



รายงานสหกิจศึกษาฉบับสมบูรณ์

ระบบวิเคราะห์และแสดงผลข้อมูลในรูปแบบกราฟของข้อมูลในลักษณะ

dnslogs ผ่าน Kibana

Visualization Security dnslogs By Kibana

นายพงศธร ทังสถดี

สาขาวิชาวิศวกรรมสารสนเทศ

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2562

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อโครงการสหกิจศึกษา	ระบบวิเคราะห์และแสดงผลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana		
ชื่อ-สกุลนักศึกษา	นายพงศธร	ทังสฤดี	
คณะ	วิศวกรรมศาสตร์	ภาควิชา	วิศวกรรมคอมพิวเตอร์
สาขาวิชา	วิศวกรรมสารสนเทศ		
ชื่อ-สกุล อาจารย์นิเทศน์	ผศ.บุญยชนะ	ภูระหงษ์	
ชื่อ-สกุล ผู้นิเทศน์งาน	คุณสมศักดิ์	ชลปฐมพิกุลเลิศ	
ชื่อสถานประกอบการ	บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน)		

บทคัดย่อ

โครงการนี้เสนอการพัฒนาาระบบวิเคราะห์และแสดงผลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana ของบริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) โดยเป็นระบบที่พัฒนาเพื่อตรวจสอบการใช้งานการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ของบุคลากรที่ใช้งานอินเทอร์เน็ตภายในบริษัท ซึ่งรับข้อมูลจาก log file และแสดงข้อมูลเกี่ยวกับจำนวนการเข้าถึงเว็บไซต์ในระยะเวลาต่างๆ ประเภทของเว็บไซต์ที่อนุญาตและไม่อนุญาตให้เข้าใช้งาน รวมถึงรายชื่อของบุคลากรที่เข้าใช้เว็บไซต์หรือเซิร์ฟเวอร์ดังกล่าว ระบบที่นำเสนอนี้สามารถใช้ตรวจสอบข้อมูลเพื่อประกอบการวิเคราะห์ หรือประเมินเกี่ยวกับการเข้าใช้งานของบุคลากรต่อไป

Co-operative Title	Visualization Security dnslogs By Kibana
Student Intern Name	Mr. Pongsathorn Tangsaradee
Faculty	Engineering Department Computer Engineering
Program	Information Engineering
Advisor Name	Asst.Prof. Boonchana Purahong
Mentor Name	Mr. Somsak Chonpathomphikullert
Company	MFEC Public Company Limited

ABSTRACT

This project presents the development of analytical system and display in graph form of data in the form of dnslogs via Kibana for MFEC Public Company Limited. The system is developed to check the usage of the website or service access of personnel who use the internet within the company Which receives information from the log file and show information about the number of website accesses in various periods Types of websites that are allowed and not allowing access Including the names of the personnel that use the said website or service. The proposed system can be used to verify information for analysis or assess the usage of personnel.

กิตติกรรมประกาศ

การจัดทำโครงการพัฒนาระบบวิเคราะห์และแสดงผลข้อมูลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana เป็นโครงการของบริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) เกิดขึ้นจากแนวคิดให้ดำเนินการโดยผลงานดังกล่าว สำเร็จลุล่วงเป็นอย่างดี เพราะได้รับคำแนะนำและการให้คำปรึกษาตลอดจนติดตามผลความคืบหน้าจากหลาย ๆ ส่วน ทางผู้จัดทำจึงขอขอบคุณทุกท่านที่ได้ให้ความช่วยเหลือตลอดระยะเวลาที่ได้มีโอกาสเข้าไปดำเนินงานโครงการสหกิจศึกษาและเรียนรู้ ประสบการณ์การทำงานต่าง ๆ ตลอดจนถึงสิ้นสุดโครงการระหว่างวันที่ 5 สิงหาคม ถึงวันที่ 22 พฤศจิกายน พ.ศ.2562

โครงการนี้ไม่อาจสำเร็จลุล่วงได้หากขาดความกรุณาของคุณสมศักดิ์ ชลปฐมพิกุลเลิศ ผู้เป็นที่เลี้ยงที่คอยช่วยเหลือ ดูแลเอาใจใส่ และให้คำปรึกษาต่าง ๆ มอบความทรงจำและประสบการณ์อันมีค่าตลอดในระยะเวลาที่ผ่านมา

ขอขอบคุณผู้ช่วยศาสตราจารย์ บุญยชนะ ภูระหงษ์ ผู้เป็นอาจารย์นิเทศโครงการสหกิจศึกษา ที่คอยให้การสนับสนุนติดตามความคืบหน้าของโครงการ ให้คำปรึกษาและแนวทางแก้ไขปัญหาต่าง ๆ

สุดท้ายนี้ขอขอบคุณเพื่อนนักศึกษาและครอบครัว ที่คอยช่วยเหลือ ผลักดัน และเป็นกำลังใจสำคัญในการฟันฝ่าอุปสรรคต่าง ๆ ตลอดมา รวมถึงผู้มีพระคุณทุกท่านที่ได้เอื้อนามไว้ ณ ที่นี้ที่เป็นส่วนหนึ่งของความสำเร็จทั้งหมดจึงขอขอบคุณไว้ ณ โอกาสนี้

พงศธร ทั้งสฤดี

สารบัญ

บทคัดย่อ	I
ABSTRACT	II
กิตติกรรมประกาศ.....	III
สารบัญ.....	IV
สารบัญรูปภาพ.....	VI
บทที่ 1 บทนำ	1
1.1 ข้อมูลสถานประกอบการที่เข้าร่วมปฏิบัติงานสหกิจศึกษา.....	1
1.2 ที่มาและความสำคัญของโครงการ	2
1.3 วัตถุประสงค์ของการปฏิบัติงาน.....	2
1.4 ขอบเขตของโครงการ	3
1.5 ประโยชน์ที่คาดว่าจะได้รับ.....	3
1.6 ขั้นตอนการดำเนินงาน.....	3
1.7 อุปกรณ์ที่ใช้ในการพัฒนา.....	4
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง	8
2.2 การทำความสะอาดข้อมูล.....	9
2.3 ประเภทของข้อมูลทางสถิติ.....	9
2.4 การจัดเก็บข้อมูลจากรางทางคอมพิวเตอร์.....	11
2.5 ภาษาที่ใช้ในการพัฒนา.....	11
2.6 ซอฟต์แวร์ที่ใช้ในการพัฒนา.....	13
บทที่ 3 วิธีการดำเนินการวิจัย.....	18

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.1 กรอบแนวคิดการวิจัย	18
3.2 การวิเคราะห์และออกแบบการทำงาน	20
บทที่ 4 สรุปผลการปฏิบัติงานสหกิจศึกษา.....	28
4.1 การสร้างแผนภูมิรูปภาพ.....	31
4.2 การนำเข้าข้อมูล	32
4.3 การลบข้อมูล	33
4.4 การเรียกดูหน้าต่างการสรุปผลข้อมูล	35
บทที่ 5 สรุปและวิจารณ์ผลการปฏิบัติงานสหกิจศึกษา.....	37
5.1 สรุปผลการปฏิบัติงานสหกิจศึกษา.....	37
5.2 ปัญหา อุปสรรคในการปฏิบัติงานสหกิจศึกษา และแนวทางแก้ปัญหา.....	37
5.3 ข้อเสนอแนะ.....	38
เอกสารอ้างอิง	39
ประวัติผู้เขียน.....	41

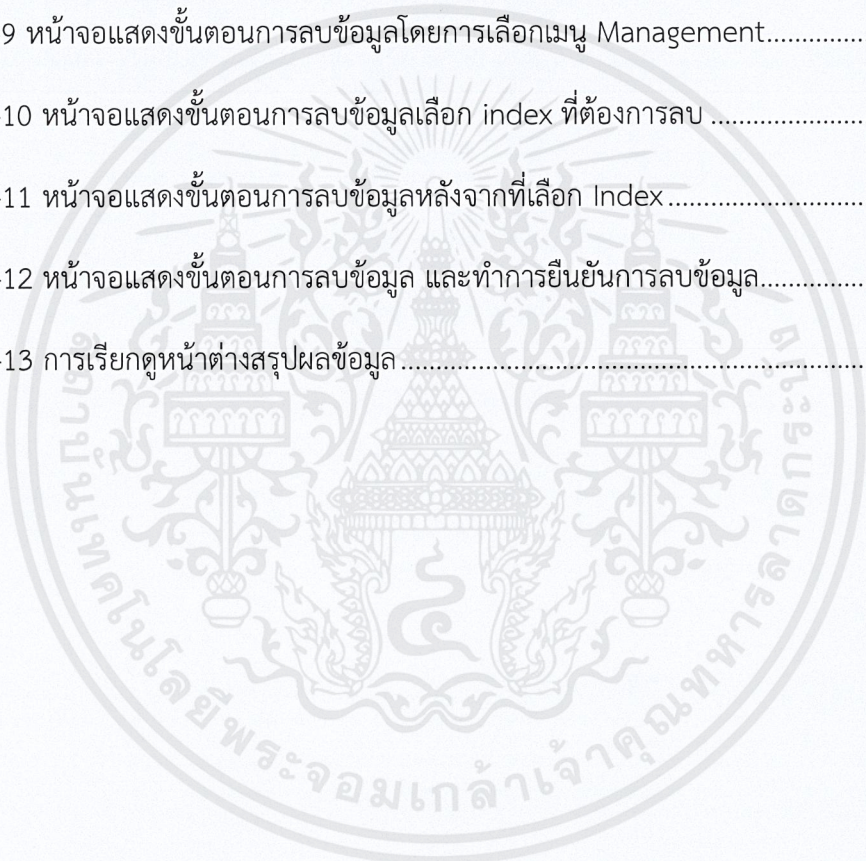
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูปภาพ

ภาพที่ 2-1 สัญลักษณ์ Python.....	12
ภาพที่ 2-2 สัญลักษณ์ Elasticsearch.....	13
ภาพที่ 2-3 สัญลักษณ์ Logstash	14
ภาพที่ 2-4 สัญลักษณ์ Kibana.....	14
ภาพที่ 2-5 สัญลักษณ์ Rsyslog.....	15
ภาพที่ 2-6 สัญลักษณ์ Filebeat	15
ภาพที่ 2-7 สัญลักษณ์ VMware.....	16
ภาพที่ 2-8 สัญลักษณ์ Ubuntu	16
ภาพที่ 2-8 สัญลักษณ์ Amazon S3.....	17
ภาพที่ 3-1 แบบจำลองการทำงานของ Waterfall Model	19
ภาพที่ 3-2 ขั้นตอนการทำงานของระบบ.....	21
ภาพที่ 3-3 ตัวอย่างข้อมูล log จาก Cisco ACS.....	22
ภาพที่ 3-4 ตัวอย่างข้อมูล log จาก Controller.....	22
ภาพที่ 3-5 ตัวอย่างโครงสร้างข้อมูล (Index) และข้อมูลที่อยู่ภายใน	24
ภาพที่ 3-6 แผนการเพิ่มข้อมูล	25
ภาพที่ 3-7 แผนภาพกิจกรรมการลบข้อมูล Index.....	26
ภาพที่ 3-8 แผนภาพกิจกรรมเรียกดูแผนภูมิรูปภาพทั้งหมด	27
ภาพที่ 3-9 แผนภาพกิจกรรมการสร้างแผนภูมิรูปภาพ.....	27
ภาพที่ 4-1 หน้าจอแสดงผลสรุปข้อมูลการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์	28
ภาพที่ 4-2 แผนภูมิรูปโดนัทที่แสดงสัดส่วนการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ต่าง ๆ มากที่สุด 10 อันดับ.....	29

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาพที่ 4-3 แผนภูมิแท่งแสดงถึงจำนวนการเข้าถึงเว็บไซต์หรือเซอร์วิสในช่วงเวลาที่กำหนด.....	30
ภาพที่ 4-4 ตารางแสดงชื่อของผู้ใช้งาน ที่อยู่ IP และจำนวนครั้งของการใช้งาน	30
ภาพที่ 4-5 การเลือกขอบเขตระยะเวลาผลการวิเคราะห์ข้อมูล	31
ภาพที่ 4-6 เมนูการเลือกสร้างแผนภูมิภาพ.....	31
ภาพที่ 4-7 เมนูเลือกประเภทแผนภูมิรูปภาพ	32
ภาพที่ 4-8 หน้าจอแสดงผลเมื่อทำการนำเข้าสู่ข้อมูล.....	32
ภาพที่ 4-9 หน้าจอแสดงขั้นตอนการลบข้อมูลโดยการเลือกเมนู Management.....	33
ภาพที่ 4-10 หน้าจอแสดงขั้นตอนการลบข้อมูลเลือก index ที่ต้องการลบ	34
ภาพที่ 4-11 หน้าจอแสดงขั้นตอนการลบข้อมูลหลังจากที่เลือก Index.....	34
ภาพที่ 4-12 หน้าจอแสดงขั้นตอนการลบข้อมูล และทำการยืนยันการลบข้อมูล.....	35
ภาพที่ 4-13 การเรียกดูหน้าตาต่างสรุปผลข้อมูล.....	36



บทที่ 1

บทนำ

1.1 ข้อมูลสถานประกอบการที่เข้าร่วมปฏิบัติงานสหกิจศึกษา

จุดเริ่มของบริษัทที่มีชื่อว่า เอ็ม เอฟ อี ซี จำกัด หรือ MFEC เริ่มก่อตั้งขึ้นเมื่อปี 2540 เป็นการรวมทุนระหว่าง บริษัท โมเดอร์นฟอรัม อินทิเกรชั่น เซอร์วิสเซส จำกัด กับกลุ่มผู้บริหาร ที่มีความชำนาญการ มีความมุ่งมั่นที่จะสร้างสรรค์ผลงานที่ตอบโจทย์กับลูกค้าเป็นความสำคัญ กลุ่มลูกค้าในระยะแรกจะเป็นงานวางระบบไอที ไม่ว่าจะเป็นงานการเงินของธนาคาร งานภาครัฐ โดยบริษัทมีความความก้าวหน้าอย่างต่อเนื่อง

บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ได้มีพันธมิตรทางธุรกิจกับทางบริษัท มีผู้ประกอบการทั้งในประเทศ และต่างประเทศ โดยทางบริษัทได้มีพัฒนาการของงานด้วยมาตรฐาน ด้านเทคโนโลยีสารสนเทศ ประกอบกับวิสัยทัศน์และกลยุทธ์ที่มุ่งเน้นการเติบโตอย่างยั่งยืน ทั้งยังมี บริการด้านให้คำปรึกษา ให้บริการด้านการพัฒนา และวางระบบเครือข่าย ซึ่งประกอบด้วยอุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์ต่อพ่วง และอุปกรณ์ที่เกี่ยวข้องกับโครงข่ายต่าง ๆ งานติดตั้ง และทดสอบระบบ ตลอดจนการให้บริการด้านบำรุงรักษาสำหรับลูกค้าทั้งภาครัฐและเอกชน โดยสามารถแบ่งธุรกิจหลักออกเป็น 3 ประเภท ได้แก่

1. ธุรกิจบริการให้คำปรึกษา และพัฒนางานด้านเทคโนโลยีสารสนเทศ บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ประกอบธุรกิจให้คำปรึกษา และพัฒนางาน ด้านเทคโนโลยีสารสนเทศแบบครบวงจร เพื่อวิเคราะห์และออกแบบระบบที่สอดคล้อง เพื่อตอบสนองความต้องการด้านการใช้งานของลูกค้า การเก็บรวบรวมข้อมูลทางธุรกิจเพื่อนำมาประมวลผล ประกอบการตัดสินใจทางธุรกิจ เพื่อช่วยสร้างจุดแข็งในการแข่งขันทางการตลาดของลูกค้า

