ระบบการตรวจจับข้อมูลและวิเคราะห์ข้อมูลและวิเคราะห์ข้อมูลเชิงลึกในองค์กร กรณีศึกษาสถานประกอบการเอกชนแห่งหนึ่ง

SYSLOG DETECTION AND IN-DEPTH ANALYSIS SYSTEM FOR ORGANIZATION

นายณัฐพล บุญไทย

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศทางธุรกิจ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยี ไทย-ญี่ปุ่น
พ.ศ. 2560

ระบบการตรวจจับข้อมูลและวิเคราะห์ข้อมูลและวิเคราะห์ข้อมูลเชิงลึกในองค์กร กรณีศึกษาสถานประกอบการเอกชนแห่งหนึ่ง

SYSLOG DETECTION AND IN-DEPTH ANALYSIS SYSTEM FOR ORGANIZATION

นายณัฐพล บุญไทย

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศทางธุรกิจ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย - ญี่ปุ่น
ปีการศึกษา 2560

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(ดร. สรรม์พร เจริญพิทย์)

..... กรรมการสอบ
(อาจารย์ภัสมะ เจริญพงษ์)

..... อาจารย์ที่ปรึกษา
(อาจารย์ฐนสิน ญาติสูงเนิน)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์นุชนารถ พงษ์พานิช)

ชื่อโครงงาน	ระบบการตรวจจับข้อมูลและวิเคราะห์ข้อมูลเชิงลึกในองค์กร กรณีศึกษาสถานประกอบการเอกชนแห่งหนึ่ง Syslog detection and In-depth analysis system for organization.
ผู้เขียน	ณัฐพล บุญไทย
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชาเทคโนโลยีสารสนเทศทางธุรกิจ
อาจารย์ที่ปรึกษา	อาจารย์ฐนสิน ญาติสูงเนิน
พนักงานที่ปรึกษา	คุณนิติวัฒน์ พงษ์นยศาสตร์ และคุณพิทมญช์ อภิรักษ์ขิต
ชื่อบริษัท	บริษัท เอ-โฮสต์ จำกัด
ประเภทธุรกิจ/สินค้า	ผู้ให้บริการด้าน Hosing Service, IBM และ Oracle Product

บทสรุป

การปฏิบัติสหกิจศึกษาได้รับตำแหน่ง Assistant Technical Consultant (Channel IBM Service) ปฏิบัติหน้าที่ผู้ช่วยด้านเอกสารสำหรับส่งมอบลูกค้า และจัดทำเอกสารแจ้งการอัพเดตระบบ รวมไปถึงการวาดแผนผังโครงสร้าง (Infrastructure) ให้กลายเป็นระบบโครงสร้างใหม่ พร้อมสำหรับการใช้งานกับบุคคลภายในองค์กร และเรียนรู้ระบบคำสั่งคอมพิวเตอร์ (Command line)

จากการได้รับปฏิบัติในหน้าที่ต่าง ๆ ทำให้เรียนรู้และได้รับประสบการณ์งานทางด้าน System Engineer ซึ่งสามารถตรวจสอบระบบคอมพิวเตอร์ภายใน เรียกใช้แสดงผลหรือควบคุมเพื่อใช้งานระบบภายใน และทำให้เข้าใจถึงวิธีการปฏิบัติสำหรับงานทางด้าน System Engineer มากขึ้น ทำให้สามารถนำประสบการณ์ต่าง ๆ ที่ได้รับไปประยุกต์ใช้ต่อการปฏิบัติงานในอนาคต

Project's name	Syslog detection and In-depth analysis system for organization.
Writer	Natthapol Boonthai
Faculty	Information Technology, Business Information Technology
Faculty Advisor	Tanasin Yatsungnoen
Job Supervisor	Nitiwat Pongnayasart, Pittamon Apirakkhit
Company's name	A-Host Company Limited.,
Business Type / Product	Application and Hosting Service, Distributer IBM and Oracle product

Summary

Co-operative Education has been appointed as Assistant Technical Consultant. Provide system update documentation. Including drawing a structure to become a new structure. Ready for use with people inside the organization. And learn the command line system.

I have been working in various roles. To learn and gain experience in the field of System Engineer, which can monitor the internal computer system. Use display or control to operate the system internally. And to understand how to work for System Engineer more to bring the experience. To be applied to the future work.

กิตติกรรมประกาศ

การได้ทำสหกิจศึกษา ณ บริษัท เอ-โฮสต์ จำกัด ในการจัดวิชา สหกิจศึกษา ตั้งแต่วันที่ 16 พฤษภาคม พ.ศ. 2560 ถึงวันที่ 29 กันยายน พ.ศ. 2560 ส่งผลทำให้เกิดการพัฒนาศักยภาพในการเรียนรู้และประสบการณ์จากการปฏิบัติงานจริง ซึ่งเป็นประสบการณ์ที่ทำให้พัฒนาความสามารถในการคิด วิเคราะห์ ปรับปรุงองค์ความรู้ให้เหมาะสมกับอนาคตที่พัฒนาอยู่ตลอดเวลา สำหรับการทำโครงงานสหกิจนี้ สามารถบรรลุไปได้ด้วยดี ด้วยความช่วยเหลือ ดังนี้

คุณบุญประสิทธิ์ ตั้งชัยสุข ที่เห็นความสำคัญในการปฏิบัติสหกิจศึกษา ที่มีคุณค่าแก่การพัฒนาศักยภาพรอบด้าน และให้ปฏิบัติสหกิจศึกษา ณ บริษัทแห่งนี้

คุณสุชัย เย็นฤดี ที่จัดอบรมเพื่อเตรียมความพร้อมก่อนเข้าปฏิบัติสหกิจศึกษา ทำให้ได้รับความรู้และคำแนะนำสิ่งที่เหมาะสมกับความสามารถ เมื่อเริ่มสหกิจศึกษาสามารถทำงานที่รับมอบหมายได้ ตลอดระยะเวลาที่ปฏิบัติงานสหกิจศึกษา

คุณพิชานน จะเรียมพันธ์, คุณนิติวัฒน์ พงษ์นยศาสตร์, คุณพิทมญช์ อภิรักษ์ขิต ที่ให้ความกรุณารับข้าพเจ้า เข้ามาปฏิบัติงานในแผนก IBM Channel Service ในการปฏิบัติสหกิจศึกษาในครั้งนี้

คุณสุชัย เย็นฤดี, คุณนิติวัฒน์ พงษ์นยศาสตร์, คุณพิทมญช์ อภิรักษ์ขิต, คุณสาธิษฐ์ ปอเจริญ, คุณวรวุฒิ สนามคงศักดิ์, คุณไพโรจน์ ทองดี, คุณศรุต เสรารมย์, คุณณัฐกมล สอนประหยัด, คุณจีรภัทร ใจเพ็ชร, คุณธนกฤต อิทธิไมย์ยะ คุณธนากร เพ็ชรผึ้ง และคุณดำรงรักษ์ ช่วยค้ำชู ที่ให้คำปรึกษาแนะนำเกี่ยวกับความรู้ทางด้านการทำงานต่าง ๆ รวมถึงทุกคนในแผนก และบุคคลท่านอื่น ๆ ที่มิได้กล่าวนาม ที่ได้ให้คำแนะนำช่วยเหลือไม่มากก็น้อยในการปฏิบัติงานสหกิจศึกษาและจัดทำรายงานฉบับนี้ให้บรรลุผลตามเป้าหมายไปได้ด้วยดี ขอขอบคุณ ไว้ ณ ที่นี้

หากมีความผิดพลาดประการใดในรายงานฉบับนี้ ทางผู้จัดทำขอน้อมรับไว้เพื่อปรับปรุงแก้ไขในโอกาสต่อไป

นายณัฐพล บุญไทย

ผู้จัดทำรายงาน

29 กันยายน 2560

สารบัญ

สารบัญรูป

รูป **หน้า**

สารบัญตาราง

ตาราง **หน้า**

บทที่ 1
บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการ[1]

ชื่อหน่วยงาน บริษัท เอ-โฮสต์ จำกัด (A-HOST Company Limited)

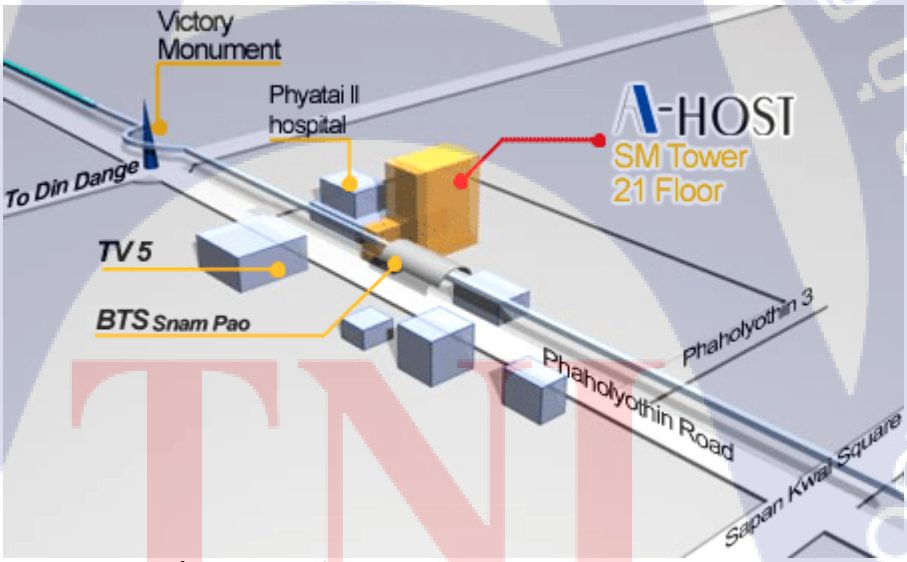
ที่ตั้ง เลขที่ 979/52-55 ชั้น21 อาคาร SM Tower ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400

โทรศัพท์ 02-298-0625-32

แฟกซ์ 02-298-0053

เว็บไซต์ http://www.a-host.co.th

อีเมล์ marketing@a-host.co.th



ภาพที่ 1.1 แผนที่ตั้ง บริษัท เอ-โฮสต์ จำกัด[1]

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร[1]

บริษัท เอ-โฮสต์ จำกัด ก่อเมื่อปี พ.ศ. 2542 เป็นบริษัทหนึ่งในเครือของบริษัท เมโทร ซิสเต็มส์ คอร์เปอเรชั่น (มหาชน) จำกัด และเป็นผู้เชี่ยวชาญด้านบริการจัดวางระบบไอที และบริการเสริมต่าง ๆ สำหรับลูกค้าตั้งแต่ธุรกิจขนาดย่อมไปจนถึงขนาดกลาง

ธุรกิจหลักของบริษัท เอ-โฮสต์ คือ การให้บริการโฮสติ้ง (Hosting) และบริการระบบไอทีด้วยผลิตภัณฑ์ของออราเคิล (Oracle) และไอบีเอ็ม (IBM) ซึ่งเป็นซอฟท์แวร์สำหรับการวางแผนบริหารทรัพยากรขององค์กร (ERP) ระดับแนวหน้าของโลก

ในการดำเนินธุรกิจของ เอ-โฮสต์ ตลอดระยะเวลา 10 ปี ไม่เพียงแต่ในฐานะผู้บุกเบิกธุรกิจโฮสติ้ง (Hosting) และธุรกิจการให้บริการแอพพลิเคชัน (Application) ในรูปแบบ ASP เท่านั้น แต่ เอ-โฮสต์ ยังได้ทำการติดตั้งระบบไอที รวมทั้งผลิตภัณฑ์ของออราเคิล (Oracle) ให้กับลูกค้าจนประสบความสำเร็จมาแล้วเป็นจำนวนมาก ซึ่งหลายรายเป็นหนึ่งในร้อยบริษัทชั้นนำของประเทศไทย แต่ที่สำคัญกว่านั้นก็คือการที่ เอ-โฮสต์ ได้สานสัมพันธ์กับลูกค้า และพันธมิตรทางธุรกิจอย่างแนบแน่นจนกลายเป็นหุ้นส่วนทางกลยุทธ์ และเป็นผู้สนับสนุนสำคัญที่มีส่วนช่วยผลักดันให้ธุรกิจของลูกค้าเติบโตสู่ความสำเร็จ

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร[1]

ภาพที่ 1.2 คณะผู้บริหารบริษัท เอ-โฮสต์ จำกัด ของแต่ละแผนก[1]

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง	Assistant Technical Consultant
หน้าที่งานที่ได้รับมอบหมาย	วาดโครงสร้างการเชื่อมต่อ Internet Infrastructure และ System Infrastructure โดยใช้โปรแกรม Visio และการทำเอกสารต่าง ๆ ทางด้าน System Engineer

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

ชื่อ	นายนิติวัฒน์ พงษ์นยศาสตร์
ตำแหน่ง	Technocal Consultant
ชื่อ	นายพิทมญช์ อภิรักษ์ขิต
ตำแหน่ง	Assistant Technical Consultant

1.6 ระยะเวลาที่ปฏิบัติงาน

ปฏิบัติงานสหกิจศึกษาเป็นระยะเวลา 4 เดือน 15 วัน นับตั้งแต่วันที่ 16 พฤษภาคม 2560 ถึงวันที่ 29 กันยายน 2560

1.7 ที่มาและความสำคัญของปัญหา

ปัจจุบันภายในองค์กรมีเหตุการณ์ (Event) ที่เกิดขึ้นและต้องการโปรแกรมในการจัดเก็บและตรวจจับ (monitoring) เหตุการณ์ที่เกิดขึ้น และเนื่องจากต้องการโปรแกรมที่สามารถใช้งานโปรแกรมใช้งานได้อย่างเสรี (Open Source) ดังนั้นจึงจัดทำโครงงานนี้เพื่อตรวจสอบเหตุการณ์ที่ผิดปกติ (Alert) ที่เกิดขึ้น

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

1.) มีความเข้าใจในโครงสร้างของระบบ

2.) สามารถเข้าใจการทำงานเซอร์วิส (Service) ต่าง ๆ รวมถึงการใช้งานไฟร์วอลล์ (Firewall)

3.) สามารถติดตั้งโปรแกรมด้วยคอมมานด์ไลน์ (Command line) ได้

4.) เข้าใจคำสั่งต่าง ๆ ที่ต้องการเรียกใช้งาน

5.) โปรแกรมพร้อมทำงานจริง สามารถส่งมอบให้ผู้อื่นดูแลต่อได้

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

1.) นำความรู้ที่ได้รับไปประยุกต์ใช้กับงานและหน้าที่จะได้รับในอนาคต

2.) สามารถทำงานร่วมกับผู้อื่นได้ดียิ่งขึ้น

3.) เข้าใจในการทำเอกสารประกอบตลอดระยะเวลาในการทำโครงงาน

4.) มีความรู้ในการเตรียมพร้อมการนำเสนอโครงงาน

5.) การรับผิดชอบต่อหน้าที่หรืองานที่ได้รับมอบหมาย

6.) สามารถทำงานในสถานการณ์ของการทำงานจริงได้

7.) มีทักษะความรู้ในการทำงานเฉพาะทางได้ดีขึ้น

1.10 นิยามศัพท์เฉพาะ

Event : เหตุการณ์ที่เกิดภายในระบบภายใน เช่น การเข้าเชื่อมต่อระบบภายใน

Monitoring : การตรวจสอบและการจับเหตุการณ์ที่เกิดขึ้น

Open-souce : โปรแกรมฟรีที่สามารถใช้งานได้อย่างอิสระ

Alert : การแจ้งเตือนที่ผิดปกติ

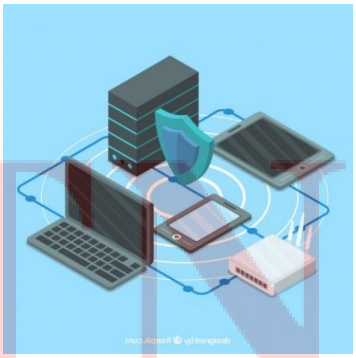
Service : การใช้งานบริการของโปรแกรม

บทที่ 2
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

ในการปฏิบัติงานสหกิจศึกษาครั้งนี้ ได้นำความรู้ทางด้านทฤษฎีและเทคโนโลยีสารสนเทศใช้ในการปฏิบัติงานตลอดการปฏิบัติสหกิจศึกษา ซึ่งเป็นการนำความรู้จากการเรียนรู้ศึกษาและประสบการณ์ต่าง ๆ นำมาใช้ในการทำโครงการสำหรับการจบการศึกษาในครั้งนี้เพื่อให้สอดคล้องกับทฤษฎีที่นำมาใช้

2.1 ทฤษฎีที่เกี่ยวข้องกับระบบรักษาความปลอดภัย (Security System)[2]

การรักษาความปลอดภัย (Security) ของระบบเทคโนโลยีสารสนเทศ (Information Technology) ถือเป็นหัวใจหลักที่สำคัญในการดำเนินธุรกิจ เนื่องจากปัจจุบันด้วยความสำคัญของระบบเทคโนโลยีสารสนเทศ (Information Technology) พัฒนาให้มีความสามารถสูงยิ่งขึ้นทุกวัน และการโจมตีระบบเครือข่าย (Network) ก็ยิ่งซับซ้อนขึ้นทุกวัน ทำให้องค์กรต่าง ๆ ต้องหันมาลงทุนทางด้านการรักษาความปลอดภัยของระบบเครือข่าย (Network) เพื่อไม่ให้ข้อมูลที่มีความสำคัญและเป็นความลับ ถูกทำลายหรือถูกขโมยไป รวมไปถึงการควบคุมและดูแลระบบเพื่อไม่ให้เกิดการหยุดการทำงาน (Downtime) ในระบบเครือข่าย ที่นำมาซึ่งความเสียหายต่อระบบธุรกิจอย่างมหาศาล



ภาพที่ 2.1 การเชื่อมระบบเครือข่ายที่มีระบบรักษาความปลอดภัย[2]

2.1.1 นิยามของ Security information and event manament (SIEM)[2]

ระบบรักษาความปลอดภัยของข้อมูลและการจัดการเหตุการณ์ (Security Information and Event Management) หรือ SIEM คือ ระบบที่กลายเป็นคำตอบหลักเพื่อตรวจจับและยับยั้งทุกการโจมตีให้ได้มาก

ที่สุด ด้วยแนวคิดในการนำข้อมูลทางด้านความปลอดภัยจากอุปกรณ์ทั้งหมด มาประมวลผลร่วมกับภายในระบบเครือข่าย (Network) เพื่อตรวจหาการโจมตีต่าง ๆ ที่อาจหลุดรอดมาจากอุปกรณ์รักษาความปลอดภัยแต่ละชนิดมาได้ โดยการทำหาความสัมพันธ์ (Correlation) เพื่อค้นหาพฤติกรรมการโจมตีระบบเครือข่ายที่กำลังเกิดขึ้น และทำการแจ้งเตือนผู้ดูแลระบบแบบ Real-Time เพื่อทำการยับยั้งเหตุการณ์ให้ได้ทันท่วงที อีกทั้งยังมีการสรุปข้อมูลทางด้านความปลอดภัยทั้งหมดเพื่อสร้างรายงาน (Reporting) สำหรับใช้ได้ทั้งการตรวจสอบตามวิธีการหาความสัมพันธ์ (Compliance) และการวางแผนในการเสริมความปลอดภัยให้ระบบเครือข่ายขององค์กร

2.1.2 คุณลักษณะที่ดีของ Security information and event manament (SIEM)[2]

ระบบ SIEM ที่ดี ควรจะต้องสามารถกำหนด (Custom) ได้ตามความต้องการขององค์กร แต่ละองค์กรมีระบบแอพพลิเคชั่น (Application) เพื่อตอบสนองความต้องการของธุรกิจที่แตกต่างกัน พฤติกรรมการใช้งานของผู้ใช้งานที่แตกต่างกัน และผู้ดูแลระบบก็ต้องตรวจสอบหรือเฝ้าระวังภัยต่าง ๆ ที่แตกต่างกัน ดังนั้นระบบ SIEM ที่ดี ควรจะต้องเปิดให้แต่ละองค์กรสามารถนำมาปรับใช้เข้ากับระบบเทคโนโลยีสารสนเทศ (Information Technology) ภายในองค์กรให้ได้มากที่สุด ไม่ว่าจะเป็นการรวบรวมข้อมูลจากข้อมูลเครื่อง (Machine Data) ของอุปกรณ์เครือข่าย (Network) ได้หลากหลายรูปแบบเพื่อให้สามารถติดตั้งใช้งานได้อย่างยืดหยุ่น ทั้งจาก Log, SNMP (Simple Network Management Protocol) , Network Traffic, Network Flow, API (Application Programming Interface) และอื่น ๆ รวมถึงความสามารถในการประมวลผลหรือค้นหาเหตุการณ์ (Event) ต่าง ๆ และนำมาแสดงผลหรือแจ้งเตือนไปยังผู้ดูแลระบบในแต่ละกลุ่มได้ตามต้องการ ให้ทำงานและประสานงานเพื่อการรักษาความปลอดภัยขององค์กรเป็นไปได้อย่างราบรื่นสูงสุด

2.1.3 ข้อดีและข้อเสียของ Security Information and Event Manament (SIEM)[3]

กล่าวถึงหลักการทำงานของเทคโนโลยี SIEM นั้น การทำงานหลักของระบบ SIEM จะพึ่งพาข้อมูลที่จะเข้ามาในระบบด้วย Log จากอุปกรณ์ทางด้านความมั่นคงปลอดภัยและระบบงานต่าง ๆ ที่ติดตั้งใช้งานในเครือข่ายองค์กร ยกตัวอย่างเช่น Firewall, IPS (Intrusion Prevention System) , Antivirus รวมไปถึงแอพพลิเคชัน (Application) ระบบฐานข้อมูล (Database) ในองค์กร เช่น Web Application, Database Server, File Server เป็นต้น ซึ่งในปัจจุบัน Log ที่กล่าวถึงข้างต้น มีข้อมูลที่ไม่เพียงพอให้กับระบบ SIEM วิเคราะห์หาภัยคุกคามที่เกิดได้ เนื่องจากข้อจำกัดดังต่อไปนี้

2.1.3.1 รูปแบบการติดตั้งเพื่อนำเข้าข้อมูล (Deployment Form Factor)[3]

Agent การติดตั้งซอฟต์แวร์ขนาดเล็ก ลงบนระบบงานและระบบความมั่นคงปลอดภัย เพื่อดึงข้อมูล Log จากระบบต่าง ๆ แล้วส่งมาที่ระบบ SIEM ซึ่งก่อให้เกิดผลกระทบต่อประสิทธิภาพการทำงานของระบบต้นทาง ประการแรกเนื่องจากต้องใช้ทรัพยากรจากระบบ ประการที่สองส่งผลให้การบริหารจัดการทำได้ยากหาก Agent นั้น ๆ หยุดทำงานลงไป ทำให้ขาดความคล่องตัวในการทำงานและเกิดข้อขัดแย้งกับการบริหารจัดการระบบที่ต้องมีการร้องขอเพื่อทำการติดตั้งบำรุงรักษาและอัพเกรด (Upgrade) ซอฟต์แวร์ (Software) ต่าง ๆ

