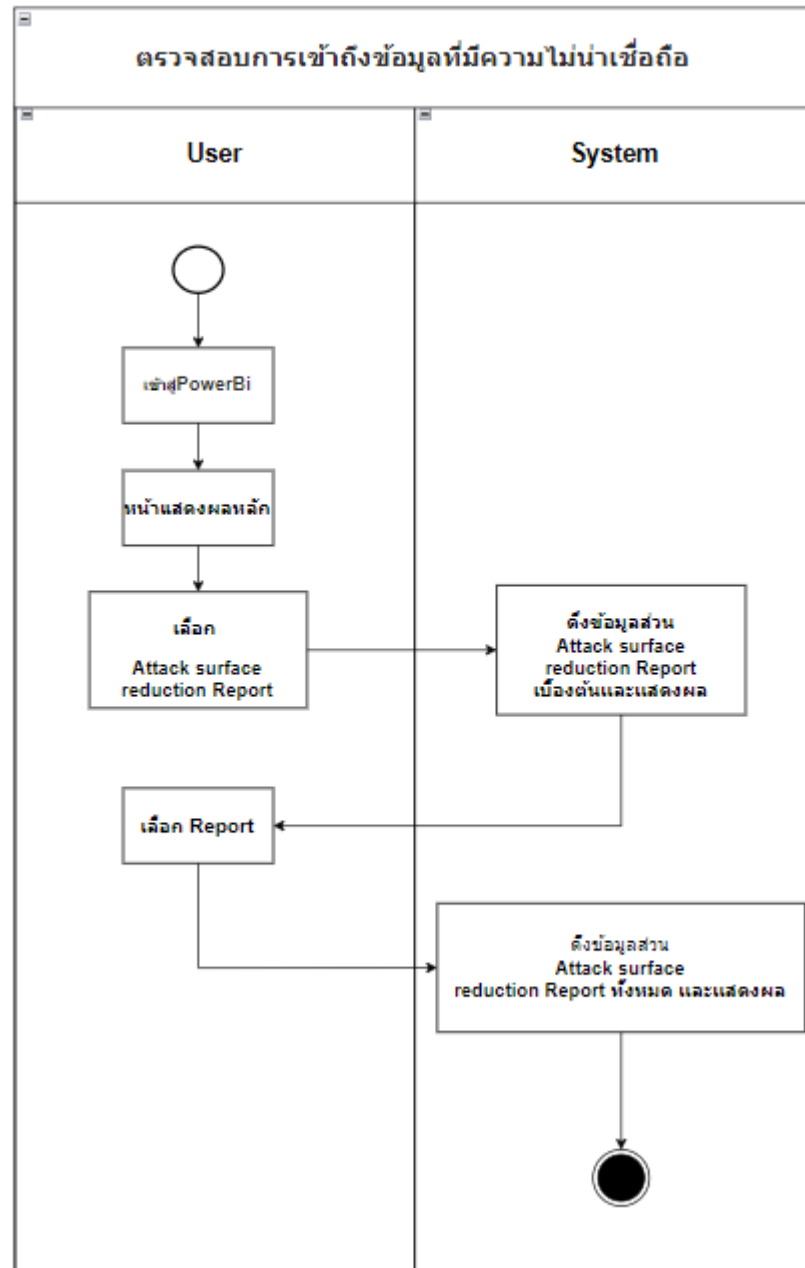
ภาพที่ 3.7 แผนภาพแอคทีวิตีตรวจสอบความเสี่ยงภายในระบบ

3.3.2.6 การแจ้งเตือนความเสี่ยงไปยังอีเมล(Email)และบันทึกลงระบบ



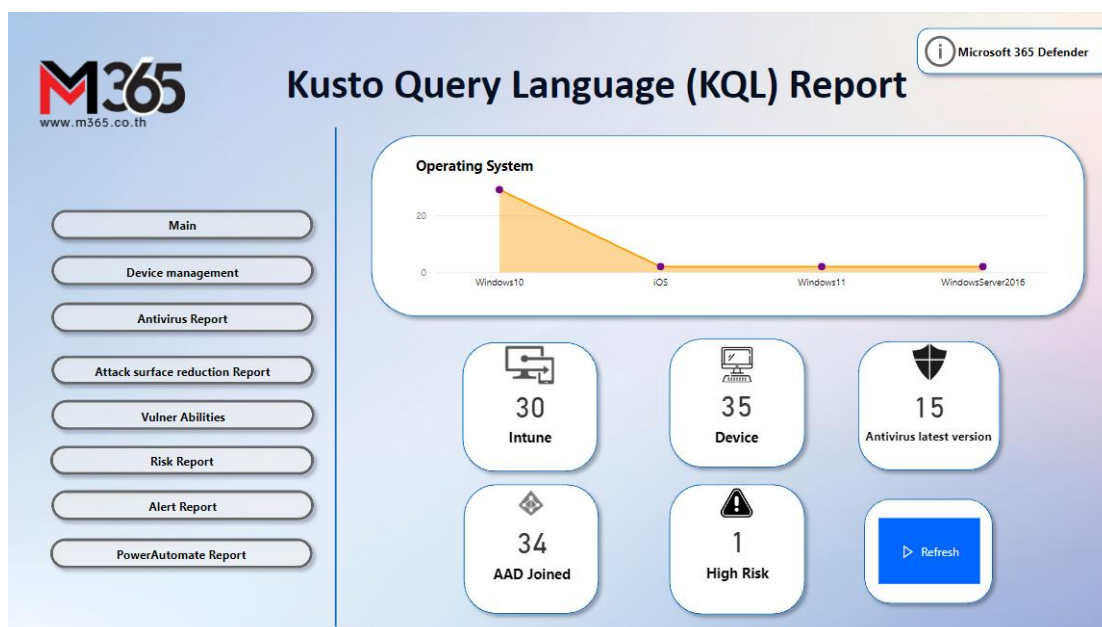
ภาพที่ 3.8 แผนภาพแอคทีวิตี้แจ้งเตือนความเสี่ยงไปยังอีเมล(Email)และบันทึกลงระบบ

3.3.2.7 การตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ



ภาพที่ 3.9 แผนภาพแอคทิวิตี้ตรวจสอบการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ

3.4 การออกแบบส่วนต่อประสานของระบบ



ภาพที่ 3.10 หน้าการใช้งานหลัก

หน้าการใช้งานหลัก โดยจะมีการแสดงข้อมูลของเครื่องที่ ถูกตั้งค่ากลุ่มในระบบ,จำนวนเครื่อง ,เครื่องที่ระบบป้องกันไวรัสเป็นรุ่นล่าสุดแล้ว, เครื่องที่ทำการติดตั้งระบบโดเมนสร้างความน่าเชื่อถือด้วยเอเอดี(AAD joined) ,เครื่องที่มีความเสี่ยงสูง ,สามารถกดที่ ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)เพื่อเข้าสู่หน้าเว็บไซต์



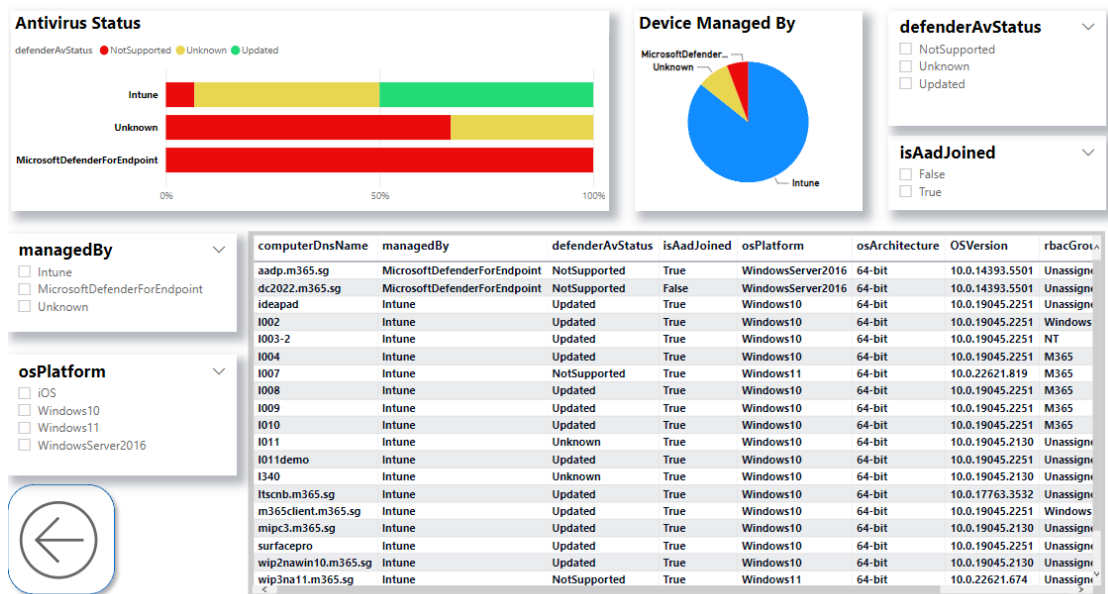
ภาพที่ 3.11 การจัดการอุปกรณ์(Device management)หน้าแสดงผลหลัก

การจัดการอุปกรณ์(Device management) หน้าแสดงผลหลักจะสามารถดูข้อมูลของเครื่องระบบที่เฉพาะเจาะจงได้ ทั้งในส่วน การจัดการโดยระบบอะไร(Device Managed By) ระบบป้องกันไวรัสมีสถานะแบบไหน(Antivirus) และมีกี่เครื่องที่ได้ทำการเข้าร่วมเอเอดี(AAD Join)

การจัดการความปลอดภัยโดยระบบอะไร(Device Managed By) เป็นความสามารถสำหรับอุปกรณ์ที่ได้รับการจัดการโดย ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender) เพื่อรับการกำหนดค่าความปลอดภัยสำหรับ Microsoft Defender