2. ธุรกิจพัฒนาและวางระบบ บริการในด้านการออกแบบ จัดทำ พัฒนา และติดตั้งระบบคอมพิวเตอร์เครือข่าย รวมถึง ระบบสารสนเทศ เช่น ระบบจัดเก็บข้อมูล ระบบรักษาความปลอดภัยของข้อมูล ระบบการเชื่อมต่อ เครือข่ายขององค์กร รวมถึงระบบซอฟต์แวร์การจัดการเกี่ยวกับระบบสารสนเทศที่สามารถ ตอบสนองความต้องการของลูกค้าได้อย่างมากที่สุด

3. ธุรกิจบริการ ให้บริการด้านการดูแลบำรุงรักษา และสนับสนุนในด้านเทคนิคสำหรับระบบคอมพิวเตอร์ ทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์ เพื่อเพิ่มประสิทธิภาพในการทำงานของระบบ และช่วยลด ภาระค่าใช้จ่ายในการจัดจ้างบุคลากรเพื่อทำการดูแลบำรุงรักษาโดยเฉพาะ อีกทั้งมี บริการซ่อมแซม อุปกรณ์ฮาร์ดแวร์ที่จำเป็นอย่างสม่ำเสมอ

1.2 ที่มาและความสำคัญของโครงการ

เนื่องจาก บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ได้จัดโครงการสหกิจศึกษาระหว่าง บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) กับ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในส่วนงานที่เกี่ยวกับ Network ซึ่งงานที่ได้รับมอบหมายให้พัฒนาระบบ วิเคราะห์และแสดงผลข้อมูลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs โดยแสดงเกี่ยวกับปริมาณ การเข้าถึงเซิร์ฟเวอร์หรือเว็บไซต์ในอินเทอร์เน็ตขององค์กร ผ่าน Kibana เพื่อตรวจสอบชื่อ ประเภท จำนวนครั้งในการเข้าถึงของเว็บไซต์หรือเซิร์ฟเวอร์ จึงได้มีการมอบหมายงานให้นักศึกษาทำการศึกษา และหาความรู้เกี่ยวกับเทคโนโลยีเกี่ยวกับ Ubuntu OS, VMware, ELK Stack เพื่อให้ นักศึกษา มีความรู้ความสามารถในการพัฒนาระบบวิเคราะห์ได้อย่างมีประสิทธิภาพ

1.3 วัตถุประสงค์ของการปฏิบัติงาน

วัตถุประสงค์ของโครงการสหกิจศึกษาเป็นเป้าหมายเพื่อให้ผู้ปฏิบัติงานสหกิจศึกษาได้มีความ รับผิดชอบต่อหน้าที่ ต่องานที่ได้รับมอบหมาย โดยสามารถแบ่งเป็นรายละเอียดของวัตถุประสงค์ของ โครงการสหกิจศึกษาได้ดังนี้

1. เพื่อวิเคราะห์ปริมาณการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ภายในองค์กรทั้งในปัจจุบัน และ แนวโน้มการใช้งานในอนาคต
2. เพื่อสรุปผลข้อมูลการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ของพนักงาน รวมถึงผู้ที่ได้เข้าถึง หรือใช้ งาน อินเทอร์เน็ตขององค์กร
3. เพื่อติดตามความเคลื่อนไหว การเข้าถึงเซิร์ฟเวอร์ หรือเว็บไซต์
4. เพื่อสร้างความสะดวกในตรวจสอบปริมาณการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ด้วยการสรุปผล ข้อมูล

1.4 ขอบเขตของโครงการ

ผู้ปฏิบัติงานสหกิจศึกษาได้รับมอบหมายให้ทำระบบวิเคราะห์ข้อมูลการใช้เข้าใช้งานเว็บไซต์หรือเซอร์วิส โดยที่ทำการเก็บข้อมูลการเข้าถึงเว็บไซต์ ทำการวิเคราะห์ปริมาณการเข้าถึงเว็บไซต์ รวมถึง การแสดงผลอันดับของผู้เข้าถึงเว็บไซต์หรือเซอร์วิสมากที่สุดไปหาผู้ที่ใช้น้อยกว่าตามลำดับ โดยการพัฒนานั้นจะใช้ ซอฟต์แวร์ Elasticsearch, Logstash และ Kibana เป็นหลักในการพัฒนาที่สามารถสร้างแผนภูมิรูปภาพแสดงถึงปริมาณการใช้งานอินเทอร์เน็ตของผู้ใช้ได้เข้าใจง่าย

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. นักศึกษาได้รับความรู้และเข้าใจเกี่ยวกับการนำข้อมูลมาประยุกต์กับ ELK Stack
2. ระบบวิเคราะห์ข้อมูลที่ได้รับการพัฒนา จะเพิ่มประสิทธิภาพในการตรวจสอบข้อมูลและเป็นประโยชน์ต่อองค์กร

1.6 ขั้นตอนการดำเนินงาน

ในการดำเนินการจัดทำโครงการ ประกอบด้วยขั้นตอนและระยะเวลาดังนี้

ตารางที่ 1.1 ตารางแสดงขั้นตอนการดำเนินงาน

ตารางแสดงขั้นตอนการดำเนินงาน					
ลำดับ	หัวข้องาน	ส.ค	ก.ย	ต.ค	พ.ย
1	กำหนดรายละเอียดและดำเนินการทำโครงการ		→		
2	ได้รับมอบหมายในการศึกษาและจัดทำวิดีโอการใช้งานเบื้องต้นของ Cisco Webex Meeting				→

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.7 อุปกรณ์ที่ใช้ในการพัฒนา

1.7.1 ภาษาที่ใช้ในการพัฒนา

ภาษาที่ใช้ในการพัฒนานั้นเป็นส่วนหนึ่งของการพัฒนาระบบในครั้งนี้ เนื่องจากซอฟต์แวร์ ที่ใช้จำเป็นต้องมีการตั้งค่า เพื่อปรับแต่งการใช้งาน รวมถึงบางขั้นตอนการทำงานของระบบ ต้องการความสะดวก โดยภาษาทางคอมพิวเตอร์ที่ผู้ปฏิบัติงานสหกิจศึกษาได้เลือกใช้มีดังนี้

Python

ภาษาเขียนโปรแกรมระดับสูงที่มีความนิยมนกันอย่างแพร่หลาย Python เป็นภาษา Interpreter ที่ออกแบบมาให้โค้ดสามารถอ่านและทำความเข้าใจได้ง่าย โดยภาษานั้นเป็นแบบ ไดนามิกส์ มีระบบจัดการหน่วยความจำอัตโนมัติ และสนับสนุนการเขียนโปรแกรมหลากหลายรูปแบบ

CSV

โดย CSV นั้นย่อมาจาก Comma Separated Value โดยเป็นไฟล์ข้อความประเภทหนึ่ง ที่ใช้สำหรับเก็บข้อมูล โดยใช้เครื่องหมายจุลภาค หรือ (,) ในการแบ่งข้อความออกจากกัน โดยนามสกุลของไฟล์นั้นจะเป็น .csv สามารถเปิดได้ด้วยโปรแกรมอ่านไฟล์ข้อความทั่วไป (Text Editor)

YAML หรือ YML

เป็นภาษา Markup ซึ่งจะแสดงข้อมูลโครงสร้างรูปแบบ โดยส่วนมากจะพบในรูปแบบของ Tag ตัวอย่างภาษา Markup เช่น HTML, XML ภาษา YAML เป็นภาษาที่สั้น และเข้าใจง่าย โดยตัวภาษานั้นจะไม่มี Tag ที่เข้ามาเกี่ยวข้อง แต่จะใช้การเว้นวรรคในการแยกข้อมูลออกจากกัน

1.7.2 ซอฟต์แวร์ที่ใช้ในการพัฒนา

ในการพัฒนาระบบวิเคราะห์และแสดงผลข้อมูลในรูปแบบของแผนภูมิรูปภาพ จำเป็นต้องใช้เครื่องมือ Open Source ที่ชื่อ ELK Stack ที่ประกอบด้วย Elasticsearch, Logstash และ Kibana โดยมี Service ที่ทำการส่งข้อมูลการใช้งาน (log) โดย Beats จะเป็นตัวที่ทำหน้าที่เก็บข้อมูล เพื่อทำการส่งไปยัง Logstash ที่เป็นตัวจัดการข้อมูลก่อนเข้าบันทึกในฐานข้อมูล Elasticsearch

โดยข้อมูลที่ส่งนั้นจำเป็นต้องมี Index หรือ Field ที่เป็นตัวจำแนกข้อมูลออกจากกัน ดังนั้นหน้าที่ของ Logstash คือ การกำหนดโครงสร้างให้แก่ข้อมูลให้เป็นระเบียบก่อนทำการส่งไปยัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Elasticsearch ที่เปรียบเสมือนคลังเก็บข้อมูลใหญ่และเป็นตัวค้นหาข้อมูลจาก Field ที่ได้ทำการแบ่งมาก่อนหน้า เมื่อข้อมูลมีความพร้อมแล้ว การนำข้อมูลออกมาแสดงผลในรูปแบบของแผนภูมิรูปภาพนั้นจะใช้ Kibana ที่มีหน้าที่แสดงผลออกมาในรูปแบบของแผนภูมิรูปภาพ อีกทั้งมี 1 เครื่องมือสำหรับช่วยเหลือการวิเคราะห์ข้อมูลที่สามารถสรุปผลข้อมูลออกมาในรูปแบบอย่างง่ายได้

นอกจากนี้ยังมีการใช้ Service นอกเหนือจากหน้าที่การเก็บข้อมูลและแสดงผลแล้วนั้น ยังมี Service ที่ทำหน้าที่สร้างบันทึกการใช้งานของอุปกรณ์ หรือการแสดงสถานะต่าง ๆ ของ Service ตัวอย่างเช่น Syslog หรือ Eventlog ในระบบปฏิบัติการ Windows โดยไฟล์ Log นั้นจะมีนามสกุลเป็น .log หรือ .csv โดยจะมีซอฟต์แวร์ที่เลือกใช้ดังนี้

Elasticsearch

เป็นเครื่องมือที่ใช้ในการค้นหาข้อความในคลังข้อมูลที่สามารถจัดเก็บข้อมูลได้ขนาดใหญ่ มีความรวดเร็วในการค้นหา การจัดเก็บนั้นสามารถแบ่งออกเป็น Cluster โดยภายใน Cluster จะมีข้อมูลต่างกันไปชื่อว่า Index และภายในข้อมูลแต่ละ Index นั้นจะมี Field หรือ Column ที่ต่างกัน ไปขึ้นอยู่กับแหล่งที่มาของข้อมูล

Logstash

เครื่องมือรวบรวมข้อมูลพร้อมกับการแปลงข้อมูล มีความสามารถที่จะช่วยในเรื่องของการจัดโครงสร้างข้อมูล ประเภทข้อมูล โดยสามารถแบ่งการทำงานหลัก ๆ ออกเป็น 3 ส่วน คือ Input ส่วนที่นำข้อมูลเข้า Filter ส่วนของการปรับปรุงข้อมูล และ Output คือ ปลายทางของ ข้อมูลที่จะนำไปเก็บไว้ และจะมีการทำคัดกรองข้อมูลเพื่อทำการวิเคราะห์ โดยข้อมูลนั้นจะถูกส่ง ต่อไปยัง Elasticsearch

Kibana

Kibana เป็นเครื่องมือสำหรับการแสดงผล โดยจะทำการอ้างอิงข้อมูลที่ได้รับการจัดเก็บ โดยผู้ใช้งานสามารถนำข้อมูลมาแสดงผลในรูปแบบของแผนภูมิรูปภาพพร้อมกับแสดงผลที่เป็นล่าสุดได้ อีกทั้งยังมีเครื่องมือช่วยเหลือที่จะทำให้การสรุปผลข้อมูลที่มีอยู่มากมายนั้นได้สามารถเข้าใจได้ ง่ายยิ่งขึ้น

Rsyslog

โปรแกรมที่ใช้สร้างเป็นแม่ข่ายรับข้อมูล Syslog จากเครื่องปลายทาง โดยเป็นการรวม ศูนย์ข้อมูลจากทั้งหมด สำหรับการพัฒนาในครั้งนี้จะนำไฟล์ข้อมูลจะเก็บไว้ใน /var/log/syslog โดยสามารถกำหนดโครงสร้างข้อมูลเป็น Json หรือ CSV และทำการส่งข้อมูล Log มาทางโพรโทคอล UDP ที่ Port 514

Filebeat

Filebeat นั้นเป็นเครื่องมือสำหรับการถ่ายโอนข้อมูล ที่มีประสิทธิภาพสูง ใช้งานง่าย มีต้นแบบโครงสร้างข้อมูลไว้เพื่อจัดโครงสร้างข้อมูลให้อยู่ในรูปแบบที่พร้อมสำหรับการค้นหา และกระดานสำหรับการแสดงผลมากมาย เช่น ข้อมูลการใช้งานของหน่วยประมวลผล ซึ่งจะแสดงในรูปแบบของตัวเลข การใช้งานของ RAM หน่วยเป็น Megabyte โดย Filebeat นั้นมีความสามารถในการจัดเก็บข้อมูลปริมาณการใช้ทรัพยากรของเซิร์ฟเวอร์ หรือซอฟต์แวร์ที่ได้ทำงานอยู่บนระบบ โดยจะแสดงเป็นชื่อของโปรแกรมที่ทำงานอยู่นั้น (Process Name) เช่น โปรแกรม Spotify ซึ่งมีสถานะกำลังทำงาน (Running) ใช้ทรัพยากรหน่วยประมวลผล 3% (CPU Usage) และใช้หน่วยความจำ 235 MB

VMware EXSi

ซอฟต์แวร์ Visualization ของคอมพิวเตอร์ที่พัฒนาโดย VMware โดยการทำงาน แบบรวมศูนย์ ทำให้สามารถจำลองระบบปฏิบัติการได้จากทรัพยากรที่มีอยู่สามารถเลือกสเปก ความต้องการ ใช้งานได้ โดยการตั้งค่าก่อนที่จะทำการ Create Virtual Machine ขึ้นมา

Ubuntu

เป็นระบบปฏิบัติการคอมพิวเตอร์แบบเปิด (Open Source) ตัวระบบปฏิบัติการเปิดตัว ครั้งแรกเมื่อวันที่ 20 ตุลาคม ค.ศ. 2004 ซึ่งเป็นพื้นฐานของ Linux ซึ่งคำว่า Ubuntu มีความหมายในภาษาอังกฤษ คือ Humanity towards others โดยระบบปฏิบัติการจะมีรุ่นใหม่ ทุก ๆ 6 เดือน และแต่ละรุ่นจะมีการสนับสนุนเป็นระยะเวลา 9 เดือน ปัจจุบันมีเวอร์ชันล่าสุด คือ 19.04 โดยซอฟต์แวร์ต่าง ๆ ที่รวมมาในระบบปฏิบัติการนั้นเป็นซอฟต์แวร์ที่ใช้ฟรี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

JRE (Java Runtime Environment)