Agentless การรับส่ง Log อีกวิธีหนึ่ง คือ ตั้งค่าให้อุปกรณ์ในระบบเครือข่ายทำการส่งข้อมูล Log มาที่ระบบ SIEM โดยตรง ข้อดีคือความสะดวก แต่มีข้อเสีย ได้แก่ ประการแรก การเปิดให้อุปกรณ์ต่าง ๆ ส่งข้อมูล Log มาทั้งหมดจะทำให้ประสิทธิภาพและทรัพยากรของระบบนั้น ๆ ลดลงไปโดยอัตโนมัติ ประการที่สอง เนื่องจากอุปกรณ์หลาย ๆ ประเภทจะทำการส่ง Log ในรูปแบบข้อมูล Plain Text ซึ่งไม่มีการเข้ารหัส จึงสุ่มเสี่ยงที่จะถูกโจมตีแบบ Man-in-the-middle และ Log ถูกเปลี่ยนแปลงแก้ไขก่อนที่จะส่งมาถึงระบบ SIEM ขององค์กร

Virtual machine traffic การตรวจสอบข้อมูลที่รับส่งมาในรูปแบบแสดงผล (Visualize) ทำได้ยาก เนื่องจากหากต้องการข้อมูลหลายชนิดของระบบงานและระบบความมั่นคงปลอดภัยที่ทำงานในvirtualization นั้น จะต้องใช้จำนวนซอฟต์แวร์ (software) Agent จำนวนมาก ก่อให้เกิดจุดที่ระบบ SIEM เข้าไปดูแลไม่ทั่วถึง

Internet of Things (IoT) ในปัจจุบันอุปกรณ์ประเภท Internet of Things ได้มีบทบาทและจำนวนมากขึ้น เช่น ระบบกล้องวงจรปิด ระบบความปลอดภัยทางด้านกายภาพ (Physical Access Control) อุปกรณ์นี้ส่วนใหญ่ไม่สามารถส่ง Log ออกมาได้ รวมถึงไม่สามารถติดตั้งซอฟต์แวร์Agent ลงไปได้ด้วยเช่นกัน ทำให้เกิดจุดอ่อนที่ระบบ SIEM ไม่สามารถไปตรวจจับได้อย่างครอบคลุมเนื่องจากไม่สามารถเก็บข้อมูล Log จากอุปกรณ์ IoT ได้

2.1.3.2 SSL Visibility[3]

ในปัจจุบันข้อมูลหลายชนิดของระบบงานและการใช้งานอินเทอร์เน็ต (internet) มีการปกป้องความลับด้วยเทคโนโลยีการเข้ารหัสลับที่เรียกว่า SSL/TLS ซึ่งเป็นข้อดีอย่างมหาศาล แต่ก็มีข้อเสีย คือ ข้อมูลที่ถูกเข้ารหัสด้วย SSL/TLS นั้นไม่สามารถถอดรหัสออกมาเพื่อส่งต่อให้ระบบ SIEM เข้าไปวิเคราะห์หาภัยคุกคามภายในได้ ส่งผลให้การลงทุนระบบรักษาความปลอดภัยหลายล้านบาทสูญเปล่า

2.1.3.3 False Positive[3]

ระบบ SIEM จำเป็นต้องมีการปรับเพื่อลดอัตราการเกิด False positive แต่ในปัจจุบันการทำ Fine-tuning ให้ระบบ SIEM มีความถูกต้องแม่นยำนั้น ได้เพิ่มความยากและมีอุปสรรคมากขึ้น เช่น การจัดเก็บข้อมูล Log ไม่ครอบคลุมเนื่องด้วยข้อจำกัดของ license ที่จะต้องสอดคล้องกับจำนวนซอฟต์แวร์ (software) Agent ที่ได้ทำการจัดซื้อ, ไม่สามารถเข้าถึงข้อมูล Log ของระบบงานบางอย่างเช่น IoT, VM, Cloud, BYOD ทำให้การวิเคราะห์ของ SIEM ไม่มีความแม่นยำเพียงพอ และไม่สามารถที่จะทำ Fine-tuning ได้อย่างมีประสิทธิภาพ เพราะไม่มีข้อมูลดิบที่จะนำเข้ามาวิเคราะห์ได้

อีกประเด็นซึ่งเป็นเรื่องสำคัญมาก คือ ทำอย่างไรที่จำแนกแยกแยะผลของการวิเคราะห์ของ SIEM ว่าเหตุการณ์ใดเป็นผลกระทบเชิงความมั่นคงปลอดภัย และเหตุการณ์ใดเป็นผลกระทบเชิงประสิทธิภาพของระบบงาน ซึ่งประเด็นนี้เป็นความท้าทายที่น่าสนใจ เพราะไม่ใช่ทุกเหตุการณ์จะเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยทั้งหมด อาจเป็นผลกระทบจากทรัพยากรในระบบงานก็เป็นได้

2.1.3.4 Hop by Hop Analytics[3]

การวิเคราะห์ของ SIEM ในปัจจุบันนั้นเป็นการวิเคราะห์แบบ Horizontal analysis หมายความว่าทำการวิเคราะห์ในมิติเดียว ซึ่งเป็นผลมาจาก SIEM เก็บข้อมูลแบบ หนึ่งต่อหนึ่ง ตัวอย่างเช่น Log จากระบบฐานข้อมูลที่ส่งเข้ามายัง SIEM ก็จะเป็น Log จากระบบฐานข้อมูลที่ตั้งอยู่ใน Data center แห่งเดียวเท่านั้น ทำให้ SIEM ไม่สามารถรู้ได้ว่าหากระบบฐานข้อมูลตอบกลับการร้องขอไปที่ผู้ใช้ที่อยู่ต่างเครือข่าย จะมีการตอบสนองที่ถูกต้องหรือไม่

สิ่งที่ขาดไปของ SIEM ก็คือการวิเคราะห์ในหลายมิติ เป็นการวิเคราะห์ข้อมูลจากหลาย ๆ Hop ของเครือข่าย (network) เพื่อทำการตรวจสอบว่า ในแต่ละช่วงของเครือข่ายที่เชื่อมต่อผ่านขอบเขตของ Router หรือ Firewall ทำงานได้ปกติ หรือมีความเสี่ยงต่อภัยคุกคามหรือไม่ โดยการวิเคราะห์และเปรียบเทียบเพื่อเชื่อมโยงความสัมพันธ์ระหว่างแต่ละ Tier ให้เกิดความแม่นยำในการตรวจจับยิ่งขึ้น

2.2 OSSEC[4]

OSSEC เป็นโปรแกรมใช้งานได้อย่างเสรี (Open Source) ที่มีระบบการตรวจจับการบุกรุก (Host-based Intrusion Detection System) หรือ HIDS ซึ่งสามารถทำงานได้หลายแพลตฟอร์ม (Multi-platform) โดยมีเครื่องมือที่สามารถทำการวิเคราะห์ความสัมพันธ์และมีประสิทธิภาพ รวมการวิเคราะห์ Log (Integrating Log Analysis), การตรวจสอบความสมบูรณ์ของไฟล์ (File Integrity Checking), การตรวจสอบรีจิสทรีของ Windows (Windows registry monitoring), การบังคับใช้นโยบายการรวมศูนย์ (Centralized policy enforcement), การตรวจหา Rootkit (Rootkit Detection), การแจ้งเตือนแบบเรียลไทม์ (Real-Time

Alerting) และการตอบสนองที่รวดเร็ว (Active Response) ทำงานบนระบบปฏิบัติการส่วนใหญ่ ได้แก่ Linux, OpenBSD, FreeBSD, MacOS, Solaris และ Windows.

ภาพที่ 2.2 OSSEC Logo[4]

2.2.1 วิธีการทำงานของ OSSEC[4]

ภาพที่ 2.3 Architecture[4]

OSSEC จะประกอบด้วย 2 ส่วนคือ OSSEC Server และ OSSEC Agent ส่วนงานของ Server หน้าที่คือ ประมวลผลและทำการวิเคราะห์ความสัมพันธ์ (correlation), แจ้งเตือนเหตุการณ์ที่ผิดปกติ (alert) เป็นต้น ส่วน Agent จะทำหน้าที่นำข้อมูลมาให้ Server หากต้องการให้เครื่องที่ต้อง monitor ให้นำ Agent ติดตั้งในเครื่องที่ต้องการ โดยมีรายละเอียดต่าง ๆ ดังนี้

2.2.1.1 OSSEC Server

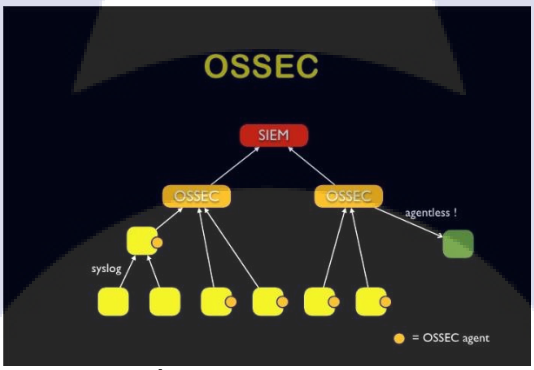
เป็นส่วนที่เป็นศูนย์กลางของ OSSEC โดยทำหน้าที่ ประมวลผล, วิเคราะห์ความสัมพันธ์ (correlation) ตรวจสอบ Log ที่ได้รับจากเครื่องที่นำ Log เข้ามาตรวจสอบได้ และยังสามารถแจ้งเตือนให้ผู้สังเกตุการณ์ได้ทั้ง E-mail และ API โดยสามารถตั้งค่าในการรับการแจ้งเตือนได้ในโปรแกรมของ OSSEC

เพราะเป็นโปรแกรมที่ตอบสนองกับเวลาปัจจุบัน (Real-time) จึงทำให้ผู้ที่ทำ monitoring สามารถแก้ไขข้อผิดพลาดได้ทันเวลา ก่อนเกิดเหตุการณ์รุกรานเกินกว่าจะแก้ไขได้

2.2.1.2 OSSEC Agent [4]

เป็นส่วนที่นำข้อมูล Log จากเครื่องต่าง ๆ ให้กับ OSSEC Server โดยการนำข้อมูลจากเหตุการณ์ (event) ที่เกิดขึ้นจากเครื่อง เก็บบันทึกเป็นข้อมูล Log และนำ Log นั้นส่งมาที่ OSSEC Server โดยใช้ Port 514 เป็นช่องทางในการส่งข้อมูล Syslog ที่มีข้อมูลของเหตุการณ์ทั้งหมดที่เกิดขึ้นจากการใช้งานหรือการเปลี่ยนแปลงต่าง ๆ ในระบบของ OSSEC Agent นั้นจะแบ่งออกเป็น 2 ระบบ ดังนี้

1. Agentless มีหน้าที่ในการนำ Log จากเครื่องที่ไม่สามารถติดตั้งโปรแกรม Agent เช่น การนำเอาข้อมูล Log ของเครื่องที่ไม่มีระบบปฏิบัติการ (Operating System) แต่อาจนำ Log ไม่เท่ากับการติดตั้ง Agent แต่ระบบของ Agentless ไปเรียกเก็บ Log จาก history Log ที่เครื่องได้สร้างทุกวัน โดย Log ที่เครื่องสร้างนั้นจะมีอายุการเก็บที่ไม่นาน Agentless จึงไปเรียกเก็บเพื่อส่งมาที่ OSSEC Server ตัวอย่าง Firewall, Printer, Scanner, Router, Switches, Database, Smart-phone เป็นต้น.



ภาพที่ 2.4 OSSEC Agentless[4]

2. Agent มีหน้าที่ในการนำ Log ของเครื่องที่ติดตั้งมีระบบปฏิบัติการ (Operating System)ที่จำเป็นต้องรู้ IP ปลายทางของเครื่องที่ต้องการเก็บ Logโดย OSSEC Server จะสร้าง Authentication key ให้กับ OSSEC Agent ทุกเครื่องโดยเป็นรหัสที่ OSSEC Server ถอดรหัสมาจากการตั้ง Agent ID + Agent Name มาเป็นรหัสที่มีความยาว 128 ตัวขึ้นไปให้กับ OSSEC Agent ในการขอเชื่อมต่อและส่ง Syslog ให้กับ OSSEC Server ในการวิเคราะห์และประมวลผล เพื่อหาความเสี่ยงภายในเหตุการณ์ (Event) ที่เกิดขึ้นตลอดเวลา

ภาพที่ 2.5 OSSEC Agent[4]

2.3 MySQL Database[5]

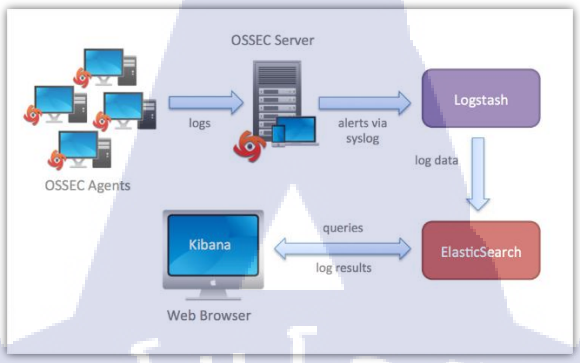
โปรแกรมระบบจัดการฐานข้อมูล ที่พัฒนาโดยบริษัท MySQL AB มีหน้าที่เก็บข้อมูลอย่างเป็นระบบ รองรับคำสั่ง SQL เป็นเครื่องมือสำหรับเก็บข้อมูล ที่ต้องใช้ร่วมกับเครื่องมืออื่น เพื่อให้ได้ระบบงานที่รองรับความต้องการของผู้ใช้ เช่น การทำงานร่วมกับเครื่องบริการเว็บ (Web Server) เพื่อให้บริการแก่ภาษา Script ที่ทำงานฝั่งเครื่องบริการ (Server-Side Script) เช่น ภาษา php ภาษา APS.Net หรือภาษา APS เป็นต้น หรือทำงานร่วมกับโปรแกรมประยุกต์ (Application Program) เช่น ภาษา Visual Basic.Net ภาษา Java และภาษา C# เป็นต้น โปรแกรมถูกออกแบบให้สามารถทำงานได้บนระบบปฏิบัติการ (Opareting System) ที่หลากหลาย และระบบฐานข้อมูลที่เป็นโปรแกรมใช้งานได้อย่างเสรี (Open Source) ที่ถูกนำไปใช้งานมากที่สุด

2.3.1 การใช้งาน MySQL

การเก็บข้อมูล (Data) สำหรับการทำ Syslog ของ OSSEC นั้นสามารถตั้งค่าให้โปรแกรมเรียกใช้งาน MySQL ได้ด้วยการตั้งค่า OSSEC Server ให้เป็นทำการพักข้อมูล Log ที่ผ่านการประมวลผลแล้ว ให้อยู่ในสภาพพร้อมใช้และสามารถเรียกใช้ข้อมูลจาก MySQL Database นี้เข้าโปรแกรมอื่นเพื่อประมวลผลต่อได้ทันที โดย OSSEC นั้นมี โครงสร้างของการสร้างฐานข้อมูล (Database) มากับการติดตั้ง OSSEC Server โดยตารางทั้งหมดของ OSSEC อ้างอิงมาจากโปรแกรมการวิเคราะห์ผลของข้อมูล (Information) แล้วสามารถนำข้อมูลนี้เข้า MySQL ได้ต้องตรงกับซินแท็ก (Syntax) ที่โปรแกรมมีเท่านั้น

ภาพที่ 2.6 MySQL Logo[5]

2.4 Elastic[6]



ภาพที่ 2.7 การใช้ Elastic ร่วมกับ OSSEC[7]

ในการทำงานของระบบ SIEM เป็นส่วนของการเรียก Syslog ในการตรวจสอบ วิเคราะห์ และประมวลผลต่าง ๆ โดยโปรแกรม OSSEC นั้นในส่วนของหน้าที่ส่วนใหญ่จะเป็นวิธีการหา ความเสี่ยงภายในระบบเครือข่าย (Network) และข้อผิดพลาดต่าง ๆ เพื่อให้ผู้ทำการ Monitor สามารถรับรู้ถึงความเสี่ยงได้เพื่อให้แก้ไขปัญหาก่อนที่เกิดความเสียหายและเป็นวงกว้างมากยิ่งขึ้นหน้าที่ของ OSSEC ช่วยด้านความปลอดภัย (Security) มากกว่าการแสดงผล (Visualize) ดังนั้นจำเป็นต้องใช้โปรแกรม Elastic ในการสร้างกราฟต่าง ๆ ให้ผู้ทำการ Monitor เข้าใจผลกระทบได้ง่ายและสามารถประเมินความเสี่ยงในอนาคตเพื่อทำการแก้ไข ปรับปรุง และเปลี่ยนแปลง สำหรับการรองรับการเรียกใช้ทรัพยากรต่าง ๆ ภายในเครื่องให้เหมาะสมเพียงพอในใช้งานในปัจจุบัน

ภาพที่ 2.8 Elastic Logo[6]

โปรแกรม Elastic เป็นโปรแกรมที่แสดงผลจากการนำข้อมูล (Data) เข้าระบบ Elastic โดยขั้นตอนของการนำข้อมูลเข้าระบบนั้นมีโปรแกรมที่ให้บริการ (Service) สำหรับการติดตั้งเป็นส่วนเฉพาะการใช้งานโปรแกรมที่ให้บริการ (Service) เกิดการทำงานผิดพลาดหรือหยุดการทำงาน (Downtime) จะทำให้ระบบ

ของ Elastic ไม่สามารถทำงานต่อไปได้ ดังนั้นจึงต้องระมัดระวัง ที่โปรแกรมมีความต้องการเรียกใช้งานโปรแกรมที่ให้บริการ (Service)ใน Elastic ตัวต่อไป ด้านความต้องการในการเรียกใช้งานทรัพยากรคอมพิวเตอร์สามารถแยกแยะได้ชัดเจน การทำงานโดยปกติ Elasticsearch เรียกใช้งาน CPU ในระดับปานกลางเพื่อให้ Kibana ทำงาน เมื่อนำข้อมูล (Data) เข้าระบบ Elastic เรียกใช้งาน Logstash ซึ่งใช้ CPU สูงมาก ทำให้โปรแกรมที่ให้บริการ (Service) ของ Elasticsearch ปิดตัวลง เพื่อให้ Logstash ทำงานได้อย่างเต็มประสิทธิภาพโดยรายละเอียดของความสามารถของแต่ละโปรแกรมให้บริการ (Service) ที่สำคัญต่อการใช้งานมี ดังนี้

2.4.1 Logstash[6]

ทำหน้าที่ในการเรียกข้อมูลเข้าระบบ Elastic ข้อมูลที่ผ่านการวิเคราะห์และประมวลผล จาก OSSEC เป็นข้อมูลใน MySQL ที่อยู่ในสภาพพร้อมใช้งาน หลักการใช้งาน คือ เขียนไฟล์ (File) ในลักษณะ .conf ให้มีความสามารถเข้าไป MySQL Database ของ OSSEC และเรียกข้อมูล (Information) ที่ Logstash ได้มานั้นจะเป็นเก็บเป็นข้อมูล .json โดยโปรแกรม Elastic นำ ข้อมูลจาก Logstash ไปวิเคราะห์ (Analysis) และประมวลผล (Process) ด้วยโปรแกรม Logstash การใช้งานต้องเรียกโปรแกรมและตามด้วยไฟล์คำสั่ง (File Configure) โปรแกรม Logstash จึงสามารถทำงานได้ เมื่อใช้งาน Logstash โปรแกรม Elasticsearch จะปิดการให้บริการ (Service) ทันทีเพื่อให้โปรแกรม Logstash ทำงานโดยใช้ Java Database Connectivity (JDBC) เพื่อใช้ทรัพยากร CPU

ภาพที่ 2.9 Logstash Logo[6]

2.4.2 Elasticsearch[6]

เสมือนศูนย์กลางของ Elastic โดย Elasticsearch มีหน้าที่ คือ วิเคราะห์ (Analysis) และประมวลผล (Process) เพื่อ Kibana ใช้งานข้อมูลต่าง ๆ ที่ Logstash ได้รับ ใช้ในการแสดงผล (Visualize) ได้ทันที โดยต้องทำการตรวจสอบที่มาของข้อมูลนั้นสามารถเรียกใช้งานได้หรือไม่ด้วยการเรียกการใช้บริการ (Service) ผ่านที่อยู่เครื่องตามด้วย Port 9200 โดยปกติโปรแกรม Elasticsearch ทำงานอยู่ตลอดเวลาในเวลาปกติ

ภาพที่ 2.10 Elasticsearch Logo[6]

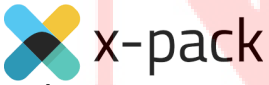
2.4.3 Kibana[6]

หน้าที่ คือ การแสดงผล (Visaulize) ข้อมูลทั้งหมดที่ได้รับจาก Elasticsearch เพื่อการทำกราฟและการทำรายงาน (Reporting) ต่าง ๆ ที่เป็นรูปภาพสามารถทำให้ผู้ทำการ Monitor เข้าใจข้อมูลภาพรวมได้ง่าย ด้วยการนำข้อมูลทำกราฟรูปแบบต่าง ๆ สามารถกำหนดเลือกวันที่, ระยะเวลา และรอบที่เกิดเหตุการณ์ (Event) ที่ต้องการได้อย่างอิสระ โดยการเรียกใช้งาน Kibana สามารถเรียกใช้งานได้ผ่าน Port 5601 และสุดท้ายนอกจากการเป็นโปรแกรมปลายทางที่ทำหน้าที่แสดงข้อมูลเป็นภาพต่าง ๆ ได้ Kibana ก็ยังมีความสำคัญต่อการเช็คสถานะการให้บริการ (Service) ทั้งหมดของ Elastic ได้โดยสามารถตรวจสอบโปรแกรมหยุดทำงาน (Downtime) สามารถแก้ไขระบบได้ถูกจุดทำให้ระบบโปรแกรมทำงานได้ปกติ

ภาพที่ 2.11 Kibana Logo[6]

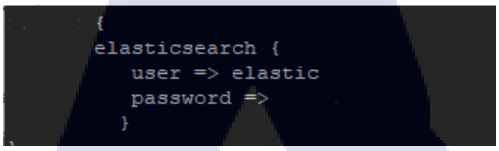
2.4.4 X-Pack[6]

ในการใช้งาน X-Pack เป็น Package ที่มีความสามารถสูงทั้งการเพิ่มประสิทธิภาพของโปรแกรม Elastic ให้มีเครื่องมือที่สามารถเรียกใช้งานเพิ่มเติม ในด้านระบบความปลอดภัย (Security) ของโปรแกรม Elastic ก็เพิ่มมากขึ้น โดย X-Pack ทำให้ทุก ๆ โปรแกรมใน Elastic จำเป็นต้องเข้าด้วยการใส่รหัสผ่านทุกโปรแกรมในการเรียกใช้งาน



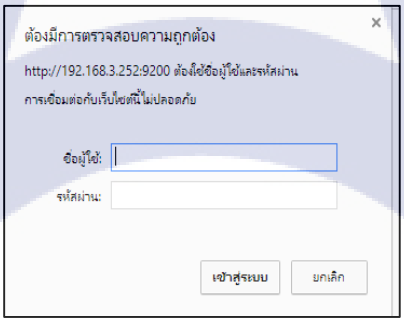
ภาพที่ 2.12 X-Pack Logo[6]

1.) Logstash การใช้งานของการดึงข้อมูลใน MySQL ต้องใส่ไฟล์คำสั่ง (File Configure) ที่จำเป็นต้องใส่ XML สำหรับการเข้ารหัสใน Logstash, Elasticsearch และ Kibana เพื่อให้ข้อมูลใน MySQL ไปถึง Kibana จำเป็นต้องใส่รหัสให้ตั้งแต่เริ่มใช้งานไปจนถึงปลายทางของโปรแกรม Elastic

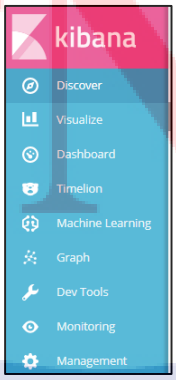


ภาพที่ 2.13 ระบบรักษาความปลอดภัยของ Logstash หลังจากติดตั้ง X-Pack

2.) Elasticsearch การได้รับข้อมูล (Data) จะไม่สามารถเข้าไปภายในเพื่อดูการวิเคราะห์ข้อมูลได้ จำเป็นต้องใส่รหัสผ่านเพื่อเข้าใช้งาน หรือการเพิ่มข้อมูลใหม่เข้าระบบ Elastic จำเป็นต้องเข้ารหัสที่ Elasticsearch ในที่อยู่ของเครื่องตามด้วย Port 9200 หากไม่เข้าจะทำให้ระบบไม่ตอบสนองกับคำสั่งใหม่ที่ทำลงไป

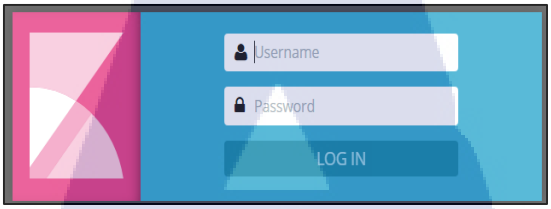


ภาพที่ 2.14 ระบบรักษาความปลอดภัยของ Elasticsearch หลังจากติดตั้ง X-Pack



ภาพที่ 2.15 เครื่องมือเพิ่มเติมของ Kibana หลังจากติดตั้ง X-Pack

3.) Kibana ในส่วนทุกท้ายที่ทำการติดตั้ง X-Pack จะสามารถใช้งานเครื่องมือที่เพิ่มเติมใหม่ได้ตามรูปภาพที่ 2.13 ได้แก่ Machine Learning, Graph และ Monitoring และมีระบบรักษาความปลอดภัยที่ติดตั้งอยู่ที่ Kibana โดยต้องเข้ารหัสก่อนเข้าโปรแกรม Kibana เพื่อใช้งานการทำรายงาน (Reporting) ต่าง ๆ



ภาพที่ 2.16 ระบบรักษาความปลอดภัยของ Kibana หลังจากติดตั้ง X-Pack

บทที่ 3
แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

ในการดำเนินการของการปฏิบัติงานเริ่มจากการเข้ารับ Requirement ของพี่ ๆ ความต้องการระบบ SIEM จนไปถึงการศึกษาระบบของ SIEM และทดลองติดตั้ง OSSEC ให้สามารถเรียกใช้บริการ (Service) ให้สามารถทำงานได้ปกติ แต่เนื่องจากโปรแกรม OSSEC นั้นไม่มีการแสดงผล (visualize) ไม่ดีเท่าที่ควร จึงจำเป็นต้องนำโปรแกรม Elastic เข้ามาเพิ่มเติมให้กับโปรแกรม SIEM ที่ทำให้ประสิทธิภาพการทำงานดีขึ้น ในด้านการทำรายงาน (Reporting) สุดท้ายคือการทำให้โปรแกรมรับ Syslog จาก Portalcaptive ให้ได้

3.1 แผนงานการปฏิบัติงาน

โครงการพัฒนาระบบ SIEM นี้ประกอบไปด้วยโปรแกรม OSSEC, Apache, PHP, MySQL, Elasticsearch, Logstash, Kibana.