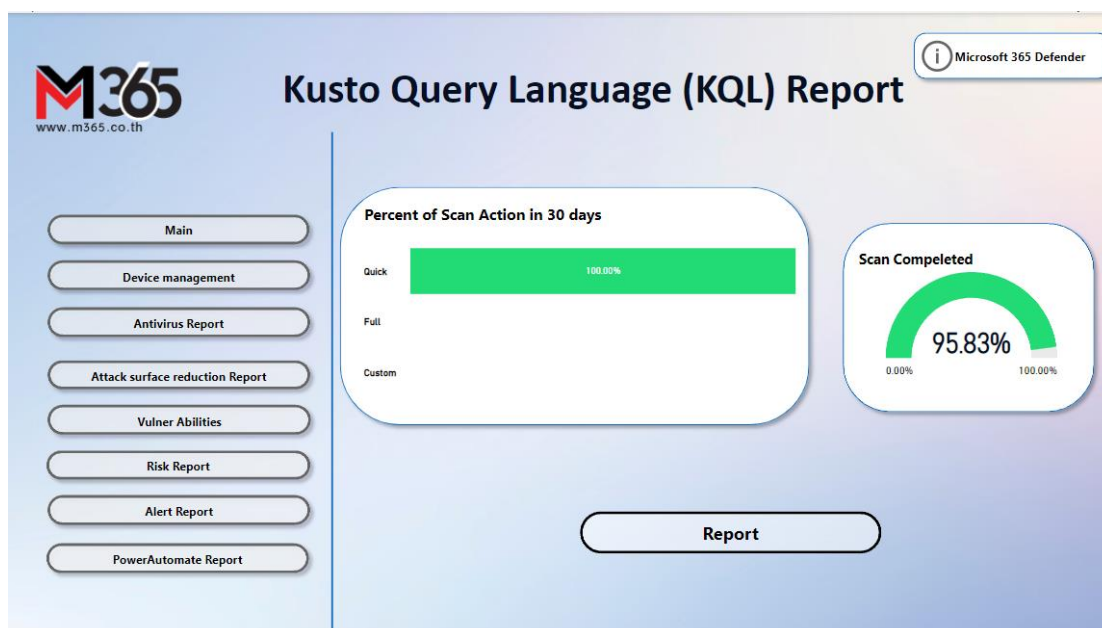
อุปกรณ์ที่เข้าร่วมโดเมนสร้างความน่าเชื่อถือด้วยเอเอดี(AAD Join) โดยเอเอดี(Azure Active Directory) สถานการณ์นี้เรียกว่าสถานการณ์จำลองการเข้าร่วมการจัดการความปลอดภัยสำหรับ ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)

สถานะของป้องกันไวรัส(Antivirus Status) คือ สถานะของ ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender) ในการ การกันมัลแวร์(AntiMalware)



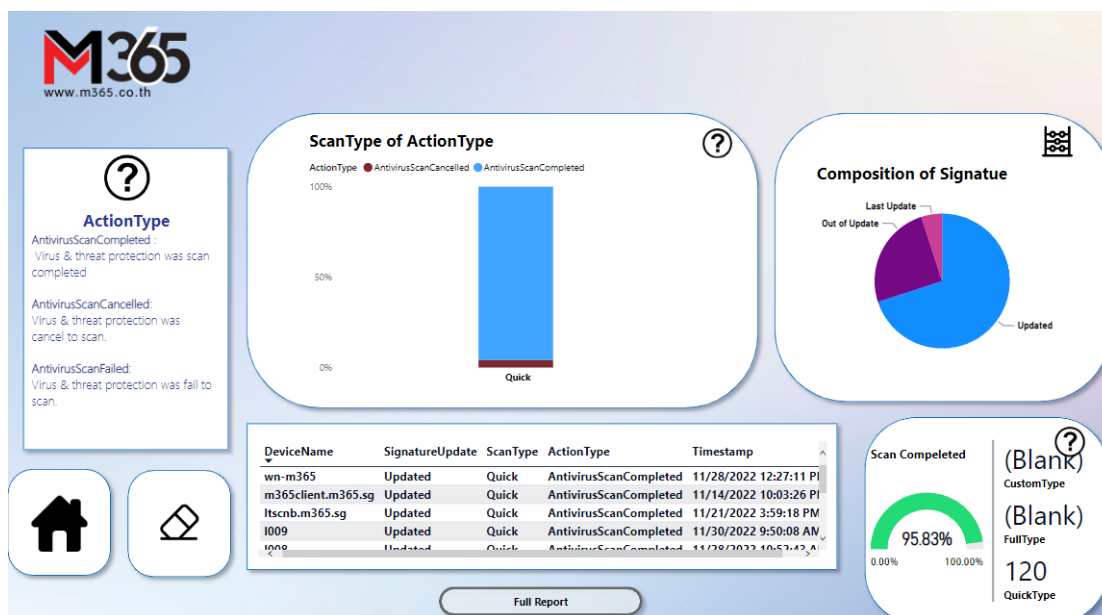
ภาพที่ 3.12 รายงานทั้งหมดของการจัดการอุปกรณ์(Device management Full Report)

รายงานทั้งหมดของการจัดการอุปกรณ์(Device management Full Report)แสดงข้อมูลในรูปแบบตาราง แล้วมีตัวเลือก(Filter)ใช้ในการแสดงข้อมูลประเภทนั้นๆ โดยกราฟที่แสดงจะมีกราฟที่แสดงข้อมูล การจัดการความปลอดภัยโดยระบบอะไร(Device Managed By) ร่วมเข้ากับ สถานะของป้องกันการกันไวรัส(Antivirus Status) และ การจัดการความปลอดภัยโดยระบบอะไร(Device Managed By) ในรูปแบบวงกลมเพิ่มเข้ามา



ภาพที่ 3.13 รายงานการป้องกันไวรัส(Antivirus Report) หน้าแสดงข้อมูลเบื้องต้น

รายงานการป้องกันไวรัส(Antivirus Report)หน้าแสดงข้อมูลเบื้องต้นการสแกนไวรัสภายใน30 วันว่าเครื่องในระบบมีการสแกน เร็ว(Quick),ทั้งหมด(Full)และ ตัวเลือก)Custom อย่างไรบ้าง

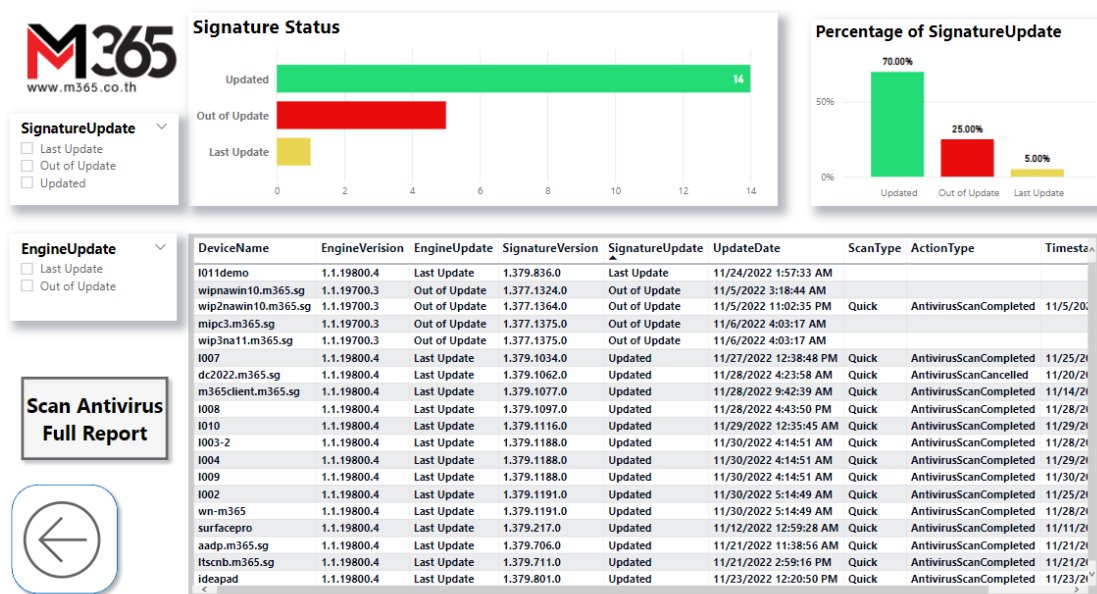


ภาพที่ 3.14 รายงานการป้องกันไวรัส(Antivirus Report)หน้าแสดงข้อมูลหลัก

รายงานการป้องกันไวรัส(Antivirus Report)หน้าแสดงข้อมูลหลักการสแกนไวรัสภายใน 30 วันว่าเครื่องในระบบมีการสแกน เร็ว(Quick),ทั้งหมด(Full)และ ตัวเลือก)Custom รวมเข้ากับรูปแบบการกระทำ(ActionType) อีกกราฟจะเป็น สถานะการป้องกัน(Signature) แสดงถึงระบบป้องกันไวรัสในเครื่องนั้นมีจำนวนเท่าไรที่ได้ทำการอัปเดต,ควรอัปเดต และ ล้าหลัง

รูปแบบการกระทำ(ActionType) มี 3 ประเภท

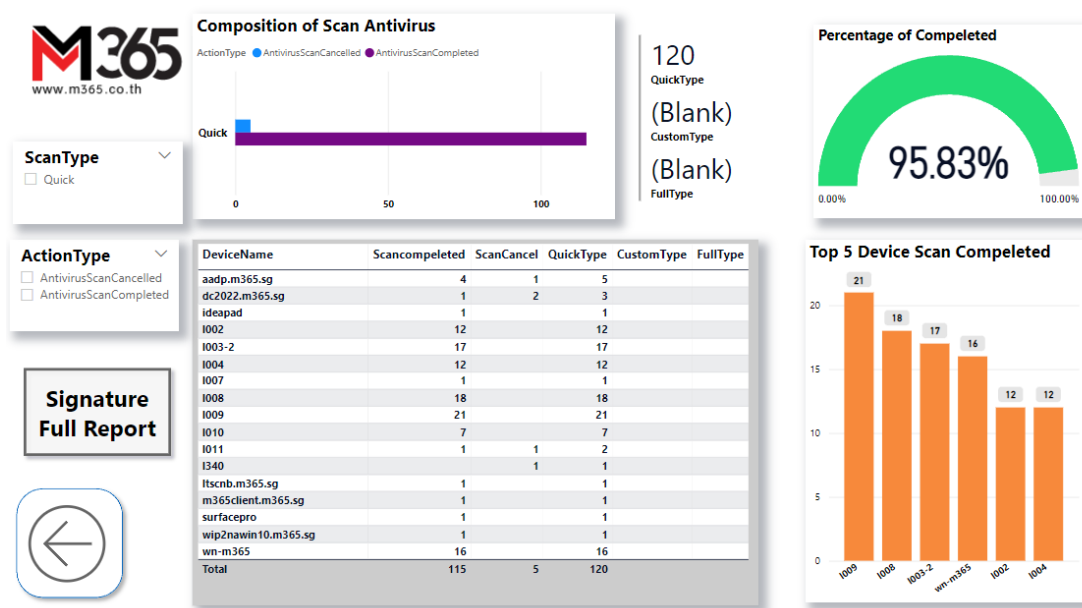
- (1)การสแกนไวรัสสำเร็จ(AntivirusScanCompleted)
- (2)การสแกนไวรัสถูกยกเลิก(AntivirusScanCancelled)
- (3)การสแกนไวรัสไม่สำเร็จ(AntivirusScanFailed)