ซอฟต์แวร์ที่ใช้เปิดใช้งานโปรแกรมที่พัฒนาด้วยภาษา Java โดยจำเป็นต้องติดตั้งเพื่อรวมการทำงานเข้ากับระบบปฏิบัติการ สำหรับการพัฒนาในครั้งนี้ เนื่องด้วยซอฟต์แวร์ส่วนใหญ่มีพื้นฐานมาจากภาษา Java ทำให้จำเป็นต้องติดตั้ง JRE เพื่อทำการประมวลผล

1.7.3 เครื่องแม่ข่ายที่ใช้พัฒนา

ลักษณะเครื่องแม่ข่าย (Server) ที่ใช้ในการพัฒนาระบบวิเคราะห์และแสดงผลข้อมูลการใช้งานอินเทอร์เน็ตในรูปแบบแผนภูมิรูปภาพโดยใช้ Kibana ทำงานบนเครื่อง Cisco TA-UNODE-G1 ซึ่งประกอบด้วย CPU Intel Xeon รุ่น E5-2699 v4 ที่ความเร็ว 2.20 GHz จำนวน 4 คอร์ หน่วยความจำ 1,024 GB และพื้นที่จัดเก็บข้อมูลที่ 1 TB โดยแบ่งทรัพยากรบางส่วน เพื่อมาจำลองเป็นคอมพิวเตอร์เสมือน ที่มีทรัพยากรของระบบดังนี้

CPU: Intel(R) Xeon E5-2699 v4 ที่ความเร็ว 2.20GHz จำนวน 4 คอร์

Memory: 32 GB

HDD: 128 GB

OS: Ubuntu version 18.04

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในส่วนของงานวิจัยหรือบทความที่เกี่ยวข้องนั้น ผู้ปฏิบัติงานสหกิจศึกษานั้นได้ทำการรวบรวมข้อมูลที่เกี่ยวข้อง ซึ่งข้อมูลเหล่านี้ล้วนเป็นข้อมูลพื้นฐานที่สำคัญต่อการปฏิบัติงานสหกิจศึกษา ไม่ว่าจะเป็นการจัดการกับข้อมูล การสรุปผลข้อมูลโดยใช้แผนภูมิรูปภาพเพื่อให้มีความเข้าใจกับข้อมูลนั้นง่ายขึ้น

2.1 การทำ Data Visualization

เป็นการนำข้อมูลที่มีอยู่มาแสดงผลในรูปของภาพแทนความคิดเพื่อแสดงความสัมพันธ์ของข้อมูลที่ซับซ้อน ง่ายต่อการทำความเข้าใจ โดยสามารถแสดงผลในรูปแบบของกราฟ หรือแผนภูมิ โดยมีการนำเสนอรูปแบบการใช้ Data Visualization ดังนี้

2.1.1 การนำเสนอแบบทิศทาง หรือแนวโน้ม (Trending) การนำเสนอข้อมูลชนิดนี้จะแสดงให้เห็นถึงข้อมูลที่เกิดขึ้นในแต่ละช่วงเวลา (Period) จะนิยมใช้กราฟในรูปแบบของ Line Chart, Bar Chart, Radar Chart และ Area Chart

2.1.2 การนำเสนอแบบกลุ่มข้อมูล (Classification) เป็นการจัดกลุ่มหมวดหมู่ให้กับข้อมูล โดยแต่ละชนิดจะแบ่งแยกออกจากกันอย่างชัดเจน จะนิยมใช้กราฟในรูปแบบของ Donut Chart, Ring Chart และ Pie Chart

2.1.3 การนำเสนอเชิงเปรียบเทียบข้อมูล (Comparison) เป็นการเปรียบเทียบผลการดำเนินงาน หรือความต่างกันของข้อมูลในแต่ละเวลา จะนิยมใช้กราฟในรูปแบบของ Bar Chart

2.1.4 การนำเสนอรูปแบบแผนที่ (Geographical) เป็นการนำเสนอข้อมูลที่พิเศษกว่า คือ จำเป็นต้องมีที่ตั้งสถานที่เข้ามาเกี่ยวข้อง อาจจะเป็นการแสดงความหนาแน่นของประชากรในพื้นที่ การที่จะแสดงผลข้อมูลครั้งนี้จำเป็นต้องนำแผนที่เข้ามาเกี่ยวข้อง

2.2 การทำความสะอาดข้อมูล

เป็นกระบวนการลบหรือนำข้อมูลที่ไม่ต้องการออก เป็นกระบวนการแก้ไขรายการข้อมูลที่ไม่ถูกต้อง หรือไม่ต้องการออกไปจากชุดข้อมูล ตารางข้อมูล หรือฐานข้อมูล โดยสามารถเลือกเฉพาะชุดข้อมูลที่จำเป็นต้องใช้งานเหลือไว้ซึ่งข้อมูลที่สำคัญ ซึ่งการปรับปรุงข้อมูล หรือทำความสะอาดข้อมูลนั้นจำเป็นต่อการทำงานด้านฐานข้อมูลขนาดใหญ่ นอกจากจะช่วยลดปริมาณข้อมูลที่ถูกบันทึกแล้วยังทำให้ข้อมูลนั้นมีคุณภาพ มีความสมบูรณ์มากที่สุด การทำความสะอาดข้อมูลเกิดขึ้นเนื่องจากมีความไม่สอดคล้องของข้อมูล อาจเกิดจากความผิดพลาดของการบันทึกข้อมูล การส่งข้อมูล หรือการสร้างความหมายของข้อมูลที่จัดเก็บที่แตกต่างกันไปให้อยู่ในรูปแบบเดียวกัน

2.3 ประเภทของข้อมูลทางสถิติ

ในการคำนวณเลขคณิตศาสตร์ทางสถิตินั้น สามารถแบ่งประเภทของข้อมูลทางสถิติ ออกเป็น 3 ประเภท คือ การแบ่งตามลักษณะของข้อมูล แบ่งตามแหล่งที่เกิดของข้อมูล และ แบ่งตามมาตราของข้อมูล ดังนี้

2.3.1 การแบ่งตามลักษณะของข้อมูลจะแบ่งเป็น 2 ลักษณะ คือ

2.3.1.1 ข้อมูลเชิงปริมาณ (Quantitative data) เป็นข้อมูลที่อยู่ในรูปตัวเลข (Numerical data) ที่แสดงถึงปริมาณ อาจจะเป็นค่าที่ไม่ต่อเนื่อง (Discrete) เช่น จำนวนรถยนต์ จำนวนบุตรในครอบครัว หรือเป็นค่าที่ต่อเนื่อง (Continuous) เช่น ความสูง น้ำหนัก อายุ เป็นต้น

2.3.1.2 ข้อมูลเชิงคุณภาพ (Qualitative data) เป็นข้อมูลที่ไม่สามารถวัดค่าตัวเลขได้ และไม่สามารถบอกค่าความแตกต่างได้ว่ามีค่าน้อยหรือค่ามากกว่ากัน อาทิ ความชอบ ความพึงพอใจ ทศนคติ เช่น 5 = ชอบมากที่สุด 4 = ชอบมาก 3 = ชอบปานกลาง 2 = ชอบน้อย 1 = ชอบน้อยที่สุด

2.3.2 การแบ่งตามแหล่งที่เกิดของข้อมูลจะแบ่งเป็น 2 ลักษณะ ดังนี้

2.3.2.1 ข้อมูลปฐมภูมิ (Primary data) เป็นข้อมูลที่ได้จากการเก็บรวบรวมจากแหล่งโดยตรง เป็นได้ทั้งข้อมูลแบบสถิติที่เกิดขึ้นเอง และข้อมูลที่ได้จากการทดลอง เช่น การทำแบบสอบถาม ความพึงพอใจ การทำรายจ่ายต่อเดือน โดยจะเป็นการเก็บรวบรวมข้อมูลที่ได้จากการวัด ทดลอง สัมภาษณ์ หรือจะเก็บจากแบบสอบถาม

2.3.2.2 ข้อมูลทุติยภูมิ (Secondary data) เป็นข้อมูลที่รวบรวมได้จากข้อมูลปฐมภูมิ เป็นที่เก็บรวบรวมจากหน่วยงานอื่นที่หนึ่ง ซึ่งผ่านการเก็บรวบรวมไว้แล้ว ตัวอย่างเช่น การเก็บข้อมูล รายได้เฉลี่ยต่อเดือนต่อประชากรที่มีรายได้ภายในพื้นที่หนึ่ง ซึ่งสามารถหาข้อมูลได้จากสำนักงานสถิติ แห่งชาติที่ได้ทำการเก็บรวบรวมไว้แล้ว

2.3.3 การแบ่งตามมาตรา (Scale) ของข้อมูลจะมี 4 ระดับ ดังนี้

2.3.3.1 มาตรฐานนามบัญญัติ (Nominal Scale) เป็นมาตราวัดที่จำแนกข้อมูลออกเป็นกลุ่มโดยข้อมูลที่อยู่ในกลุ่มเดียวกันจะมีลักษณะที่เหมือนกัน และไม่สามารถเปรียบเทียบความแตกต่างกับ ข้อมูลต่างกลุ่มได้ ตัวอย่างเช่น เพศ อาชีพ วิชา การกำหนดตัวเลขให้กับข้อมูลแต่ละกลุ่ม สามารถทำได้ เช่น 1 = เพศชาย และ 2 = เพศหญิง

2.3.3.2 มาตราเชิงอันดับ (Ordinal Scale) เป็นมาตราวัดที่จำแนกข้อมูลออกเป็นกลุ่มโดยข้อมูลที่อยู่ในกลุ่มเดียวกันจะมีลักษณะเหมือนกันและสามารถเปรียบเทียบความแตกต่างระหว่างกลุ่มได้ทำให้สามารถจัดเรียงลำดับข้อมูลภายในกลุ่มได้ เช่น ช่วงกลุ่มอายุ ช่วงอายุแรกเกิด ถึง 10 ปี = 1 และ 11-20 ปี = 2 สามารถเรียงลำดับจากมากได้หาน้อยได้ 2 1 ตามลำดับ

2.3.3.3 มาตราอันตรภาค (Interval Scale) เป็นมาตราวัดของข้อมูลเชิงปริมาณ สามารถวัดค่าของข้อมูลได้เป็นตัวเลขและสามารถบอกปริมาณของข้อมูลได้ว่ามีค่ามากน้อยเพียงใดข้อมูลระดับมาตราอันตรภาคนั้นเป็นข้อมูลที่ไม่มีศูนย์แท้ (Absolute Zero) หมายความว่า ค่าของข้อมูลที่มีค่าเป็น 0 ไม่ได้หมายความว่าค่าานั้นจะไม่มีค่า เช่น น้ำอุณหภูมิ 0 องศาเซลเซียส ไม่ได้หมายความว่าน้ำจะไม่มีอุณหภูมิ

2.3.3.4 มาตรการอัตราส่วน (Ratio Scale) เป็นมาตราวัด ของข้อมูลเชิงปริมาณ เช่นเดียวกับ มาตราอันดับภาค แต่ข้อมูลระดับมาตรการส่วนนั้นเป็นข้อมูลที่มีศูนย์แท้ คือ ค่าของข้อมูล ที่มีค่าเป็น 0 นั้นจะหมายความว่าข้อมูลนั้นไม่มีค่า เช่น นาย ก มีเงินติดตัวอยู่ 0 บาท หมายถึง นาย ก นั้นไม่มีเงินติดตัวอยู่

2.4 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

เนื่องจากปัจจุบันเป็นยุคที่เทคโนโลยีเข้ามามีบทบาทสำคัญในการใช้ชีวิต และการสื่อสารกัน ระหว่างเครือข่ายนั้นจำเป็นต้องการบันทึกความเคลื่อนไหวจราจรทางคอมพิวเตอร์ไว้ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 สามารถสรุปโดยย่อมานั้นจำเป็นต้อง ปฏิบัติตามหลักเกณฑ์ในการเก็บ log ไว้ 5 ข้อ คือ

- 1) จำเป็นต้องเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ไม่ต่ำกว่า 90 วัน
- 2) ไม่สามารถให้ผู้ดูแลระบบเข้าไปแก้ไขข้อมูลที่เก็บไว้ได้
- 3) ข้อมูลที่จัดเก็บต้องครบถ้วน ถูกต้อง และไม่ถูกแก้ไข
- 4) ระบุรายละเอียดการใช้งานของผู้ใช้ในระบบเป็นรายบุคคลได้อย่างครบถ้วน
- 5) จัดให้มีผู้ประสานงาน และให้ข้อมูลแก่เจ้าหน้าที่

2.5 ภาษาที่ใช้ในการพัฒนา

ภาษาที่ใช้ในการพัฒนานั้นเป็นส่วนหนึ่งของการพัฒนาระบบในครั้งนี้ เนื่องจากซอฟต์แวร์ ที่ใช้นั้นจำเป็นต้องมีการตั้งค่าเพื่อปรับแต่งการใช้งานโดยใช้ภาษา YAML หรือ YML รวมถึง บางขั้นตอนการทำงานของระบบนั้นต้องการความสะดวก ดังนั้นจำเป็นต้องมีการใช้ภาษา Python เพื่อลดขั้นตอนการทำงานบางอย่างลง และสามารถ ใช้ Library ที่ได้รับการเผยแพร่ เพื่อเพิ่มความ สะดวกมากยิ่งขึ้นอีกด้วย

2.5.1 Python

เป็นภาษาเขียนโปรแกรมระดับสูงที่มีความนิยมกันอย่างแพร่หลาย มีการใช้งานครั้งแรก ในปี ค.ศ.1991 ภาษา Python นั้นเป็นภาษาแบบ Interpreter ที่ออกแบบมาให้โค้ดสามารถอ่าน และทำความเข้าใจได้ง่าย และโครงสร้างของภาษานั้นจะใช้บรรทัดที่น้อยกว่า C++ และ Java โดยภาษานั้นเป็นแบบไดนามิกส์และมีระบบจัดการหน่วยความจำอัตโนมัติและสนับสนุนการเขียน โปรแกรม หลากหลายรูปแบบ โดยมีสัญลักษณ์ของ Python ดังภาพที่ 2-1



ภาพที่ 2-1 สัญลักษณ์ Python

<https://playground.cmmakerclub.com/2015/06/python/>

2.5.2 CSV

โดย CSV นั้นย่อมาจาก Comma Separated Value โดยเป็นไฟล์ข้อความประเภทหนึ่งที่ใช้สำหรับเก็บข้อมูล โดยใช้เครื่องหมายจุลภาค หรือคอมม่า (,) ในการแบ่งข้อความออกจากกัน โดยนามสกุลของไฟล์นั้นจะเป็น .csv สามารถเปิดได้ด้วยโปรแกรมอ่านไฟล์ข้อความทั่วไป หรือจะเปิดด้วยโปรแกรม Microsoft Excel โดยไฟล์ .csv จะสามารถใช้ในการทำงานด้านสถิติข้อมูลได้

2.5.3 YAML

เป็นรูปแบบภาษา Markup มีโครงสร้างภาษาที่มนุษย์สามารถอ่านได้ง่าย ซึ่งตัวภาษาจะแตกต่างกับภาษา HTML ตรงที่ไม่มี Tag ในการแยกข้อมูล ซึ่งจะใช้การเว้นวรรคเพื่อแยกข้อมูลออกจากกัน ซึ่งภาษา YAML จะนิยมใช้ในการตั้งค่าให้กับโปรแกรม โดยสามารถเข้ามาแก้ไขไฟล์นามสกุล .yaml ด้วยการโปรแกรมแก้ไขข้อความทั่วไป (Text Editor)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6 ซอฟต์แวร์ที่ใช้ในการพัฒนา