ตารางที่ 3.1 แผนการปฏิบัติงาน

หัวข้องาน	เดือน มิ.ย. 2560				เดือนที่ ก.ค.2560				เดือน ส.ค. 2560				เดือน ก.ย. 2560			
1.) ศึกษา SIEM																
2.). เลือกโปรแกรม OSSEC																
3.) ศึกษาการติดตั้ง Elastic																
4.) ลงมือติดตั้ง Elastic																
5.) ศึกษา Rules ของ OSSEC																
6.) ทดลอง Syslog ใหม่																
7.) ศึกษา OSSEC + Elastic																
8.) ศึกษา XML																
9.) แก้ไข X-Pack																
10.) แก้ไข้ข้อมูลให้ถูกต้อง																

3.2 รายละเอียดที่นักศึกษาปฏิบัติในการฝึกงาน

สหกิจศึกษาเริ่มต้นด้วยการสอนงานด้วยการจัดหาพนักงานที่มีความเชียวชาญทางด้านต่าง ๆ ฝึกอบรม แนะนำ และให้คำปรึกษาแก่นักศึกษาจนกระทั่ง จัดหาตำแหน่งที่เหมาะสมกับนักศึกษาทุกคน ทำให้มีความรู้ ความสามารถพื้นฐาน เข้าใจงานที่ได้รับมอบหมาย ทำให้จัดการงานที่ได้รับมอบหมาย จากงานที่ได้รับจากพี่พนักงานส่วนมากเป็นงานที่ต้องการใช้จริง จึงจำเป็นที่จะต้องใส่ใจในงานและให้พี่พนักงานตรวจสอบความถูกต้องของงานและสมบูรณ์ที่สุด

3.2.1 งานที่ได้รับมอบหมาย ณ สถานที่ฝึกงาน

1.) จัดทำเอกสาร Pricing Cloud ของแต่ละผู้ให้บริการ

2.) จัดทำรูปเล่ม Hardware Installation Summary

3.) จัดทำเอกสารในการ Check NMOM

4.) จัดทำเอกสาร Patch Availability

5.) จัดทำ Diagram Network DC A-HOST (Infrastructure)

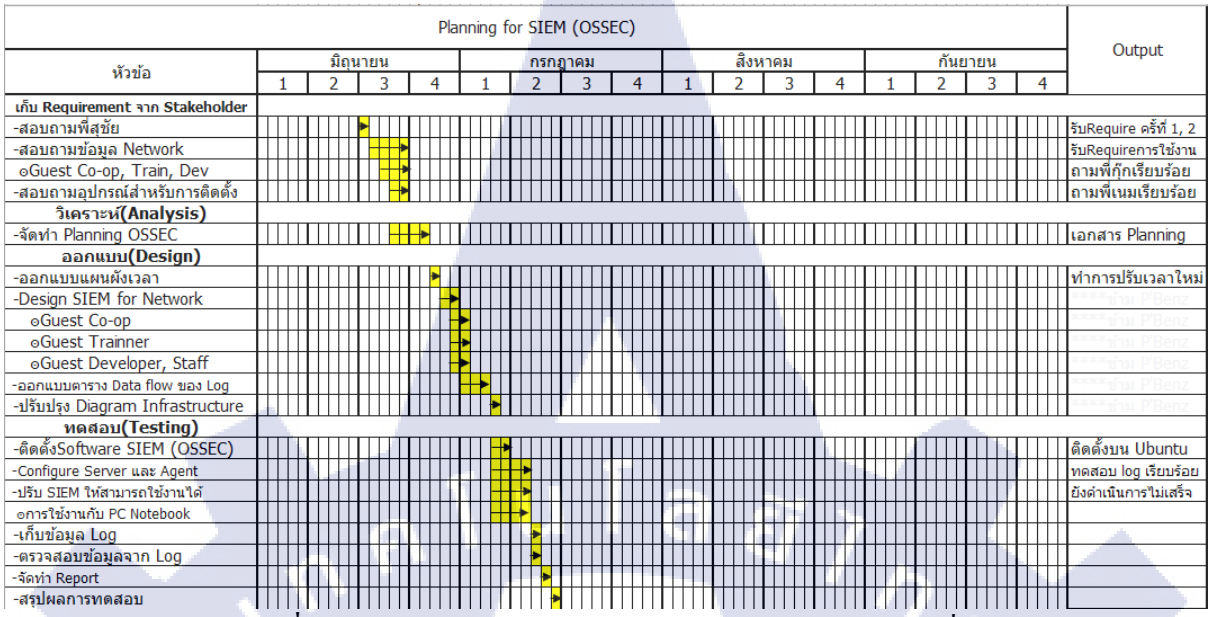
6.) จัดทำเอกสาร Payment Voucher

3.3 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงาน

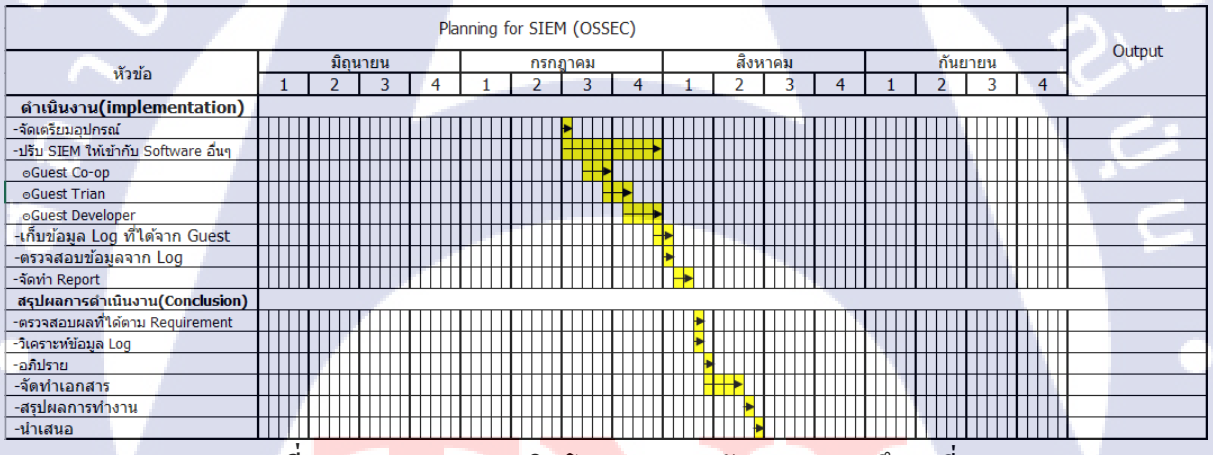
ในการดำเนินงานต่าง ๆ ก่อนที่มอบหมายงานให้ศึกษาขั้นตอนแรก คือ อธิบายถึงรายละเอียดต่าง ๆ ที่ต้องการให้ทำเพิ่มเติมหรือแก้ไขข้อมูลต่าง ๆ เอกสารต่าง ๆ รวมไปถึงการสร้างงานด้วยโปรแกรมต่าง ๆ เป็นงานที่ใช้งานจริง เมื่อมีปัญหาในการทำงาน สามารถให้พี่พนักงานสอบตรวจรายละเอียดงานที่ทำแล้ว ทำให้งานที่ทำอยู่ออกมาตรงตามความต้องการที่ถูกต้องได้

3.3.1 การวางแผนการจัดการโครงงาน

จากการได้รับมอบหมายโครงงานสำหรับการจบการศึกษา โดยมาจากความต้องการโปรแกรม SIEM ซึ่งทำหน้าที่ในการวิเคราะห์ Syslog จากนั้นจึงดำเนินการศึกษาในระบบ SIEM และเลือกโปรแกรมที่สามารถใช้งานโปรแกรมใช้งานได้อย่างเสรี (Open Source) สามารถติดตั้งและใช้งานได้อย่างอิสระ ซึ่งได้ทำการเลือกโปรแกรม OSSEC ในการนำมาทำโครงงานสำหรับการจบการศึกษา จากนั้นจึงวางแผนการทำงานโดยการคาดการณ์ในระยะเวลา 4 เดือน



ภาพที่ 3.1 การวางแผนดำเนินโครงงานสำหรับการจบการศึกษาที่ 1



ภาพที่ 3.2 การวางแผนดำเนินโครงงานสำหรับการจบการศึกษาที่ 2

โดยหลังจากนั้นจึงดำเนินการศึกษาโปรแกรม OSSEC และทำให้เข้าใจโครงงานรวมถึงการเข้ารับ Requirement ที่ต้องมีสำหรับการใช้งานที่จำเป็น โดยส่วนโปรแกรมหลักนั้นนอกจากการทำงานที่ต้องเป็นระบบ SIEM ได้แล้วจะต้องมีส่วนที่แสดงผล (Visualize) ให้ผู้ทำ Monitor ใช้งานได้อย่างสะดวก และเห็นภาพรวมของเหตุการณ์ (Event) ได้ในทันที เพื่อให้รู้ถึงการเปลี่ยนแปลงต่าง ๆ รวมถึงการปรับปรุงระบบให้ตอบสนองกับการใช้งาน โดยหลังจากนั้นจำเป็นต้องนำโปรแกรมสำหรับข้อมูล Syslog ทำการแสดงผล

(Visualize) ตามเงื่อนไข Requirement ที่ได้รับมา จึงเลือกโปรแกรม Elastic ที่มีสามารถทำงานตามที่ต้องการ โดยโปรแกรมให้บริการ (Service) ที่จำเป็นต้องติดตั้ง ดังนี้

1.) Logstash เป็นโปรแกรมที่นำข้อมูลต่าง ๆ เข้าระบบการทำงาน

2.) Elasticsearch เป็นโปรแกรมที่ประมวลผลข้อมูลทุกอย่างที่ได้รับ

3.) Kibana เป็นโปรแกรมแสดงผล (Visualize)

ได้ทำการศึกษาการใช้งานทั้ง 3 โปรแกรมและการเชื่อมต่อระหว่างกันในการทำงานต่าง ๆ รวมถึงการใช้งานโปรแกรม โดยโปรแกรม Elastic เป็นโปรแกรมที่ตอบโจทย์การแสดงผล (Visualize) สามารถใช้งานประยุกต์ใช้กับ OSSEC ได้ จึงเลือกศึกษาเพราะความสามารถของ Elastic สามารถใช้งานในการเรียกข้อมูลจาก MySQL ออกมาใช้งานได้ทันที ทำให้ระบบที่เกิดขึ้นทำงานได้อย่างปกติและสามารถทำงานได้อย่างอัตโนมัติ ง่ายต่อผู้ที่ทำการ Monitor และการทำเอกสารรายงาน (Reporting) ให้สมบูรณ์

3.3.2 ขั้นตอนการทำงานที่ได้รับมอบหมาย ณ สถานที่ฝึกงาน

1.) แจ้งงานที่ต้องการให้ทำ

2.) จดจำ บันทึกรายละเอียดงานที่ด้รับ

3.) สอบถาม เมื่อสงสัยรายละเอียดงานที่ได้รับ

4.) จัดการงานที่ได้รับมอบหมาย และให้พี่พนักงานตรวจสอบความถูกต้อง

3.3.3 ปัญหาและอุปสรรค

1.) ไม่เข้าใจงานที่มอบหมายอย่างถ่องแท้

2.) ทำงานช้า เนื่องจากไม่มีความชำนาญ

3.) งานผิดพลาดบ่อยจนทำให้เกิดการล่าช้า

บทที่ 4
สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ

4.1 ขั้นตอนและผลการดำเนินงาน

ในการดำเนินงานให้โปรแกรมสามารถใช้งานได้ จำเป็นต้องทำงานต่อกันเป็นระบบนั้น คือ ส่วนช่วยในการทำงานของ OSSEC

1.) OSSEC HIDS

2.) OSSEC-WUI

3.) Apache

4.) MySQL

ส่วนช่วยในการทำงานของ Elastic

5.) Elasticsearch

6.) Logstash

7.) Kibana

4.1.1 ขั้นตอนการติดตั้งเพื่อการใช้งาน OSSEC[7-12]

4.1.1.1 เตรียม Package และ Service[7]

Installing LAMP stack on RHEL 7 / CentOS 7

ติดตั้ง yum service ต่าง ๆ ดังนี้

yum update

- การทำ yum โปรแกรมการให้บริการ (Service) เพิ่มในระบบ

yum install mysql-devel postgresql-devel

- การทำการติดตั้งการให้บริการ (Service) MySQL

นำไฟล์ (File) .tar.gz ของ OSSEC เก็บไว้ในเครื่อง

ossec-hids.x.x.tar.gz , ossec-wui.x.x.tar.gz

4.1.1.2 การเพิ่ม User Account[7]

adduser user

- การเพิ่มบัญชีใช้งานใหม่

passwd user

- ตั้งรหัสผ่านสำหรับบัญชีใช้งาน

visudo

-เข้าไปในไฟล์ (File) สำหรับการใช้งาน sudo

เมื่อเข้ามาที่ #visudo หาบรรทัด

Allow root to run any commands anywhere

root ALL=(ALL) ALL

ให้เติม user ALL=(ALL) ALL

- เพื่อให้สิทธิ์ของบัญชี user มีสิทธิ์เท่า root

4.1.1.3 ติดตั้ง Apache[7]

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

yum install -y httpd

- การติดตั้ง httpd

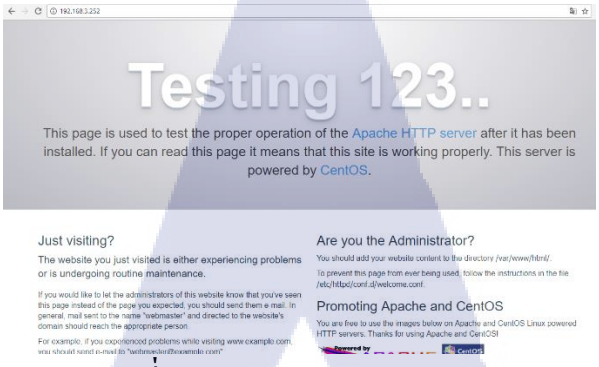
systemctl enable httpd;systemctl start httpd

- การตั้งค่าให้ httpd สามารถเปิดใช้งานได้เมื่อเปิดเครื่อง

firewall-cmd --add-service=http --permanent;firewall-cmd --reload

- การตั้งค่า firewall ให้ http และทำการบรรจุใหม่

จากนั้นเรียก localhost เพื่อทดสอบ Apache



ภาพที่ 4.1 ทดสอบ Localhost Apache

จากนั้นต้องใส่ timezone ให้กับ Apache

ด้วยการเข้าไปที่ Command line

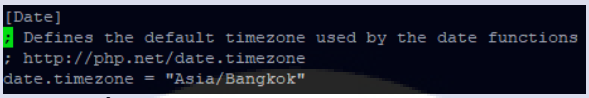
vi /etc/php.ini

- การเข้าไปในไฟล์ควบคุม (File Configure) ของโปรแกรม php

หาบรรทัด date.timezone จากนั้นใส่ "Asia/Bangkok"

date.timezone = "Asia/Bangkok"

- การใส่ประเทศและภูมิภาค



ภาพที่ 4.2 การเปลี่ยน time zone ของ Apache

4.1.1.4 ติดตั้ง MySQL[7]

sudo rpm -ivh mysql57-community-release-el7-11.noarch.rpmyum update

- ทำการ rpm ไฟล์ (File)

yum install mysql-server

- ทำการติดตั้ง MySQL Server

systmctl start mysqld

- การตั้งค่าให้ MySQL สามารถเปิดใช้งานได้เมื่อเปิดเครื่อง

mysql_secure_installation

4.1.1.5 ติดตั้ง PHP[7]

yum install php php-mysql

- การติดตั้ง php สำหรับใช้งาน MySQL

vi /var/www/html/test.php

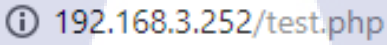
- การสร้างไฟล์ (File) สำหรับทดสอบการเรียกใช้งาน php

แล้วใส่ข้อความ <?php phpinfo(); ?>

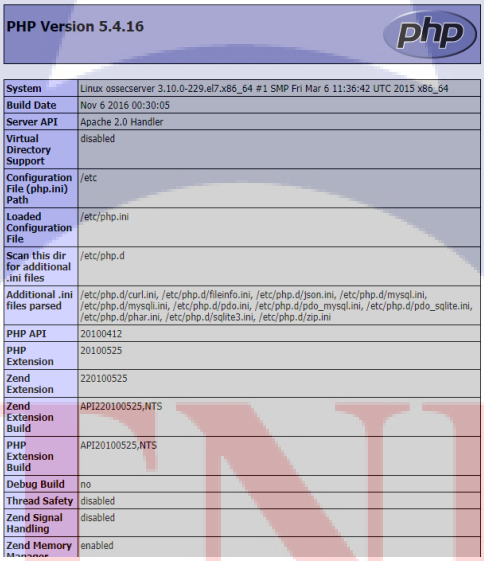
systemctl restart httpd

- การเริ่มการให้บริการ (Service) httpd ใหม่อีกครั้ง

ทดสอบด้วยการเรียก localhost แล้วตามด้วยที่อยู่ของไฟล์ (File) .php



ภาพที่ 4.3 ที่อยู่สำหรับการทดสอบ localhost การติดตั้ง PHP



ภาพที่ 4.4 การทดสอบ localhost การติดตั้ง PHP

4.1.1.6 การติดตั้ง OSSEC HIDS[7,9]

1.) ต้องติดตั้งสิ่งที่จำเป็นก่อนทำการเริ่มติดตั้ง OSSEC HIDS

yum install -y gcc php php-cgi php-devel inotify-tools httpd mysql-devel postgresql-devel