ภาพที่ 3.15 รายงานทั้งหมดของสถานะการป้องกัน(Signature Full Report)

รายงานทั้งหมดของสถานะการป้องกัน(Signature Full Report)แสดงข้อมูลในรูปแบบตาราง และมีตัวเลือก(Filter) ใช้ในการแสดงข้อมูลประเภทนั้นๆ และตัวเลือกในการเปลี่ยนหน้าไปเป็น รายงานทั้งหมดของการป้องกันไวรัส(Scan Antivirus Full Report) โดยกราฟที่แสดงจะมี กราฟที่แสดงข้อมูล สถานะการป้องกัน(Signature) ออกมาใน2รูปแบบ

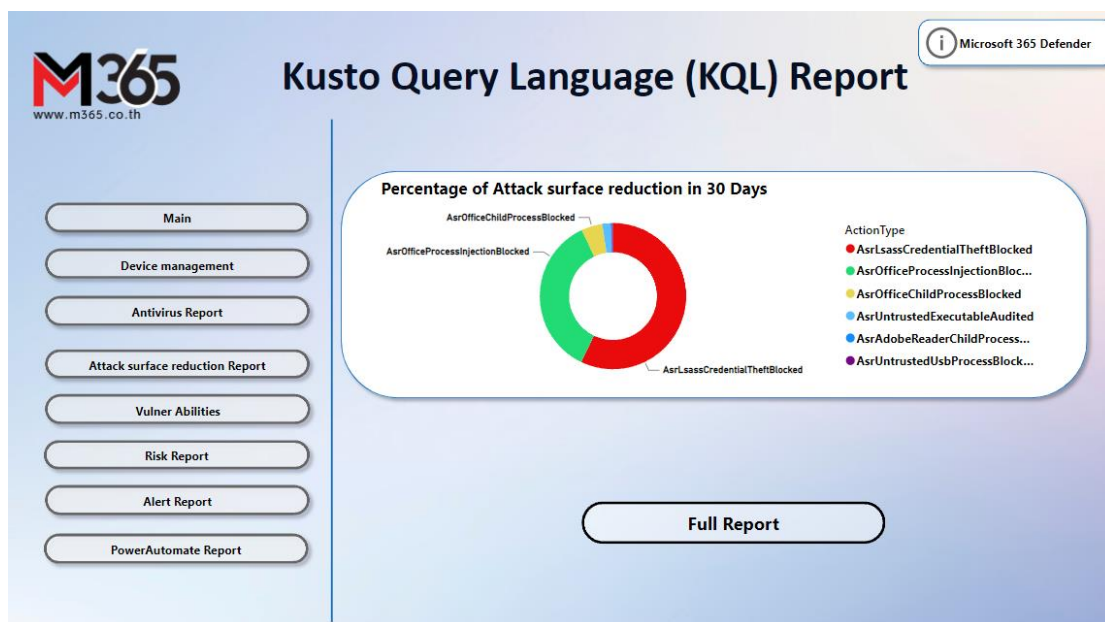
1. จำนวนแต่ละประเภท
2. เปอร์เซ็นแต่ละประเภท



ภาพที่ 3.16 รายงานทั้งหมดของการป้องกันไวรัส(Scan Antivirus Full Report)

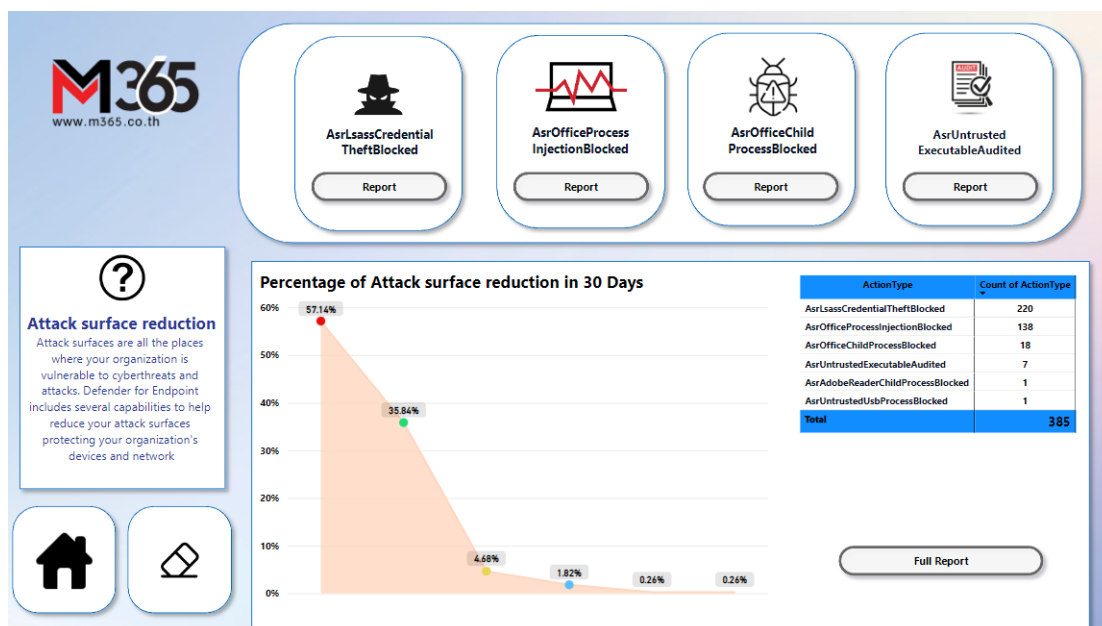
รายงานทั้งหมดของการป้องกันไวรัส(Scan Antivirus Full Report) แสดงข้อมูลในรูปแบบตาราง แล้วมีตัวเลือก(Filter) ใช้ในการแสดงข้อมูลประเภทนั้นๆและตัวเลือกในการเปลี่ยนหน้าไปเป็น รายงานทั้งหมดของสถานะการป้องกัน(Signature Full Report)โดยกราฟที่แสดงจะมี กราฟที่แสดงข้อมูล การตรวจสอบไวรัส(Scan Antivirus) ออกมาในรูปแบบ

1. จำนวนการสแกนในแต่ละประเภทที่รวมเข้ากับรวมเข้ากับรูปแบบการกระทำ (ActionType)
2. เปอร์เซ็นการสแกนสำเร็จ
3. เครื่องในระบบที่สแกนสำเร็จมากที่สุด



ภาพที่ 3.17 รายงานการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) หน้าแสดงข้อมูลเบื้องต้น

รายงานการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) หน้าแสดงข้อมูลเบื้องต้นการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือภายใน 30 วันว่าเครื่องในระบบมีสัดส่วนเปอร์เซ็นต์อย่างไรบ้าง



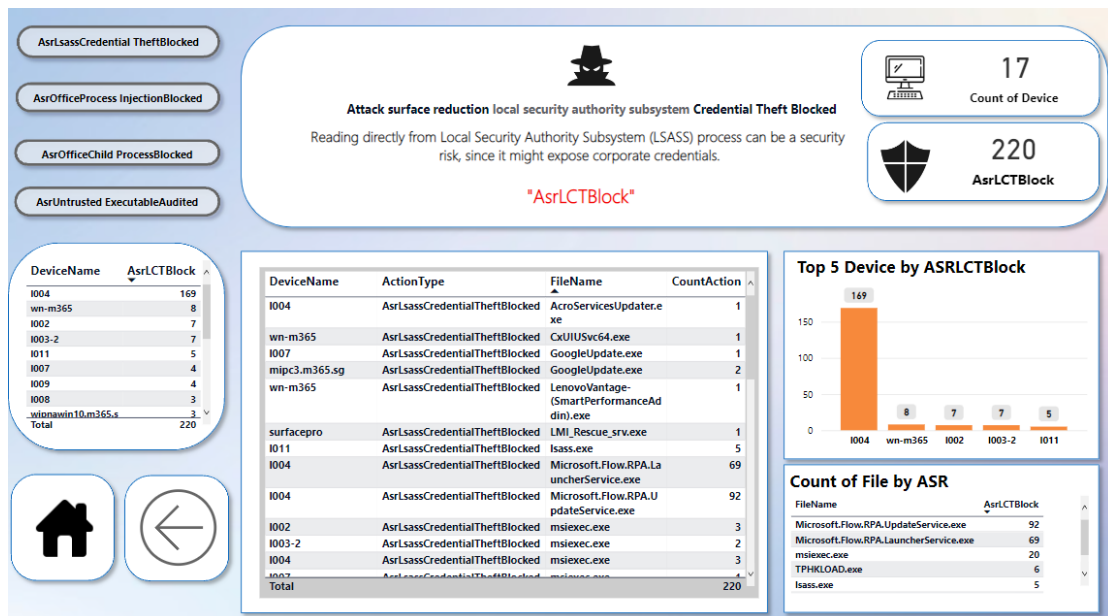
ภาพที่ 3.18 รายงานการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) หน้าแสดงข้อมูลหลัก

รายงานการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) หน้าแสดงข้อมูลหลัก หน้าแสดงข้อมูลหลักของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือภายใน 30 วันว่าเครื่องในระบบมีเข้าถึงส่วนไหนบ้าง มีการแสดงจำนวนและอัตราส่วนในรูปแบบกราฟ

การเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) คือ การใช้งานของคุณเสี่ยงต่อภัยคุกคามทางไซเบอร์และมีโอกาสถูกโจมตีได้

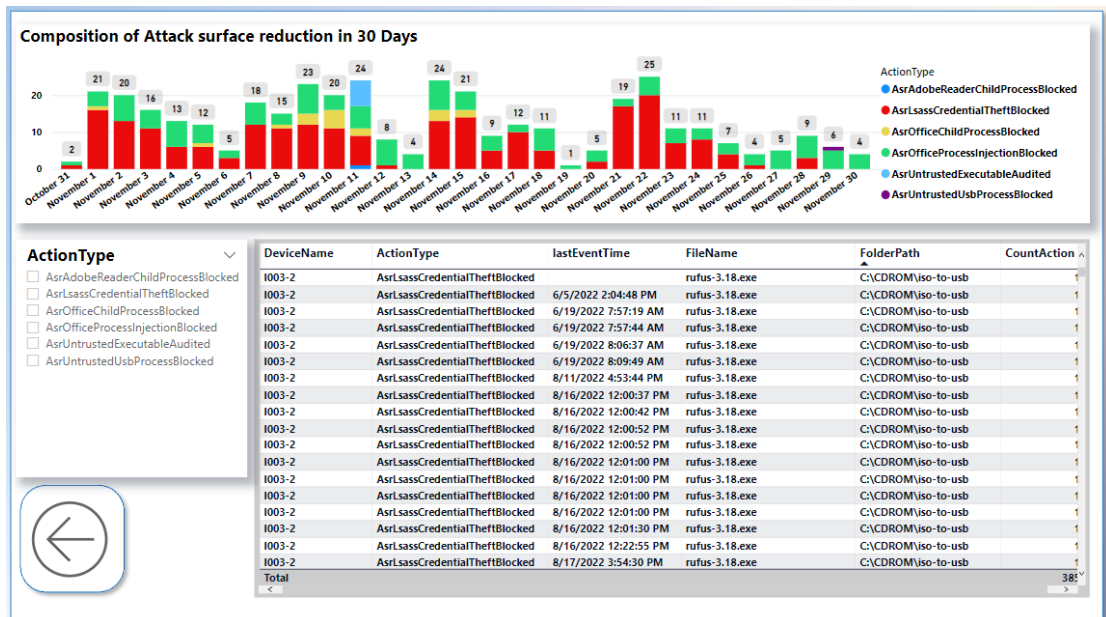
ในหน้านี้มีการเข้าถึงหน้ารายงาน 4 ประเภทที่มักเกิดขึ้นบ่อยโดย

- (1) การหยุดการโจรกรรมข้อมูล(AsrLsassCredentialTheftBlocked)
- (2) การหยุดการทำลายข้อมูล(AsrOfficeProcessInjectionBlocked)
- (3) การหยุดการเข้าถึงของมัลแวร์ (AsrOfficeChildProcessBlocked)
- (4) การตรวจสอบความไม่น่าเชื่อถือ(AsrUntrustedExecutableAudited)



ภาพที่ 3.19 ตัวอย่างหน้ารายงานแยกประเภทของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ
(Attack surface reduction)

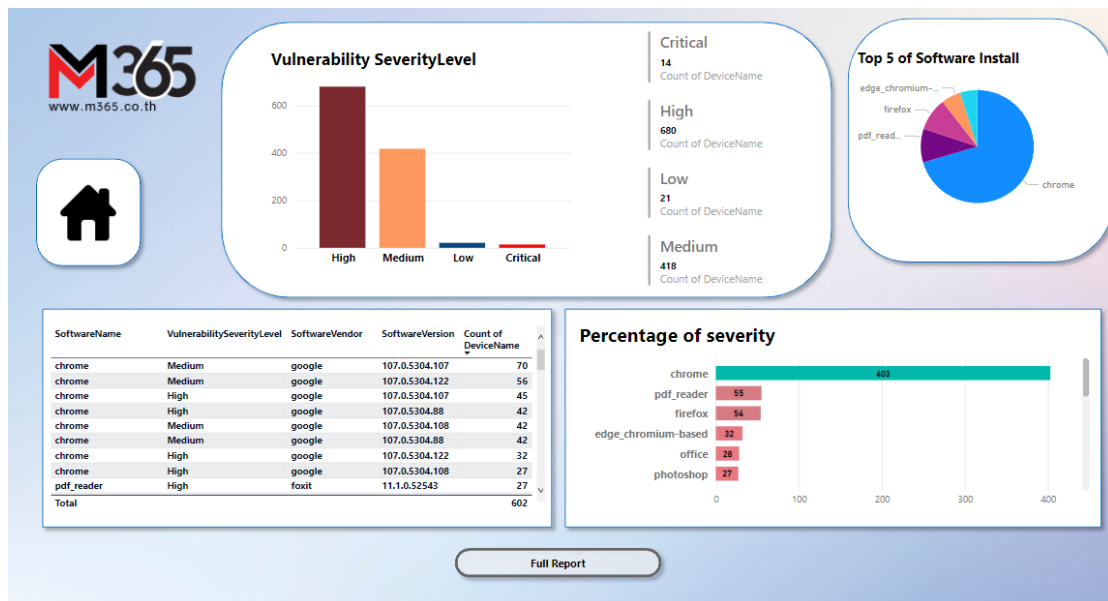
ตัวอย่างหน้ารายงานแยกประเภทของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) ที่สามารถเกิดได้บ่อยโดยมีการแสดงข้อมูลในรูปแบบตารางและกราฟจำนวนของแต่ละเครื่องในระบบที่เกิดการกระทำ,จำนวนครั้งทั้งหมดที่เกิด,โปรแกรมที่เป็นต้นเหตุ,5 อันดับที่เกิดขึ้นมากที่สุด



ภาพที่ 3.20 รายงานทั้งหมดของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ

(Attack surface reduction)

รายงานทั้งหมดของการเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction) แสดงข้อมูลในรูปแบบตาราง แล้วมีตัวเลือก(Filter) ใช้ในการแสดงข้อมูลประเภทนั้นๆ โดยกราฟที่แสดงจะมี กราฟที่แสดงข้อมูล การเข้าถึงข้อมูลที่มีความไม่น่าเชื่อถือ(Attack surface reduction)ของแต่ละวันภายใน 30 วัน

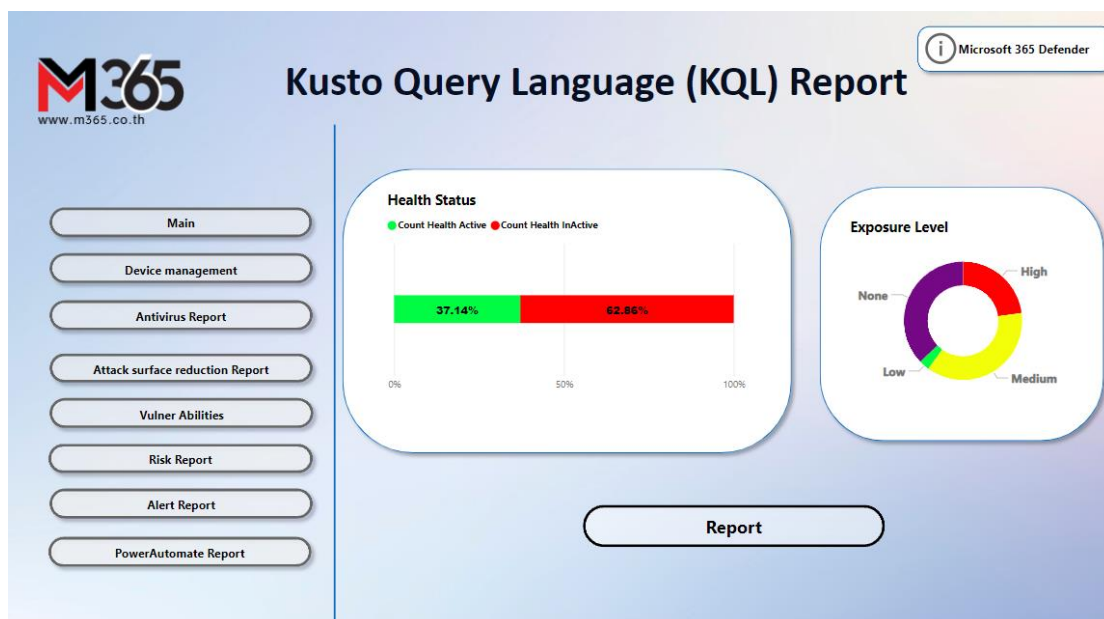


ภาพที่ 3.21 รายงานความเสี่ยงที่เกิดช่องโหว่(Vulner Abilities)

รายงานความเสี่ยงที่เกิดช่องโหว่(Vulner Abilities)หน้าแสดงข้อมูลการตรวจสอบช่องโหว่ของผู้ใช้งาน ภายใน 30 วันว่าเครื่องในระบบมีช่องโหว่ส่วนไหนบ้างแสดงข้อมูลในรูปแบบตาราง และ มีการแสดงจำนวนของแต่ละประเภทในรูปแบบกราฟ, 5 อันดับโปรแกรมที่เป็นต้นเหตุที่เกิดขึ้นมากที่สุดและโปรแกรมแต่ละโปรแกรมเกิดช่องโหว่กี่ครั้ง

รายงานทั้งหมดของความเสียหายที่เกิดช่องโหว่(Vulner Abilities Full Report)การ

ตรวจสอบช่องโหว่แสดงข้อมูลในรูปแบบตาราง ในภาพที่ใหญ่ขึ้น แล้วมีตัวเลือก(Filter) ใช้ในการแสดงข้อมูลประเภทนั้นๆ โดยกราฟที่แสดงจะมี กราฟที่แสดงข้อมูล ความเสี่ยงที่เกิดช่องโหว่(Vulner Abilities)ของแต่ละวันภายใน 30 วัน