สิ่งสำคัญที่ขาดไปไม่ได้อย่างยิ่งในการพัฒนาระบบในครั้งนี้ คือ ซอฟต์แวร์ที่ใช้ในการพัฒนา เพราะถ้าหากขาดซอฟต์แวร์ในการพัฒนาระบบในครั้งนี้มันไม่อาจสำเร็จลุล่วงไปได้ กระบวนการเก็บข้อมูล การจัดการข้อมูล การส่งข้อมูล และการนำข้อมูลไปแสดงผล ล้วนใช้ซอฟต์แวร์ในการทำงาน ซึ่งซอฟต์แวร์ที่ใช้ในการพัฒนาระบบครั้งนี้จะอยู่ในระบบปฏิบัติการ Ubuntu โดยมีซอฟต์แวร์ทั้งแบบการทำงานเบื้องหน้า และการทำงานเบื้องหลัง ดังนี้

2.6.1 Elasticsearch

เป็นเครื่องมือที่ใช้ในการค้นหาข้อความในคลังข้อมูล ที่สามารถจัดเก็บข้อมูลได้ขนาดใหญ่ มีความรวดเร็วในการค้นหา มีความสามารถในการจัดสร้างความสัมพันธ์ของข้อมูล โดยจะเพิ่มความเร็วในการค้นหา และมีความยืดหยุ่นสูง การจัดเก็บนั้นสามารถแบ่งออกเป็น Cluster และภายใน Cluster นั้นจะมีข้อมูลต่างกันไปชื่อว่า Index และภายในข้อมูลแต่ละ Index นั้นจะมี Field หรือ Column ที่ต่างกันไปขึ้นอยู่กับแหล่งที่มาของข้อมูล โดยมีสัญลักษณ์ของ Elasticsearch ดังภาพที่ 2-2



ภาพที่ 2-2 สัญลักษณ์ Elasticsearch

<https://stories.sellzuki.co.th/วิธีการ-backup-และ-restore-ข้อมูลใน-elastic-search-ด้วย-s3-b883ecd76dfc>

2.6.2 Logstash

เครื่องมือในการรวบรวม พร้อมกับการกำหนดโครงสร้างข้อมูล และจะมีการทำการคัดกรองข้อมูลเพื่อทำการวิเคราะห์ โดยความสามารถในการคัดกรองข้อมูลนั้น สามารถใช้ชนิดข้อมูล (Type) การค้นหาเฉพาะข้อความที่ต้องการ (Message) การเลือกข้อมูลชนิดที่อยู่ IP ของผู้ใช้ ความสามารถเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใช้เครื่องมือในการแปลงที่อยู่ IP ไปยังค่าพิกัดบนแผนที่ (Geo IP) การแปลงที่อยู่เลขไอพีแอดเดรสของเว็บไซต์ ไปยัง Domain Name ซึ่งข้อมูลนั้นจะถูกส่งต่อไปยัง Elasticsearch โดยมีสัญลักษณ์ของ Logstash ดังภาพที่ 2-3



ภาพที่ 2-3 สัญลักษณ์ Logstash

<https://www.pinterest.com/pin/296393219211582157/>

2.6.3 Kibana

Kibana เป็นเครื่องมือสำหรับการแสดงผล โดยจะทำการอ้างอิงข้อมูลที่จัดเก็บ โดยผู้ใช้สามารถนำข้อมูลมาแสดงผลในรูปแบบของแผนภูมิรูปภาพพร้อมกับแสดงผลที่เป็นล่าสุดได้ อีกทั้งยังมีเครื่องมือช่วยเหลือที่จะทำให้การสรุปผลข้อมูลที่มีอยู่มากมายนั้นได้สามารถเข้าใจได้อย่าง ง่ายยิ่งขึ้น โดยมีสัญลักษณ์ของ Kibana ดังปรากฏภาพที่ 2-4



ภาพที่ 2-4 สัญลักษณ์ Kibana

<https://www.thaipng.com/png-i95k38/>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6.4 Rsyslog

โปรแกรมที่ใช้สร้างเป็นแม่ข่ายรับข้อมูล syslog จากเครื่องปลายทาง เป็นการรวมศูนย์ข้อมูลจากทั้งหมด โดยไฟล์ข้อมูลจะเก็บไว้ใน `/var/log/syslog` ที่สามารถกำหนดขนาดของไฟล์ ในการบันทึกให้มีขนาดไม่เกิน Gigabyte หรือ Megabyte สามารถเก็บข้อมูลการยืนยันตัวตน (Authentication) การทำงานของโปรแกรม (Service Usage) การเข้าออกของอีเมล (Email) การเชื่อมต่อไปยังภายนอก (SSL) โดยสามารถกำหนดโครงสร้างข้อมูลเป็น json หรือ csv มีสัญลักษณ์ของ Rsyslog ดังภาพที่ 2-5

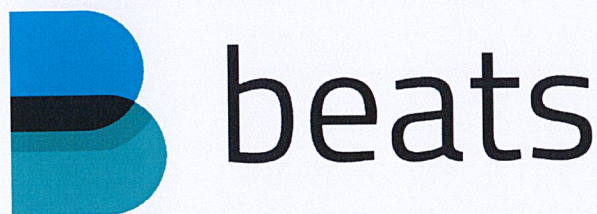


ภาพที่ 2-5 สัญลักษณ์ Rsyslog

<https://www.unixtutorial.org/rsyslog-separate-log-file-for-each-host>

2.6.5 Filebeat

Filebeat นั้นเป็นเครื่องมือสำหรับการถ่ายโอนข้อมูล ที่มีประสิทธิภาพสูง ใช้งานง่าย มีต้นแบบโครงสร้างข้อมูลไว้เพื่อจัดโครงสร้างข้อมูลให้อยู่ในรูปแบบที่พร้อมสำหรับการค้นหาและแสดงผล โดยมีสัญลักษณ์ของ Filebeat ดังภาพที่ 2-6



ภาพที่ 2-6 สัญลักษณ์ Filebeat

<https://www.elastic.co/brand>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6.6 VMware esxi

เป็นซอฟต์แวร์ Visualization ของคอมพิวเตอร์ที่พัฒนาโดย VMware โดยการทำงาน แบบรวมศูนย์ ทำให้สามารถจำลองระบบปฏิบัติการได้จากทรัพยากรที่มีอยู่ สามารถเลือก ความต้องการใช้งานได้ โดยการตั้งค่าก่อนที่จะทำการ Create Virtual Machine ขึ้นมา มีสัญลักษณ์ ของ VMware esxi ดังภาพที่ 2-7



ภาพที่ 2-7 สัญลักษณ์ VMware

<https://www.vionblog.com/patch-vmware-esxi-using-esxcli-online-repository/>

2.6.7 Ubuntu

เป็นระบบปฏิบัติการคอมพิวเตอร์ซึ่งเป็นระบบปฏิบัติการแบบเปิด (Open Source) ระบบปฏิบัตินั้นเปิดตัวครั้งแรกเมื่อวันที่ 20 ตุลาคม ค.ศ. 2004 ซึ่งเป็นพื้นฐานของ Linux คำว่า Ubuntu มีความหมายในภาษาอังกฤษ คือ Humanity towards others โดยระบบปฏิบัตินั้น จะมีการออกรุ่นใหม่ทุก ๆ 6 เดือน และแต่ละรุ่นจะมีการสนับสนุนเป็นระยะเวลา 9 เดือน ปัจจุบันมีเวอร์ชันล่าสุด คือ 19.04 โดยซอฟต์แวร์ต่าง ๆ ที่รวมมาในระบบปฏิบัตินั้นเป็นซอฟต์แวร์ที่ใช้ฟรีเกือบทั้งหมด ตัวระบบปฏิบัตินั้นเหมาะสำหรับผู้ใช้ทั่วไป มีโปรแกรมที่ทันสมัย และมีเสถียรภาพในระดับที่สูง โดยมีสัญลักษณ์ของ Ubuntu ดังภาพที่ 2-8



ภาพที่ 2-8 สัญลักษณ์ Ubuntu

<http://www.namwalab.com/2014/05/06/บทที่-2-วิธีการติดตั้ง-linux-อ/>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6.8 JRE (Java Runtime Environment)

เป็นซอฟต์แวร์ที่ใช้เปิดใช้งานโปรแกรมที่พัฒนาด้วยภาษา Java โดยจำเป็นต้องติดตั้งเพื่อรวมการทำงานเข้ากับระบบปฏิบัติการ ซึ่งเป็นโปรแกรมพื้นฐานที่จะใช้เปิดโปรแกรมที่มีการพัฒนาโดยใช้ภาษา Java ซึ่งซอฟต์แวร์ Elasticsearch และ Logstash ที่ใช้ในการพัฒนานั้น จำเป็นต้องใช้ JRE ในการเปิดใช้งาน

2.6.9 Amazon S3

Amazon S3 คือพื้นที่จัดเก็บข้อมูลคลาวด์ที่สร้างขึ้นเพื่อใช้จัดเก็บและเรียกค้นข้อมูลตามจำนวนที่ต้องการจากที่ใดก็ได้บนอินเทอร์เน็ต โดยเป็นบริการพื้นที่จัดเก็บแบบง่าย ๆ ที่ให้โครงสร้างพื้นฐานการจัดเก็บข้อมูลที่มีความทนทาน พร้อมใช้งานได้อย่างเต็มที่ และสามารถปรับขนาดได้ไม่จำกัดในราคาที่ต่ำมาก ในที่นี้จะมีการดึงข้อมูลบางส่วนเพื่อใช้งานในระบบดังกล่าว โดยที่ต้องได้รับสิทธิ์ในการเข้าถึงข้อมูลดังกล่าว โดยมีสัญลักษณ์ของ Amazon S3 ดังภาพที่ 2-9



ภาพที่ 2-8 สัญลักษณ์ Amazon S3

<https://medium.com/@iamgique/aws-s3-คืออะไร-ฉบับเข้าใจง่ายใน-2-นาที-648012fd7268>

บทที่ 3

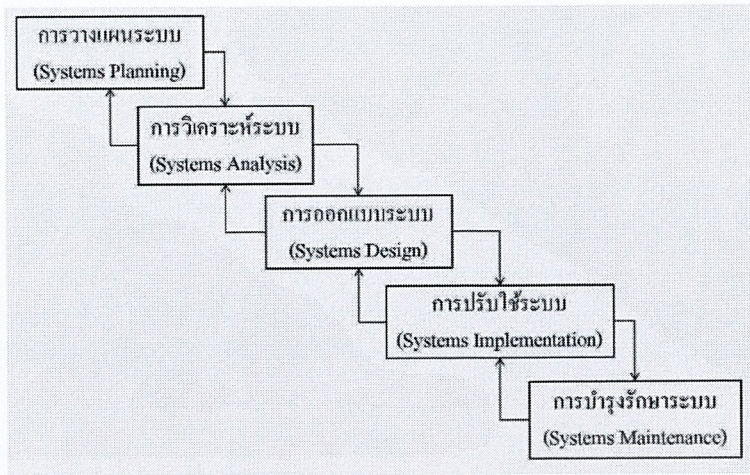
วิธีการดำเนินการวิจัย

ในการปฏิบัติงานสหกิจศึกษาครั้งนี้ ผู้ปฏิบัติงานสหกิจศึกษาได้รับมอบหมายให้จัดทำระบบวิเคราะห์และแสดงผลการเข้าถึงเว็บไซต์หรือเซอร์วิสในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana ซึ่งเป็นระบบที่พัฒนาขึ้นมาเพื่อการติดตาม วิเคราะห์ผลปริมาณการใช้เข้าถึงเว็บไซต์หรือเซอร์วิส รวมถึงความผิดปกติของปริมาณข้อมูลที่ผู้ใช้งาน และการเข้าถึงเว็บไซต์หรือเซอร์วิสที่ไม่ได้รับการอนุญาต เพื่อสรุปผลการวิเคราะห์ผลทำให้เข้าใจถึงภาพรวมของการเข้าถึงเว็บไซต์หรือเซอร์วิสต่าง ๆ และสามารถรู้ถึงไอพีแอดเดรสที่มีการเข้าถึงเว็บไซต์ต้องห้ามดังกล่าวเพื่อแก้ไขหรือป้องกันอย่างรวดเร็ว โดยการแสดงผลของแผนภูมิรูปภาพจะแสดงตามความเหมาะสมและสอดคล้องกับชนิดของข้อมูล เพื่อสามารถทำความเข้าใจได้ง่ายอย่างที่สุด

ในบทนี้จะกล่าวถึงการวิเคราะห์และออกแบบการทำงานของระบบวิเคราะห์ และแสดงผลข้อมูลการใช้งานอินเทอร์เน็ตในรูปแบบแผนภูมิรูปภาพโดยใช้ Kibana เพื่อการวิเคราะห์ และสรุปผลข้อมูลในรูปแบบของกราฟ ซึ่งประกอบด้วยกรอบแนวคิดการวิจัย การวิเคราะห์และออกแบบการทำงานโดยมีรายละเอียดดังต่อไปนี้

3.1 กรอบแนวคิดการวิจัย

การพัฒนาซอฟต์แวร์ที่ดีนั้น จำเป็นต้องมีกระบวนการพัฒนา เพื่อที่จะทำให้ซอฟต์แวร์ที่พัฒนานั้นมีคุณภาพและมีข้อผิดพลาดที่น้อยที่สุดโดยระบบที่ได้รับมอบหมายนั้นจำเป็นต้องมีการวางแผน เพื่อลดความซับซ้อนของงานผู้ปฏิบัติงานสหกิจศึกษาจึงนำกระบวนการ Adapted Waterfall Model มาใช้ตลอดระยะเวลาการพัฒนาโดยกระบวนการพัฒนานั้นจะเป็นแบบขั้นลำดับโดยจะแสดงลำดับขั้นตอนการทำงานของ Waterfall Model ดังภาพที่ 3-1



ภาพที่ 3-1 แบบจำลองการทำงานของ Waterfall Model

<http://resumeforcpe.blogspot.com/2016/12/water-fall-model-product-line-waterfall.html>

Adapted Waterfall Model คืออะไร

เป็นแบบจำลองของกระบวนการพัฒนาซอฟต์แวร์ในรูปแบบของน้ำตก ซึ่งเป็นรูปแบบที่นิยมใช้กันมาอย่างยาวนาน มีหลักการเสมือนกับน้ำตก ซึ่งไหลจากที่สูงลงที่ต่ำ ซึ่งแต่ละขั้นตอนสามารถย้อนกลับไปแก้ไขขั้นตอนที่แล้วได้ โดยในแต่ละขั้นตอน จะแบ่งเป็น 5 ขั้นตอนหลักโดยรายละเอียดของขั้นตอนมีดังนี้

1. Requirement

เป็นขั้นตอนในการเก็บความต้องการของผู้ใช้งาน ผู้พัฒนาจำเป็นต้องรู้ถึงความต้องการเพื่อที่จะกำหนดเป้าหมายในการพัฒนาซอฟต์แวร์ เพื่อที่จะได้ซอฟต์แวร์ที่ตรงกับความต้องการของผู้ใช้งานและลดความผิดพลาดที่จะเกิดขึ้นในภายหลัง

2. Design

การทำงานที่ดีจำเป็นต้องมีการวางแผนที่ดี ซึ่งในขั้นตอนของการออกแบบระบบนั้น ต้องมีการออกแบบที่รองรับการทำงานที่เหมาะสม ตรงกับความต้องการของงาน ไม่ว่าจะเป็นการวางแผนการทำงาน ระยะเวลาการพัฒนา เพื่อลดความผิดพลาดที่จะเกิดขึ้นในภายหลัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. Implementation