- การติดตั้งเครื่องมือสำหรับการใช้งาน httpd MySQL

firewall-cmd --add-port=1514/udp --permanent;firewall-cmd --reload

- การตั้งค่า firewall ให้ Port 1514 UDP และทำการบรรจุใหม่

firewall-cmd --add-port=514/udp --permanent

- การตั้งค่า firewall ให้ Port 514 UPD

firewall-cmd --add-port=514/tcp --permanent

- การตั้งค่า firewall ให้ Port 514 TCP

firewall-cmd --reload

- ทำการบรรจุใหม่

2.) ลงโปรแกรมที่ทำการตรวจสอบ Syslog

yum -y install rsyslog

- ติดตั้งโปรแกรม rsyslog

vi /etc/rsyslog.conf

- เข้าไปแก้ไฟล์ควบคุม (File Configure) ของ rsyslog.conf

หาคำสั่ง

Provides UDP syslog reception

#$ModLoad imudp

#$UDPServerRun 514

Provides TCP syslog reception

#$ModLoad imtcp

#$InputTCPServerRun 514

ให้แก้ไขเป็น ดังนี้

Provides UDP syslog reception

$ModLoad imudp

$UDPServerRun 514

Provides TCP syslog reception

$ModLoad imtcp

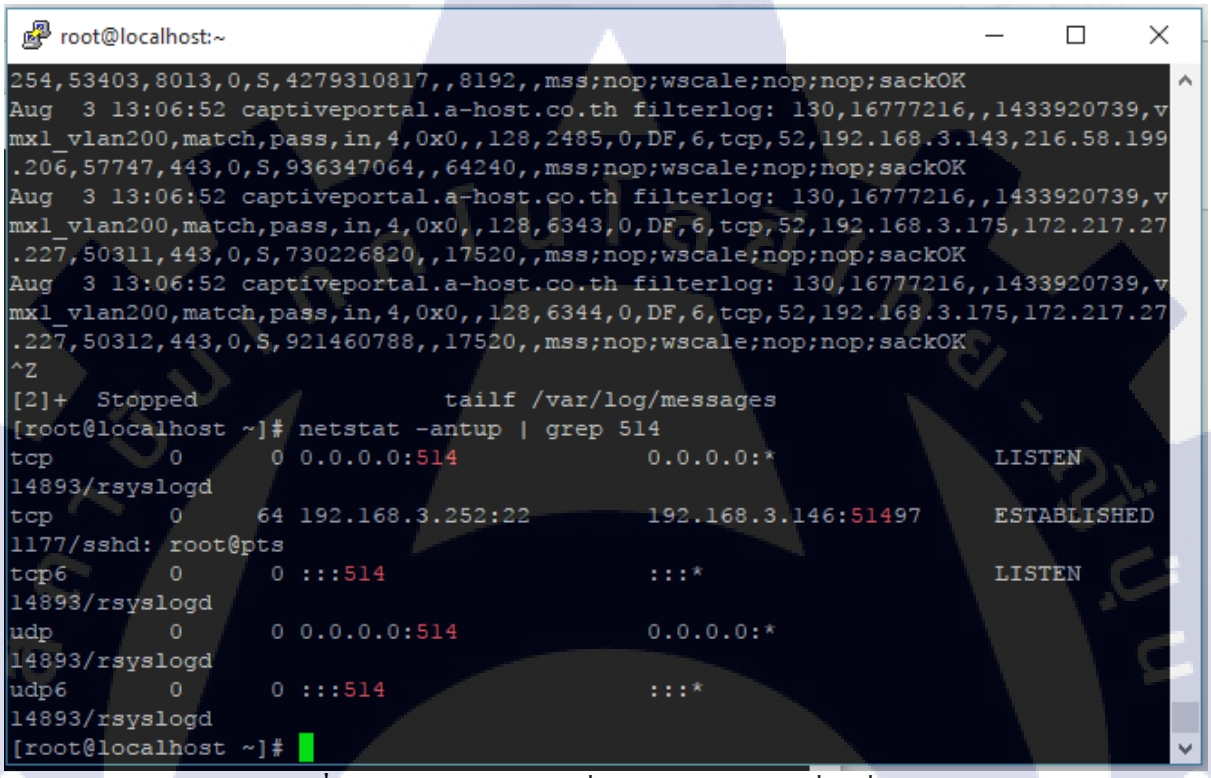
$InputTCPServerRun 514

ทำการ Restart syslog Service

systemctl restart rsyslog.service

เช็คว่า port 514 มีการทำงานอยู่หรือไม่

netstat -antup | grep 514

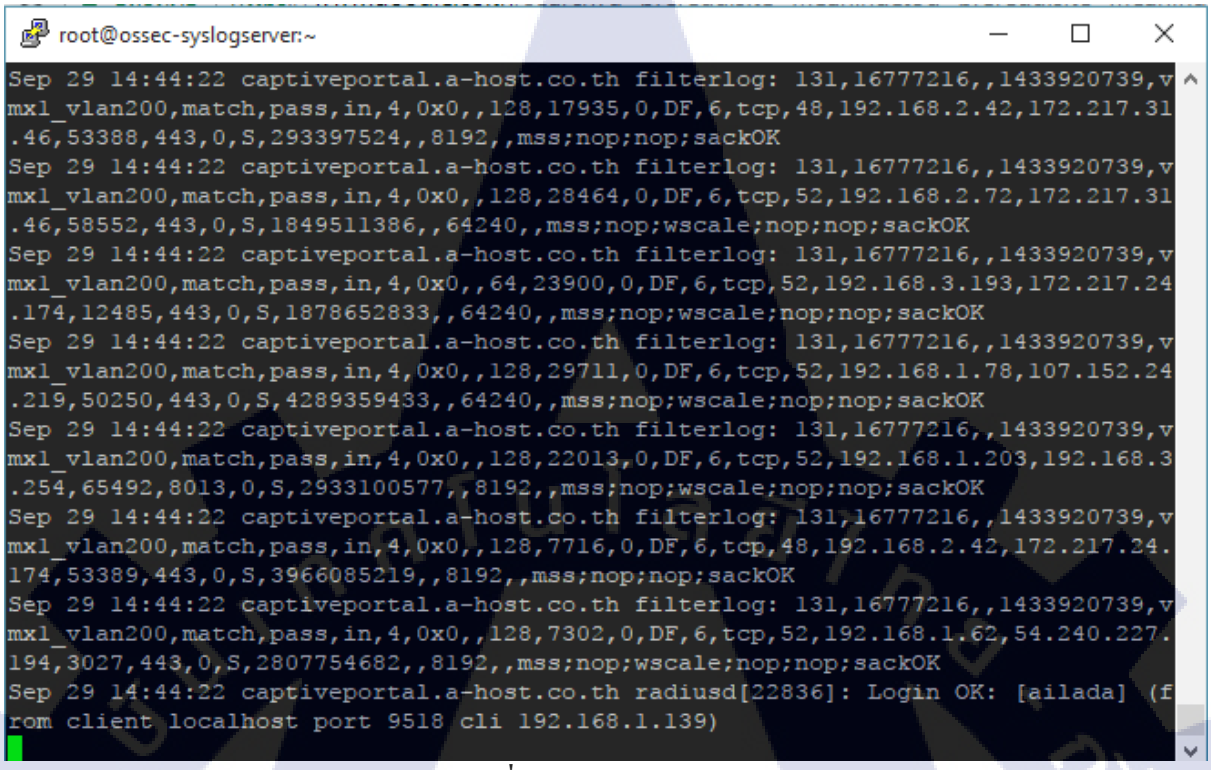


ภาพที่ 4.5 การทดสอบ Port ที่ส่ง Syslog ให้กับเครื่องที่ใช้งาน

เมื่อเสร็จทำการทดสอบการทำงาน rsyslog ที่เกิดภายในเครื่อง

tailf /var/Log/messages

- การเรียกดูข้อมูลของ log ที่ได้รับ



ภาพที่ 4.6 เช็คการรับ Syslog

4.1.1.7 การติดตั้ง OSSEC HIDS Server[7]

1.) ดาวน์โหลด (Download) OSSEC HIDS จากเว็ปไซต์ ossec.github.io เพื่อทำการติดตั้ง

tar –zxf ossec-hids

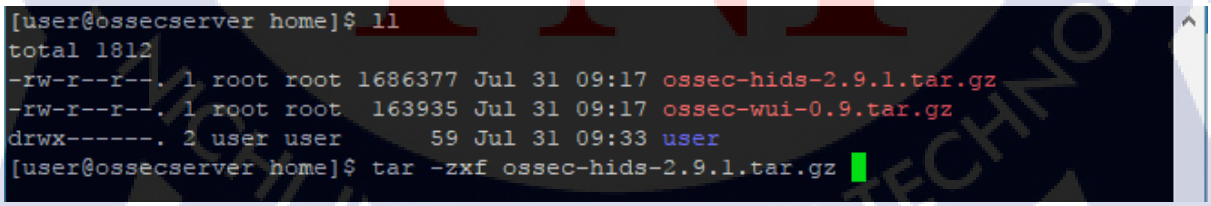
- การคลายไฟล์ (File) ที่ถูกบีบอัด

cd ossec-hids/

- การเข้าแฟ้มข้อมูล (Folder) ossec-hids

DATABASE=mysql ./install.sh

- การติดตั้ง OSSEC พร้อมกับฐานข้อมูล MySQL



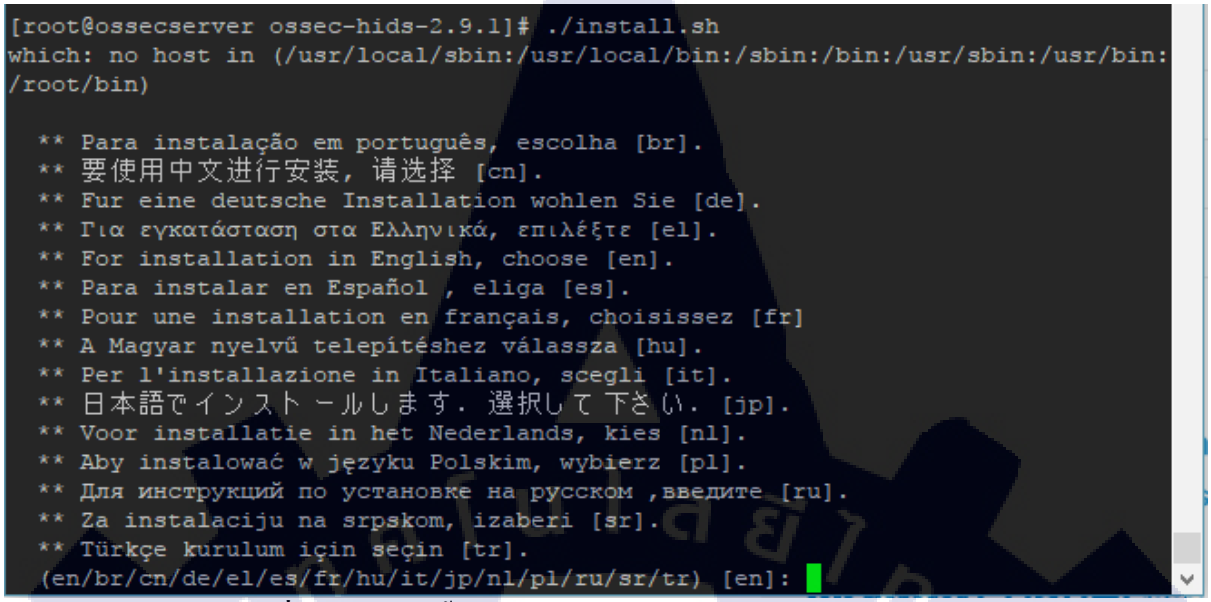
ภาพที่ 4.7 การคลายไฟล์ tar.gz เพื่อติดตั้ง OSSEC-HIDS-2.9.1

```
drwxrwxr-x. 7 user user    4096 Jun 19 22:32 ossec-hids-2.9.1
-rw-r--r--. 1 root root 1686377 Jul 31 09:17 ossec-hids-2.9.1.tar.gz
drwxrwxr-x. 7 user user    4096 Dec 30  2015 ossec-wui-0.9
-rw-r--r--. 1 root root  163935 Jul 31 09:17 ossec-wui-0.9.tar.gz
[user@ossecserver ~]$
```

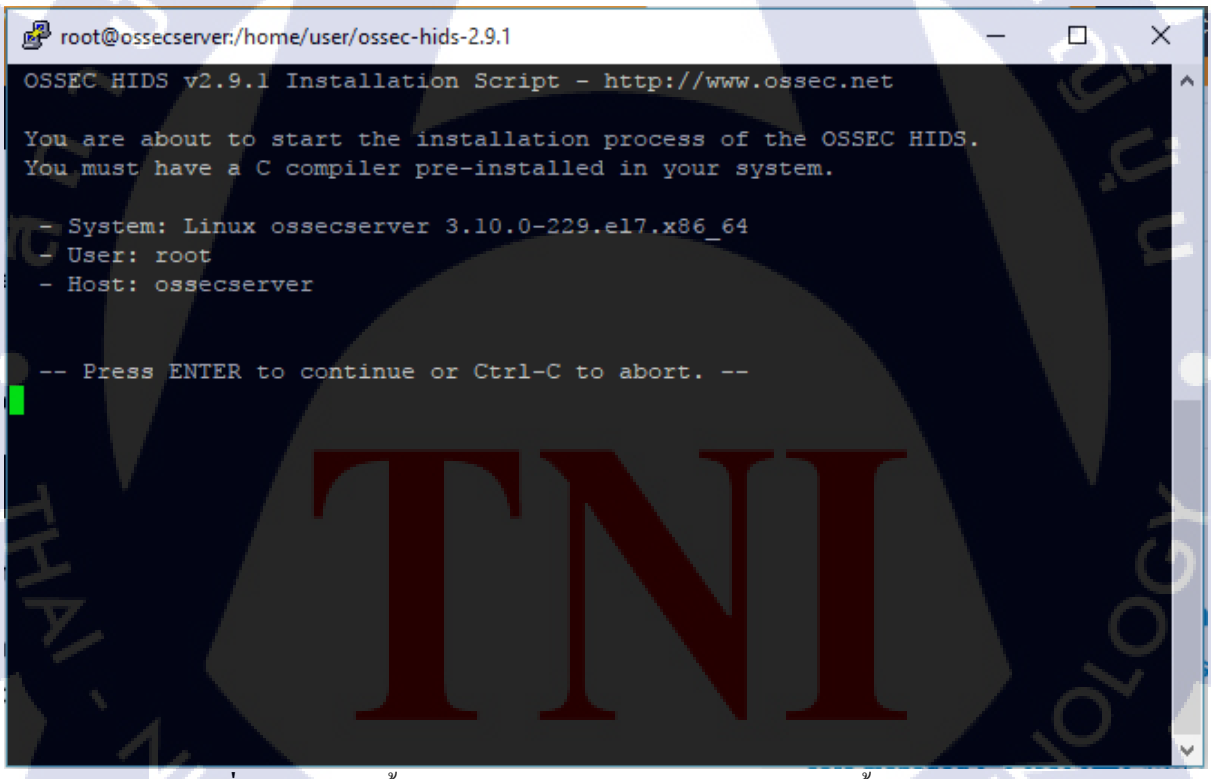
ภาพที่ 4.8 ตรวจสอบแฟ้มข้อมูลที่ทำการคลายออกมา

```
user@ossecserver:~/ossec-hids-2.9.1
-rw-r--r--. 1 root root  163935 Jul 31 09:17 ossec-wui-0.9.tar.gz
[user@ossecserver ~]$ ll
total 1820
drwxrwxr-x. 7 user user    4096 Jun 19 22:32 ossec-hids-2.9.1
-rw-r--r--. 1 root root 1686377 Jul 31 09:17 ossec-hids-2.9.1.tar.gz
drwxrwxr-x. 7 user user    4096 Dec 30  2015 ossec-wui-0.9
-rw-r--r--. 1 root root  163935 Jul 31 09:17 ossec-wui-0.9.tar.gz
[user@ossecserver ~]$ cd ossec-hids-2.9.1
[user@ossecserver ossec-hids-2.9.1]$ ll
total 116
drwxrwxr-x.  4 user user  4096 Jun 19 22:32 active-response
-rw-rw-r--.  1 user user   583 Jun 19 22:32 BUGS
-rw-rw-r--.  1 user user  6965 Jun 19 22:32 CHANGELOG
-rw-rw-r--.  1 user user   310 Jun 19 22:32 CONFIG
drwxrwxr-x.  7 user user  4096 Jun 19 22:32 contrib
-rw-rw-r--.  1 user user  4245 Jun 19 22:32 CONTRIBUTORS
drwxrwxr-x.  4 user user  4096 Jun 19 22:32 doc
drwxrwxr-x.  4 user user  4096 Jun 19 22:32 etc
-rw-rw-r--.  1 user user  1850 Jun 19 22:32 INSTALL
-rwxrwxr-x.  1 user user 33000 Jun 19 22:32 install.sh
-rw-rw-r--.  1 user user 24710 Jun 19 22:32 LICENSE
-rw-rw-r--.  1 user user  2193 Jun 19 22:32 README.md
drwxrwxr-x. 32 user user  4096 Jun 19 22:32 src
[user@ossecserver ossec-hids-2.9.1]$
```

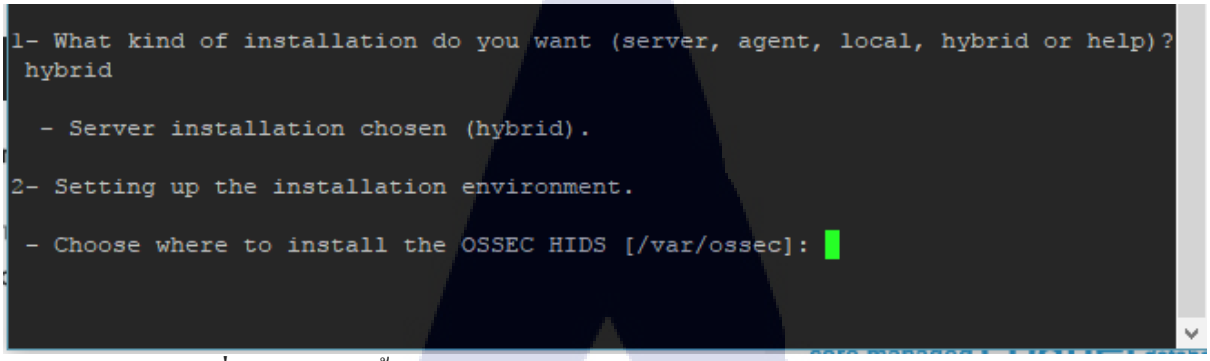
ภาพที่ 4.9 เข้าแฟ้มข้อมูล OSSEC-HIDS-2.9.1



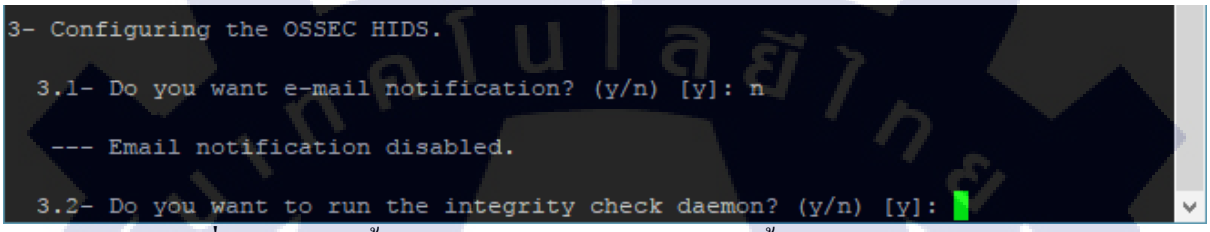
ภาพที่ 4.10 การติดตั้ง OSSEC-HIDS-2.9.1 ด้วยการเรียกใช้ install.sh



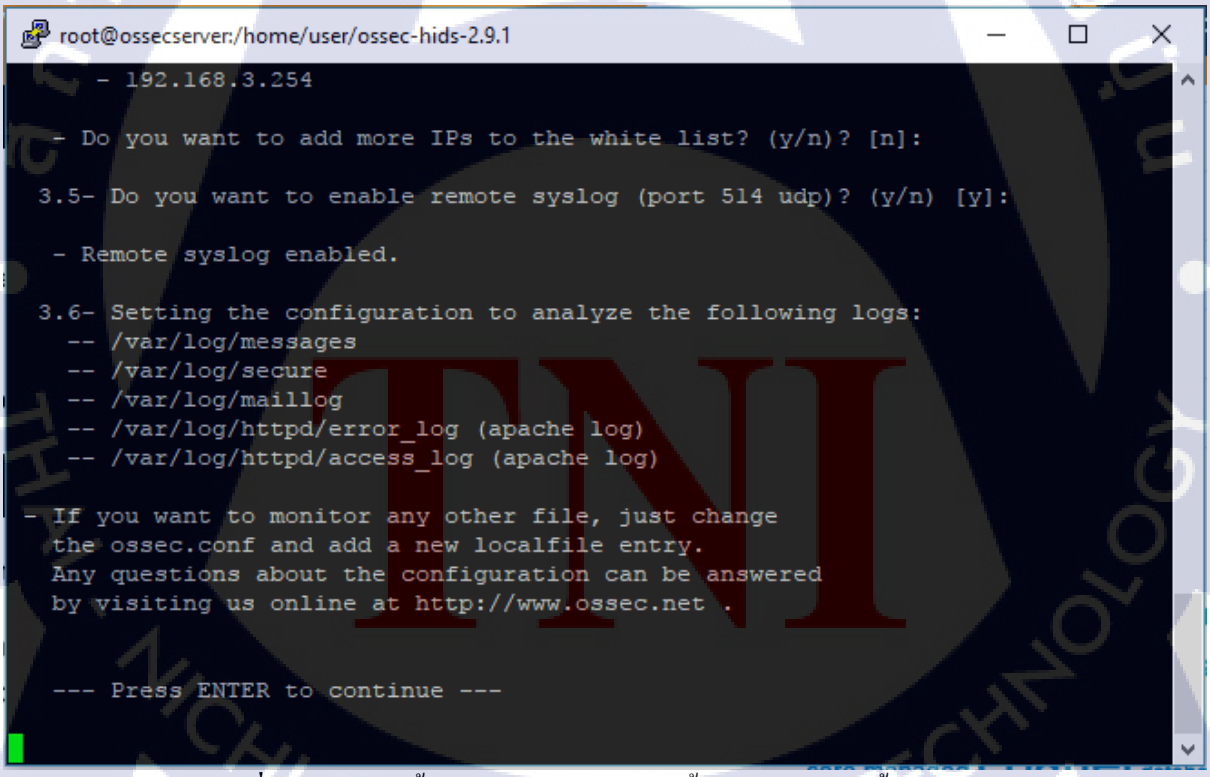
ภาพที่ 4.11 การติดตั้ง OSSEC-HIDS-2.9.1 แจ้งข้อมูลก่อนติดตั้งของโปรแกรม



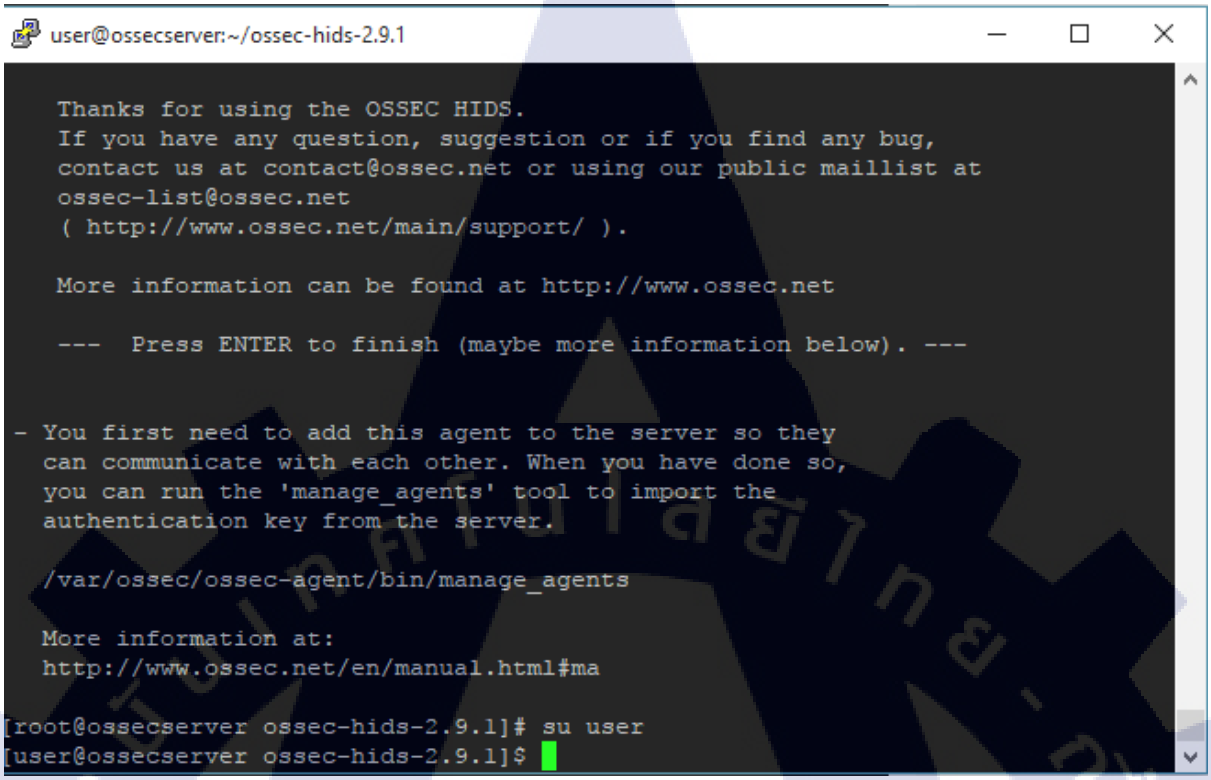
ภาพที่ 4.12 การติดตั้ง OSSEC-HIDS-2.9.1 แจ้งชนิดและตำแหน่งของโปรแกรม



ภาพที่ 4.13 การติดตั้ง OSSEC-HIDS-2.9.1 แจ้งการติดตั้ง Integrity check daemon



ภาพที่ 4.14 การติดตั้ง OSSEC-HIDS-2.9.1 ตั้งค่าก่อนการติดตั้งโปรแกรม



ภาพที่ 4.15 การติดตั้ง OSSEC-HIDS-2.9.1 แจ้งการติดตั้งเมื่อเสร็จสิ้น

2.) เมื่อจบการขั้นตอนการติดตั้ง OSSEC-HIDS ทำการเรียกใช้งานบริการ (Service)

/var/ossec/bin/ossec-control start

Started ossec-maild...