ภาพที่ 3.23 รายงานความเสี่ยง(Risk Report)หน้าแสดงข้อมูลเบื้องต้น

รายงานความเสี่ยง(Risk Report)หน้าแสดงข้อมูลเบื้องต้น หน้าแสดงข้อมูลเบื้องต้นการตรวจสอบความเสี่ยงภายใน30 วันว่าเครื่องในระบบมีสัดส่วนเปอร์เซ็นต์ของเครื่องที่เปิด/ปิดระบบป้องกัน และ อัตราส่วนความร้ายแรงที่เกิดขึ้นกับเครื่องให้ระบบ



ภาพที่ 3.24 รายงานความเสี่ยง(Risk Report)หน้าแสดงข้อมูล หน้าแสดงข้อมูลหลัก

รายงานความเสี่ยง(Risk Report)หน้าแสดงข้อมูล หน้าแสดงข้อมูลหลัก ของการเข้าถึงข้อมูลที่มีความความเสี่ยงภายใน30 วัน แสดงให้เห็นว่า เครื่องในระบบมีเข้าถึงส่วนไหนบ้าง มีการแสดงจำนวนและอัตราส่วนในรูปแบบกราฟว่าเครื่องที่เปิด/ปิดระบบป้องกันอย่างไรบ้าง, อัตราส่วนความร้ายแรง และ คะแนนความเสี่ยง โดย

คะแนนความเสี่ยง(Exposure Level)จะมองเห็นโดย ไมโครซอฟต์เฟนเดอร์365(Microsoft 365 Defender) ซึ่งสะท้อนให้เห็นว่าองค์กรของคุณมีความเสี่ยงต่อภัยคุกคามความปลอดภัยทางไซเบอร์มากน้อยเพียงใด

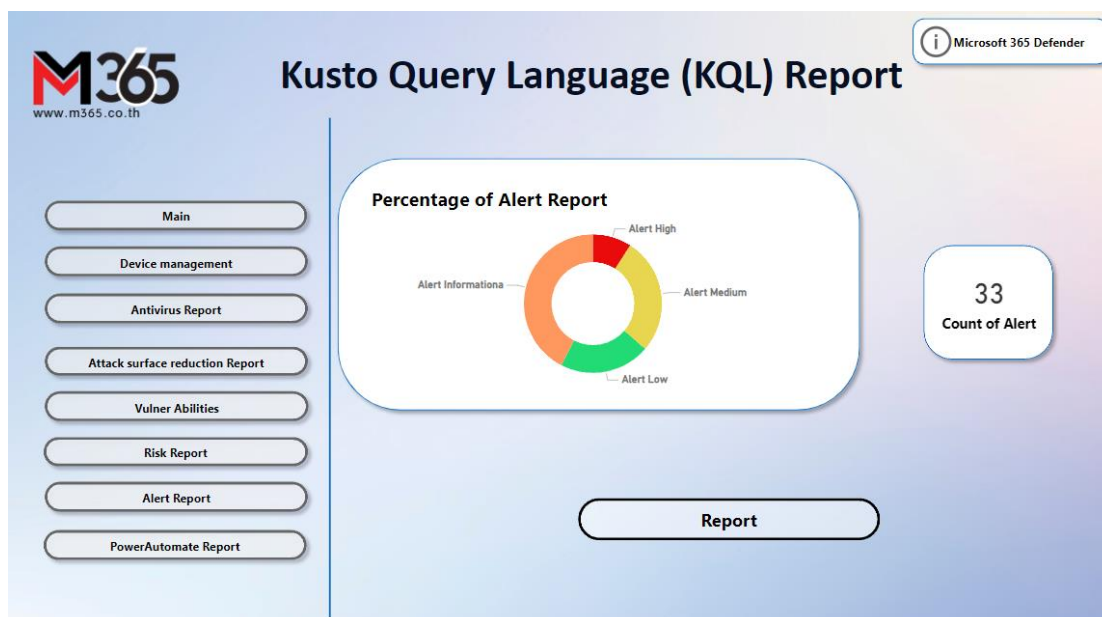
สถานะอุปกรณ์ที่มีปัญหาเกี่ยวกับเซ็นเซอร์(Health Status) ให้ข้อมูลเกี่ยวกับความสามารถของอุปกรณ์แต่ละเครื่องในการให้ข้อมูลและสื่อสารกับบริการ ไมโครซอฟต์เฟนเดอร์365(Microsoft 365 Defender)

คะแนนความเสี่ยง(RiskScore)ของอุปกรณ์ตามกลไกต่างๆ คะแนนนี้มีไว้เพื่อวัดระดับความเสี่ยงของเครื่อง ซึ่งบ่งชี้ถึงโอกาสที่ได้รับการโจมตี



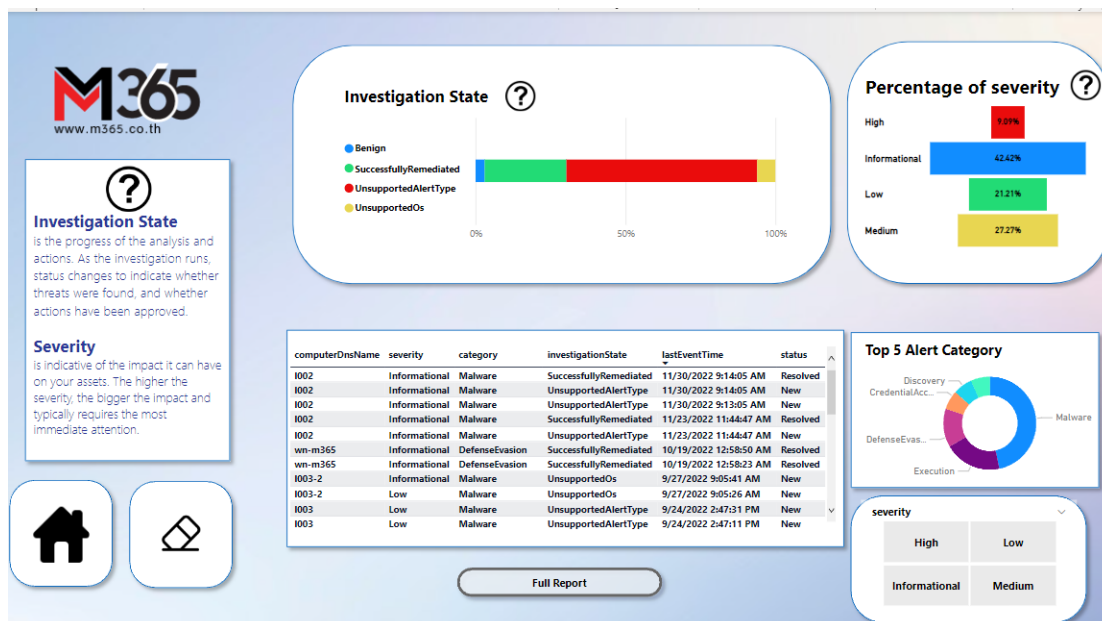
ภาพที่ 3.25 รายงานทั้งหมดของความเสี่ยง(Risk Full Report)

รายงานทั้งหมดของความเสี่ยง(Risk Full Report) การตรวจสอบช่องโหว่แสดงข้อมูลในรูปแบบตาราง ในภาพที่ใหญ่ขึ้น แล้วมีตัวเลือก Filter ใช้ในการแสดงข้อมูลประเภทนั้นๆ โดยกราฟที่แสดงจะมี กราฟที่แสดงข้อมูล เครื่องที่เปิด/ปิดระบบป้องกันอย่างไรบ้างรวมเข้ากับอัตราส่วนความร้ายแรง ภายใน 30 วัน



ภาพที่ 3.26 รายงานการแจ้งเตือนภัยคุกคาม(Alert Report)หน้าแสดงข้อมูลเบื้องต้น

รายงานการแจ้งเตือนภัยคุกคาม(Alert Report)หน้าแสดงข้อมูลเบื้องต้นการตรวจสอบภัยคุกคามภายใน30 วันว่าเครื่องในระบบมีสัดส่วนเปอร์เซ็นต์ของประเภทของภัยคุกคามและจำนวนทั้งหมดที่เกิดขึ้น

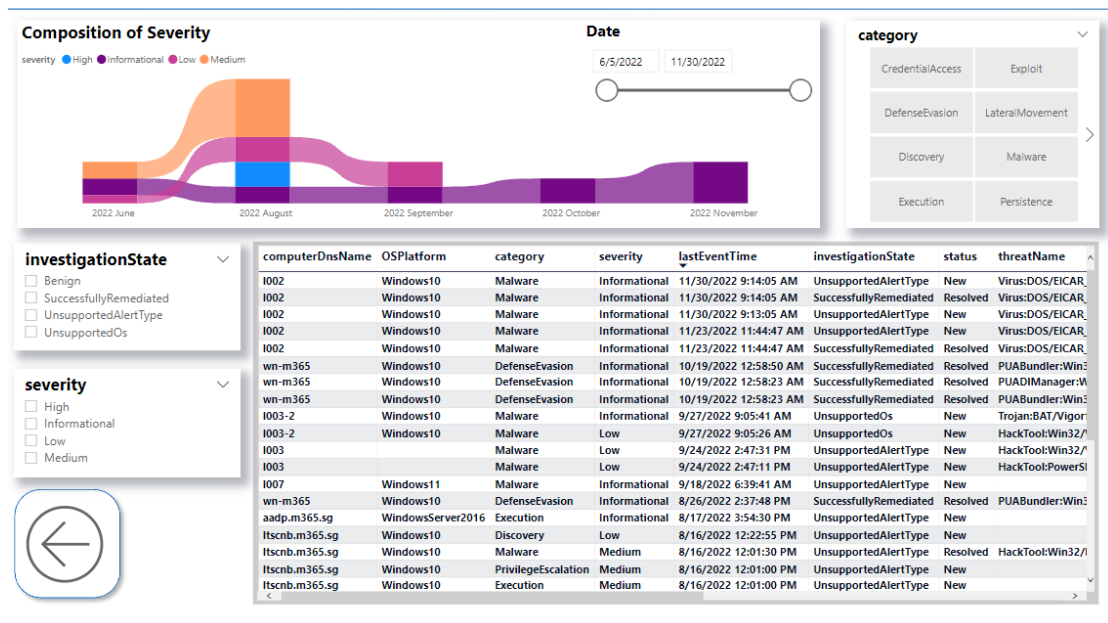


ภาพที่ 3.27 รายงานการแจ้งเตือนภัยคุกคาม(Alert Report)หน้าแสดงข้อมูลหลัก

รายงานการแจ้งเตือนภัยคุกคาม(Alert Report)หน้าแสดงข้อมูลหลักของการเกิดของภัยคุกคามภายใน 30 วัน แสดงให้เห็นว่า เครื่องในระบบมีการเกิดระดับไหนบ้าง และอัตราส่วนของความรุนแรงในรูปแบบกราฟว่าภัยคุกคามที่เกิดขึ้นมีเท่าไร และ 5 อันดับประเภทภัยคุกคามที่เกิดขึ้นบ่อย โดย