ขั้นตอนลงมือพัฒนา จะเป็นการทำงานภายหลังจากการรับความต้องการ การวางแผน ซึ่งจะต้องเลือกใช้เครื่องมือในการพัฒนาที่เหมาะสม โดยคำนึงถึงระยะเวลาที่ใช้ เพื่อไม่ให้มีผลกระทบที่ตามมา

4. Verification

ขั้นตอนการตรวจสอบงาน ให้เป็นไปตามความต้องการของลูกค้า ที่ได้ทำการระบุเอาไว้ การตรวจสอบนั้น จะต้องเป็นไปตามที่ระบุ ไม่ว่าจะเป็นเรื่องของงบในการพัฒนา ระยะเวลาในการส่งมอบงาน การพัฒนาจำเป็นต้องเป็นไปตามข้อตกลง ที่ได้สร้างไว้ในขั้นต้น

5. Maintenance

การซ่อมบำรุง เป็นขั้นตอนสุดท้ายหลังการส่งมอบระบบที่ได้ทำการพัฒนา ซึ่งเมื่อเกิดข้อผิดพลาด หรือระบบนั้นมีความผิดปกติ ผู้พัฒนาจำเป็นต้องมีการบำรุงรักษา คอยแก้ไขปัญหา ที่เกิดขึ้น หรือปรับปรุงประสิทธิภาพของระบบให้ดียิ่งขึ้น

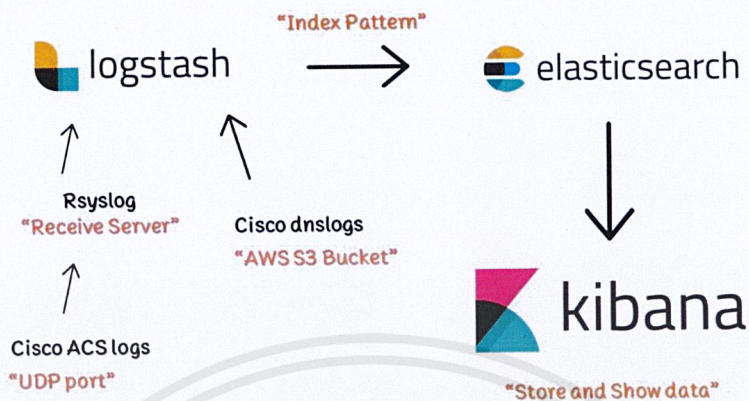
แบบจำลอง Adapted Waterfall Model โดยในแต่ละขั้นตอนเมื่อดำเนินงานอยู่ สามารถย้อนกลับมายังขั้นตอนก่อนหน้าเพื่อแก้ไขข้อผิดพลาดซึ่งไม่ได้จำกัดอยู่แค่หมวดหมู่งานการพัฒนาซอฟต์แวร์ เท่านั้น จะเห็นได้ว่าการนำแบบจำลองนี้ไปปรับใช้ในการทำงานอื่นได้ โดยการคำนึงถึงผลกระทบ ที่จะเกิดขึ้นในอนาคต ซึ่งการทำงานที่ดีนั้นจำเป็นต้องมีการวางแผนที่ดี และเหมาะสม ซึ่งถือว่า เป็นการนำแบบจำลองไปใช้ในชีวิตประจำวันได้อีกด้วย

3.2 การวิเคราะห์และออกแบบการทำงาน

ผู้ปฏิบัติงานสหกิจศึกษาได้มีการพัฒนาระบบวิเคราะห์และแสดงผลข้อมูลการใช้งานอินเทอร์เน็ตในรูปแบบแผนภูมิรูปภาพโดยใช้ Kibana เพื่อการวิเคราะห์และสรุปผลข้อมูลในรูปแบบของแผนภูมิรูปภาพ ระบบจะแบ่งส่วนเป็นการแสดงผลการสรุปข้อมูลการใช้งานอินเทอร์เน็ต โดยข้อมูลจะเป็น การเข้าเว็บ ที่อยู่ไอพีแอดเดรสเว็บไซต์จะมีการเชื่อมต่อ โดยมีการวิเคราะห์และออกแบบระบบการทำงานให้ลักษณะของแผนภาพ เพื่ออธิบายถึงความสัมพันธ์ของโครงสร้างภายในระบบ เพื่อให้ผู้พัฒนาได้เข้าใจถึงการทำงานของระบบง่ายขึ้น โดยมีแผนภาพต่าง ๆ ดังต่อไปนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนการทำงานของระบบ จะแสดงดังภาพที่ 3-1 ดังนี้



ภาพที่ 3-2 ขั้นตอนการทำงานของระบบ

คำอธิบายขั้นตอนการทำงานของระบบนั้น สามารถแบ่งขั้นตอนเป็น 5 ขั้นตอน คือ

ขั้นตอนที่ 1 : การเก็บข้อมูลการใช้งาน (log) เพื่อส่งต่อมายังเครื่องแม่ข่ายในการเก็บข้อมูล

ขั้นตอนที่ 2 : เป็นการเก็บรวบรวมข้อมูล (log) โดยเครื่องแม่ข่ายจะเป็นศูนย์รวมของข้อมูล
ที่มาจาก 2 แหล่งที่มา โดยใช้ซอฟต์แวร์ Rsyslog ในการทำ Syslog Server โดยข้อมูลการใช้งาน (log) จะแยกเป็น 2 แหล่งได้แก่ 1.ข้อมูลการใช้งาน (log) จาก Cisco ACS และ
2. ข้อมูลการใช้งาน (Log) จาก AWS S3 Bucket ข้อมูล log จาก Cisco ACS เป็น Log ที่ได้จากระบบความปลอดภัย ซึ่งจะทำให้การพิสูจน์ตัวตน และกำหนดสิทธิ์ การใช้งานของผู้ใช้ในระบบเครือข่าย โดยจะเก็บข้อมูล เช่น Username และ Password เอาไว้ โดยการใช้งาน Cisco ACS ทำให้สามารถกำหนดสิทธิ์การใช้งานของผู้ใช้ในรูปแบบต่าง ๆ และยังสามารถรับโปรโตคอลที่ใช้ในการพิสูจน์ตัวตนได้หลากหลาย โดยข้อมูลที่ได้ถูกบันทึก และตัวอย่าง ของชุดข้อมูลจะแสดงดังภาพ 3-3 ดังนี้ เวลาที่ได้ทำการบันทึกข้อมูลลงในระบบ (Timestamp)

- ชื่อของสถานที่
- เวอร์ชันของ ACS
- ที่อยู่ IP ของอุปกรณ์ (Device IP Address)
- ที่อยู่ IP ปลายทาง (Destination IP Address)
- Port ของการเชื่อมต่อ (Destination Port)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

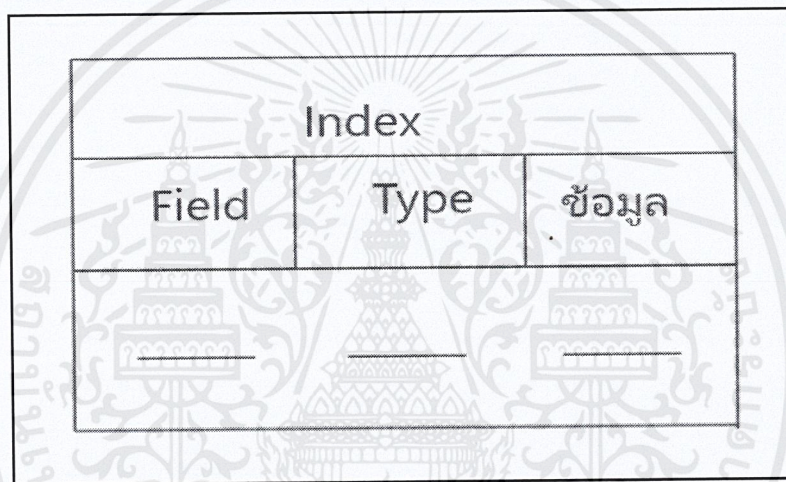
- เวลาที่ได้ทำการบันทึกการเข้าถึงเว็บไซต์หรือเซอร์วิสดังกล่าวโดยจะระบุเป็นไทม์โซนของ UTC (Timestamp)
- ข้อมูลรายละเอียดเฉพาะตัวแรกของรีเควส ตามลำดับข้อมูลละเอียด (Most Granular Identity)
- ข้อมูลรายละเอียดทั้งหมดเกี่ยวกับรีเควสนั้น. (Identities)
- IP ภายในที่ทำการรีเควส (InternalIp)
- IP ภายนอกที่ทำการรีเควส (ExternalIp)
- สถานะของรีเควสที่ได้รับอนุญาต หรือ ไม่ได้รับอนุญาต ให้เข้าถึงโดเมนดังกล่าว (Action)
- ประเภทของรีเควส (QueryType)
- โค้ดที่ทำการส่งกลับมาจาก DNS (ResponseCode)
- โดเมนเป้าหมายที่ทำการรีเควสไปถึง (Domain)
- ประเภทของเนื้อหาที่เข้าถึงเว็บไซต์หรือเซอร์วิสดังกล่าว (Categories)
- ประเภทของข้อมูลรายละเอียดเฉพาะตัวแรกของรีเควส ตามลำดับข้อมูลละเอียด (Most Granular Identity Type)
- ประเภทของรายละเอียด เช่น Roaming Computer, Network (Identity Types)
- ประเภทของปลายทางที่ถูกบล็อกหรือไม่ได้รับอนุญาต (Blocked Categories)
- ชื่อผู้ใช้งาน (User-Name)
- ที่อยู่ IP ของผู้ใช้งาน (Framed-IP-Address ที่มีประเภทข้อมูลเป็น IPV4)

ขั้นตอนที่ 3 : เมื่อข้อมูล (log) มีการเก็บรวบรวมไว้ในที่เดียวกันแล้ว จะใช้ซอฟต์แวร์ Logstash ในการกำหนดการนำเข้า ข้อมูล (Input File) ในระหว่างการทำงาน จะมีการกรองข้อมูล (Filter) เพื่อคัดกรองเฉพาะข้อมูลที่ต้องการใช้งาน โดยนำข้อมูลที่ต้องการไปสร้างเป็นโครงสร้างข้อมูล (Index) ที่ประกอบด้วยหัวข้อของข้อมูล (Field) ชนิดของข้อมูล (Type) และข้อมูล

1. การปรับปรุงข้อมูล

ข้อมูลที่ได้จากการจัดเก็บนั้นมีทั้งแบบข้อมูลสำเร็จพร้อมใช้งาน และทั้งที่ไม่พร้อมใช้งาน โดยข้อมูลที่ไม่พร้อมใช้งานนั้นผู้ใช้งานจำเป็นต้องทำการปรับปรุงข้อมูลนั้นด้วยการระบุหัวข้อของข้อมูล (Field) เพื่อให้ง่ายต่อการวิเคราะห์ข้อมูล และสามารถจำแนกข้อมูลออกเป็นหมวดหมู่ได้ ขั้นตอนนี้จะใช้ Service ที่ชื่อ Logstash ในการทำงาน และมีรายละเอียดการทำงานดังต่อไปนี้

1.1 ผู้ใช้งานจำเป็นต้องกำหนดชื่อของข้อมูล (Index) โดยภายในโครงสร้างข้อมูลจะแสดง ดังภาพที่ 1-4



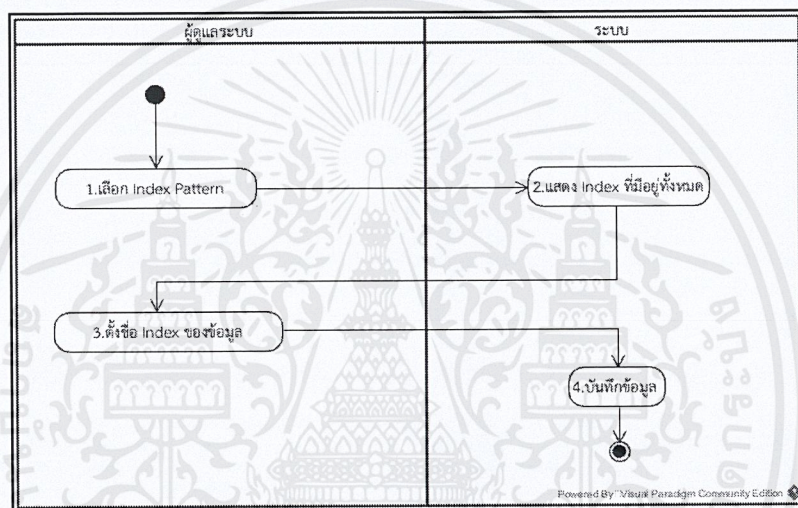
ภาพที่ 3-5 ตัวอย่างโครงสร้างข้อมูล (Index) และข้อมูลที่อยู่ภายใน

1.2 ผู้ใช้สามารถกำหนดชนิดของข้อมูล (Type) ที่อยู่ภายใต้หัวข้อที่จะเป็นตัว จำแนก ข้อมูลออกจากกัน ซึ่งชนิดของข้อมูลนั้นสามารถทำให้ข้อมูลภายในแต่ละหัวข้อของ ข้อมูล (Field) นั้นมีความสามารถในการกระทำเกี่ยวกับข้อมูลได้ เช่น การนำข้อมูลชนิด Number เพื่อใช้เครื่องมือ ค้นหาค่าที่มากที่สุด โดยจะมีชนิดของข้อมูล (Type) เช่น

- String
- Number
- IP
- Timestamp

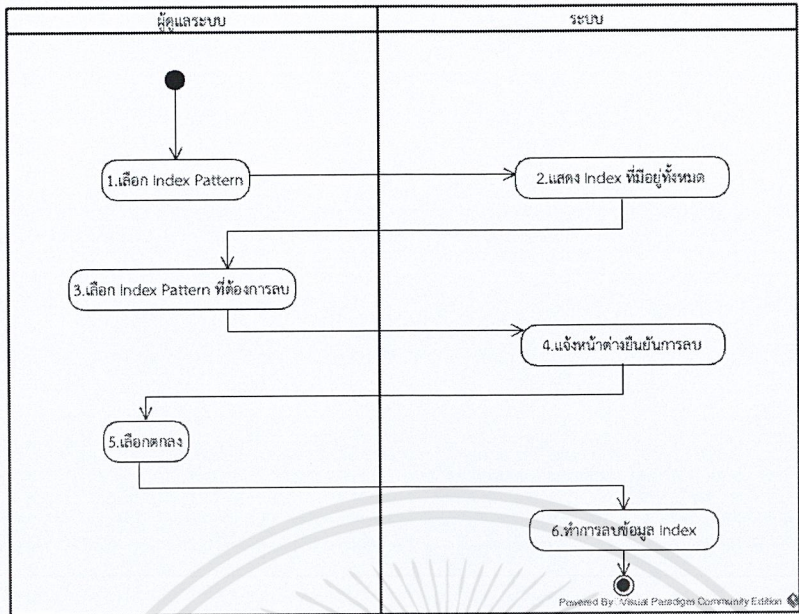
ขั้นตอนที่ 4: เมื่อผ่านกระบวนการคัดกรองข้อมูล (Filter) โครงสร้างข้อมูลที่ได้จะบันทึกลงใน Elasticsearch เป็นโครงสร้างข้อมูล (Index) ใช้สามารถกำหนดหัวข้อของข้อมูล (Field) ที่ จะทำการส่งต่อได้