Started ossec-execd...

Started ossec-analysisd...

Started ossec-Logcollector...

Started ossec-remoted...

Started ossec-syscheckd...

Started ossec-monitord...

Completed.

4.1.1.8 การติดตั้ง OSSEC WUI[7]

1.) การติดตั้งโปรแกรมของ OSSEC สำหรับการใช้งาน Web user interface

tar zxf ossec-wui.0.9.tar.gz

- การคลายไฟล์ (File) บีบอัด

mv ossec-wui-0.9/ /var/www/html/ossec-wui

- การย้ายแฟ้มข้อมูล (Folder) ให้ไปอยู่ที่ Apache

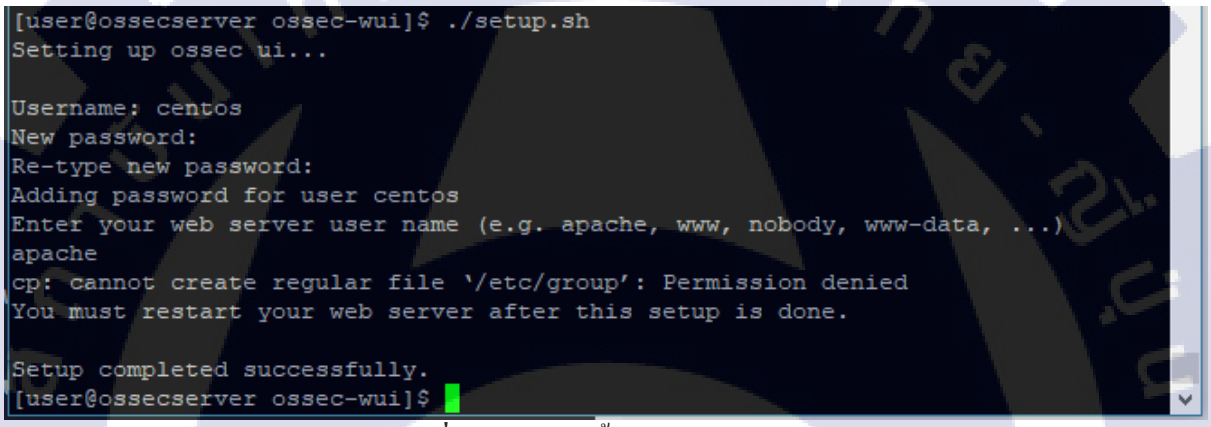
2.) จากนั้นย้ายแฟ้มข้อมูล (Folder) ไปไว้ที่ตำแหน่ง (Path) html เพื่อให้เว็ปไซต์ใช้งานได้

cd /var/www/html/ossec-wui/

3.) จากนั้นทำการติดตั้ง OSSEC WUI

./setup.sh

- ติดตั้งโปรแกรม OSSEC WUI



ภาพที่ 4.16 การติดตั้ง OSSEC-WUI .0.9

4.) เพิ่มสิทธิ์อนุญาตสำหรับการเชื่อมต่อ (Set permissions)

usermod -a G ossec apache

- การให้สิทธิ์ของ user ossec มีสิทธิ์เท่ากับ apache

chmod 770 tmp/

- การตั้งค่าในการ อ่าน เขียน ยืนยัน ในตำแหน่ง (Path) ที่ tmp

chgrp apache tmp/

- การเปลี่ยนกลุ่มของตำแหน่ง (Path) เป็นของ apache

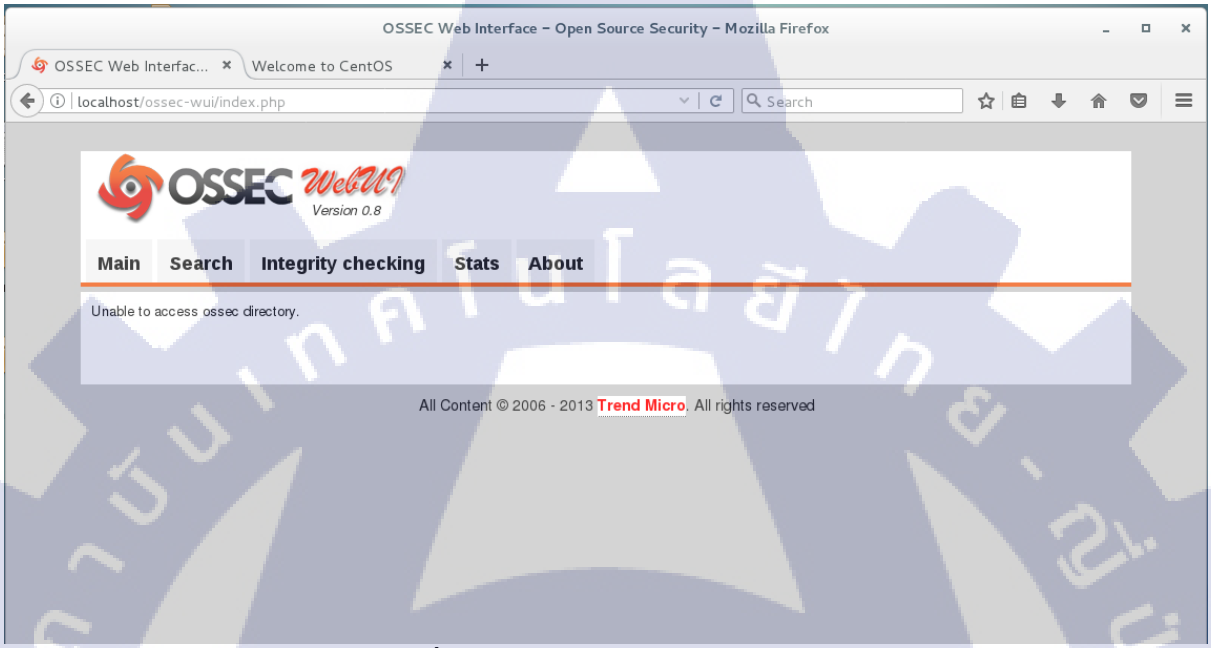
systemctl restart httpd

- การเริ่มการให้บริการ (Service) httpd ใหม่อีกครั้ง

/var/ossec/bin/ossec-control restart

- การเริ่มการให้บริการ (Service) OSSEC ใหม่อีกครั้ง

เปิดเว็บไซต์ ตามด้วยตำแหน่ง (Path๗) ของ OSSEC-WUI ที่ทำการติดตั้ง

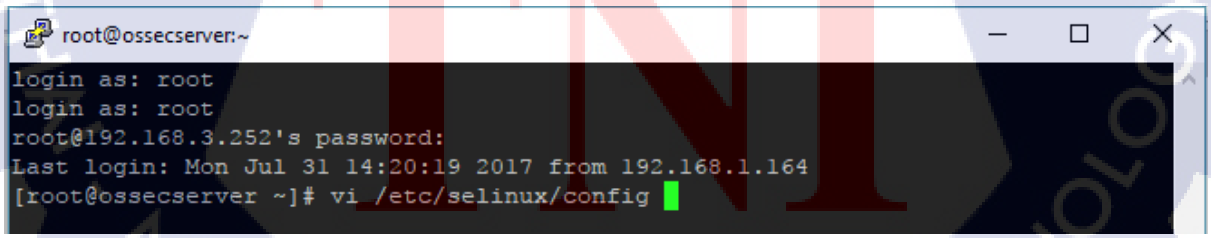


ภาพที่ 4.17 การเรียกใช้ OSSEC-WUI .0.9

5.) เว็บไซต์ OSSEC-WUI ไม่ทำงานแก้ไขที่ Selinux โดยการใช้ Command line

vi /etc/selinux/config

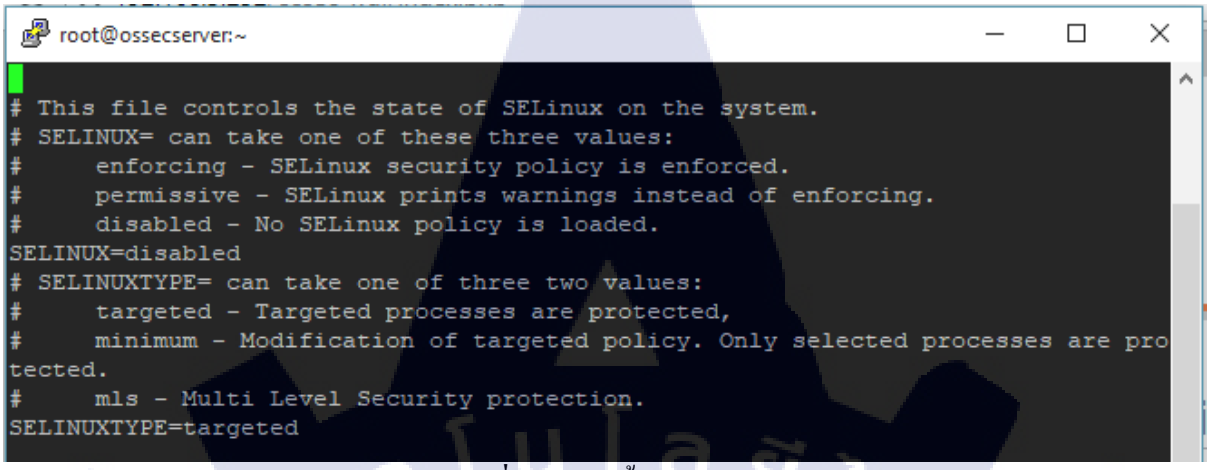
- การเข้าไปในไฟล์ควบคุม (File Configure) ของ Linux Security



ภาพที่ 4.18 ตำแหน่งของ Selinux

ให้เปลี่ยนชื่อ SELINUX= enforcing

เป็น SELINUX= disabled



ภาพที่ 4.19 การตั้งค่า Selinux

restorecon –r /var/www/html/

ทำการ restart เครื่องหลังจากที่ทำการติดตั้งเสร็จหมดทุกขั้นตอน

reboot

- การเริ่มเปิดใหม่อีกครั้ง

4.1.2 การเชื่อม Database[12]

1.) หลังจากการติดตั้ง OSSEC และ MySQL เสร็จสิ้นให้ทำการดาวน์โหลด (Download) mysql57-community-release-el7-9.noarch.rpm ได้ที่ https://dev.mysql.com/downloads/repo/yum/

ภาพที่ 4.20 การดาวน์โหลด mysql57-community-release-el7-9.noarch.rpm

นำโปรแกรมเข้าไปที่ เครื่อง Centos7 ด้วยโปรแกรม FileZilla

rpm -ivh mysql57-community-release-el7-9.noarch.rpm

- ทำการ rpm ไฟล์ (File)

yum install mysql-server

- การทำ yum โปรแกรมการให้บริการ (Service) ของ MySQL Server เพิ่มในระบบ

systemctl enable mysqld.service

- การตั้งค่าให้เปิดการทำงานโปรแกรมการให้บริการ (Service) ของ MySQL Server

systemctl start mysqld.service

- การตั้งค่าเปิดโปรแกรมการให้บริการ (Service) ของ MySQL Server

systemctl status mysqld

- การตรวจสอบสถานะโปรแกรมการให้บริการ (Service) MySQL

/var/ossec/bin/ossec-control enable database

- การตั้งค่าให้เปิดการทำงานโปรแกรมการให้บริการ (Service) ของ Database ในโปรแกรม OSSEC

ตรวจสอบระบบมีการสร้างรหัสหรือไม่ ทำการเช็คและเก็บรหัสเอาไว้

sudo grep 'temporary password' /var/Log/mysqld.Log

- การค้นหาคำ

ตัวอย่าง. [Note] A temporary password is generated for root@localhost: mqRfBU_3Xk>r

2.) จากนั้นเริ่มทำการติดตั้ง Configuring MySQL

mysql_secure_installation

นำเอารหัสที่ระบบสร้างขึ้นมาใส่ใน

[root@localhost ~]# mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root: *** ตัวอย่าง @1s2d3F4 ***

Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : Yes

จากนั้นกด Enter เพื่อ skipping

ภาพที่ 4.21 การตั้งค่า MySQL

3.) ทำการเข้า mysql -u root –p

Mysql> create database ossec;

- การสร้างระบบฐานข้อมูล (Database)

Mysql> create user 'ossecuser'@'192.168.3.252' identified by '@1s2d3F4';

- การสร้างบัญชีการเข้าใช้งาน Database และสร้างรหัสผ่าน

Mysql> grant all on ossec.* to 'ossecuser' identified by '@1s2d3F4';

- การตั้งค่าสิทธิ์การใช้คำสั่งทั้งหมดให้กับบัญชีของ ossec

Mysql> grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on ossec.* to

'ossecuser'@'192.168.3.252';

- การตั้งค่าสิทธิ์การใช้งานคำสั่ง query ให้กับบัญชี ossec และตั้งค่าที่อยู่ของ IP (IP Addess)

Mysql> flush privileges;

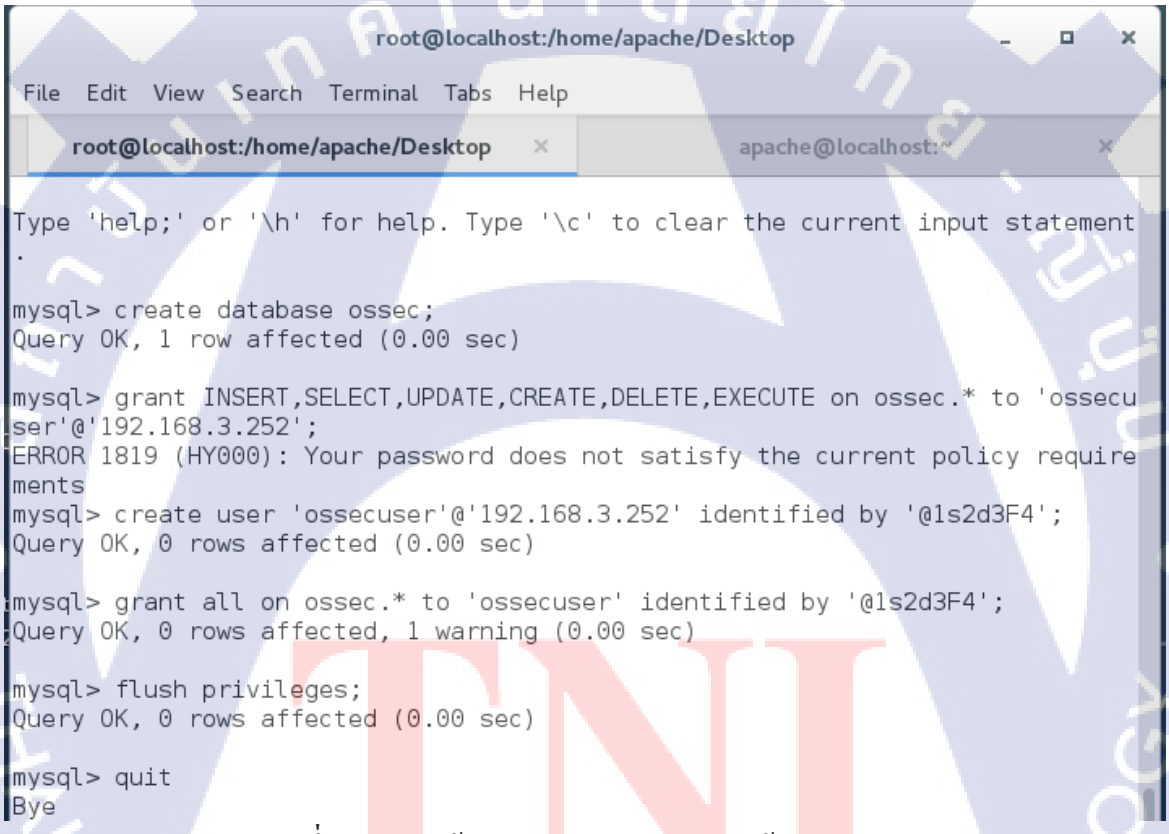
- ยืนยันการตั้งค่า

Mysql> quit

- การออกจากระบบ MySQL

เข้าไปที่ไฟล์ (File) ที่ทำการ tar ออกมาตั้งแต่แรก โดยเข้าไปแล้วไปที่ src/os_dbd เพื่อให้ schema

mysql -u root -p ossec < mysql.schema



ภาพที่ 4.22 การสร้าง MySQL สำหรับการใส่ข้อมูล OSSEC

4.) เข้าไปที่ ossec.conf เพื่อทำการตั้งค่าให้ OSSEC HIDS ใช้งาน MySQL ได้

vi /var/ossec/etc/ossec.conf

เพิ่มคำสั่ง เพื่อทำการตั้งค่า (Configure) คำว่าใต้ </global> ในไฟล์ (File) ossec.conf

```
<database_output>
    <hostname>192.168.3.252</hostname>
    <username>ossecuser</username>
    <password>@1s2d3F4</password>
    <database>ossec</database>
    <type>mysql</type>
</database_output>
```

- คำสั่งที่จำเป็นสำหรับการเชื่อมต่อ MySQL

หลังจากใส่การตั้งค่าให้ออกจาก ossec.conf

```
# /var/ossec/bin/ossec-control enable database
```

- การตั้งค่าให้เปิดการทำงานโปรแกรมการให้บริการ (Service) ของ Database ในโปรแกรม OSSEC

```
# /var/ossec/bin/ossec-control restart
```

- การเริ่มการให้บริการ (Service) OSSEC ใหม่อีกครั้ง

เช็ค Debug ของ ossec สามารถเช็คได้ด้วย

```
# /var/ossec/bin/ossec-dbd -df
```

การใช้งาน MySQL

```
# mysql -u root -p
```

- การเข้าระบบ MySQL ด้วยบัญชีของ root

```
mysql> use ossec;
```

- การใช้งานระบบฐานข้อมูล (Database) ชื่อ ossec

```
mysql> show tables;
```

- การเรียกแสดงตารางในระบบฐานข้อมูล (Database)

```
mysql> select * from alert;
```

- การเรียกดูข้อมูลตั้งหมดในตารางข้อมูล alert

4.1.3 ขั้นตอนการติดตั้งเพื่อการใช้งาน Elastic[7]

1.) การตั้งค่า (Configure) firewalld สำหรับ Elastic

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

```
# firewall-cmd --add-port=9200/udp --permanent
```