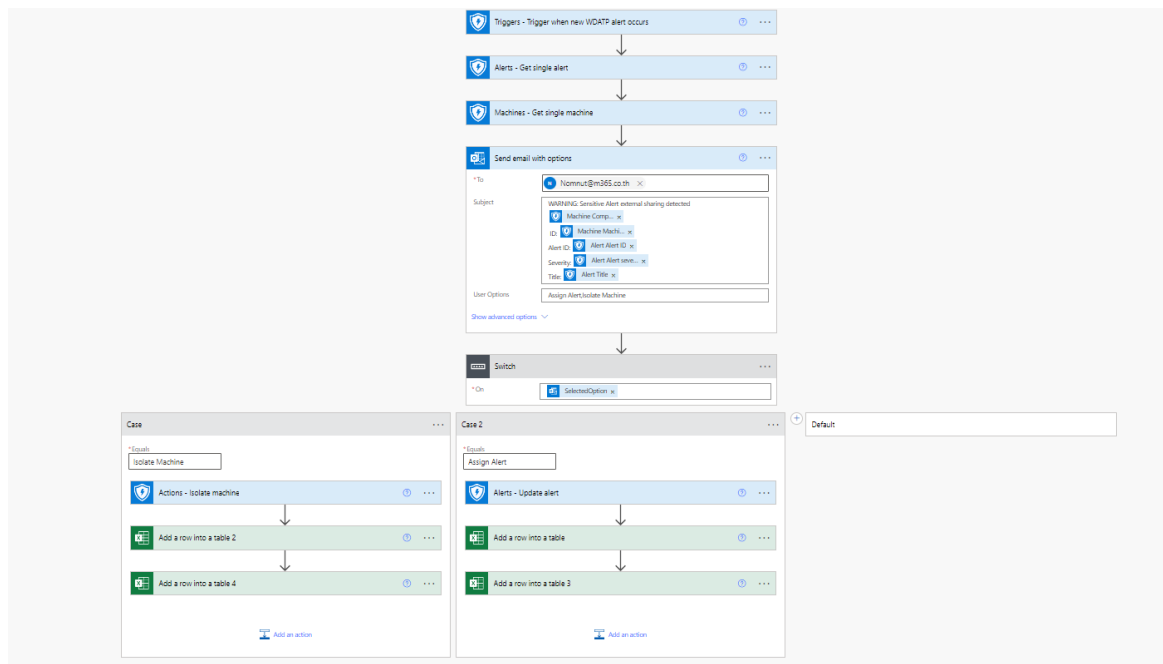
การตรวจสอบสถานะ(Investigation State)เพื่อระบุว่าพบภัยคุกคามหรือไม่ และการดำเนินการได้รับการอนุมัติหรือไม่

ความรุนแรง(Severity) แสดงถึงผลกระทบก็จะใหญ่ระดับไหนอย่างไรได้รับการดูแลหรือไม่



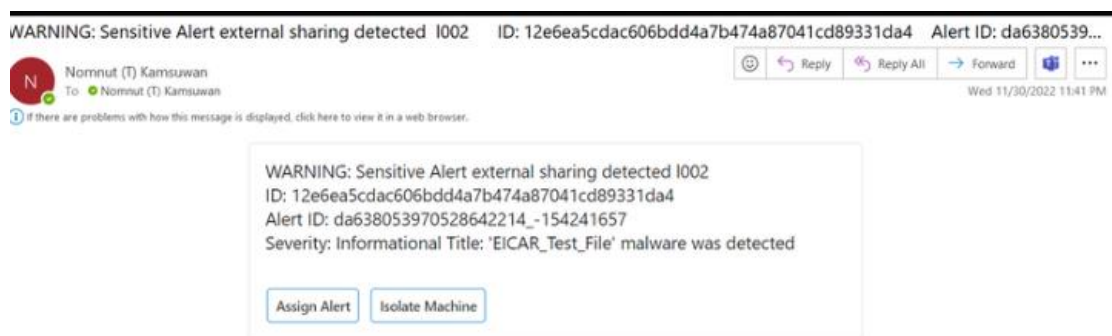
ภาพที่ 3.28 รายงานทั้งหมดของการแจ้งเตือนภัยคุกคาม(Alert Full Report)

รายงานทั้งหมดของการแจ้งเตือนภัยคุกคาม(Alert Full Report)แสดงข้อมูลในรูปแบบตาราง แล้วมีตัวเลือก(Filter) ใช้ในการแสดงข้อมูลประเภทนั้นๆ โดยกราฟที่แสดงจะมี กราฟที่แสดงความรุนแรงที่เกิดขึ้นเข้ากับวัน/เดือน/ปี



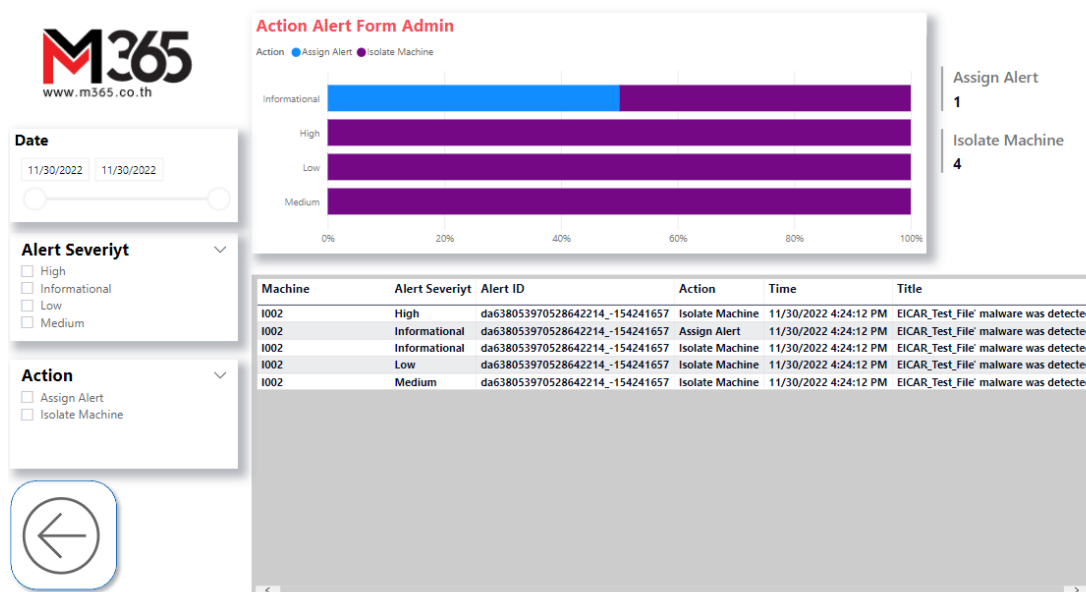
ภาพที่ 3.29 ระบบแจ้งเตือนความเสี่ยงไปยังอีเมล(Email)

ระบบแจ้งเตือนความเสี่ยงไปยัง อีเมล(Email) ทำงานโดยเมื่อเกิดความเสี่ยงขึ้นจะทำการนำรหัสความเสี่ยงไปเทียบกับรหัสเครื่องผู้ใช้งานในระบบ โดยคำสั่งของผู้ดูแลระบบและรายละเอียดความเสี่ยงจะถูกบันทึกลงใน เอ็กเซลออนไลน์(Excel Online)



ภาพที่ 3.30 อีเมล(Email)แจ้งเตือนถึงผู้ดูแลระบบ

อีเมล(Email)แจ้งเตือนถึงผู้ดูแลระบบว่าความเสี่ยงที่ได้ขึ้นมีรายละเอียดเป็นอย่างไร โดยแสดงรหัสของความเสี่ยงที่เกิดและประเภทของความเสี่ยง โดยผู้ดูแลระบบสามารถสั่งการว่าจะ รับทราบความเสี่ยงที่เกิดขึ้น หรือ สั่งระงับเครื่องที่เกิดความเสี่ยง



ภาพที่ 3.31 รายงานการเก็ยคำสั่งของพาวเวอร์ออโต้เมท(PowerAutomate Report)

รายงานการเก็ยคำสั่งของพาวเวอร์ออโต้เมท(PowerAutomate Report)หน้าแสดงข้อมูลการสั่งการจาก อีเมล(Email) ที่แจ้งเตือนไปยังผู้ดูแลระบบโดยว่าผู้ดูแลได้สั่งการไปยังเครื่องที่เกิดความเสี่ยงอย่างไร

3.5 ประเด็นที่น่าสนใจและสิ่งที่ท้าทาย

ประเด็นที่น่าสนใจ

-การตรวจสอบระบบความปลอดภัยและสถานะของเครื่องคอมพิวเตอร์ภายในระบบขององค์กรได้อย่างง่ายดายและครบถ้วนโดยผู้ใช้งานไม่ต้องมีความรู้ด้าน เคคิวแอล(KQL)

-ระบบการแจ้งเตือนเมื่อเกิดความเสี่ยงให้กับผู้ดูแลระบบให้สามารถจัดการปัญหาเฉพาะหน้าได้