การเพิ่มข้อมูล (Index) ผู้ใช้สามารถเพิ่มข้อมูลของไฟล์ที่มีนามสกุล .csv หรือ .log ได้ และ ทำการอัปโหลดไฟล์ไปยังพื้นที่จัดเก็บข้อมูล และระบบจะสร้างข้อมูลที่ได้ถูกจัดเก็บ ในรูปของ Index ที่จะแสดงผลในโปรแกรม Kibana โดยจะแสดงขั้นตอนการทำงานดังภาพที่ 3-6



ภาพที่ 3-6 แผนการเพิ่มข้อมูล

จากแผนภาพที่ 3-6 จะกล่าวถึงในส่วนของการเพิ่มข้อมูล โดยผู้ใช้งานจำเป็นต้องเลือก Index ที่ต้องการเพิ่ม โดยเลือกเมนู Management เพื่อเข้าสู่เมนูการจัดการทั้งหมด และเลือกในส่วนของ Index Pattern แล้วทำการเลือก Create Index pattern จากนั้นก็เลือกชุดของข้อมูล และทำการตั้งชื่อให้กับ Index ที่จะสร้างขึ้นมา จากนั้นกด Save เพื่อบันทึกข้อมูลภาพการลบข้อมูล ผู้ใช้สามารถลบข้อมูลได้ ระบบจะแสดงข้อมูล Index ที่มีอยู่ โดยผู้ใช้งานจำเป็นต้องเลือกข้อมูล Index ที่ต้องการจะลบระบบจะแสดงหน้าต่างการยืนยันก่อนที่จะทำการลบข้อมูลออกไป โดยจะแสดงขั้นตอนการทำงานดังภาพที่ 3-3

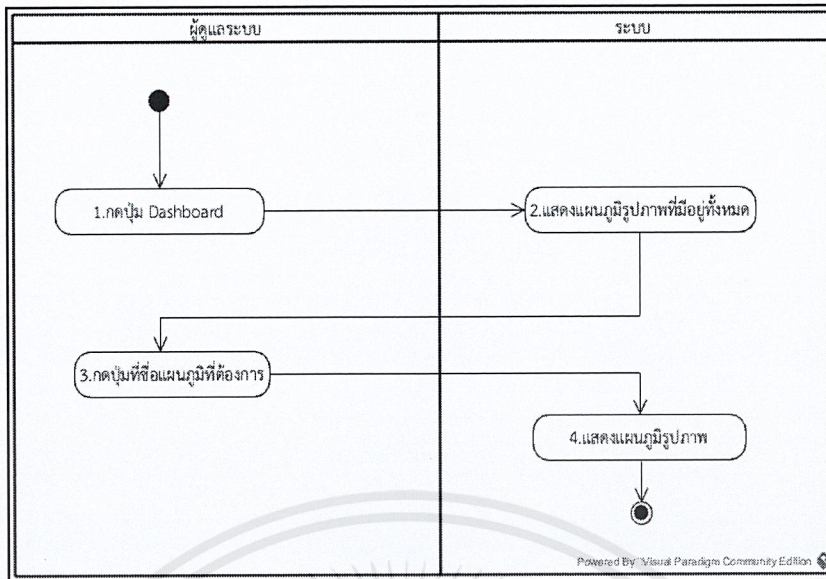


ภาพที่ 3-7 แผนภาพกิจกรรมการลบข้อมูล Index

ภาพที่ 3-7 จะกล่าวถึงในส่วนของการลบข้อมูล โดยผู้ใช้งานจำเป็นต้องเลือก Index ที่ต้องการลบ โดยเลือกเมนู Management เพื่อเข้าสู่เมนูการจัดการทั้งหมด และเลือกในส่วนของ Index Management แล้วทำเครื่องหมายหน้า Index ที่ต้องการลบ แล้วเลือก Manage และเลือก Delete เพื่อทำการลบข้อมูลและสามารถนำไปแสดงผลได้ในขั้นตอนสุดท้าย คือ

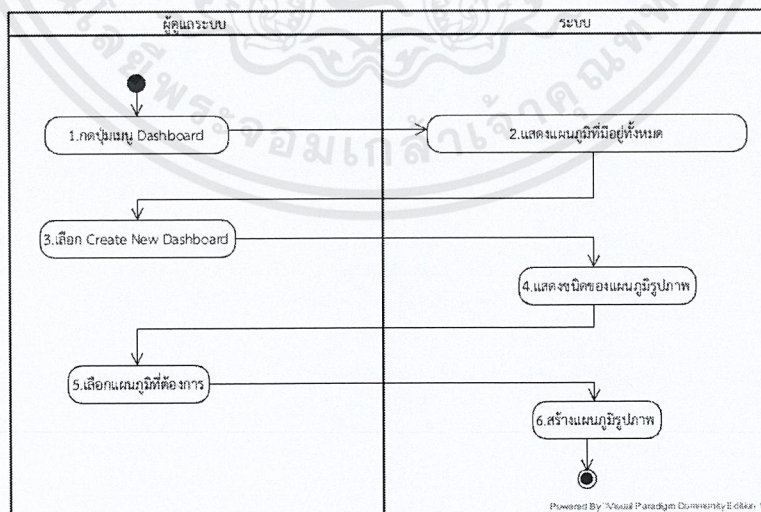
ขั้นตอนที่ 5: การทำงานของซอฟต์แวร์ Kibana การแสดงผล (Visualization) โดยซอฟต์แวร์จะใช้ โครงสร้างข้อมูลที่ได้สร้างขึ้น เพื่อวิเคราะห์ผลในการแสดงผลข้อมูล (Data Visualization)

ภาพกิจกรรมการเรียกดูแผนภูมิรูปภาพทั้งหมด โดยผู้ใช้งานสามารถเลือกดูแผนภูมิรูปภาพที่จะใช้ในการแสดงผลของข้อมูล โดยระบบจะมีให้เลือก โดยจะแสดงข้อมูลแผนภูมิรูปภาพทั้งหมด โดยจะแสดงแบบจำลองการทำงานดังภาพที่ 3-8



ภาพที่ 3-8 แผนภาพกิจกรรมเรียกดูแผนภูมิรูปภาพทั้งหมด

จากแผนภาพกิจกรรมที่ 3-8 จะเป็นการเรียกดูแผนภูมิรูปภาพ โดยเลือกเมนู Visualize ตามด้วยการเลือกชนิดของแผนภูมิที่ต้องการ เลือกชุดข้อมูล (Index) ที่ต้องการที่จะวิเคราะห์ผล จากนั้นเลือก Field ของข้อมูลเพื่อทำการแสดงผลการสร้างแผนภูมิรูปภาพ ผู้ดูแลระบบสามารถสร้างแผนภูมิได้ โดยการเลือกชนิดของแผนภูมิที่ต้องการ และทำการเลือกชุดข้อมูล (Index) เพื่อทำการสรุปผลข้อมูล โดยจะแสดงแผนภาพกิจกรรม การสร้างแผนภูมิรูปภาพ ดังภาพที่ 3-9



ภาพที่ 3-9 แผนภาพกิจกรรมการสร้างแผนภูมิรูปภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

สรุปผลการปฏิบัติงานสหกิจศึกษา

การปฏิบัติงานสหกิจศึกษาตลอดระยะเวลา 4 เดือน หรือ 16 สัปดาห์ นับตั้งแต่วันที่ 5 สิงหาคม พ.ศ. 2562 จนถึงวันที่ 22 พฤศจิกายน พ.ศ. 2562 ภายใต้การปฏิบัติงาน ใน บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) โดยผู้ปฏิบัติงานสหกิจศึกษาได้รับมอบหมายให้พัฒนาระบบวิเคราะห์และแสดงผลข้อมูลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana โดยเริ่มจากการศึกษาการทำงานของตัวSoftwareที่ใช้รวมถึงข้อมูลที่จะต้องใช้ในการทำแผนภูมิรูปภาพ เพื่อที่จะทำให้สรุปผลออกมาได้ตรงตามความต้องการของผู้ใช้มากที่สุด

ในบทนี้จะเป็นการสรุปผลของการปฏิบัติงานสหกิจศึกษาตลอดระยะเวลา 4 เดือน ที่ได้ทำการพัฒนาระบบระบบวิเคราะห์และแสดงผลข้อมูลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana ซึ่งจะอธิบายรายละเอียดของส่วนต่าง ๆ ภายในระบบที่ได้ทำการพัฒนา ดังต่อไปนี้

หน้าต่างแสดงผลข้อมูลการใช้งานอินเทอร์เน็ตระบบจะแสดงผลการสรุปข้อมูล 3 รูปแบบ คือ แผนภูมิแท่ง แผนภูมิรูปโดนัทโดยจะแสดงผล เป็น 10 อันดับผู้ที่เข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ต่าง ๆ มากที่สุด 10 อันดับในระยะเวลา 30 วันที่ผ่านมา และตาราง แสดงชื่อผู้ใช้งาน และที่อยู่ IP เพื่อที่จะใช้ติดตามหรือจัดการผลผู้ใช้งานเหล่านั้นด้วยมาตรการที่เหมาะสมได้

ผังรูปภาพที่ 4-1



ภาพที่ 4-1 หน้าจอแสดงผลสรุปข้อมูลการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คำอธิบายภาพที่ 4-1 เป็นหน้าต่างแสดงภาพรวมการสรุปผลข้อมูล โดยจะมีแผนภูมิจำนวน 3 ชนิด คือ แผนภูมิรูปโดนัท ที่ด้ายซ้ายและด้านขวา จะแสดงสัดส่วนของประเภทของเว็บไซต์และรายละเอียดของเว็บไซต์ที่เข้าถึงมาก 10 อันดับ ต่อเวลาที่กำหนด แผนภูมิแท่งจะแสดงจำนวนรีเคสทั้งหมดภายในอินเทอร์เน็ตขององค์กร โดยแบ่งตามเวลาที่กำหนดซึ่งสามารถกำหนดเป็นรายวัน รายชั่วโมงหรือรายเดือน

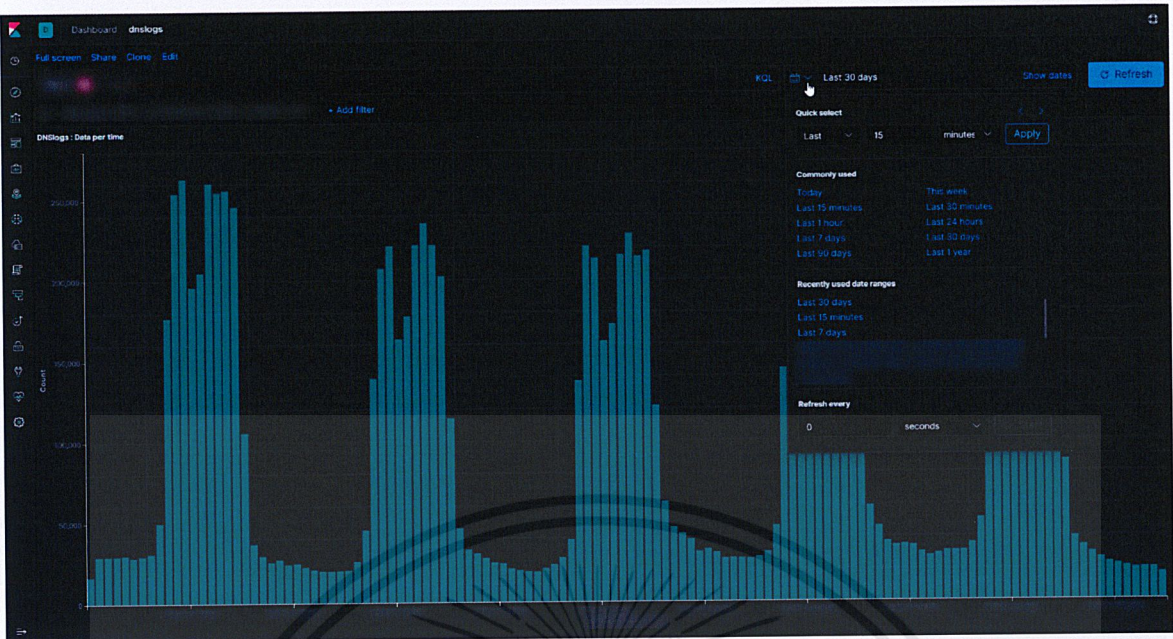


ภาพที่ 4-2 แผนภูมิรูปโดนัทแสดงสัดส่วนการเข้าถึงเว็บไซต์หรือเซอร์วิสต่าง ๆ มากที่สุด 10 อันดับ

คำอธิบายภาพที่ 4-2 แผนภูมิรูปโดนัท เป็นการแบ่งสัดส่วนการเข้าถึงเว็บไซต์หรือเซอร์วิสของผู้ใช้งาน แบ่งออกเป็นสองวงซ้อนกัน โดยวงด้านในจะแสดงถึง IP ที่เข้าเว็บไซต์หรือเซอร์วิสนั้น ๆ มากที่สุด 10 อันดับ และวงด้านนอกจะแสดงรายละเอียดถึง IP ดังกล่าว (วงด้านใน) ว่าเป็นผู้คนใดที่ใช้ IP ดังกล่าวบ้าง ป้ายกำกับบอกถึงรายละเอียดและสัดส่วนการใช้งานคิดเป็นร้อยละต่อทั้งหมด หน่วยเป็นเปอร์เซ็นต์ (%)

สำหรับการใช้แผนภูมิแท่งในการนำเสนอข้อมูลจะแสดงถึงจำนวนการเข้าเว็บไซต์หรือเซอร์วิสมากที่สุด โดยที่แนวนอนจะแสดงช่วงเวลาทีรีเคสถูกส่งและในแนวตั้งนั้น จะแสดงถึงจำนวนการรีเคสที่เข้าถึงเว็บไซต์หรือเซอร์วิสแสดงดังภาพที่ 4-3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



ภาพที่ 4-3 แผนภูมิแท่งแสดงถึงจำนวนการเข้าถึงเว็บไซต์หรือเซิร์ฟเวอร์ในช่วงเวลาที่กำหนด

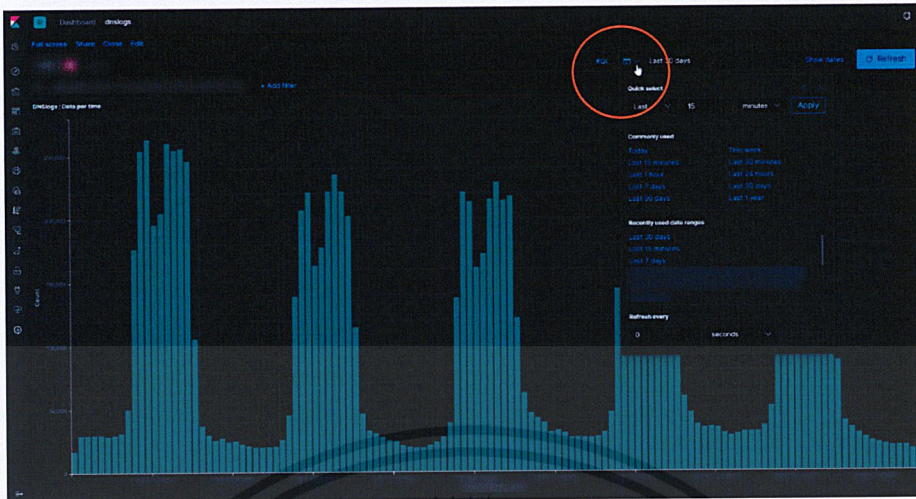
เมื่อผู้ใช้มีแผนภูมิแท่ง และแผนภูมิรูปโดนัทที่แสดงสัดส่วนการใช้งาน รวมถึงผู้ใช้งานอินเทอร์เน็ตสูงสุดแล้ว หากผู้ดูแลจำเป็นต้องการที่จะทราบที่อยู่ IP สามารถดูได้จากตารางข้อมูล ที่จะแสดงข้อมูลชื่อผู้ใช้งาน (Username) และ ที่อยู่ IP Address ของผู้ใช้งานได้ ดังภาพที่ 4-4

Internal IP	Identities	Count
		4,153,160
		3,303,925
		2,551,189
		2,286,335
		650,651
		643,963
		534,837
		529,131
		515,813
		507,759

ภาพที่ 4-4 ตารางแสดงชื่อของผู้ใช้งาน ที่อยู่ IP และจำนวนครั้งของการใช้งาน

ผู้ใช้งานสามารถเลือกขอบเขตของการแสดงผลของข้อมูลได้ โดยการเลือก Absolute ความหมาย คือ ระยะเวลาที่แน่นอน หรือ Relative คือ การเลือกที่จะดูข้อมูลที่มีหน่วยเป็นระยะเวลา วัน ชั่วโมง หรือนาทีก่อนหน้านี้ได้ ดังภาพที่ 4-5

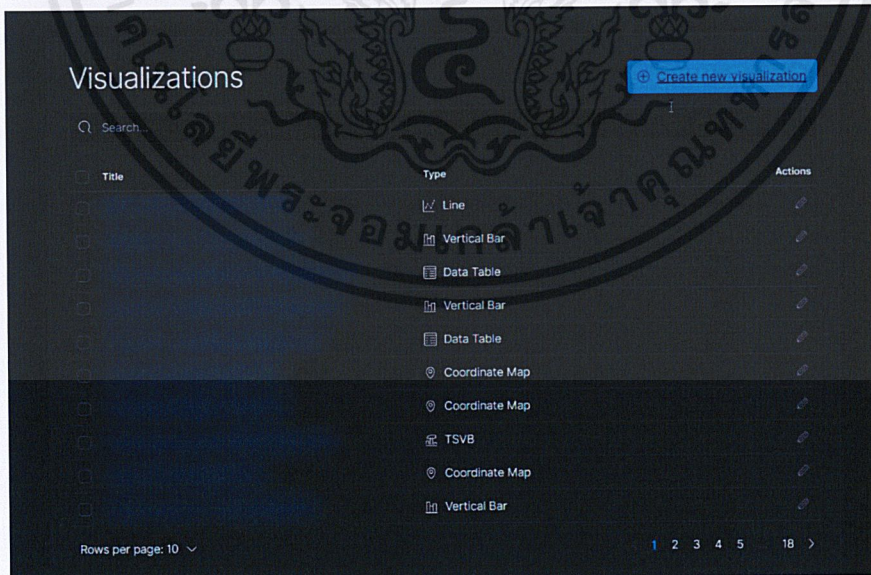
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



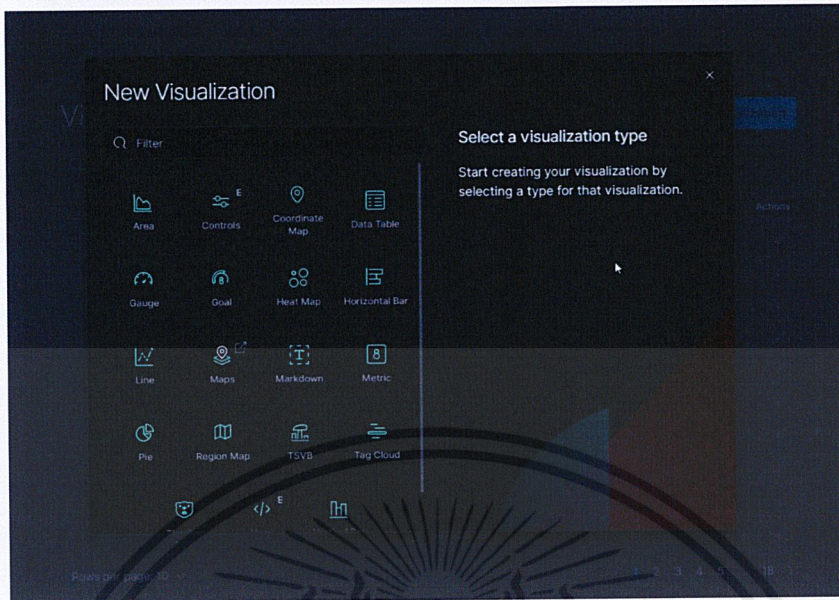
ภาพที่ 4-5 การเลือกขอบเขตระยะเวลาผลการวิเคราะห์ข้อมูล

4.1 การสร้างแผนภูมิรูปภาพ

ผู้ใช้สามารถเลือกที่จะสร้างแผนภูมิรูปภาพ โดยการนำข้อมูลที่ผ่านการวิเคราะห์สรุปเพื่อการ นำเสนอ ในรูปแบบของแผนภูมิ สามารถเลือกได้ไม่ว่าจะเป็น กราฟเส้น กราฟแท่ง โคนัท หรือการ สรุปผลในรูปแบบของ ตารางได้ ดังในรูปภาพที่ 4-6 และ รูปภาพที่ 4-7



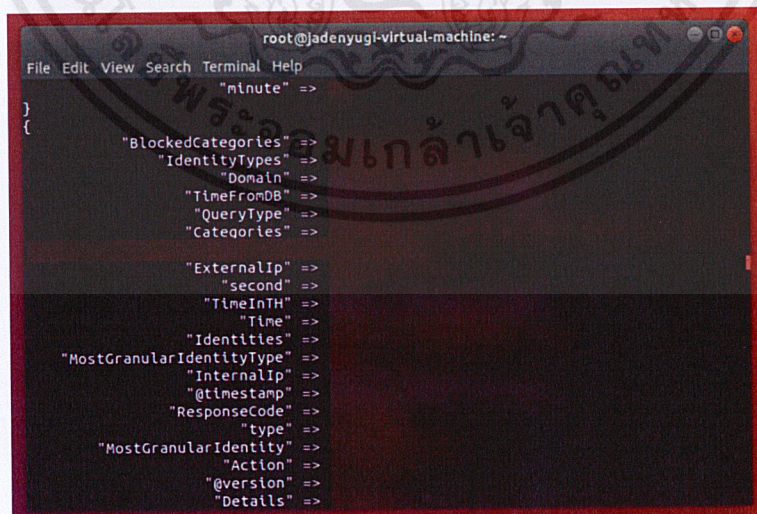
ภาพที่ 4-6 เมนูการเลือกสร้างแผนภูมิภาพ



ภาพที่ 4-7 เมนูเลือกประเภทแผนภูมิรูปภาพ

4.2 การนำเข้าข้อมูล

การที่จะวิเคราะห์ข้อมูลได้นั้นจำเป็นต้องมีกระบวนการนำเข้าข้อมูลก่อน ดังนั้นผู้ใช้ จำเป็นต้องมีการนำข้อมูลเข้า เพื่อคัดกรองข้อมูล และนำข้อมูลนั้นสร้างเป็นโครงสร้างข้อมูล เพื่อให้ง่ายต่อการวิเคราะห์และแสดงผลของข้อมูล ดังภาพที่ 4-8

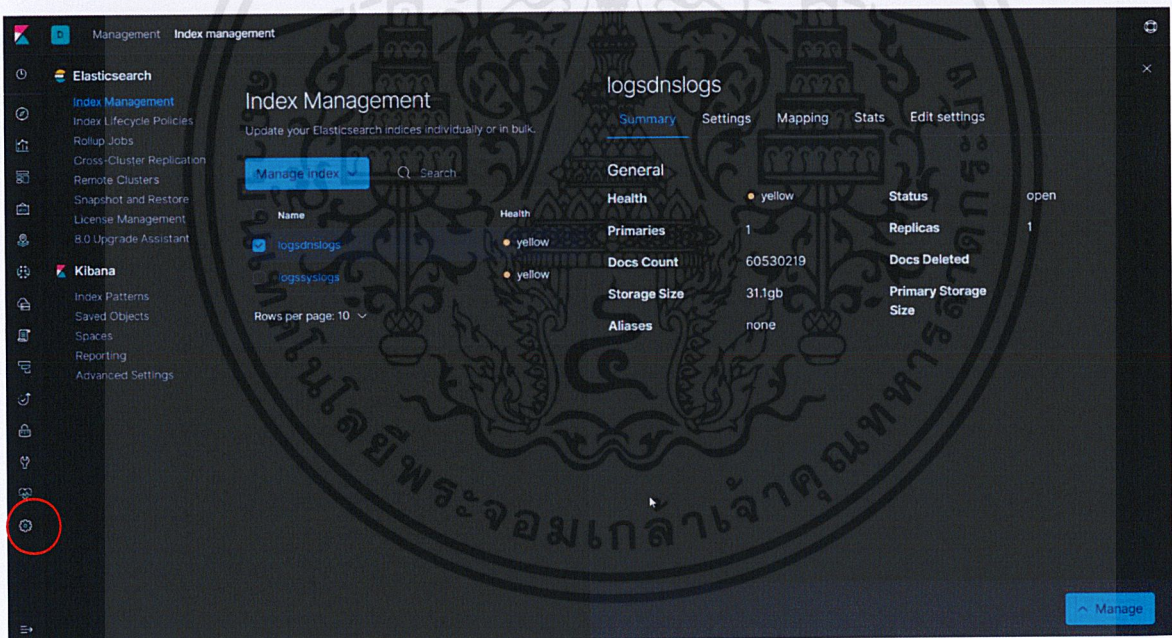


ภาพที่ 4-8 หน้าจอแสดงผลเมื่อทำการนำเข้าข้อมูล

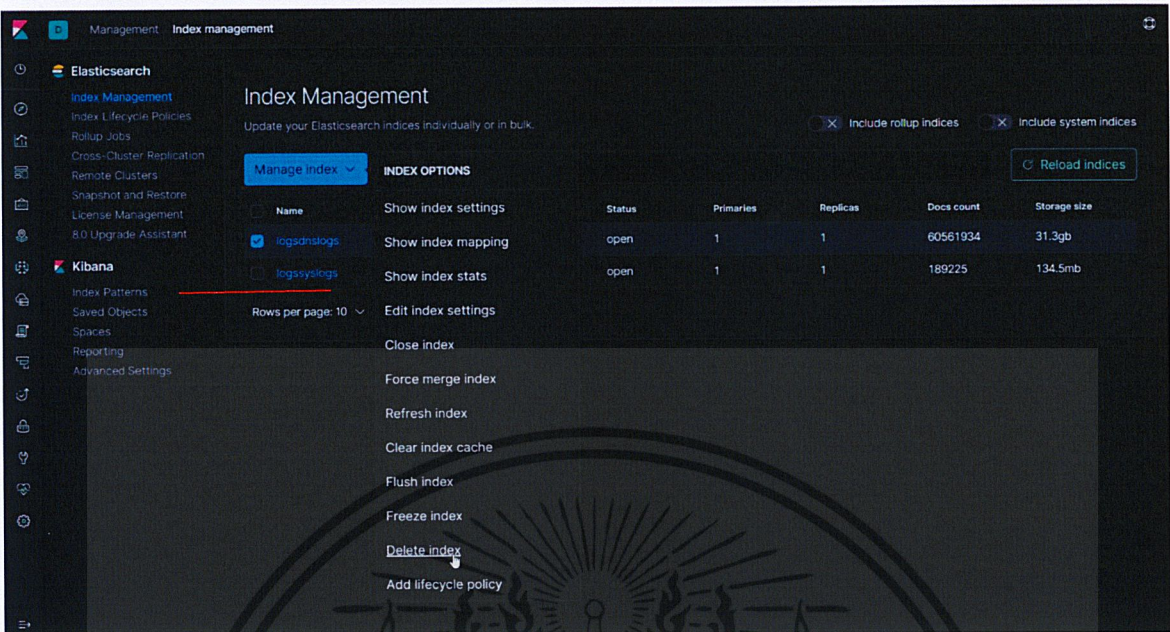
4.3 การลบข้อมูล

เมื่อผู้ใช้งานสามารถนำข้อมูลเข้าได้แล้ว และหากมีความจำเป็นที่ต้องการจะลบข้อมูล Index สามารถทำได้โดยการเลือกข้อมูล Index ที่ต้องการ การลบข้อมูลนั้นจะเป็นการลบข้อมูลที่บันทึกใน Elasticsearch ซึ่งทำได้โดยการเข้าไปลบด้วยตัวเอง หรือจะเป็นการตั้งค่าเพื่อการลบข้อมูลอัตโนมัติ โดยการตั้งเวลาการเก็บข้อมูลสามารถทำได้โดยการเลือกเมนู Management ตามด้วยเลือก

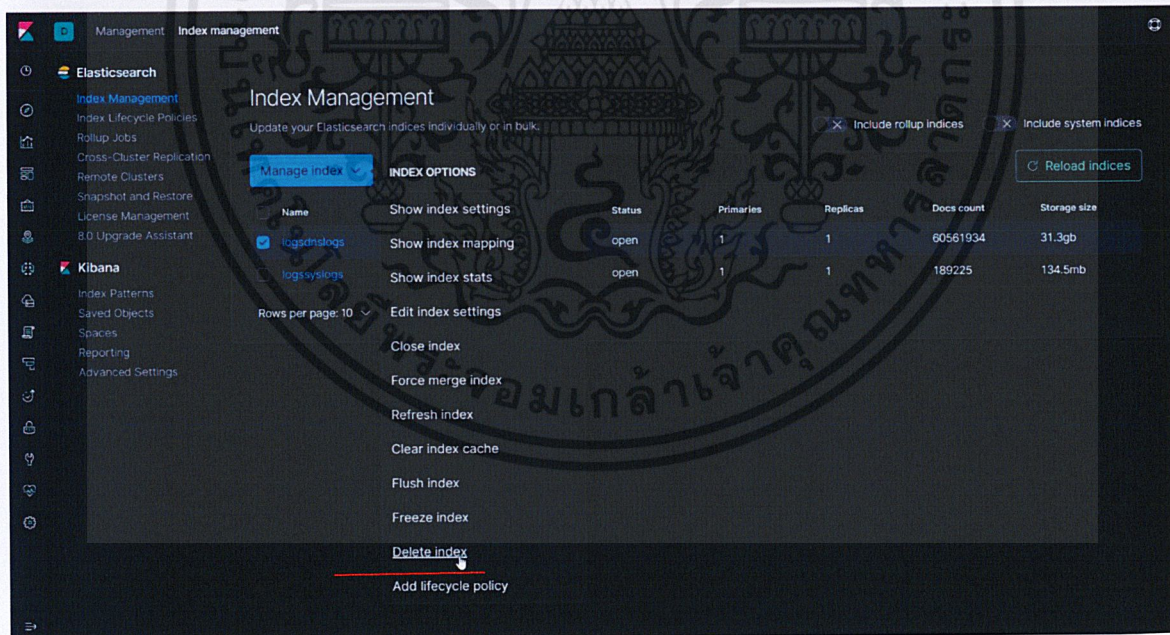
Index management ในหัวข้อของ Elasticsearch จากนั้นเลือก Index ที่ต้องการจะลบ ทำเครื่องหมาย ที่ Index ที่ต้องการลบจากนั้นเลือก Manage Index และตามด้วยเลือก Delete Index ระบบจะทำการแสดงหน้าต่างยืนยันการลบ เลือก Confirm เพื่อยืนยันการลบข้อมูล ดังในรูปภาพที่ 4-9 ถึง รูปภาพที่ 4-10 ซึ่งจะเป็นขั้นตอนการลบข้อมูล Index ที่ต้องการดังนี้