- การตั้งค่า firewall ให้ Port 9200 UDP

firewall-cmd --add-port=9200/tcp --permanent

- การตั้งค่า firewall ให้ Port 9200 TCP

firewall-cmd --add-port=5601/udp --permanent

- การตั้งค่า firewall ให้ Port 5601 UDP

firewall-cmd --add-port=5601/tcp --permanent

- การตั้งค่า firewall ให้ Port 5601 TCP

firewall-cmd --reload

- ทำการบรรจุใหม่

2.) การ Update Java

หา Java โดยเป็น File ในรูปแบบ .rpm สำหรับ Centos 7

sudo yum -y localinstall jre-8u144-linux-x64.rpm

- ทำ yum การให้บริการ (Service) Java - jre

3.) การติดตั้ง Elasticsearch

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

- การทำ rpm ไฟล์ (File) GPG-KEY Elasticsearch

vi /etc/yum.repos.d/elasticsearch.repo

- การสร้างไฟล์ควบคุม (File Configure) repo ของ Elasticsearch

จากนั้นให้ใส่ข้อมูลด้านล่างลงไปในไฟล์ (File)

```
[elasticsearch-5.x]
name=Elasticsearch repository for 5.x packages
baseurl=https://artifacts.elastic.co/packages/5.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

sudo yum install elasticsearch

- การทำ yum โปรแกรมการให้บริการ (Service) ของ Elasticsearch เพิ่มในระบบ

sudo /bin/systemctl daemon-reload

- ทำการบรรจุใหม่

sudo /bin/systemctl enable elasticsearch.service

- การตั้งค่าให้เปิดการทำงานโปรแกรมการให้บริการ (Service) ของ Elasticsearch

sudo systemctl start elasticsearch.service

- การตั้งค่าเปิดโปรแกรมการให้บริการ (Service) ของ Elasticsearch

sudo journalctl --unit Elasticsearch

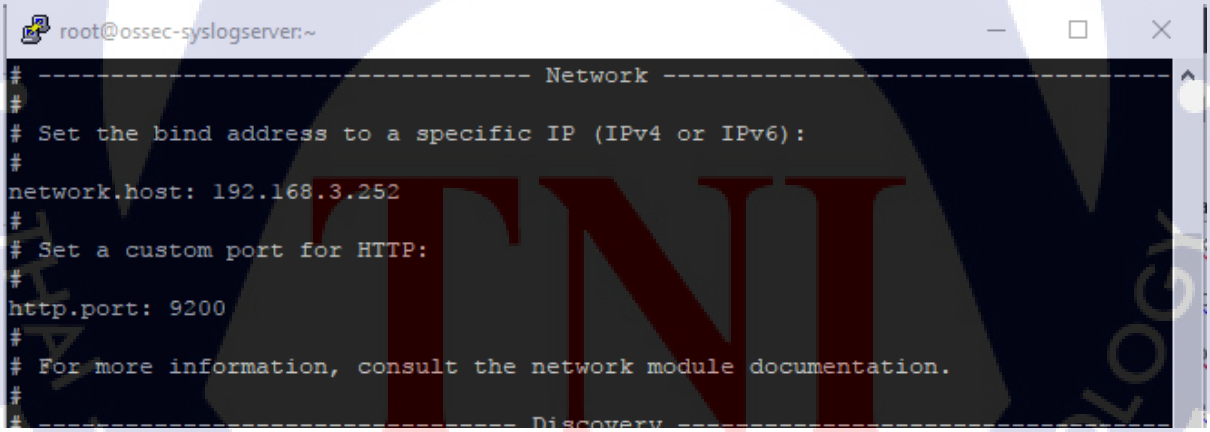
- เช็คสถานะของ Elasticsearch

#vi /etc/elasticsearch/Elasticsearch.yml

ให้ทำการตั้งค่า (Configure) สำหรับการเตรียมความพร้อมสำหรับการใช้งานและนำ # ออกในคำสั่งที่ต้องการเรียกใช้

Network.host:192.168.3.252

http:port:9200



ภาพที่ 4.23 การตั้งค่า host ของ Elasticsearch

4.) การติดตั้ง Kibana

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

vi /etc/yum.repos.d/kibana.repo

- การสร้างไฟล์ควบคุม (File Configure) repo ของ Kibana

จากนั้นให้ใส่ข้อมูลด้านล่างลงไปในไฟล์ (File)

[kibana-5.x]

name=Kibana repository for 5.x packages

baseurl=https://artifacts.elastic.co/packages/5.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY- kibana

enabled=1

autorefresh=1

type=rpm-md

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

yum install kibana

- การทำ yum โปรแกรมการให้บริการ (Service) ของ Kibana เพิ่มในระบบ

/bin/systemctl daemon-reload

- ทำการบรรจุใหม่

/bin/systemctl enable kibana.service

- การตั้งค่าให้เปิดการทำงานโปรแกรมการให้บริการ (Service) ของ Kibana

systemctl start kibana.service

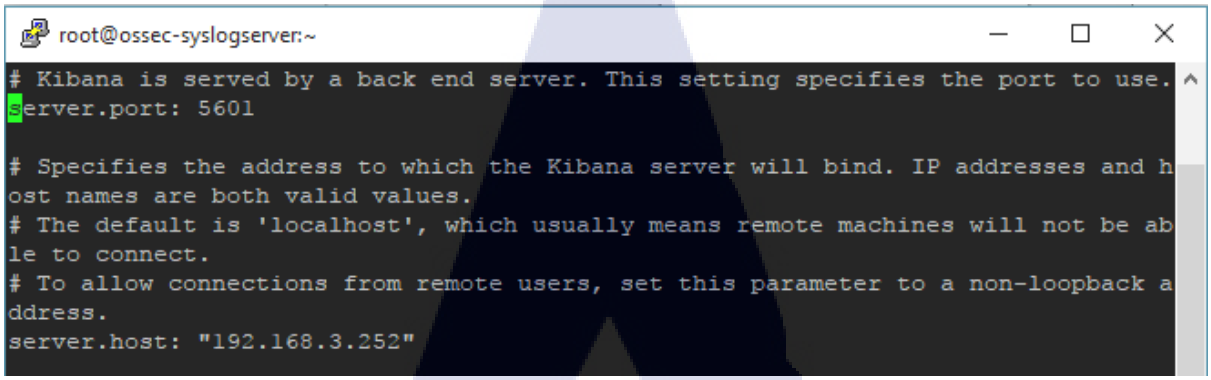
- การตั้งค่าเปิดโปรแกรมการให้บริการ (Service) ของ Kibana

vi /etc/kibana/kibana.conf

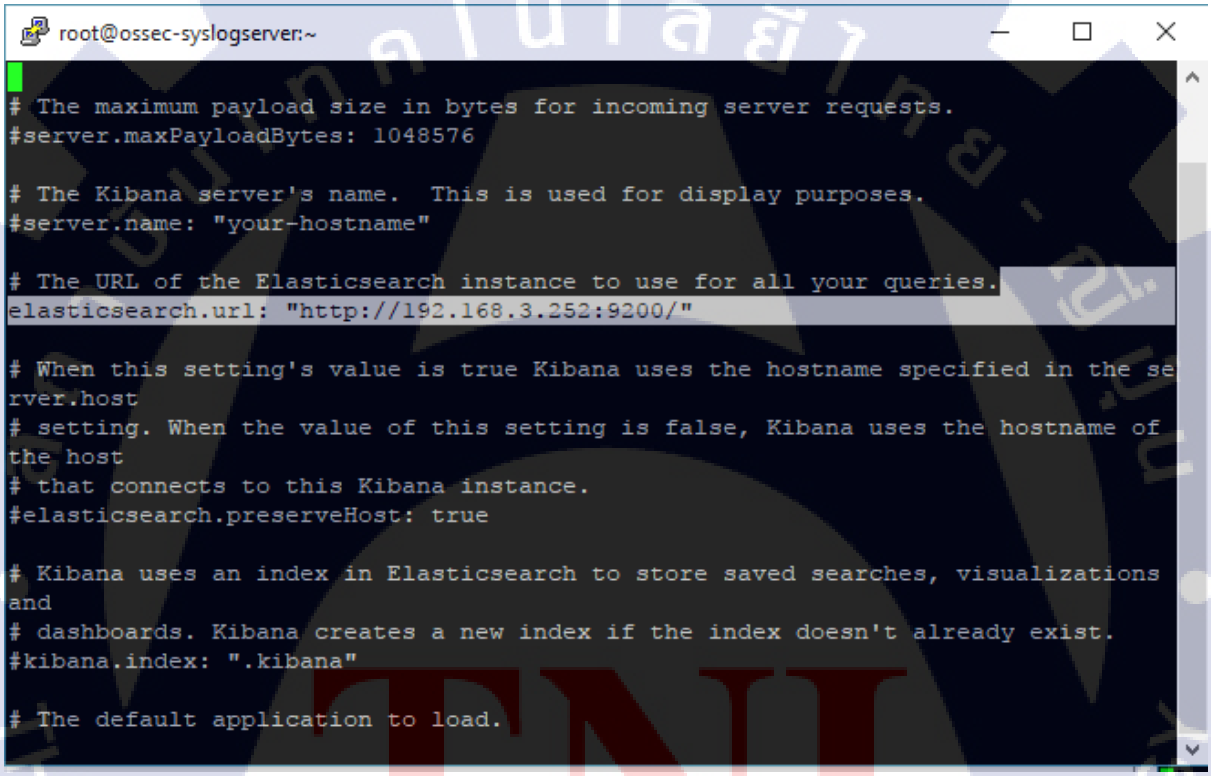
ให้ทำการตั้งค่า (Configure) สำหรับการเตรียมความพร้อมสำหรับการใช้งานและนำ # ออกในคำสั่งที่ต้องการเรียกใช้

server.port: 5601

server.host: "192.168.3.252"



ภาพที่ 4.24 การตั้งค่า host ของ Kibana



ภาพที่ 4.25 การตั้งค่าให้ Kibana เห็น host Elasticsearch

5.) การติดตั้ง Logstash

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

vi /etc/yum.repos.d/logstash.repo

- การสร้างไฟล์ควบคุม (File Configure) repo ของ Logstash

[Logstash-5.x]

name=Elastic repository for 5.x packages

baseurl=https://artifacts.elastic.co/packages/5.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY- logstash

enabled=1

autorefresh=1

type=rpm-md

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

yum install logstash

- การทำ yum โปรแกรมการให้บริการ (Service) ของ Logstash เพิ่มในระบบ

/bin/systemctl daemon-reload

- ทำการบรรจุใหม่

/bin/systemctl enable logstash.service

- การตั้งค่าให้เปิดการทำงานโปรแกรมการให้บริการ (Service) ของ Logstash

systemctl start logstash.service

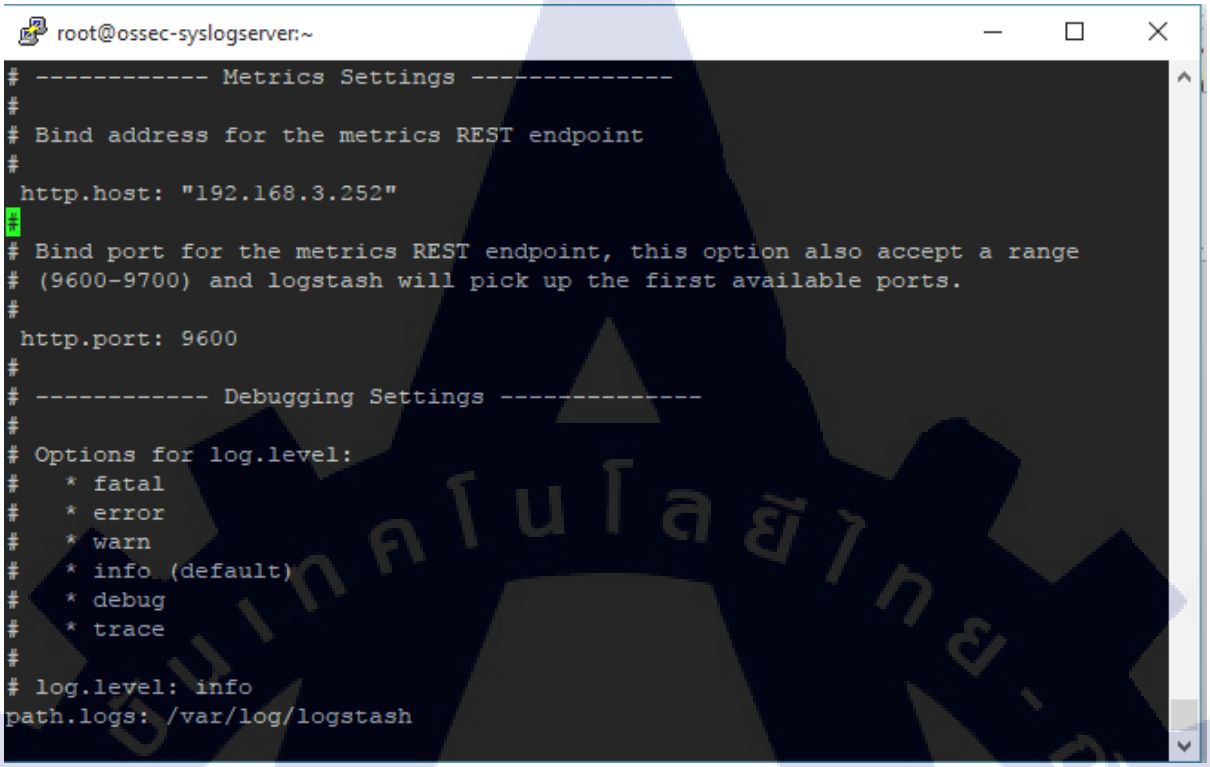
- การตั้งค่าเปิดโปรแกรมการให้บริการ (Service) ของ Elasticsearch

vi /etc/ logstash / logstash.conf

ทำการตั้งค่า (Configure) สำหรับการเตรียมความพร้อมสำหรับการใช้งานและนำ # ออกในคำสั่งที่ต้องการเรียกใช้

http.host:“192.168.3.252”

http.port:9600

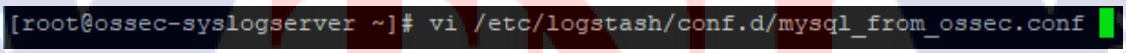


ภาพที่ 4.26 การตั้งค่า Host ของ Logstash

4.1.4 การนำเอาข้อมูลเข้า Database MySQL[8]

เมื่อสร้าง Database เอาไว้แล้วต้องการสร้างไฟล์ (File) .conf เพื่อดึงข้อมูลจาก MySQL โดยปกติไฟล์ (File) สำหรับการควบคุม (Configure) จะอยู่ในตำแหน่ง (Path) /etc/Logstash/conf.d ทั้งหมด

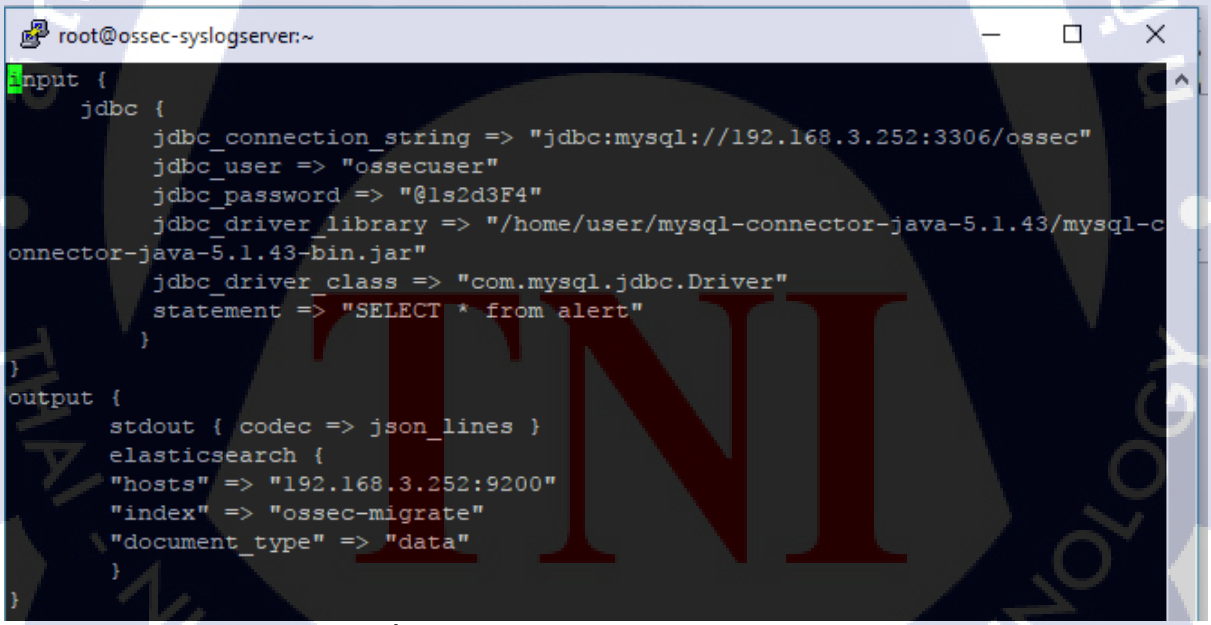
1.) ให้สร้างไฟล์ (File) .conf ตัวอย่าง mysql_from_ossec.conf



ภาพที่ 4.27 ตำแหน่งของการสร้างไฟล์สำหรับการควบคุม

```
input {
    jdbc {
        jdbc_connection_string => "jdbc:mysql://192.168.3.252:3306/ossec" *** ที่อยู่ของ Database ***
        jdbc_user => "ossecuser" ***user ที่มีสิทธิ์ใน Database และต้อง grant ให้ทั้งหมด***
        jdbc_password => "@1s2d3F4" *** password ของ user ***
```

```
        jdbc_driver_library => "/home/user/mysql-connector-java-5.1.43/mysql-connector-java-5.1.43-
bin.jar" *** ต้องโหลด mysql-connector-java เพื่อเป็น library ของ jdbc ***
        jdbc_driver_class => "com.mysql.jdbc.Driver" *** รูปแบบของ driver ***
        statement => "SELECT * from alert" *** ระบบตารางที่ต้องการให้ข้อมูลแสดงผล ***
       }
}
output {
    stdout { codec => json_lines } *** ข้อมูลที่นำออกมาแสดงผลในรูปแบบ json ***
    elasticsearch {
    "hosts" => "192.168.3.252:9200" *** ที่อยู่ของ host elasticsearch ***
    "index" => "ossec-migrate" *** ตั้งชื่อชุดข้อมูลนี้จะไปแสดงผลอยู่ใน Kibana ***
    "document_type" => "data" *** ระบุชนิดของเอกสาร  ***
    }
}
```



ภาพที่ 4.28 การสร้างไฟล์ควบคุมให้กับ Logstash

2.) สั่งให้ Logstash เก็บข้อมูลใน Database Mysql

/usr/share/Logstash/bin/Logstash -f /etc/Logstash/conf.d/mysql_from_ossec.conf

```
[root@ossec-syslogserver kibana]# /usr/share/logstash/bin/logstash -f /etc/logst
ash/conf.d/mysql_from_ossec.conf
```

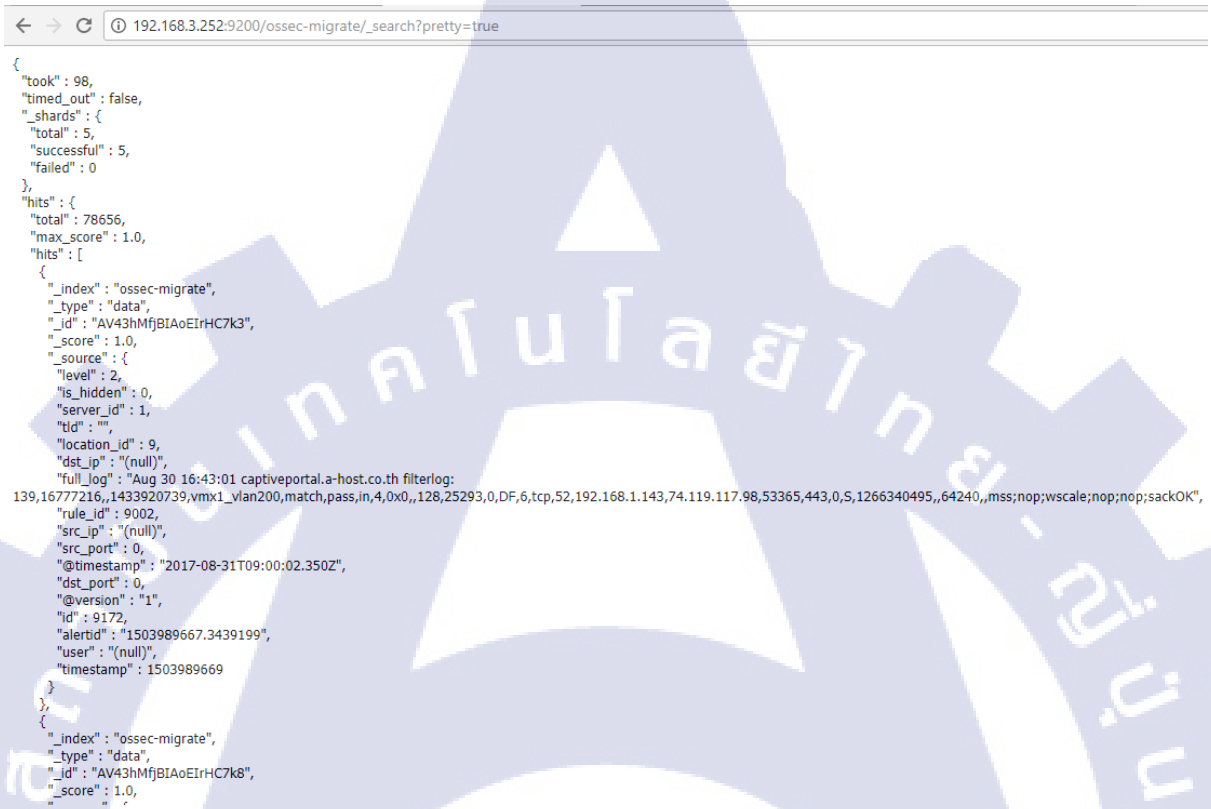
ภาพที่ 4.29 การเรียกใช้งาน Logstash ให้สามารถใช้งานไฟล์ควบคุม

เมื่อสั่งไปคำสั่งไปแล้ว จะเห็นข้อมูลระหว่างการดึงข้อมูลจาก Mysql Database เข้า Logstash

```
root@ossec-syslogserver:~
17:07:11.270 [Ruby-0-Thread-5: /usr/share/logstash/vendor/bundle/jruby/1.9/gems/
logstash-output-elasticsearch-7.3.8-java/lib/logstash/outputs/elasticsearch/http
_client/pool.rb:224] WARN  logstash.outputs.elasticsearch - Attempted to resurre
ct connection to dead ES instance, but got an error. {:url=>"http://192.168.3.25
2:9200/", :error_type=>LogStash::Outputs::ElasticSearch::HttpClient::Pool::HostU
nreachableError, :error=>"Elasticsearch Unreachable: [http://192.168.3.252:9200/
][Manticore::SocketException] Connection refused (Connection refused)"}
17:07:12.266 [[main]>worker0] WARN  logstash.outputs.elasticsearch - UNEXPECTED
POOL ERROR {:e=>#<LogStash::Outputs::ElasticSearch::HttpClient::Pool::NoConnecti
onAvailableError: No Available connections>}
17:07:12.266 [[main]>worker0] ERROR logstash.outputs.elasticsearch - Attempted t
o send a bulk request to elasticsearch, but no there are no living connections i
n the connection pool. Perhaps Elasticsearch is unreachable or down? {:error_mes
sage=>"No Available connections", :class=>"LogStash::Outputs::ElasticSearch::Htt
pClient::Pool::NoConnectionAvailableError", :will_retry_in_seconds=>8}
17:07:12.270 [[main]>worker1] WARN  logstash.outputs.elasticsearch - UNEXPECTED
POOL ERROR {:e=>#<LogStash::Outputs::ElasticSearch::HttpClient::Pool::NoConnecti
onAvailableError: No Available connections>}
17:07:12.270 [[main]>worker1] ERROR logstash.outputs.elasticsearch - Attempted t
o send a bulk request to elasticsearch, but no there are no living connections i
n the connection pool. Perhaps Elasticsearch is unreachable or down? {:error_mes
sage=>"No Available connections", :class=>"LogStash::Outputs::ElasticSearch::Htt
pClient::Pool::NoConnectionAvailableError", :will_retry_in_seconds=>8}
```

ภาพที่ 4.30 การเรียกใช้งาน Logstash ให้สามารถใช้งานไฟล์ควบคุม

3.) ตรวจสอบการทำงาน Logstash การทำ Query ได้ด้วยการเรียก http://192.168.3.252:9200/ossec-migrate/_search?pretty=true



ภาพที่ 4.31 ตรวจสอบ Elasticsearch ได้รับ Log จากตำแหน่งจากการใช้ไฟล์ควบคุม

4.) เข้าเว็ปไซต์ Kibana เข้าไปที่ Dev Tools เพื่อเรียกใช้งาน Console สำหรับการ POST ข้อมูลให้แสดงใน Kibana

ภาพที่ 4.32 เครื่องมือ Dev Tools ใน Kibana

5.) Console พิมพ์ POST /ossec-migrate/_search?pretty=true โดย ossec-migrate ใช้เป็นชื่อ index ตั้งไว้ในไฟล์ (File) .conf สร้างที่ /etc/Logstash/conf.d/

ภาพที่ 4.33 การให้ Kibana เรียกใช้งาน Query

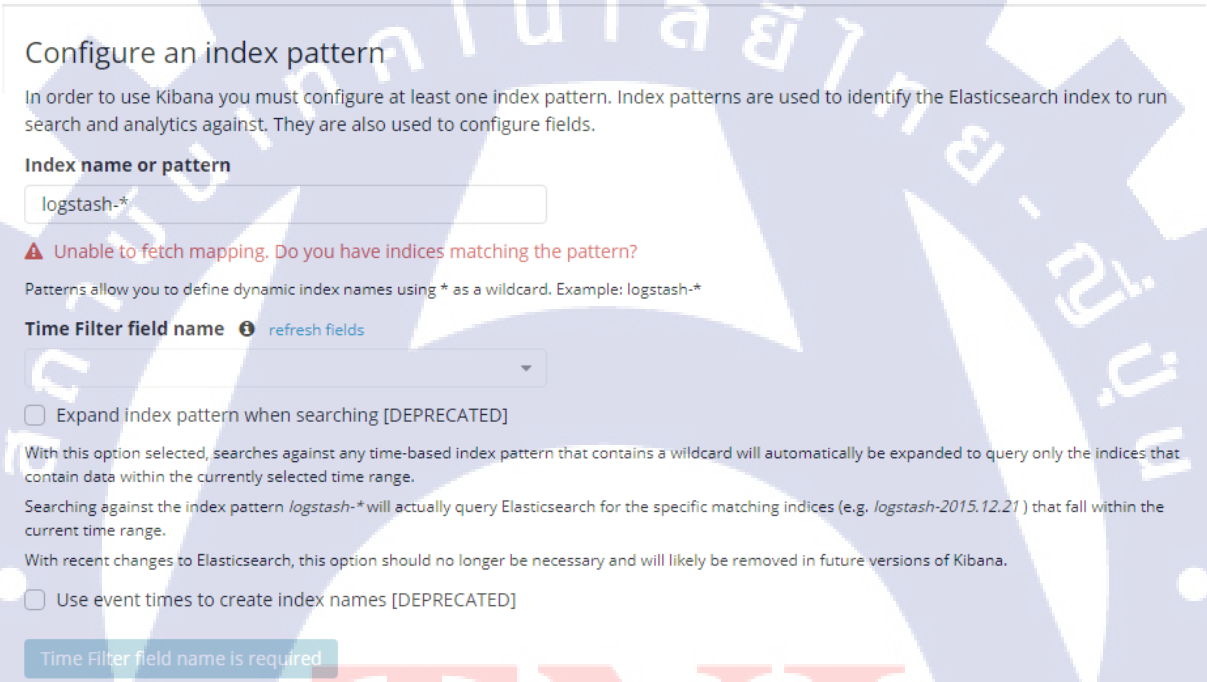
6.) ไปที่ Management

ภาพที่ 4.34 เครื่องมือ Management ใน Kibana

7.) เพื่อให้ข้อมูลเข้าใน Patterns ของ service Kibana

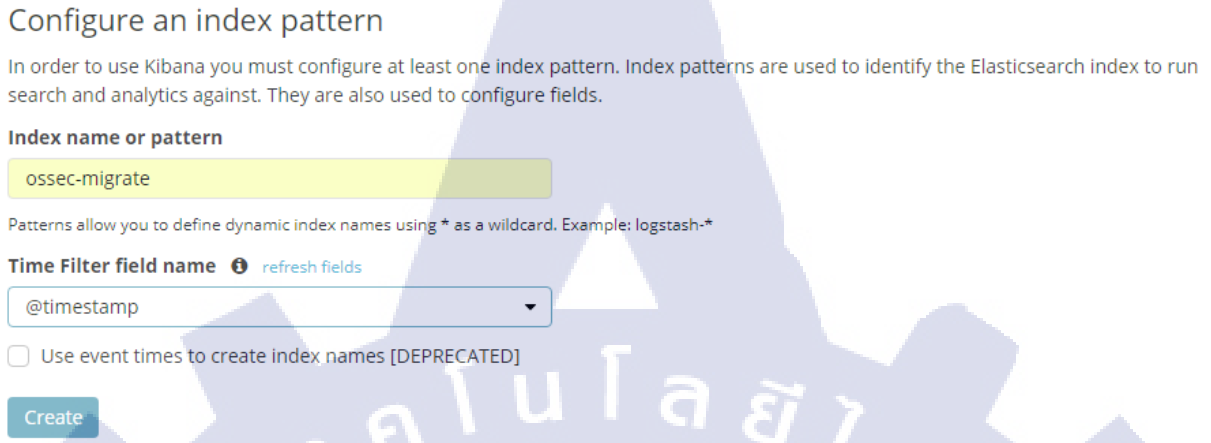
ภาพที่ 4.35 การเข้า Index Patterns

8.) เข้าที่ Index Patterns เลือกที่ช่อง Index name or pattern



ภาพที่ 4.36 หน้าต่างการ Configure an index pattern

9.) ใส่ชื่อของ index ที่เข้าตั้งเอาไว้ ใส่ในช่อง Time Filter field name สามารถเรียกข้อมูลได้



ภาพที่ 4.37 การใส่ Index name or pattern

4.1.5 การติดตั้ง X-Pack[6,8]

เป็น Package ที่มีความสามารถสูงทั้งการเพิ่มประสิทธิภาพของโปรแกรมต่าง ๆ ใน Elastic ให้มีเครื่องมือที่สามารถเรียกใช้งานได้เพิ่มเติมแล้ว ในด้านระบบความปลอดภัยของโปรแกรม Elastic เพิ่มมากขึ้นเช่นกัน โดย X-Pack จะทำให้ทุก ๆ โปรแกรมใน Elastic

1.) ส่วนของ Elasticsearch

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

systemctl stop Elasticsearch.service

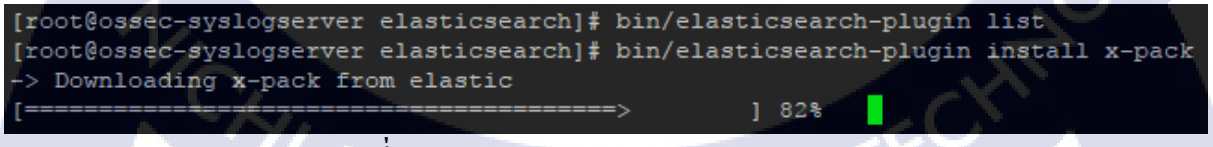
- การตั้งค่าปิดโปรแกรมการให้บริการ (Service) ของ Elasticsearch

cd /usr/share/elasticsearch

- เปิดโปรแกรม Elasticsearch

bin/elasticsearch-plugin install x-pack

- ติดตั้งแพ็คเกจ (Package) X-Pack ในโปรแกรม Elasticsearch



ภาพที่ 4.38 การอัพเกรด X-Pack ของ Elasticsearch

2.) ส่วนของ Kibana

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

cd /usr/share/kibana

- เปิดโปรแกรม Kibana

bin/kibana-plugin install x-pack

- ติดตั้งแพ็คเกจ (Package) X-Pack ในโปรแกรม Kibana