สิ่งที่ท้าทาย

-การแสดงผลข้อมูลระบบความปลอดภัยได้อย่างครบถ้วนและใช้งานได้ง่าย

-การออกแบบส่วนที่เชื่อมต่อระหว่างผู้ใช้งานกับระบบ(UX/UI) ที่ใช้งานง่ายทุกคนสามารถใช้งานได้

ตารางที่ 4.1 แผนการดำเนินงาน(ต่อ)

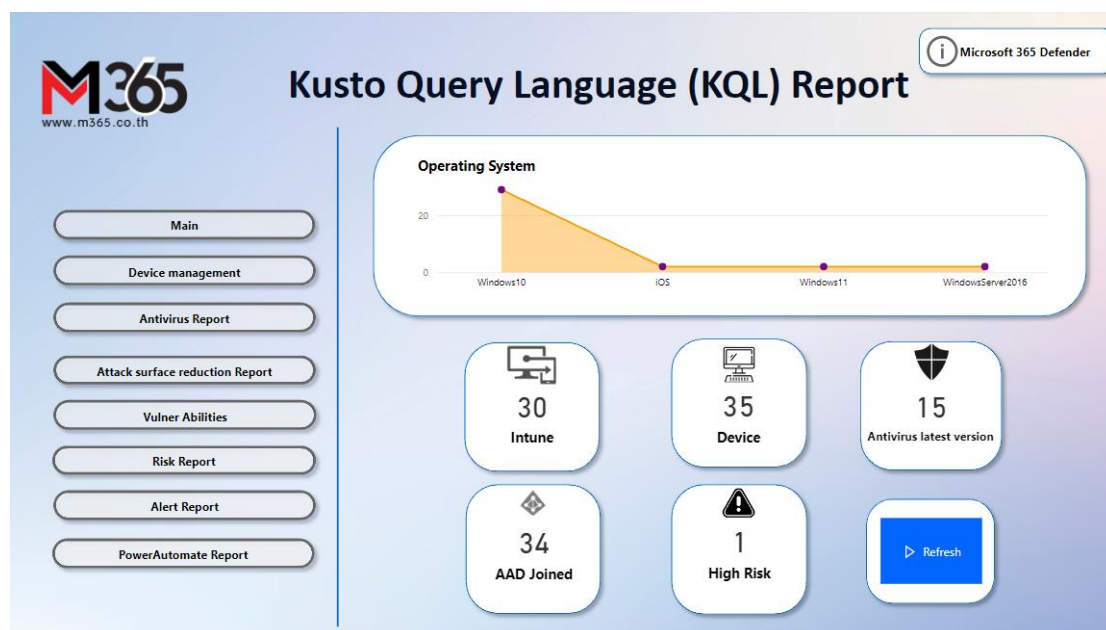
กิจกรรม/ขั้นตอน	มิ.ย. 65					ก.ค. 65					ส.ค. 65					ก.ย. 65					ต.ค.65					พ.ย. 65				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	1	2	3	4	5	
15.แก้ไขระบบการส่งแจ้งเตือน																														
16.ศึกษาการใช้โอดาต้า (OData) ในการดึงข้อมูลเอพียู(API)																														
17.ประชุมในสถานที่กับทีมที่ทำงาน และรับคำแนะนำไปปรับปรุงตัวงาน																														
18.ออกแบบหน้าแสดงผลการสั่งการจากเครื่องของผู้ดูแลระบบ																														
19.การทำการทดสอบ																														
20.การทำแบบสำรวจการใช้งาน																														
21.จัดทำเอกสารโครงการ																														

4.2 ข้อเสนอแนะ/ปรับปรุงในอนาคต

ถ้าต้องปรับปรุงตัวโครงการในครั้งนี้ จุดที่ต้องการแก้ไขจะอยู่ในเรื่องการออกแบบเพราะเพราะเรื่องรูปร่างในการใช้งานก็เป็นเรื่องสำคัญ ไม่น้อยไปกว่าข้อมูลภายในที่ดี และช่วงแรกอาจเน้นเรื่องการทำความเข้าใจกับตัวข้อมูลก่อนทำการดึง เพราะ ช่วงแรกนั้นมีการดึงข้อมูลที่ไม่จำเป็นมามากเกินไปแล้วลองกับข้อมูลพื้นฐานเลย จึงทำให้เกิดระบบที่ไม่ได้มาตรฐานแล้วสุดท้ายก็ต้องกลับมาแก้ไขใหม่ และลองเครื่องมือใหม่ๆ เยอะๆ เพราะในการทำโครงการครั้งนี้ช่วงแรกใช้แค่KQL อย่างเดียวข้อมูลจึงไม่มีความหลากหลาย

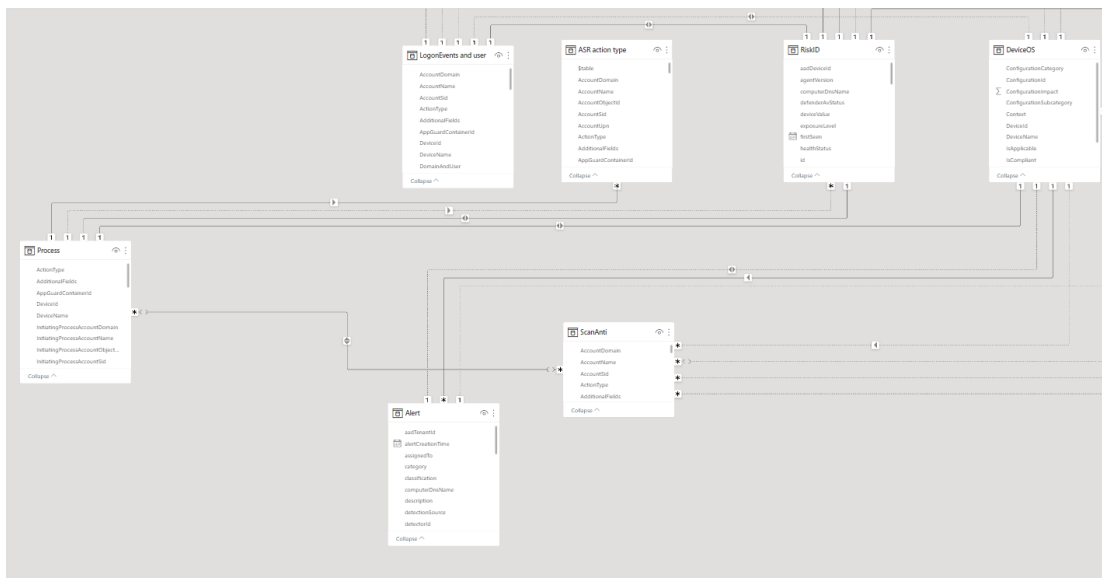
4.3 ผลการดำเนินงาน

- ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL)
- เชื่อมต่อระหว่างผู้ใช้งานกับระบบ(User interface)
- การเชื่อมต่อข้อมูลเข้ากับฐานข้อมูล



ภาพที่ 4.1 ผลการดำเนินงานการเชื่อมต่อระหว่างผู้ใช้งานกับระบบ(User interface)

ภาพที่ 4.1 ผลการดำเนินงานการเชื่อมต่อระหว่างผู้ใช้งานกับระบบ(User interface)คือ ออกแบบประสบการณ์ผู้ใช้(UX/UI) โดยได้ทำการใช้โปรแกรม พาวเวอร์บีไอ(Power Bi)ในการออกแบบเพื่อให้ผู้ใช้งานได้เห็นภาพที่ชัดเจนกับแอปพลิเคชันจริงมากที่สุด ดังภาพ โดยระบบจะมีรูปแบบที่เรียบง่ายตรงไปตรงมาทุกคนสามารถใช้งานได้ง่ายแม้จะไม่มีความรู้ด้านงานใช้ ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)เนื่องจาก การเชื่อมต่อระหว่างผู้ใช้งานกับระบบ(User interface) ที่ค่อนข้างชัดเจน



ภาพที่ 4.2 ผลการดำเนินงาน การเชื่อมต่อข้อมูลเข้ากับฐานข้อมูล

ภาพที่ 4.2 ผลการดำเนินงานของ การเชื่อมต่อข้อมูลเข้ากับฐานข้อมูล คือ การดำเนินงานภายใน พาวเวอร์บีไอ(Power Bi)จะมีการใช้เคคิวแอล(KQL) สำหรับการพัฒนาร่วมกับ โอดาต้า(OData) ให้สามารถเชื่อมต่อกับ เอพีไอ(API) ของ ไมโครซอฟต์ดีเฟนเดอร์365(Microsoft 365 Defender)ในการดึงข้อมูลด้านความปลอดภัย

4.4 ผลการทดสอบ

การทดสอบโครงการ

4.3.1 ทดสอบว่าผู้ใช้งานของแอปพลิเคชันนั้นจะสามารถใช้งานได้ง่ายและเต็มประสิทธิภาพหรือไม่ (Usability Testing)

4.3.2 ทดสอบว่าระบบนั้นสามารถทำงานตรงตามคำสั่งหรือไม่ และเชื่อมต่อเข้ากับระบบได้มีประสิทธิภาพแค่ไหน และตรวจสอบว่าเชื่อมต่อกับฐานข้อมูลได้(Functional Testing)

4.4.1 ผลการสำรวจความพึงพอใจจากผู้ใช้งานแอปพลิเคชัน

ระดับคะแนน แบ่งออกเป็น 3 ระดับ

คือ ดี (2.5 - 3) ผ่าน (1.5 - 2.4) ต้องปรับปรุง (น้อยกว่า 1.4)

โดยคะแนนอ้างอิงจาก

- (1) รายงานตรวจสอบข้อมูลที่ครบถ้วน
- (2) หน้าตารายงานที่สวยงาม
- (3) หน้าตารายงานที่เข้าใจได้ง่าย
- (4) ระบบการแจ้งเตือนเมื่อเกิดความเสี่ยง

ตารางที่ 4.2 ผลการสำรวจความพึงพอใจจากผู้ใช้งานแอปพลิเคชัน

หัวข้อ	คะแนนความพึงพอใจเฉลี่ย	ระดับคะแนน
รายงานตรวจสอบข้อมูลที่ครบถ้วน	2.5	ดี
หน้าตารายงานที่สวยงาม	2	ผ่าน
หน้าตารายงานที่เข้าใจได้ง่าย	2.5	ดี
ระบบการแจ้งเตือนเมื่อเกิดความเสี่ยง	3	ดี