ภาพที่ 4-9 หน้าจอแสดงขั้นตอนการลบข้อมูลโดยการเลือกเมนู Management

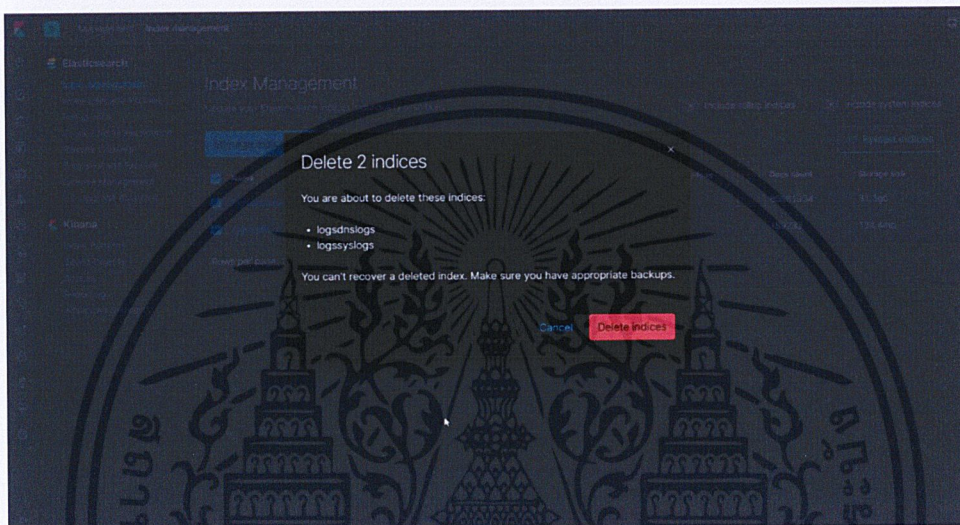


ภาพที่ 4-10 หน้าจอแสดงขั้นตอนการลบข้อมูลเลือก index ที่ต้องการลบ



ภาพที่ 4-11 หน้าจอแสดงขั้นตอนการลบข้อมูลหลังจากที่เลือก Index

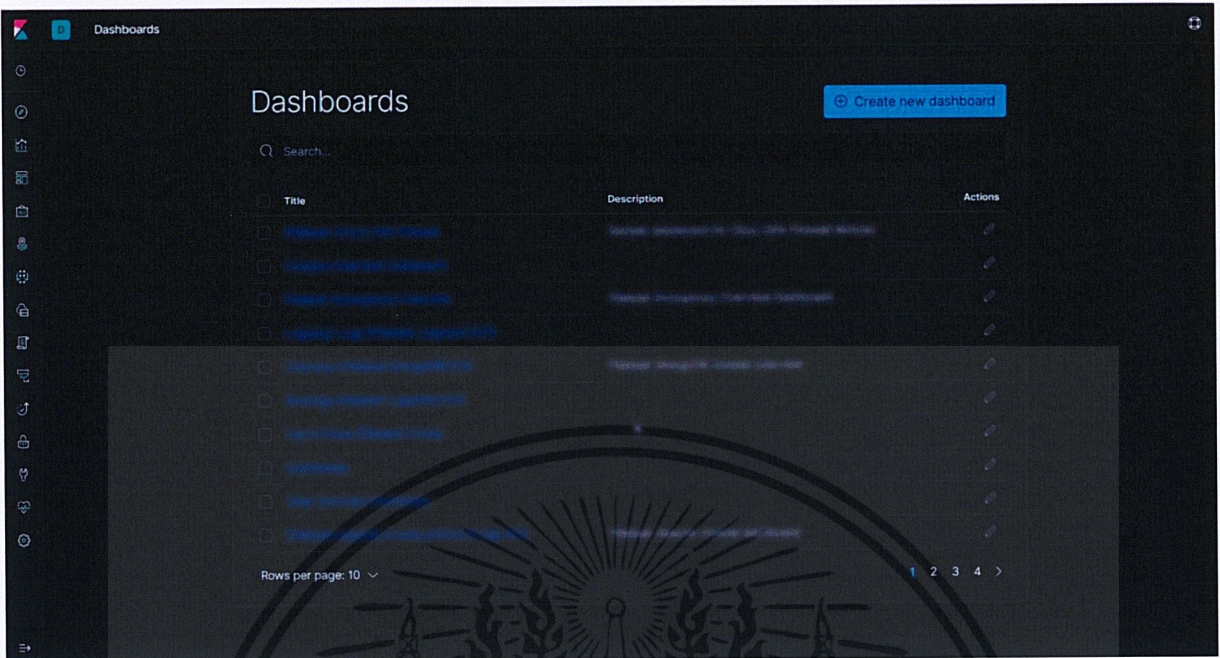
การลบข้อมูล Index นั้นจะเป็นการลบข้อมูลที่ได้ทำการบันทึกในซอฟต์แวร์ Elasticsearch ซึ่งหากทำการลบข้อมูล ซึ่งขั้นตอนการลบนั้น จำเป็นต้องมีความระมัดระวังเป็นอย่างสูง เพราะการลบ ข้อมูล Index จะทำให้แผนภูมิต่าง ๆ ที่ได้ทำการอ้างอิงจากชุดข้อมูล Index ที่ลบไปนั้นเสียหายได้ ซึ่งหน้าต่างแสดงการยืนยันในการลบข้อมูลจะแสดงดังภาพที่ 4-12 ดังนี้



ภาพที่ 4-12 หน้าจอแสดงขั้นตอนการลบข้อมูล และทำการยืนยันการลบข้อมูล

4.4 การเรียกดูหน้าต่างการสรุปผลข้อมูล

ผู้ใช้สามารถเลือกเมนู Dashboard แล้วทำการค้นหาหน้าต่างสรุปผลข้อมูลได้โดยการกดปุ่ม ค้นหาแผนภูมิรูปภาพที่สร้างเอาไว้ได้ โดยการค้นหานี้จำเป็นต้องมีการบันทึกหน้าต่างสรุปผลมาก่อน โดยหน้าต่างสรุปผลทั้งหมดนั้นจะถูกแสดงบนหน้าจอ โดยเรียงจากหน้าต่างสรุปผลที่ถูกสร้างใหม่ล่าสุดดังภาพที่ 4-13



ภาพที่ 4-13 การเรียกดูหน้าต่างสรุปผลข้อมูล

คำอธิบายภาพที่ 4-13 เป็นการเรียกดูหน้าต่างสรุปผลข้อมูลที่ได้ทำการบันทึกเอาไว้ จากการสร้างแผนภูมิรูปภาพ โดยหน้าต่างสรุปผลนั้นจะเป็นการรวบรวมแผนภูมิต่าง ๆ ไว้ด้วยกัน เพื่อที่จะสามารถติดตามความเคลื่อนไหวของข้อมูลได้ มีความสามารถในการแบ่งปันหน้าต่างสรุปผล ให้กับผู้อื่น ที่จะสามารถเข้ามาดูหน้าต่างการสรุปผลได้อีกด้วย สามารถทำได้โดยการแชร์การเข้าถึงผ่านเว็บไซต์ (URL Link)

บทที่ 5

สรุปและวิจารณ์ผลการปฏิบัติงานสหกิจศึกษา

5.1 สรุปผลการปฏิบัติงานสหกิจศึกษา

หลังจากได้ปฏิบัติงานสหกิจศึกษา ณ บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ในตำแหน่ง ผู้ปฏิบัติงานสหกิจศึกษาในแผนก Network ฝ่าย Hybrid Infrastructure ซึ่งได้ดำเนินงานตามแผนงานที่ผู้นิเทศงานมอบหมายในการปฏิบัติงานสหกิจศึกษาครั้งนี้มอบหมาย โดยมีการมอบหมายงานตามความเหมาะสม โดยมีการทำงานเอกสาร การตั้งค่าอุปกรณ์ การนำเสนอข้อมูล และได้รับมอบหมายในการทำระบบวิเคราะห์และแสดงผลข้อมูลการใช้งานอินเทอร์เน็ตในรูปแบบกราฟ โดยใช้ Kibana และการทำวิดีโอ User Guide การใช้งานเบื้องต้นของ Cisco Webex Meeting โดยประสบการณ์ที่ได้รับ คือ ได้เรียนรู้ถึงความแปลกใหม่ของสายอาชีพรวมถึงความแตกต่างจากการเรียนในห้องเรียนทั้งได้เรียนรู้ด้วยตัวเอง ได้ทดลองสิ่งต่าง ๆ การหาทางแก้ไขปัญหาด้วยตัวเองและการทำงานร่วมกันกับผู้อื่น

จากการปฏิบัติงานสหกิจศึกษา ณ บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ในตำแหน่ง ผู้ปฏิบัติงานสหกิจศึกษา แผนก Network ฝ่าย Hybrid Infrastructure ครั้งนี้ได้รับมอบหมายให้พัฒนาระบบวิเคราะห์และแสดงผลข้อมูลเข้าถึงเว็บไซต์หรือเซอร์วิสภายในองค์กรในรูปแบบภูมิรูปภาพโดยใช้ Kibana ช่วยให้การจัดการระเบียบข้อมูลให้เป็นโครงสร้างตามที่ต้องการ รวมไปถึงการนำเสนอในรูปแบบภูมิซึ่งง่ายต่อการวิเคราะห์ข้อมูลที่ได้ ไม่ว่าจะเก็บเว็บไซต์หรือเซอร์วิสที่อนุญาตหรือไม่อนุญาตให้เข้าถึงจำนวนการเข้าถึง รวมไปถึงไอพีแอดเดรสของผู้ที่เข้าใช้เว็บไซต์หรือเซอร์วิสนั้น ๆ เพื่อนำไปประกอบการแก้ปัญหาภายในองค์กร

5.2 ปัญหา อุปสรรคในการปฏิบัติงานสหกิจศึกษา และแนวทางแก้ปัญหา

เนื่องจากการปฏิบัติงานสหกิจศึกษาตลอดระยะเวลา 16 สัปดาห์ ทั้งการพัฒนาระบบ การเรียนรู้ภาษา การพัฒนาโปรแกรมใหม่ ๆ นั้นจำเป็นต้องทำความเข้าใจ เรียนรู้ เพื่อที่จะใช้ในการพัฒนาสิ่งนั้น การที่ไม่เข้าใจใหม่ ๆ หน้าที่ของผู้ปฏิบัติงานสหกิจศึกษา คือต้องหมั่นศึกษา เพื่อนำความรู้ไปประกอบการทำงานและการเรียนรู้นั้นทำให้ สามารถนำความรู้ไปใช้ ในอนาคตได้

5.3 ข้อเสนอแนะ

ในการปฏิบัติงานสหกิจศึกษา ณ บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) เป็นระยะเวลา 16 สัปดาห์ ผู้ปฏิบัติงานสหกิจศึกษามีข้อเสนอแนะเพื่อเป็นแนวทางสำหรับผู้ปฏิบัติงานสหกิจศึกษาดังนี้

1. ผู้ปฏิบัติงานสหกิจศึกษาต้องหมั่นศึกษาหาความด้วยตนเอง เนื่องจากเทคโนโลยีนั้นก้าวหน้าอยู่ทุกเมื่อ จำเป็นต้องเรียนรู้สิ่งใหม่ ๆ อยู่เสมอ
2. จำเป็นต้องมีระเบียบ มีความรับผิดชอบต่อหน้าที่
3. ต้องรู้จักการปรับตัว เรียนรู้ที่จะเข้ากับสังคมใหม่ ๆ การให้ความช่วยเหลือกับผู้อื่น



เอกสารอ้างอิง

[1] บันทึกการทดลองติดตั้ง ELK Stack — Elasticsearch Logstash Kibana. (2019) [ออนไลน์].

วันที่สืบค้น 19 November 2019, เข้าถึงได้จาก :

<https://medium.com/@hatoriz/%E0%B8%9A%E0%B8%B1%E0%B8%99%E0%B8%97%E0%B8%B6%E0%B8%81%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%97%E0%B8%94%E0%B8%A5%E0%B8%AD%E0%B8%87%E0%B8%95%E0%B8%B4%E0%B8%94%E0%B8%95%E0%B8%B1%E0%B9%89%E0%B8%87-elk-stack-elasticsearch-logstash-kibana-2e125c53cebdelas>

[2] Elasticsearch introduction | Elasticsearch Reference [7.4] | Elastic. (2019) [ออนไลน์].

วันที่สืบค้น : 19 November 2019, เข้าถึงได้จาก

<https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html>

[3] Logstash Introduction | Logstash Reference [7.4] | Elastic. (2019) [ออนไลน์].

วันที่สืบค้น : 19 November 2019, เข้าถึงได้จาก

<https://www.elastic.co/guide/en/logstash/current/introduction.html>

[4] Introduction | Kibana Guide [7.4] | Elastic. (2019) [ออนไลน์]. วันที่สืบค้น: 19 November 2019,

เข้าถึงได้จาก: <https://www.elastic.co/guide/en/kibana/current/introduction.html>

[5] ESXi | Bare Metal Hypervisor | VMware. (2019) [ออนไลน์]. วันที่สืบค้น: 19 November 2019,

เข้าถึงได้จาก: <https://www.vmware.com/products/esxi-and-esx.html>

[6] การติดตั้ง VMware Server บน Windows. (2019) [ออนไลน์]. วันที่สืบค้น: 19 November 2019,

เข้าถึงได้จาก: <https://www.softmelt.com/article.php?id=100>

[7] การพัฒนาระบบด้วย Waterfall - GlurGeek.Com. (2019) [ออนไลน์].

วันที่สืบค้น : 19 November 2019, เข้าถึงได้จาก :

<http://www.glurgeek.com/education/%E0%B8%A3%E0%B8%B0%E0%B8%9A%E0%B8%9A%E0%B8%88%E0%B8%B3%E0%B8%A5%E0%B8%AD%E0%B8%87%E0%B8%81%E0%B8%A3%E0%B8%B0%E0%B8%9A%E0%B8%A7%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%97%E0%B8%B3%E0%B8%87%E0%B8%B2/>

[8] พัฒนาระบบ (2) - วิเคราะห์ออกแบบระบบ. (2019) [ออนไลน์]. วันที่สืบค้น : 19 November 2019,

เข้าถึงได้จาก : <http://www.macare.net/analysis/index.php?id=-8>

[9] Common DNS Request Types. (2019). วันที่สืบค้น : 19 November 2019, เข้าถึงได้จาก :

<https://support.umbrella.com/hc/en-us/articles/232252848-Common-DNS-Request-Types>

ประวัติผู้เขียน

หัวข้อโครงการ	ระบบวิเคราะห์และแสดงผลข้อมูลในรูปแบบกราฟของข้อมูลในลักษณะ dnslogs ผ่าน Kibana
ชื่อ - สกุล	นายพงศธร ทังสฤดี
คณะ	วิศวกรรมศาสตร์
ภาควิชา	วิศวกรรมคอมพิวเตอร์
สาขาวิชา	วิศวกรรมสารสนเทศ
วันเดือนปีเกิด	1 ธันวาคม 2540
ที่อยู่	กรุงเทพมหานคร ประเทศไทย
ช่องทางการติดต่อ	titanguardian.15@gmail.com

ประวัติส่วนตัว