```
[root@ossec-syslogserver kibana]# bin/kibana-plugin install x-pack
Attempting to transfer from x-pack
Attempting to transfer from https://artifacts.elastic.co/downloads/kibana-plugins/x-pack/x-pack-5.5.2.zip
Transferring 119363535 bytes....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Plugin x-pack already exists, please remove before installing a new version
[root@ossec-syslogserver kibana]#
```

ภาพที่ 4.39 การอัพเกรด X-Pack ของ Kibana

ให้ดูว่ามี X-Pack ของ Kibana ตัวใดเข้ามาติดตั้งในโปรแกรม

cd /usr/share/kibana

- เปิดโปรแกรม Kibana

bin/kibana

- ใช้งานโปรแกรม Kibana

จะได้ข้อมูลดังนี้

```
[root@ossec-syslogserver kibana]# bin/kibana
  log   [07:08:45.604] [info][status][plugin:kibana@5.5.2] Status changed from uninitialized to green - Ready
  log   [07:08:46.689] [info][status][plugin:elasticsearch@5.5.2] Status changed from uninitialized to yellow - Waiting for Elasticsearch
  log   [07:08:51.047] [info][status][plugin:xpack_main@5.5.2] Status changed from uninitialized to yellow - Waiting for Elasticsearch
  log   [07:08:54.717] [error][status][plugin:xpack_main@5.5.2] Status changed from yellow to red - Request Timeout after 3000ms
  log   [07:08:54.717] [error][status][plugin:elasticsearch@5.5.2] Status changed from yellow to red - Request Timeout after 3000ms
  log   [07:09:05.023] [error][status][plugin:graph@5.5.2] Status changed from uninitialized to red - Request Timeout after 3000ms
  log   [07:09:05.040] [info][status][plugin:monitoring@5.5.2] Status changed from uninitialized to green - Ready
  log   [07:09:38.099] [warning][reporting] Generating a random key for xpack.reporting.encryptionKey. To prevent pending reports from failing on restart, pleas
e set xpack.reporting.encryptionKey in kibana.yml
  log   [07:09:38.140] [error][status][plugin:reporting@5.5.2] Status changed from uninitialized to red - Request Timeout after 3000ms
  log   [07:09:38.616] [error][status][plugin:security@5.5.2] Status changed from uninitialized to red - Request Timeout after 3000ms
  log   [07:09:38.618] [warning][security] Generating a random key for xpack.security.encryptionKey. To prevent sessions from being invalidated on restart, plea
se set xpack.security.encryptionKey in kibana.yml
  log   [07:09:38.634] [warning][security] Session cookies will be transmitted over insecure connections. This is not recommended.
  log   [07:09:38.773] [error][status][plugin:searchprofiler@5.5.2] Status changed from uninitialized to red - Request Timeout after 3000ms
  log   [07:09:38.793] [error][status][plugin:ml@5.5.2] Status changed from uninitialized to red - Request Timeout after 3000ms
  log   [07:09:38.869] [info][status][plugin:ml@5.5.2] Status changed from red to yellow - Waiting for Elasticsearch
  log   [07:09:38.879] [error][status][plugin:xpack_main@5.5.2] Status changed from red to red - Authentication Exception
  log   [07:09:38.879] [error][status][plugin:graph@5.5.2] Status changed from red to red - Authentication Exception
  log   [07:09:38.880] [error][status][plugin:reporting@5.5.2] Status changed from red to red - Authentication Exception
  log   [07:09:38.880] [error][status][plugin:security@5.5.2] Status changed from red to red - Authentication Exception
  log   [07:09:38.882] [error][status][plugin:searchprofiler@5.5.2] Status changed from red to red - Authentication Exception
  log   [07:09:38.883] [error][status][plugin:ml@5.5.2] Status changed from yellow to red - Authentication Exception
  log   [07:09:38.884] [error][status][plugin:elasticsearch@5.5.2] Status changed from red to red - Authentication Exception
  log   [07:09:38.895] [error][status][plugin:tilemap@5.5.2] Status changed from uninitialized to red - Authentication Exception
  log   [07:09:38.900] [error][status][plugin:watcher@5.5.2] Status changed from uninitialized to red - Authentication Exception
  log   [07:09:38.928] [info][status][plugin:grokdebugger@5.5.2] Status changed from uninitialized to green - Ready
  log   [07:09:38.946] [info][status][plugin:console@5.5.2] Status changed from uninitialized to green - Ready
  log   [07:09:38.964] [info][status][plugin:metrics@5.5.2] Status changed from uninitialized to green - Ready
  log   [07:09:40.034] [info][status][plugin:timelion@5.5.2] Status changed from uninitialized to green - Ready
  log   [07:09:40.057] [fatal] Port 5601 is already in use. Another instance of Kibana may be running!
FATAL Port 5601 is already in use. Another instance of Kibana may be running!
```

ภาพที่ 4.40 การดู Service ที่เข้ามาติดตั้งในโปรแกรม

3.) ส่วนของ Logstash

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

cd /usr/share/Logstash

- เปิดโปรแกรม Logstash

bin/Logstash-plugin install x-pack

- ติดตั้งแพ็คเกจ (Package) X-Pack ในโปรแกรม Logstash

```
[root@ossec-syslogserver logstash]# bin/logstash-plugin install x-pack
Downloading file: https://artifacts.elastic.co/downloads/logstash-plugins/x-pack
/x-pack-5.5.2.zip
Downloading [=============================================================] 100%
Installing file: /tmp/studtmp-ef2f559833llc92afb493279e31315a97b9d0e763363f7bb89
482fb43ae8/x-pack-5.5.2.zip
Install successful
[root@ossec-syslogserver logstash]#
```

ภาพที่ 4.41 การอัพเกรด X-Pack ของ Logstash

4.) เมื่อลง X-Pack ทั้งหมดเรียบร้อยแล้ว ให้ทำการ reboot เพื่อ restart ค่า Configure ใหม่ทั้งหมด หลังจากที่ทำการ reboot แล้วให้ตรวจสอบการให้บริการ (service) ทั้งหมด

systemctl status elasticsearch.service

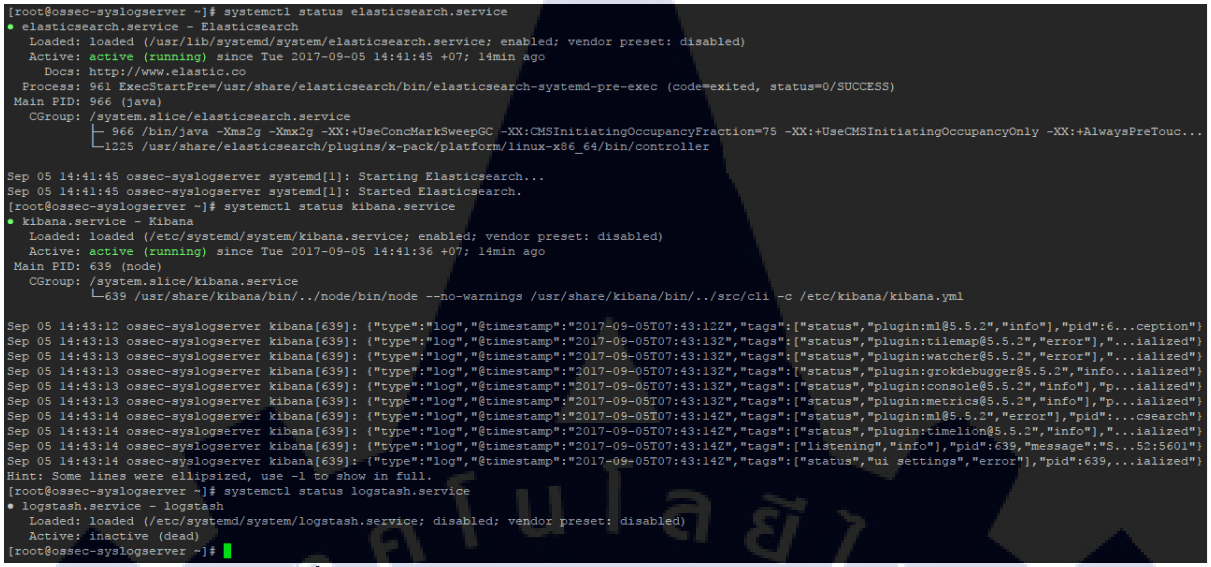
- ตรวจสอบการให้บริการ (Service) ของ Elasticsearch

systemctl status kibana.service

- ตรวจสอบการให้บริการ (Service) ของ Kibana

systemctl status logstash.service

- ตรวจสอบการให้บริการ (Service) ของ Logstash

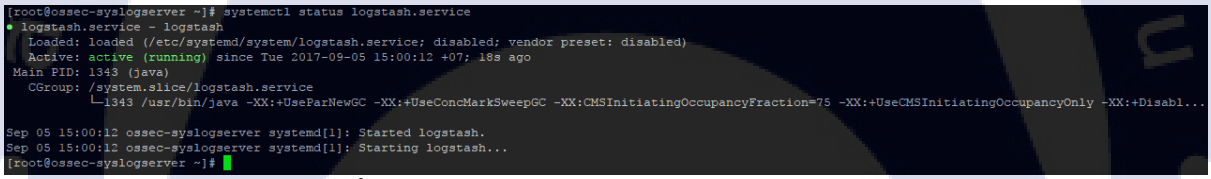


ภาพที่ 4.42 การตรวจสอบสถานะของการให้บริการของ Elastic

Elasticsearch และ Kibana ทำงานเป็นปกติ แต่ Logstash inactive (dead) อยู่ ให้ทำการเปิด service

systemctl start logstash.service

- การตั้งค่าเปิดโปรแกรมการให้บริการ (Service) ของ Elasticsearch

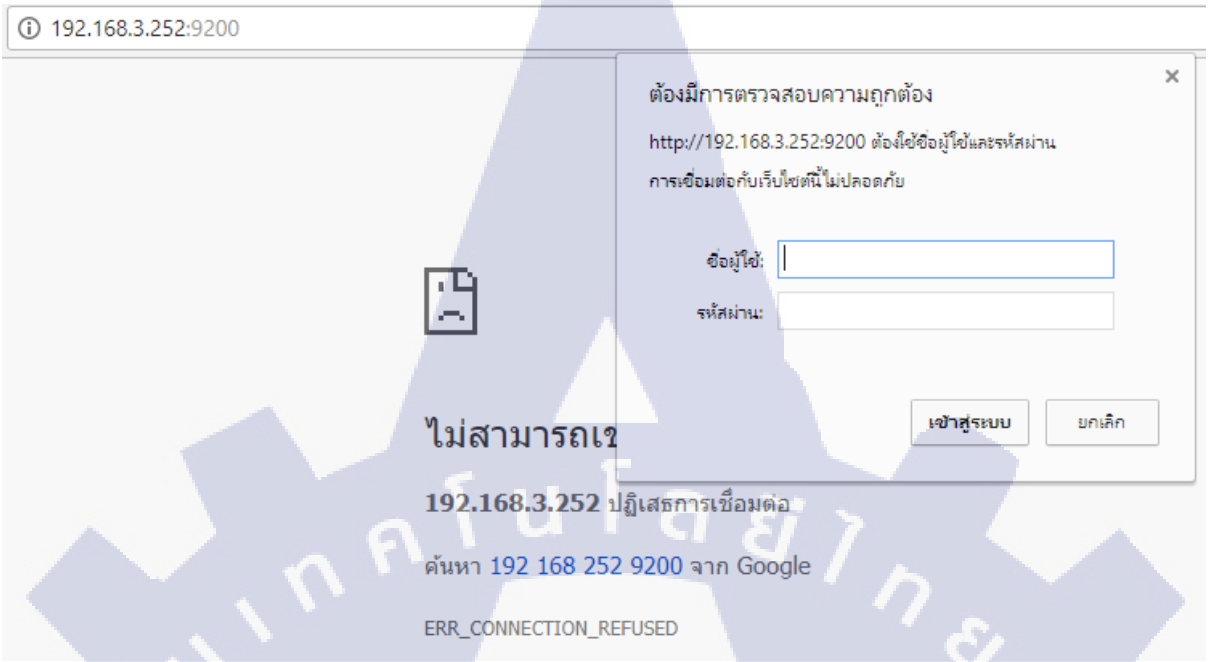


ภาพที่ 4.43 การเปิด Logstash การให้บริการของ Elastic

5.) เข้าเว็ปไซต์เข้าไปที่ 192.168.3.252:9200 โดยใช้

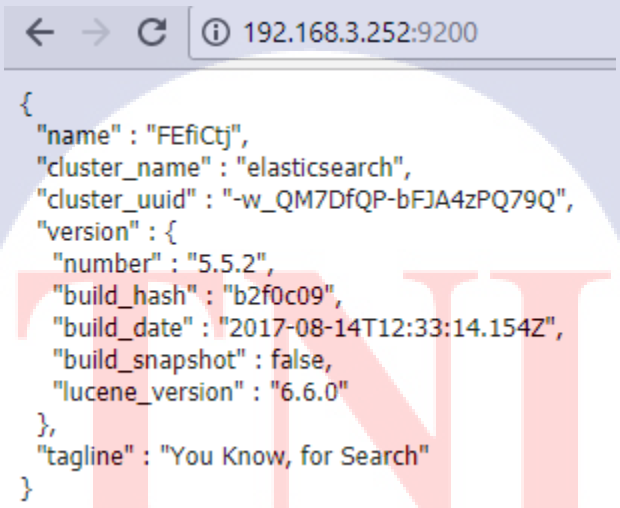
Username: elastic

Password: changeme



ภาพที่ 4.44 การเข้ารหัสของ Elasticsearch หลังจากติดตั้ง Package

สามารถเห็น Process ของการใช้งาน Elasticsearch ได้แบบปกติในรูปแบบที่ติดตั้ง X-pack เรียบร้อย



ภาพที่ 4.45 การเข้ารหัสของ Elasticsearch หลังจากติดตั้ง X-Pack

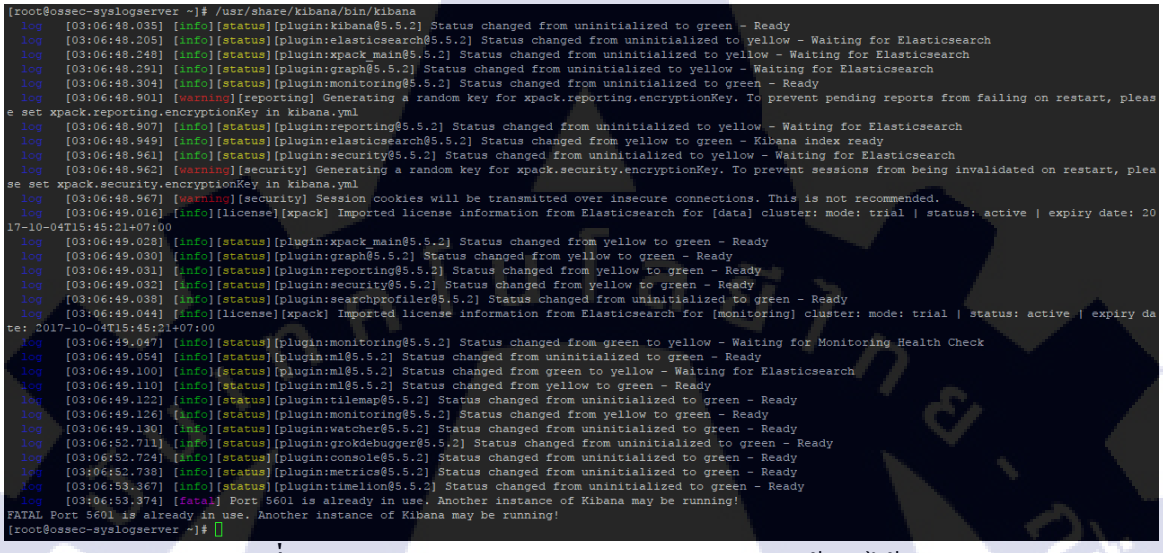
Elasticsearch สามารถใช้งานได้ปกติ

6.) ส่วนของ Kibana

เริ่มต้นการติดตั้งด้วย Command line ดังนี้

cd /usr/share/kibana/bin/kibana

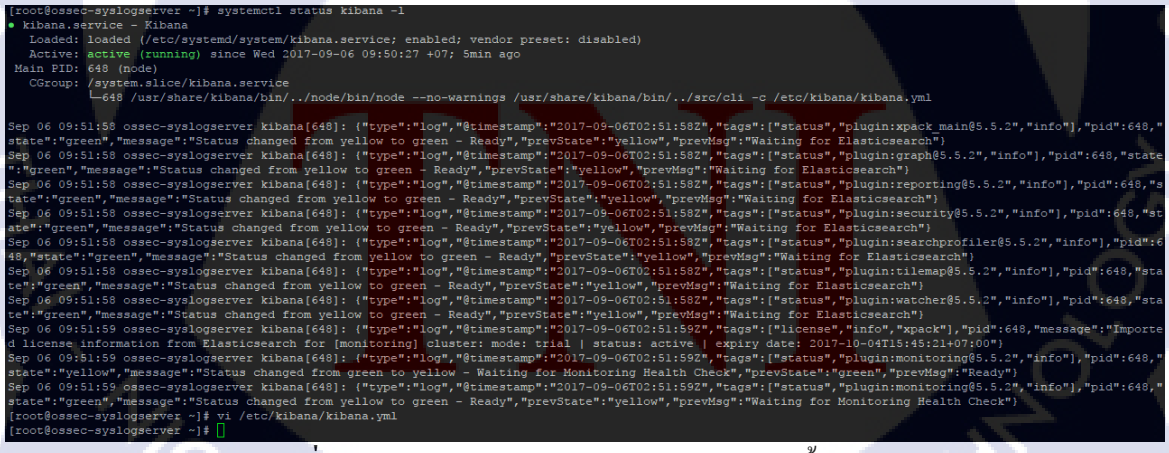
- ใช้งานโปรแกรม Kibana



ภาพที่ 4.46 สถานะของ Package เสริมสามารถเรียกใช้งานได้ปกติ

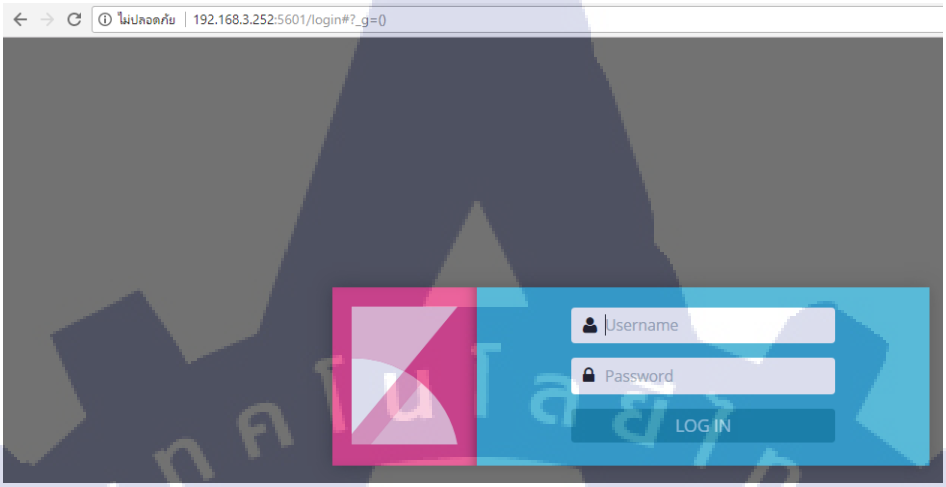
systemctl status kibana.service -l

- ตรวจสอบการให้บริการ (Service) ของ Kibana แบบแสดงรายละเอียด



ภาพที่ 4.47 การดูสถานะของ Kibana หลังจากติดตั้ง X-Pack

เข้าเว็บไซต์ 192.168.3.252:5601 เพื่อตรวจสอบว่า X-Pack ทำให้ Kibana ต้องมีการเข้ารหัส



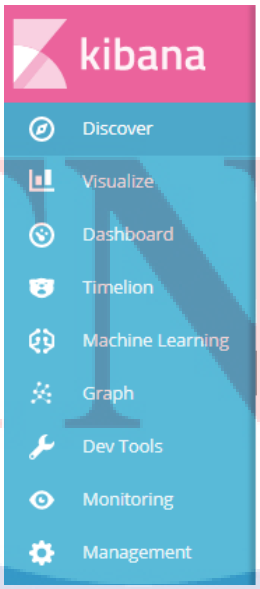
ภาพที่ 4.48 การเข้ารหัสของ Kibana หลังจากติดตั้ง X-Pack

ติดตั้งสำเร็จ Login อยู่ในหน้าเว็ปไซต์ Kibana

Username : elastic

Password : changeme

มีเครื่องมือจากการลง Package เสริมของ x-pack เข้ามาเพิ่มเติมในส่วนของ Kibana



ภาพที่ 4.49 เครื่องมือเพิ่มเติมของ Kibana หลังจากติดตั้ง X-Pack

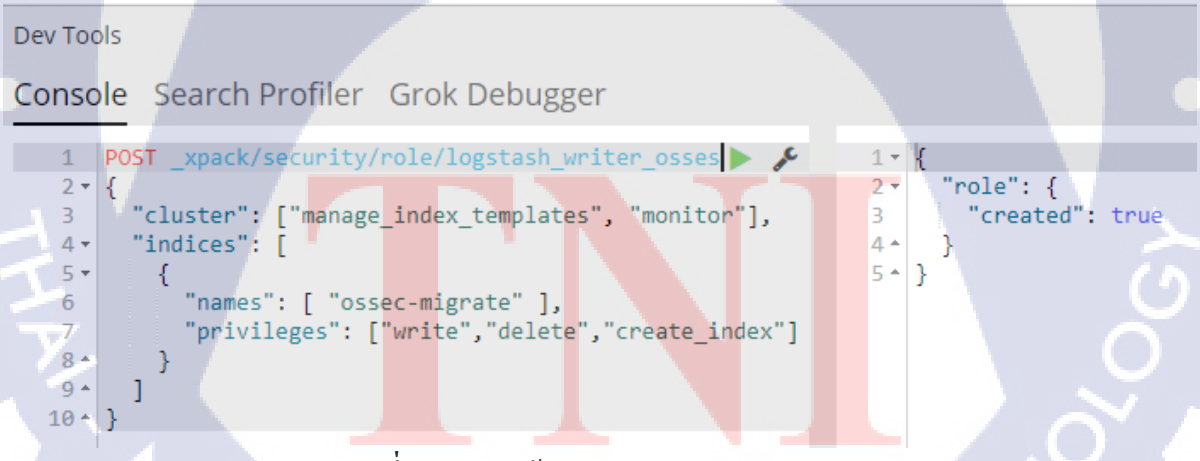
4.1.6 การเพิ่มข้อมูล (Update data) หลังจากติดตั้ง X-Pack[6,8]

การติดตั้ง X-Pack ทำให้ระบบรักษาความปลอดภัย (security) การให้บริการ (Service) ทั้งหมดของ Elastic ทั้งหมดเพิ่มมากขึ้นไปด้วย ดังนั้นการเพิ่มข้อมูล (Update data) โดยใช้ Logstash จำเป็นต้องใส่รหัสในไฟล์ควบคุม (File Configure) .conf เพื่อให้สามารถเรียกใช้งาน Elasticsearch ได้

1.) ต้องสร้าง Rule ในโปรแกรม kibana