จากตารางที่ 4.2 ผลการสำรวจความพึงพอใจจากผู้ใช้งานแอปพลิเคชัน ผู้ใช้งานนั้นมีความพึงพอใจในด้านการแสดงผลอยู่ระดับที่ผ่านถึงดี เช่น ใช้งานง่ายไม่ซับซ้อน หน้าตาแอปพลิเคชันที่สวยงาม การแสดงผลที่เป็นระเบียบและเข้าใจง่าย แต่อาจมีสีที่มากเกินไป ด้านระบบการเชื่อมต่อเข้ากับฐานเก็บข้อมูลสามารถเชื่อมต่อได้อยู่ในระดับดี เช่น ดึงข้อมูลได้ครบถ้วนและรวดเร็ว

บทที่ 5

สรุปผลการปฏิบัติสหกิจ

จากการที่ได้ไปฝึกงาน ปฏิบัติสหกิจและได้เรียนรู้งานในครั้งนี้ ได้มีโอกาสในการทำโปรเจกต์ในครั้งนี้ได้ตั้งแต่การหาเทคโนโลยีใหม่ๆ แล้วศึกษาเทคโนโลยีของทางองค์กร มีการวางแผนการใช้ความรู้ต่างๆมารวมกันก่อนการเริ่มออกแบบ ตั้งแต่การหาวิธีการดึงข้อมูล, เก็บข้อมูล ที่จะต้องมีความละเอียดรอบคอบเพื่อการดึงข้อมูลให้ได้ครบถ้วนตามที่ได้รับมอบหมาย และ การออกแบบหน้าแสดงผล ที่ให้ผู้ใช้งานนั้นสามารถใช้งานได้ง่าย ต้องมีการได้รับคำแนะนำ ประกอบการออกแบบด้วย ยิ่งเป็นเป็นการทำงานในรูปแบบทำงานที่บ้าน(Work form Home) โอกาสสื่อสารที่น้อยเป็นแรงผลักดันให้เรียนรู้ความสามารถ skill ในด้านการสื่อสารเพื่อให้คำแนะนำปรับปรุงตัวงานออกมาให้ดีที่สุด จากการได้ฝึกงานในครั้งนี้ถือว่าเป็นประสบการณ์การทำงานจริงที่มีประโยชน์ต่อผู้จัดทำอย่างมาก

ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) เป็นโปรเจกต์ที่ต้องปรับปรุงแก้ไขจากระบบเดิม จึงทำให้การที่จะมีข้อมูลที่ครบถ้วนมากกว่านั้นทำให้ต้องมาการเชื่อมต่อกับข้อมูลที่เยอะมาก ทำให้ระหว่างการทำงานนั้นเกิดปัญหาเป็นบางช่วง จึงต้องมีการเตรียมความพร้อมของข้อมูลให้ดี โดยจึงข้อมูลมาให้ร่วมกันอยู่ในรูปแบบตารางย่อยก่อน เพื่อลดปัญหาการเสียเวลาการทำแสดงผลที่ไม่ได้มาตรฐาน

ระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) ได้ถูกออกแบบให้มีหน้ารายงานทั้งหมด 7 หน้า และ ระบบการแจ้งเตือนอัตโนมัติอีก 1 ระบบ ผู้จัดทำโครงการคาดหวังว่าหลังจากที่ได้ทำระบบรายงานความปลอดภัย โดยใช้เคคิวแอล (Security Report System by KQL) จะมีโอกาสได้ถูกใช้ในองค์กรเพื่อประกอบการตรวจสอบความปลอดภัยนอกจากนี้ผู้จัดทำหวังว่าโครงการนี้จะเป็นประโยชน์ในภายภาคหน้าได้

บรรณานุกรม

[1] Api (Application programming interface) คืออะไร (2021 March 28) .Api (Application programming interface) คืออะไร

<https://aoostudio.com/coding/api-application-programming-interface->

%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/

[2] อินเทลลิเจนซ์ บีสเนซ (2021 Mar 14) . UI Design : หลักการออกแบบแอปพลิเคชัน ที่ต้องรู้ !! .

<https://intbizth.com/%E0%B8%AB%E0%B8%A5%E0%B8%B1%E0%B8%81%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%AD%E0%B8%AD%E0%B8%81%E0%B9%81%E0%B8%9A%E0%B8%9A%E0%B9%81%E0%B8%AD%E0%B8%9E%E0%B8%9E%E0%B8%A5%E0%B8%B4%E0%B9%80%E0%B8%84%E0%B8%8A/>

[3] คิวรี (Query).Select Query การแสดงข้อมูล ของฐานข้อมูล .

<https://www.sits39.com/selectquery%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%81%E0%B8%AA%E0%B8%94%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%82%E0%B8%AD%E0%B8%87%E0%B8%90%E0%B8%B2%E0%B8%99%E0%B8%82/>

[4] What is a Kusto query? . Kusto Query Language (KQL) .

<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/>

[5] What is Power BI? . Microsoft Power BI . <https://powerbi.microsoft.com/en-us/what-is-power-bi/>

[6] OData คืออะไร(2017 Nov 3). OData (โอดาต้า) คืออะไร เป็นมาตรฐานโปรโตคอลสำหรับการสร้างและการใช้ข้อมูล .

<https://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73->

%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/4873-what-is-odata.html#:~:text=OData%20(%E0%B9%82%E0%B8%AD%E0%B8%94%E0%B8%B2%E0%B8%95%E0%B9%89%E0%B8%B2)%20%E0%B8%AB%E0%B8%A3%E0%B8%B7%E0%B8%AD%20Open,%E0%B8%88%E0%B8%B0%E0%B9%84%E0%B8%94%E0%B9%89%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9B%E0%B8%A5%E0%B9%88%E0%B8%AD%E0%B8%A2%E0%B8%95%E0%B8%B1%E0%B8%A7

[7] Power Automate คืออะไร. ใครคือกลุ่มเป้าหมายที่ต้องการสำหรับ Power Automate . <https://learn.microsoft.com/th-th/power-automate/frequently-asked-questions>

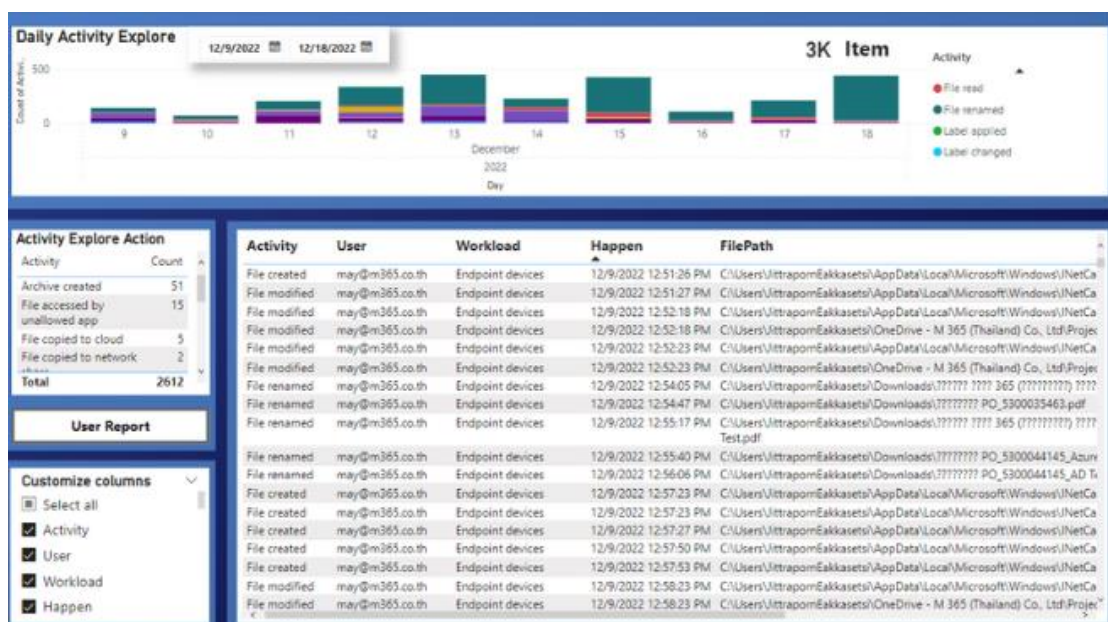
[8] รู้จักกับ Microsoft 365 Defender (2020 Dec 25). การป้องกันและตรวจจับมัลแวร์ขั้นสูงด้วย Microsoft 365 Defender . <https://www.techtalkthai.com/protect-yourself-from-advanced-malware-by-microsoft-365-defender/>

ภาคผนวก

ภาคผนวก ก. งานอื่น ๆ เพิ่มเติม

ระหว่างการปฏิบัติสหกิจศึกษาระยะเวลา 6 เดือนได้มีโอกาสได้เข้าร่วมกิจกรรมกับพี่ที่ทำงานไม่ว่าจะประชุมเจอหน้ากันทั่วไป, ทานข้าวหรือได้นำเสนอผลงานต่าง ๆ เพื่อเป็นการพัฒนาความสัมพันธ์ในองค์กรนอกจากการทำงานที่บ้าน(Work from Home)

1. ได้รับมอบหมายในการต่อยอดงานในการทำหน้ารายงานนำเสนอกับโปรเจกอื่น พร้อมทั้งสร้างระบบบันทึกประวัติอัตโนมัติ การดึงข้อมูลรายวันมาเก็บที่ฐานข้อมูลและแสดงผล



2. มีโอกาสได้เสนอผลงานให้กับลูกค้าในงาน Microsoft Thailand เป็นงานที่น่าเสนอผลงานร่วมกับสินค้าของทางบริษัท



3. การทานอาหารฉลองสิ้นปีพร้อมทั้งจับฉลากของขวัญกัน เป็นการสร้างความผูกพันในทีมงานและกิจกรรมนี้ได้รับไอแพด จากการจับฉลาก