```
POST _xpack/security/role/Logstash_writer_osses
{
 "cluster": ["manage_index_templates", "monitor"],
 "indices": [
  {
   "names": [ "ossec-migrate" ],
    "privileges": ["write","delete","create_index"]
  }
 ]
}
```

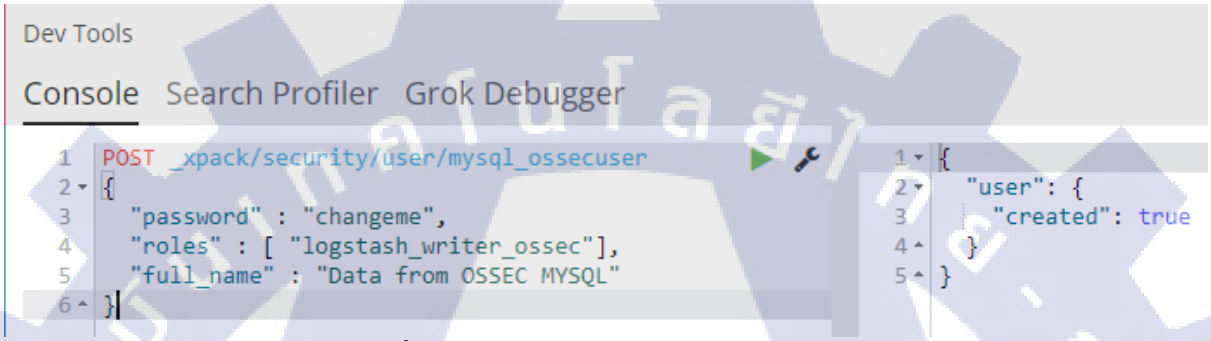
โดยต้องใส่ “names” ให้ตรงกับ "index" ใน .conf ที่ได้สร้างไว้



ภาพที่ 4.50 การสร้าง Rule ในโปรแกรม Kibana

2.) ต้องสร้าง user สำหรับการใช้งาน Rule ที่สร้างไว้

```
POST _xpack/security/user/mysql_ossecuser
{
 "password" : "changeme",
 "roles" : [ "Logstash_writer_ossec"],
 "full_name" : "Data from OSSEC MYSQL"
}
```



ภาพที่ 4.51 การสร้าง user ในโปรแกรม Kibana

3.) สร้าง .conf เพื่อเพิ่ม User& Pass เข้าไปในการเรียกข้อมูลจาก Logstash และคัดกรองด้วย Elasticsearch

```
input {
 elasticsearch {
  ...
  user => Logstash_internal
  password => changeme
 }
}
filter {
 elasticsearch {
  ...
  user => Logstash_internal
```

```
    password => changeme
  }
}
output {
  elasticsearch {
    ...
    user => Logstash_internal
    password => changeme
  }
}
```

ตัวอย่าง

```
input {
      jdbc {
            jdbc_connection_string => "jdbc:mysql://192.168.3.252:3306/ossec"
            jdbc_user => "ossecuser"
            jdbc_password => "@1s2d3F4"
            jdbc_driver_library => "/home/user/mysql-connector-java-5.1.43/mysql
-connector-java-5.1.43-bin.jar"
            jdbc_driver_class => "com.mysql.jdbc.Driver"
            statement => "SELECT * from alert"
          }
        elasticsearch {
           user => elastic
           password => changeme
          }
}
filter {
        elasticsearch {
           user => elastic
           password => changeme
          }
}
output {
        stdout { codec => json_lines }
        elasticsearch {
        "hosts" => "192.168.3.252:9200"
        "index" => "ossec-migrate"
        "document_type" => "data"
        user => elastic
        password => changeme
        }
}
```

ภาพที่ 4.52 การใส่รหัสในไฟล์ .conf หลังจากติดตั้ง X-Pack

4.) Update Data เข้าไปใหม่อีกครั้งด้วยการเรียก Logstash -f

/usr/share/Logstash/bin/Logstash -f /etc/Logstash/conf.d/mysql_from_ossec.conf

```
ash-core/lib/logstash/plugins/registry.rb:138:in `lookup'", "/usr/share/logsta
sh/logstash-core/lib/logstash/plugins/registry.rb:180:in `lookup_pipeline_plug
in'", "/usr/share/logstash/logstash-core/lib/logstash/plugin.rb:140:in `lookup
'", "/usr/share/logstash/logstash-core/lib/logstash/pipeline.rb:100:in `plugin
'", "(eval):16:in `initialize'", "org/jruby/RubyKernel.java:1079:in `eval'", "
/usr/share/logstash/logstash-core/lib/logstash/pipeline.rb:72:in `initialize'"
, "/usr/share/logstash/logstash-core/lib/logstash/pipeline.rb:156:in `initiali
ze'", "/usr/share/logstash/logstash-core/lib/logstash/agent.rb:286:in `create_
pipeline'", "/usr/share/logstash/logstash-core/lib/logstash/agent.rb:95:in `re
gister_pipeline'", "/usr/share/logstash/logstash-core/lib/logstash/runner.rb:3
14:in `execute'", "/usr/share/logstash/vendor/bundle/jruby/1.9/gems/clamp-0.6.
5/lib/clamp/command.rb:67:in `run'", "/usr/share/logstash/logstash-core/lib/lo
gstash/runner.rb:209:in `run'", "/usr/share/logstash/vendor/bundle/jruby/1.9/g
ems/clamp-0.6.5/lib/clamp/command.rb:132:in `run'", "/usr/share/logstash/lib/b
ootstrap/environment.rb:71:in `(root)'"]}
15:49:44.039 [LogStash::Runner] ERROR logstash.agent - Cannot create pipeline
{:reason=>"Couldn't find any filter plugin named 'elasticsearch'. Are you sure
 this is correct? Trying to load the elasticsearch filter plugin resulted in t
his error: Problems loading the requested plugin named elasticsearch of type f
ilter. Error: NameError NameError"}
15:49:44.721 [[.monitoring-logstash]-pipeline-manager] INFO  logstash.outputs.
elasticsearch - Elasticsearch pool URLs updated {:changes=>{:removed=>[], :add
ed=>[http://logstash_system:xxxxxx@localhost:9200/]}}
15:49:44.723 [[.monitoring-logstash]-pipeline-manager] INFO  logstash.outputs.
elasticsearch - Running health check to see if an Elasticsearch connection is
working {:healthcheck_url=>http://logstash_system:xxxxxx@localhost:9200/, :pat
h=>"/"}
15:49:45.544 [[.monitoring-logstash]-pipeline-manager] WARN  logstash.outputs.
elasticsearch - Attempted to resurrect connection to dead ES instance, but got
 an error. {:url=>"http://logstash_system:xxxxxx@localhost:9200/", :error_type
=>LogStash::Outputs::ElasticSearch::HttpClient::Pool::HostUnreachableError, :e
rror=>"Elasticsearch Unreachable: [http://logstash_system:xxxxxx@localhost:920
0/][Manticore::SocketException] Connection refused (Connection refused)"}
15:49:45.549 [[.monitoring-logstash]-pipeline-manager] INFO  logstash.outputs.
elasticsearch - New Elasticsearch output {:class=>"LogStash::Outputs::ElasticS
earch", :hosts=>["http://localhost:9200"]}
15:49:45.549 [[.monitoring-logstash]-pipeline-manager] INFO  logstash.pipeline
 - Starting pipeline {"id"=>".monitoring-logstash", "pipeline.workers"=>1, "pi
peline.batch.size"=>2, "pipeline.batch.delay"=>5, "pipeline.max_inflight"=>2}
15:49:45.551 [[.monitoring-logstash]-pipeline-manager] INFO  logstash.pipeline
 - Pipeline .monitoring-logstash started
15:49:48.756 [LogStash::Runner] WARN  logstash.agent - stopping pipeline {:id=
>".monitoring-logstash"}
15:49:49.020 [Api Webserver] INFO  logstash.agent - Successfully started Logst
ash API endpoint {:port=>9600}
```

ภาพที่ 4.53 การดึงข้อมูลของ Logstash หลังจากติดตั้ง X-Pack

5.) POST /ossec-migrate/_search?pretty=true เพื่อให้ Kibana เรียกข้อมูลจาก Elasticsearch

ภาพที่ 4.54 การให้ Kibana เรียกใช้งาน Query หลังจากติดตั้ง X-Pack

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

หลังจากที่ได้ทำการศึกษาเรียนรู้ขั้นตอนการใช้งานโปรแกรมระบบการเชื่อมต่อของโปรแกรมที่ได้สร้างขึ้นการเชื่อมต่อตั้งแต่ขั้นตอนแรกด้วยการทำการ Syslog จากเครื่องระบบเครือข่าย (Network) ภายในส่งมาที่เครื่องของ OSSEC Server ด้วยวิธีนี้ทำให้ Log ที่ได้รับผ่านการตรวจสอบและขั้นกรองจากโปรแกรมที่ได้สร้างขึ้นมาโดยสามารถบอกความเสี่ยงของ Log ข้อมูลของ Log ที่ได้รับรวมได้ถึงการทำแสดงผล (Visualize) ให้ผู้ที่ทำการ Monitor เข้าใจถึงระดับความเสี่ยงได้

5.2 แนวทางการแก้ไขปัญหา

การได้เข้ารับ Requirement ของพี่ ๆ ความต้องการระบบ SIEM จึงได้พยายามในการศึกษาค้นคว้าหาวิธีการติดตั้งและใช้งานระบบของโปรแกรมจนกระทั่งสามารถใช้งานได้ ด้วยการหาคู่มือจากอินเทอร์เน็ต (Internet) และทำการศึกษาจนสามารถแก้ไขปัญหาได้

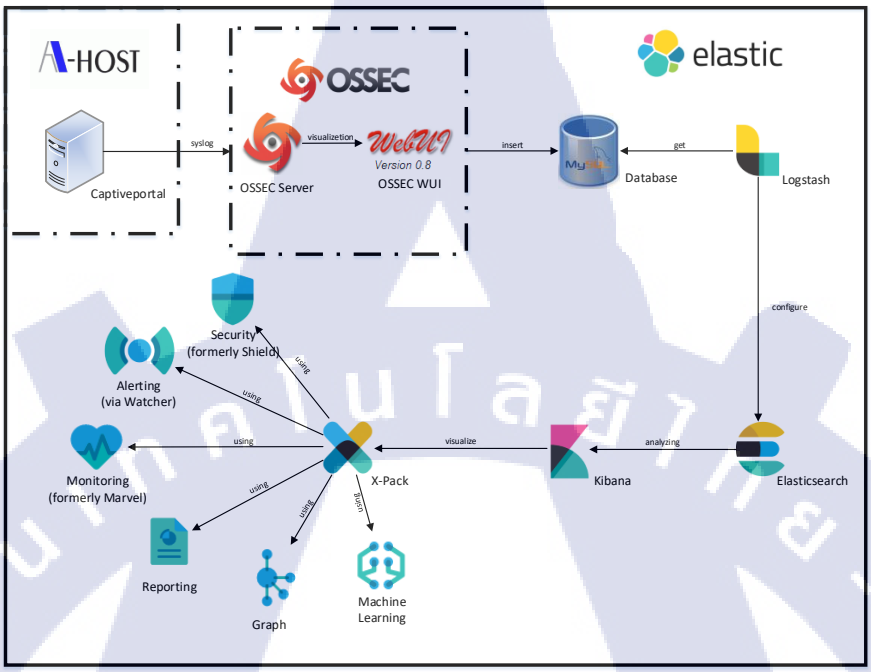
5.3 ข้อเสนอแนะจากการดำเนินงาน

การเรียนรู้อย่างสม่ำเสมอทำให้พัฒนาศักษภาพ และเพิ่มประสิทธิภาพในเการเข้าใจสิ่งใหม่ ๆ เพราะอนาคตงานไม่ได้มีแค่อย่างใดอย่างหนึ่ง แต่เราต้องพัฒนาเพื่อตอบปัญหาของงานนั้น ๆ ได้

5.4 ผลลัพธ์จากการติดตั้งโปรแกรม

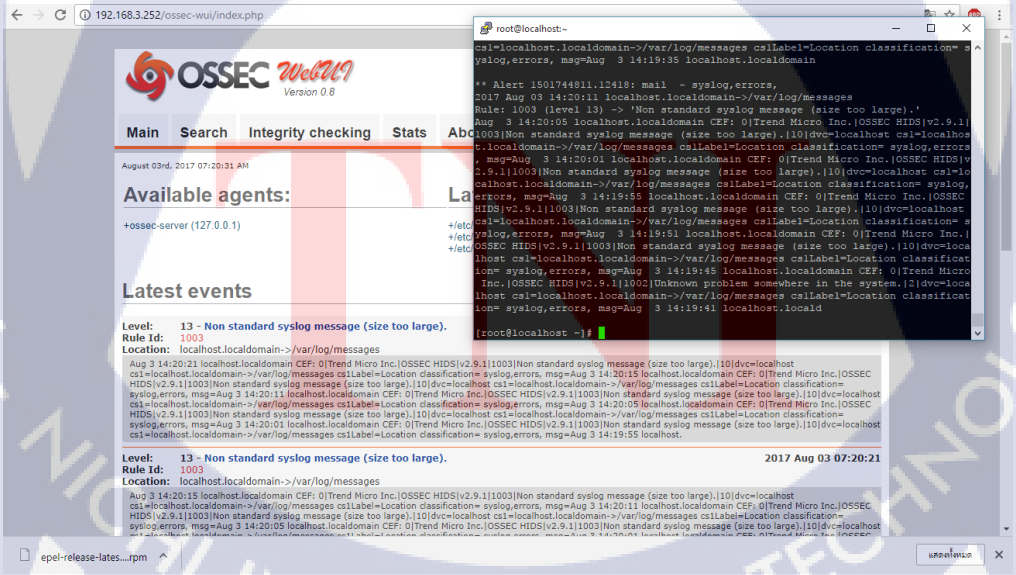
จากการได้ทำการศึกษาค้นคว้าหาวิธีการติดตั้งโปรแกรมจนกระทั่งโปรแกรมสามารถทำงานได้อย่างปกตินั้นจำเป็นต้องนำ Log จากเครื่อง Network Server มายังเครื่องที่ได้ทำการติดตั้งโปรแกรมจำเป็นต้องทำการตรวจสอบการได้รับ Syslog มาที่โปรแกรมตรวจสอบ Log ด้วยโปรแกรม OSSEC จัดเก็บข้อมูลที่ผ่านการตรวจสอบด้วยโปรแกรม MySQL Database และสุดท้ายคือการนำข้อมูลแสดงผลในรูปแบบข้อมูลกราฟและข้อมูลรูปภาพต่าง ๆ ทำให้ผู้ที่ทำการ Monitor ใช้งานได้มีกระบวนการและตัวอย่างโปรแกรม ดังนี้

ตัวอย่างกระบวนการทำงานของโปรแกรมในระบบ

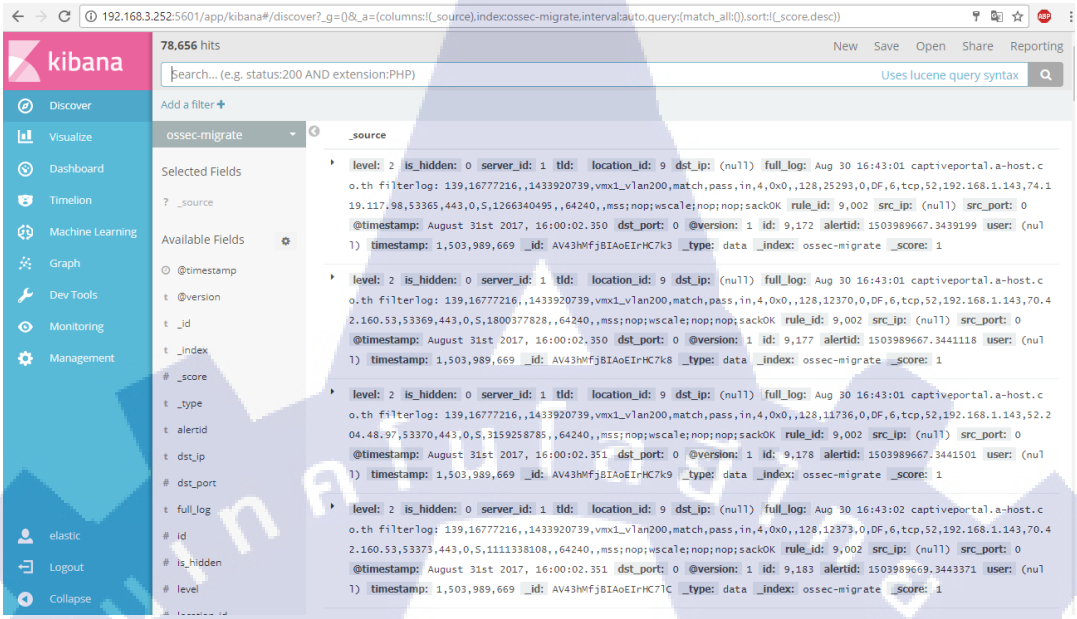


ภาพที่ 5.1 กระบวนการทำงานของโปรแกรม

ตัวอย่างโปรแกรมการทำงานบนระบบ



ภาพที่ 5.2 Interface OSSEC



ภาพที่ 5.3 การแสดง Discover Kibana

เอกสารอ้างอิง

1. A-Host Company Limited. Contact Us. [ออนไลน์]. 2560.
แหล่งที่มา: http://www.a-host.co.th/index.php?option=com_content&view=article&id=27&Itemid=128

2. ทีมงาน TechTalkThai. SIEM and Beyond – ทำความรู้จักกับเทคโนโลยี SIEM และการต่อยอดที่เหนือกว่า SIEM อีกระดับ. [ออนไลน์]. 2558.
แหล่งที่มา: https://www.techtalkthai.com/siem-and-beyond/

3. ทีมงาน TechTalkThai. เหตุใด SIEM ยังไม่เพียงพอ?. [ออนไลน์]. 2560.
แหล่งที่มา: https://www.techtalkthai.com/why-siem-not-enough/

4. OSSEC Project Team. About. [ออนไลน์]. 2560.
แหล่งที่มา: https://ossec.github.io/about.html

5. Visual edit. มายเอสคิวเอล. [ออนไลน์] 2560.
แหล่งที่มา: https://goo.gl/7ZtRVw

6. ทีมงาน Elastic. Resources and Training. [ออนไลน์]. 2560.
แหล่งที่มา: https://www.elastic.co/learn

7. kmibei. Installing OSSEC HIDS on CentOS 7. [ออนไลน์]. 2560.
แหล่งที่มา: https://kmibei.com/04/03/2017/installing-ossec-hids-on-centos-7/

8. Vineeth Mohan. Migrating MySql Data Into Elasticsearch Using Logstash. [ออนไลน์]. 2559.
แหล่งที่มา: https://qbox.io/blog/migrating-mysql-data-into-elasticsearch-using-logstash

9. aquerubin. Revert 'NOT NULL' for src_ip and dst_ip. This was mistakenly added in. [ออนไลน์]. 2559.
แหล่งที่มา: https://github.com/ossec/ossec-hids/blob/master/src/os_dbd/mysql.schema

10. Steve Lodin. dumb OSSEC database question. [ออนไลน์]. 2555.
แหล่งที่มา: https://groups.google.com/forum/#!msg/ossec-list/z6cXq1iZYTo/2aPGtkBdc4sJ

11. Gabriel Cánepa. How To Install Elasticsearch, Logstash, and Kibana (ELK Stack) on CentOS/RHEL 7. [ออนไลน์]. 2559.
แหล่งที่มา: https://www.tecmint.com/install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-rhel-7/

12. Linode. How to Install MySQL on CentOS 7. [ออนไลน์]. 2560.
แหล่งที่มา: https://www.linode.com/docs/databases/mysql/how-to-install-mysql-on-centos-7

ภาคผนวก

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล ณัฐพล บุญไทย

วัน เดือน ปีเกิด 17 พฤษภาคม 2538

ประวัติการศึกษา

ระดับประถมศึกษา โรงเรียนเกวลินวิทยา

ระดับมัธยมศึกษา โรงเรียนนวมินทราชินูทิศ เตรียมอุดมศึกษาพัฒนาการ

ระดับอุดมศึกษา สถาบันเทคโนโลยีไทย-ญี่ปุ่น

ทุนการศึกษา - ไม่มี -

ประวัติการฝึกอบรม - ไม่มี -

ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -