ระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บเซิร์ฟเวอร์

Mini SOC : Web Server

นาย ธริช พงษ์รชนี

Tarish Pongrashani

สารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษา

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมเครือข่ายและความมั่นคงปลอดภัย

สารสนเทศ แขนงความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

คณะวิทยาการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีมหานคร

ปีการศึกษา 2562

หัวข้อ	ระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บเซิร์ฟเวอร์ Mini SOC: Web Server
ชื่อนักศึกษา	ธริช พงษ์รชนี
รหัสนักศึกษา	6017810019
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาวิศวกรรมเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
ปีการศึกษา	2562
อาจารย์ที่ปรึกษา	ผศ.ดร. เอกรัฐ รัฐกาญจน์

บทคัดย่อ

สารนิพนธ์ฉบับนี้เป็นการออกแบบและจัดการศูนย์ปฏิบัติการความมั่นคงปลอดภัยระบบสารสนเทศ (Security Operation Center Design and Management) ขนาดเล็ก (Mini SOC : Web Server) โดยเก็บเฉพาะ Log ของ Web Server เท่านั้น เพื่อใช้สำหรับการวิเคราะห์และเฝ้าระวัง (Monitor) ภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นกับระบบ และหาแนวทางรับมือ ยับยั้ง ป้องกันภัยคุกคาม ที่อาจจะเกิดขึ้นกับระบบ ก่อให้เกิดความเสียหายกับองค์กรได้ โดยการส่ง Log จาก Web Server มายังระบบวิเคราะห์ Log (SIEM) และใช้ AlienVault SIEM ในการวิเคราะห์ Log ซึ่ง AlienVault SIEM เป็นซอฟต์แวร์โอเพนซอร์ส (Open Source Software – OSS) ที่สามารถนำมาใช้งานได้โดยไม่มีค่าใช้จ่ายอีกทั้งช่วยลดต้นทุนในองค์กร และไม่เสี่ยงต่อการละเมิดลิขสิทธิ์

กิตติกรรมประกาศ

การทำสารนิพนธ์ในครั้งนี้ได้รับแรงบันดาลใจจากการเรียนวิชาการออกแบบและจัดการศูนย์ปฏิบัติการความมั่นคงปลอดภัยระบบสารสนเทศ (Security Operation Center Design and Management) และเกิดเป็นแนวความคิดที่จะนำความรู้จากที่เรียน มาประยุกต์ใช้กับการทำงานในปัจจุบันให้เกิดประโยชน์สูงสุด

ขอขอบพระคุณอาจารย์ที่ปรึกษา ผศ.ดร.เอกรัฐ รัฐกาญจน์ และ ดร.นันทา จันทร์พิทักษ์ ที่คอยสนับสนุน และมีส่วนทำให้สารนิพนธ์นี้สำเร็จลุล่วงได้ตามเป้าหมายที่กำหนดไว้ ขอขอบพระคุณอาจารย์ไชยณัฐ จามรมาน ที่ให้แรงบันดาลใจในการทำสารนิพนธ์นี้ และคอยให้คำแนะนำ ชี้แนะแนวทาง เกี่ยวกับออกแบบระบบ Mini SOC ในครั้งนี้

สุดท้ายนี้ ขอขอบพระคุณคุณแม่ที่ส่งเสริมและสนับสนุนในการศึกษา ขอขอบพระคุณรุ่นพี่ รุ่นน้อง เพื่อนๆ และทุกคนที่ช่วยเหลือในเรื่องต่างๆ ที่เกี่ยวข้องกับการทำสารนิพนธ์ฉบับนี้

ธริช พงษ์รชนี

มีนาคม 2562

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

บทที่ 1

บทนำ

ปัจจุบันการเฝ้าระวังดูแลความพร้อมของระบบเป็นสิ่งสำคัญ รวมถึงกระบวนการที่ต้องดำเนินการเมื่อมีเหตุการณ์ผิดปกติ อย่างไรก็ตาม นอกจากการวางมาตรการต่างๆ ให้รัดกุมแล้ว ยังจำเป็นที่จะต้องมีการตรวจสอบการเข้าถึงระบบต่างๆ เป็นประจำอย่างต่อเนื่อง จึงต้องมีหน่วยงานที่เฝ้าระวังด้านความมั่นคงปลอดภัย (Security Operation Center - SOC) เพื่อดูแลและตรวจสอบการเข้าถึงระบบต่างๆ ขององค์กร ว่ามีการเข้าถึงที่ผิดปกติ หรือมีการบุกรุกจากภายนอกหรือไม่ และมีกระบวนการตอบสนองต่อการบุกรุกได้อย่างรวดเร็ว แต่เหตุการณ์ในด้านความปลอดภัยนี้ อาจเกิดขึ้นได้ตลอดเวลาเช่นกัน ซึ่งบางครั้งทีมงานความปลอดภัยขององค์กร อาจจะไม่สามารถดูแลทั่วถึงได้

สำหรับศูนย์ความปลอดภัย จะทำหน้าที่เฝ้าระวังเหตุการณ์ที่ผิดปกติ และป้องกันระบบขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต หากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมินผล ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบ และความเสียหายที่อาจเกิดขึ้นกับองค์กรนั้นๆ ให้อยู่ในระดับที่ไม่รุนแรง

ในองค์กรหรือหน่วยงานขนาดเล็ก มักจะมีปัญหาเรื่องงบประมาณในการลงทุนเกี่ยวกับ SOC โดยต้องลงทุนด้านฮาร์ดแวร์ ซอฟแวร์ ปัญหาด้านบุคลากรที่ไม่เพียงพอ จึงไม่สามารถดูแลระบบได้ทั่วถึง รวมถึงการขาดผู้เชี่ยวชาญเพื่อให้คำปรึกษา และปัญหาเหล่านี้อาจเป็นสาเหตุที่ทำให้องค์กรเกิดความสูญเสียได้

การป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีนั้น ต้องมีการเฝ้าระวังระบบจากภายในองค์กรอย่างสม่ำเสมอ ในโครงงานนี้ผู้จัดทำ ได้เล็งเห็นปัญหาดังกล่าว จึงได้มีความคิดจัดทำระบบเพื่อเฝ้าระวังความปลอดภัยจากผู้ไม่ประสงค์ดีในรูปแบบขนาดเล็ก (Mini SOC) ขึ้น คือจำกัดระบบที่เฝ้าระวัง และมีการกำหนดรูปแบบของเหตุการณ์การบุกรุก (Use case) ที่ใช้ในการกำหนดเงื่อนไข (Rule) การเฝ้าระวัง และสร้างใบรายงานการแจ้งเตือน (Incident Ticket) การบุกรุก ไปยังผู้ดูแลระบบ เพื่อลดความเสี่ยงต่อความเสียหาย ที่จะเกิดขึ้นกับองค์กร ในขณะเดียวกันนั้น ก็สามารถจำกัดค่าใช้จ่ายในการลงทุนเกี่ยวกับ SOC ได้

1.1 ปัญหาและแรงจูงใจ

เนื่องจาก Web Server เป็นระบบมีทั้งที่ให้บริการภายในองค์กรเอง และให้บริการกับลูกค้าภายนอก และสามารถเข้าถึงได้จากภายนอกองค์กรในบางส่วนแล้ว นอกจากการใช้อุปกรณ์ Security

จำพวก Firewall เพียงอย่างเดียว อาจไม่เพียงพอที่จะป้องกันการผู้ไม่ประสงค์ดี (Hacker) ในการเข้าถึง Web Server ในส่วนที่ไม่ได้รับอนุญาตได้ เพราะในปัจจุบันนี้มีวิธีการหลบเลี่ยง การตรวจจับ (Bypass) มากมายหลายวิธี รวมทั้งภัยคุกคามทางด้านไซเบอร์ต่างๆ ที่ไม่สามารถ คาดเดาเหตุการณ์ล่วงหน้า ซึ่งอาจจะเกิดกับระบบ Web Server ได้ ถ้าไม่มีการเก็บ Log มาวิเคราะห์เพื่อเฝ้าระวัง หรือขาดการเฝ้าระวังอย่างเพียงพอ

ปัจจัยสำคัญ ที่เป็นแรงจูงใจให้กับ Hacker ในการพยายามเข้าถึง Web Server ในส่วน ที่ไม่ได้รับอนุญาตให้เข้าถึงนั้น คือโจรกรรมข้อมูลสำคัญ ๆ เหล่านั้นไปขาย ซึ่งเป็นความเสียหาย ใหญ่หลวงจนประเมินมูลค่าได้ยาก เพราะนอกจากก่อให้เกิดความเสียหายต่อชื่อเสียงขององค์กร ส่งผลกระทบทำให้ลูกค้าขาดความเชื่อมั่น ในการรักษาความปลอดภัยของข้อมูล ตลอดจนสูญเสียโอกาสในการแข่งขันทางด้านธุรกิจขององค์กร อีกทั้งในการโจมตีระบบ Web Server เพื่อให้ระบบหยุดชะงักจนไม่สามารถให้บริการได้ ก็เป็นความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบ Web Server ขององค์กร ถ้าไม่มีการเฝ้าระวัง และถ้าหากเกิดเหตุการณ์นี้ขึ้นกับระบบ Web Server แล้ว ความเสียหายที่เกิดขึ้นยากต่อการประเมินมูลค่าเช่นกัน

ปัจจัยด้านการลงทุนในการจัดซื้ออุปกรณ์ Security อย่างเช่น Web Applications Firewall (WAF) หรือ Intrusion Prevention System (IPS) เพื่อเสริมสร้างความปลอดภัยให้กับระบบ Web Server แต่ในระบบที่เฝ้าระวังขนาดเล็กนั้น การจัดซื้อ WAF เพื่อนำมาใช้เฝ้าระวังในระบบจึงไม่สัมพันธ์กับงบประมาณ เนื่องจากการลงทุนเพื่อจัดซื้ออุปกรณ์ Security นั้น มีมูลค่าสูง เมื่อเทียบกับองค์กรขนาดเล็ก จึงเป็นเหตุให้ไม่สามารถจัดสรรงบประมาณที่เพียงพอ จนสามารถจัดตั้งหน่วยงาน Security ได้

1.2 แนวทางในการแก้ไขปัญหา

จากปัญหาที่กล่าวมาข้างต้น และความเสียหายที่อาจจะเกิดขึ้นจากการเฝ้าระวังที่ไม่เพียงพอ ทำให้เกิดแรงจูงใจในการหาทางนำเสนอรูปแบบการเฝ้าระวังเหตุการณ์การบุกรุกจาก Hacker และภัยคุกคามทางไซเบอร์ โดยการเก็บ Log ของ Web Server มาวิเคราะห์ผ่าน AlienVault SIEM และกำหนดเงื่อนไข (Use Case) ในการ Monitor Web Server เพื่อป้องกันความเสียหายที่อาจ จะเกิดขึ้น ซึ่งสามารถจำแนกเป็นหมวดหมู่ ดังนี้.

หมวดที่ 1 การเข้าถึงและการพิสูจน์ตัวตน (Access and Authentication)

หมวดที่ 2 การปฏิบัติการ/การให้บริการ (Service Monitoring)

หมวดที่ 3 การเปลี่ยนแปลงการตั้งค่า (Configuration Change)

หมวดที่ 4 พฤติกรรมการใช้งานที่ผิดปกติ (Abnormal Traffic)

หมวดที่ 5 การโจมตีที่รู้จัก (Known Threat)

1.3 วัตถุประสงค์

1.3.1 เพื่อลดค่าใช้จ่ายในการลงทุนการเฝ้าระวังความปลอดภัยของระบบจากผู้ไม่ประสงค์ดี

1.4. ขั้นตอนการดำเนินงาน

1.4.1 ติดตั้งระบบ Web Server: Word Press (Implement Web Server)

1.4.2. ติดตั้งระบบไฟร์วอล Fortinet (Implement Firewall)

1.4.3. ติดตั้งระบบ AlienVault SIEM (Implement AlienVault OSSIM)

1.4.4. ติดตั้งระบบตรวจจับภัยคุกคาม Snort (Implement Snort)

1.4.5. Design Threat Modelling เพื่อทำ Use Case

1.4.6. Config Use Case, Dashboard Alert บน AlienVault OSSIM

1.5 ขอบเขตของโครงงาน

1.5.1 ระบบสามารถตรวจสอบภัยคุกคามที่เกิดขึ้นบน Web Server ได้

1.5.2 ระบบสามารถแสดงผลการตรวจสอบเพื่อใช้ในการวิเคราะห์ได้

1.5.3 ระบบสามารถทำรายงานผลเพื่อใช้วัดผลได้

บทที่ 2

พื้นฐานและทฤษฎีที่เกี่ยวข้อง

2.1 Security Operations Center: SOC

Security Operations Center (SOC) คืออะไร

Security Operations Center คือ ศูนย์การรักษาความปลอดภัย หรือ SOC ทำหน้าที่คล้ายสำนักงานใหญ่ด้านความปลอดภัยในเครือข่าย ที่เป็นศูนย์รวมของทั้งหน่วยงานจริงและ ในรูปแบบเสมือนที่ใช้ในการทดสอบระบบ เพื่อเอื้อในการตอบสนองปัญหาด้านความปลอดภัย และเหตุการณ์ฉุกเฉินที่อาจจะเกิดขึ้นได้อย่างไม่คาดคิด ซึ่งโมเดลลักษณะนี้ถูกใช้กันโดยกว้างขวาง ในชื่อ IDR ที่จะสามารถจำลอง และจัดการความปลอดภัยได้ในขั้นสูงเลยทีเดียว โดยศูนย์รักษาความปลอดภัยในรูปแบบนี้ อาจจะแตกต่างจากที่เคยคิด หรือจินตนาการเหมือนในภาพยนตร์สงคราม ที่ต้องนั่งประชุมกันในห้องมืดและมีการวางแผนอย่างซับซ้อน แต่ถึงจะแตกต่างกันเพียงไร เป้าหมายยังคงเหมือนกัน คือ การป้องกันภัยคุกคามและบริหารความเสี่ยงที่จะเข้ามา

ใครคือคนที่ต้องการ Security Operations Center (SOC)

ไม่ว่าองค์กรนั้นจะมีขนาดเล็กหรือขนาดใหญ่ ก็ล้วนต้องการความปลอดภัยทั้งนั้น ในบางองค์กรอาจมีทีมเฉพาะด้าน ในตรวจสอบและดูแลความปลอดภัยอยู่แล้ว อย่างไรก็ตามเหตุการณ์ด้านความปลอดภัยนี้อาจจะเกิดขึ้นได้ตลอดเวลา ซึ่งบางครั้งทีมงานความปลอดภัยขององค์กร อาจจะ ไม่สามารถดูแลได้ตลอดเวลา อีกทั้งยังมีความซับซ้อนในระดับสูงอีกด้วย

แต่ไม่ว่าปัญหาที่เกิดขึ้นจะมีความซับซ้อนเพียงใด SOC จะสามารถช่วยทีมงานความปลอดภัยขององค์กร เพื่อดูแลและบริหารจัดการข้อมูล สร้างความปลอดภัยขององค์กรได้ดียิ่งขึ้น นอกจากนั้น SOC ยังเป็นศูนย์กลางเชิงยุทธศาสตร์ เพื่อให้ทีมงานทราบถึงสิ่งที่ใหญ่กว่า และแนวโน้มด้านความปลอดภัยในระยะยาวอีกด้วย

สำหรับศูนย์ความปลอดภัยทั่วไปแล้ว จะทำหน้าที่แจ้งเตือนข่าวสารด้านความปลอดภัย ตรวจสอบภัยคุกคามที่จะเข้ามา ซึ่งสามารถสร้างความปลอดภัยได้ในระดับหนึ่ง แต่ SOC สามารถทำงานได้เหนือกว่าไปอีกขั้นในการตรวจสอบรายงานเหล่านั้นว่าผิดพลาดหรือไม่ เพราะบางครั้ง สิ่งเหล่านั้นอาจจะไม่ใช่ภัยคุกคาม และหากการทำงานของ SOC มีประสิทธิภาพสูง ก็สามารถตอบสนองและเหมาะสมเป็นอย่างมากในการกู้คืนและดูแลข้อมูลของเจ้าหน้าที่ในองค์กร

SOC ถือเป็นการรวมตัวของระบบที่มีประสิทธิภาพสูงในการรักษาความปลอดภัย ด้านเครือข่ายขององค์กร ที่มีการทำงานที่ซับซ้อน เหมาะกับการทำงานที่มีเครือข่ายที่ต้องใช้งาน ซึ่งด้วยเหตุนี้เองทำให้ SOC เหมาะกับงานใช้งานในเครือข่ายขององค์กรมากกว่าการใช้ภายในบ้าน

การวางรากฐานองค์กรให้พร้อมสำหรับ Security Operations Center (SOC)

ระบบความปลอดภัยที่ดีจะต้องมาจากรากฐานที่มั่นคงด้วยเช่นเดียวกัน ซึ่งองค์กรเองต้องวางรากฐานไว้ให้มั่นคงก่อนที่จะใช้ SOC อย่างมีประสิทธิภาพ 3 ประการ

ประการแรกคือ “การมีโปรแกรมจัดการเบื้องต้นที่ดี” ซึ่งในส่วนนี้รวมถึงการมีเทคโนโลยี ในการป้องกันภัยคุกคามต่าง ๆ รวมถึงระบบการแสกนหาช่องโหว่อย่างสม่ำเสมอและ สามารถเชื่อมโยงกับส่วนอื่น ๆ ได้อีกด้วย

ประการที่สองคือ “แผนตอบสนองต่อเหตุการณ์ที่เกิดขึ้น” การวางแผนการรับมือ ที่มีประสิทธิภาพ โดยมีเป้าหมายที่ชัดเจนจะใช้ให้ SOC ในโปรแกรม IDR เพิ่มประสิทธิภาพ ในการตรวจจับภัยคุกคาม และตอบสนองปัญหาที่จะมาทำลายระบบเครือข่ายได้เป็นอย่างดี

ประการที่สามคือ “ขั้นตอนการกู้คืนอย่างเป็นระบบ” ซึ่งเมื่อเกิดภัยคุกคามจนสร้างความเสียหายให้กับข้อมูลแล้ว จะสามารถมีแผนรับมือที่ดี ซึ่งแผนที่ดีจะทำให้องค์กรสามารถกู้ข้อมูล และดำเนินงานได้ตามปกติ โดยไม่ส่งผลกระทบต่องานและองค์กร

การเริ่มสร้าง SOC อย่างมีประสิทธิภาพ

ก่อนที่จะเริ่มมี SOC ที่มีประสิทธิภาพนั้น องค์กรควรจะพิจารณาถึงความซับซ้อนของระบบความปลอดภัย ซึ่งอาจจะมีการจ้างหน่วยงานภายนอก หรือดำเนินการด้วยตัวเองนั้น มีองค์ประกอบ 3 ส่วนดังนี้

People: หัวใจสำคัญหลักในการสร้าง SOC ที่ดี ซึ่งความเข้าใจในระบบของผู้ใช้งานไม่ว่าจะเป็นการตรวจสอบและการวิเคราะห์ SOC จะต้องมีพื้นฐานด้านความปลอดภัยในเทคโนโลยีเครือข่ายเสียก่อน โดยหากมีผู้ชำนาญการในองค์กรอยู่แล้วก็ไม่ใช่ปัญหา แต่ประสิทธิภาพจะเกิดขึ้นได้ก็ต่อเมื่อในแต่ละระบบจะต้องมีการแบ่งหน้าที่การดูแลได้อย่างลงตัว รู้หน้าที่ของตัวเองว่ารับผิดชอบระบบไหนส่วนไหน ทีมวิเคราะห์เมื่อพบข้อผิดพลาด จะต้องแจ้งเตือนให้ทีมแก้ไขได้อย่างรวดเร็ว ในทางเดียวกันทีมแก้ไขจะต้องอุดช่องโหว่ให้ได้อย่างรวดเร็วเช่นเดียวกันเมื่อได้รับแจ้ง ซึ่งปัญหาที่

พบได้มากที่สุดในองค์กรก็คือ ความชัดเจนและลำดับในการทำงาน จึงทำให้เกิดช่องโหว่ขึ้นกับระบบความปลอดภัย ง่ายต่อการเข้าถึงได้ของภัยคุกคาม

Processes: ในส่วนของกระบวนการ คือการสร้างขั้นตอนระหว่างบุคคลและเทคโนโลยี ที่เคยได้กล่าวกันไปแล้ว ซึ่งเมื่อหากเริ่มใช้ SOC คือการเริ่มต้นทำความเข้าใจรายงานความปลอดภัย การอ่านค่าต่างๆ เพื่อให้มีความเข้าใจในการรวบรวมและวิเคราะห์เมตทริกซ์ได้ กระบวนการเหล่านี้จะต้องมีความแม่นยำเพียงพอที่จะทำให้แน่ใจได้ว่ามีการจัดการนำไปสู่การหาต้นตอ (Root Cause) และแก้ปัญหาได้อย่างตรงจุด หากทำงานโดยไร้ขั้นตอน ก็จะยิ่งทำลายประสิทธิภาพของ SOC ลงไปได้ โดยประเด็นทั้งหมดคือ การทำความเข้าใจเกี่ยวกับหัวใจของการรักษาความปลอดภัยในเครือข่าย ซึ่งการประสานงานของทั้ง 3 ปัจจัยจะสร้างประสิทธิภาพสูงสุดของ SOC ตั้งแต่การเริ่มต้นใช้งาน

Technology: SOC คือส่วนหนึ่งของความปลอดภัยทางเทคโนโลยี ในการตัดสินใจว่าอะไร ที่เหมาะกับ SOC การประสานงานระหว่าง บุคลากรและเทคโนโลยี คือส่วนสำคัญการวิเคราะห์พฤติกรรมของผู้ใช้ การตรวจสอบการทำงานอย่าง Real Time และการหมั่นอัปเดตเทคโนโลยีใหม่อยู่เสมอ เพื่อใช้ปรับปรุงกระบวนการทำงานให้ต่อเนื่อง

2.2 Web Server: WordPress

Web Server คือ Server ที่ให้บริการแจกจ่ายข้อมูลแก่ Client โดยอาศัยการทำงานแบบ HTTP (Hypertext Transfer Protocol) เป็น Protocol เบื้องต้น ที่ทำงานบน Transmission Control Protocol (TCP) ที่ใช้ในการจัดรูปแบบ การรับส่ง การเชื่อมโยงเอกสาร และสื่อผสมต่าง ๆ เช่นรูปภาพ ข้อความ รวมไปถึงภาพเคลื่อนไหว และข้อมูลเสียง ซึ่งเป็นการบริการพื้นฐานของ World Wide Web (www) มีการทำงานที่มีทั้งฝั่ง server จัดเตรียม และส่งข้อมูลต่างๆ ที่มีการร้องขอ จากทางฝั่ง Client โดยใช้ Web Browser ในการร้องขอข้อมูล จากฝั่ง Server เพื่อนำมาแสดงผลให้กับผู้ใช้งาน โดยปกติแล้ว Apache Web Server ทำงานที่ Port 80 สำหรับ HTTP และ Port 443 สำหรับ HTTPS

2.3 Security information and event management (SIEM)

ซอฟต์แวร์ด้านข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (SIEM) นั้น ได้ถูกนำไปใช้ ในรูปแบบต่าง ๆ นานกว่าทศวรรษ และมีการพัฒนาอย่างมีนัยสำคัญในช่วงเวลานั้น การใช้งาน SIEM ให้มุมมองแบบองค์รวมของสิ่งที่เกิดขึ้นบนเครือข่ายแบบเรียลไทม์ และช่วยให้ทีมงานด้านไอทีมีความพร้อมในเชิงรุกมากขึ้น ในการต่อสู้กับภัยคุกคามความปลอดภัย

สิ่งที่ไม่เหมือนใครเกี่ยวกับการใช้งาน SIEM คือการรวมการจัดการทางด้านความปลอดภัยของเหตุการณ์ ซึ่งดำเนินการวิเคราะห์เหตุการณ์ และบันทึกข้อมูลแบบเรียลไทม์ เพื่อใช้ความสัมพันธ์ของเหตุการณ์ในการตรวจจับการคุกคาม การตอบสนองเหตุการณ์ นำมาวิเคราะห์ข้อมูลและสร้างรายงาน สำหรับองค์กรที่ต้องการการมองเห็นที่สมบูรณ์ และการควบคุมสิ่งที่เกิดขึ้น บนเครือข่ายในแบบเรียลไทม์การใช้งาน SIEM นั้น มีความสำคัญ

2.4 Threat Modeling

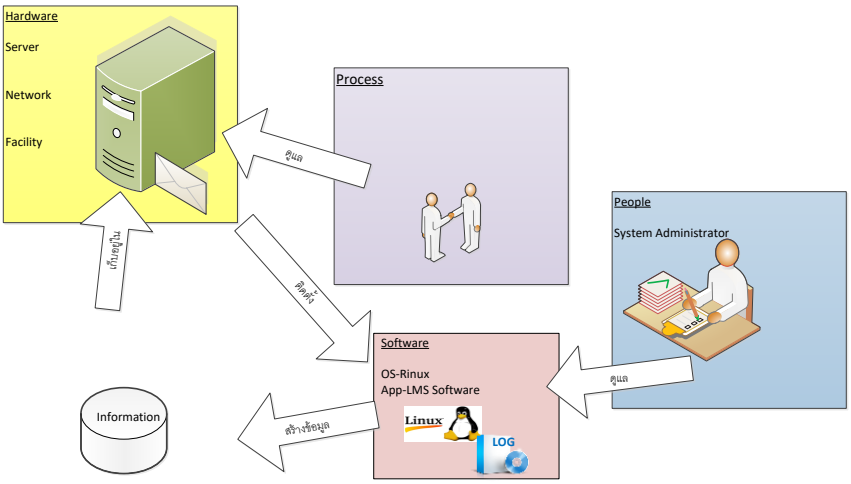
การสร้างแบบจำลองภัยคุกคาม เป็นกระบวนการที่จำลองเหตุภัยคุกคามที่อาจเกิดขึ้น เช่น ช่องโหว่เชิงโครงสร้าง สามารถถูกพบและประเมินความสำคัญได้ โดยใช้สมมติฐานจากมุมมองของผู้โจมตี จุดประสงค์ของการสร้างแบบจำลองภัยคุกคาม คือเพื่อให้การวิเคราะห์อย่างเป็นระบบเกี่ยวกับรูปแบบของผู้โจมตี ที่น่าจะเป็นไปได้ เพื่อคาดการณ์รูปแบบของการโจมตีที่เป็นไปได้ มากที่สุด และสินทรัพย์ที่ผู้โจมตีต้องการมากที่สุด การสร้างแบบจำลองภัยคุกคามตอบคำถาม เช่น “สินทรัพย์ที่มีมูลค่าสูงอยู่ที่ไหนในระบบ”,“ จุดที่เสี่ยงที่สุดในการถูกโจมตีคืออะไร?”, “ภัยคุกคามที่เป็นไปได้มากที่สุดคืออะไร” และ “มีรูปแบบการโจมตีอื่นอีกหรือไม่ที่ยังนึกไม่ถึง?” โดยทั่วไปแล้ว คนส่วนใหญ่มีการสร้างแบบจำลองภัยคุกคามบางรูปแบบในชีวิตประจำวันโดยไม่รู้ตัว บางคนใช้แบบจำลองภัยคุกคาม เพื่อพิจารณาสิ่งที่อาจผิดพลาด ในระหว่างการขับรถตอนเช้า ไปทำงานเพื่อหลีกเลี่ยงอุบัติเหตุที่อาจเกิดขึ้น ลองมองย้อนไปมากกว่านั้น การสร้างแบบจำลอง การคุกคามถูกเพื่อจัดลำดับความสำคัญของการเตรียมป้องกันทางทหารตั้งแต่สมัยโบราณอีกด้วย

2.4 Asset

ทรัพย์สิน(Asset) หมายความว่า รายการทรัพย์สินที่อยู่ภายใต้ขอบเขตของการขอรับรองมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ซึ่งแบ่งได้ 8 ประเภท คือ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และสารสนเทศ บุคลากร อุปกรณ์สนับสนุนการทำงาน กระบวนการสำคัญ อุปกรณ์เครือข่าย และหน่วยงานที่เกี่ยวข้อง

2.4.1 วิธีการรวบรวมรายการทรัพย์สิน

การรวบรวมรายการทรัพย์สิน ทีมงานผู้เกี่ยวข้องจะต้องดำเนินการเก็บรวบรวมรายการทรัพย์สิน ที่หน่วยงานมีหน้าที่รับผิดชอบ โดยอาจใช้เทคนิคการวาดภาพประกอบการรวบรวมรายการทรัพย์สิน



รูปที่ 1 แผนภาพเทคนิคการรวบรวมทรัพย์สิน

ประเภทของทรัพย์สินสามารถแบ่งได้ 8 ประเภท คือ (1) ฮาร์ดแวร์ (2) ซอฟต์แวร์ (3) ข้อมูลและสารสนเทศ (4) บุคลากร (5) อุปกรณ์สนับสนุนการทำงาน (6) กระบวนการสำคัญ (7) อุปกรณ์เครือข่าย (8) หน่วยงานที่เกี่ยวข้อง รายละเอียดประเภททรัพย์สิน ความหมายและตัวอย่างทรัพย์สินในตารางที่ 1

ตารางที่ 1 ประเภททรัพย์สิน ความหมายและตัวอย่างทรัพย์สิน

ลำดับ	ประเภททรัพย์สิน	หมายถึง	ตัวอย่างทรัพย์สิน
1	ฮาร์ดแวร์ (Hardware)	■ เครื่องคอมพิวเตอร์ ■ อุปกรณ์ต่อพ่วงที่ทำงานร่วมกับคอมพิวเตอร์	■ เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ ■ เครื่องคอมพิวเตอร์ไคลเอนท์
2	ซอฟต์แวร์ (Software)	■ ระบบปฏิบัติการ ■ โปรแกรมอัตถประโยชน์ ■ โปรแกรมตรวจสอบวิเคราะห์และป้องกันระบบ	■ OS Linux/Unix
3	อุปกรณ์สนับสนุนการทำงาน (Facility)	■ อุปกรณ์สนับสนุนการทำงาน ได้แก่ ระบบไฟฟ้า, ประปา	■ ระบบสนับสนุนต่าง ๆ

ลำดับ	ประเภททรัพย์สิน	หมายถึง	ตัวอย่างทรัพย์สิน
4	ข้อมูลและสารสนเทศ (Data and Information)	■ ข้อมูลรูปแบบสำเนาถาวร ■ ข้อมูลรูปแบบอิเล็กทรอนิกส์ ■ เอกสารสำเนาถาวร ■ เอกสารอิเล็กทรอนิกส์	■ ผังเครือข่ายคอมพิวเตอร์ ■ ไฟล์ฐานข้อมูล ■ เอกสารฟอร์มขั้นตอนการปฏิบัติ ■ ไฟล์ขั้นตอนการปฏิบัติ
5	บุคลากร (Personnel)	■ บุคลากรตามตำแหน่งหรือความรับผิดชอบ ทั้งที่เป็นบุคลากรภายในและภายนอกที่เข้ามาปฏิบัติงานประจำ	■ ผู้ดูแลระบบคอมพิวเตอร์
6	กระบวนการสำคัญ (Process)	■ งานที่ต้องปฏิบัติเป็นประจำ ■ งานที่ต้องรับผิดชอบ	■ กระบวนการสำรองข้อมูล ■ กระบวนการติดตามตรวจสอบระบบ
7	อุปกรณ์เครือข่าย (Network)	■ อุปกรณ์เครือข่ายคอมพิวเตอร์	■ สวิทช์ เราท์เตอร์ ไฟร์วอลล์
8	หน่วยงานที่เกี่ยวข้อง (Organization)	■ หน่วยงานที่เกี่ยวข้องกับห้องเดต้าเซ็นเตอร์ทั้งหน่วยงานภายนอกและหน่วยงานภายใน	■ Vendor

2.4.2 วิธีการประเมินความสำคัญของทรัพย์สิน

หลังจากรวบรวมรายการทรัพย์สินแล้ว ให้พิจารณาจัดกลุ่มรายการทรัพย์สินที่มีลักษณะการทำงานหรือการใช้งานคล้ายกัน สัมพันธ์กัน แล้วกำหนดชื่อกลุ่มรายการทรัพย์สินนั้นๆ ใช้เป็นตัวแทนทรัพย์สินในการประเมินความเสี่ยง โดยการประเมินความเสี่ยง จะเริ่มจากการประเมินความสำคัญของทรัพย์สิน ซึ่งจะดำเนินการประเมินว่า กลุ่มทรัพย์สินมีความสำคัญด้านใดบ้างในความสำคัญ 4 ด้าน อันได้แก่ ด้านความลับ ความถูกต้อง ความพร้อมใช้ กฎหมายและกฎระเบียบ ที่เกี่ยวข้อง เพื่อจะสามารถนำไปใช้ประเมินหาภัยคุกคาม ที่ทำให้เกิดผลกระทบต่อด้านความลับ ความถูกต้อง ความพร้อมใช้ หรือกฎหมายและกฎระเบียบที่เกี่ยวข้อง

ตารางที่ 2 การประเมินความสำคัญด้านความมั่นคงปลอดภัยสารสนเทศของทรัพย์สิน

ความสำคัญด้านความมั่นคงปลอดภัยสารสนเทศของทรัพย์สิน		
C	Confidentiality	การรักษาความลับ เพื่อไม่ให้ข้อมูลลับหรือที่สำคัญถูกเปิดเผยโดยมิชอบหรือโดย ไม่ได้รับอนุญาต
I	Integrity	การรักษาความถูกต้องครบถ้วนเพื่อไม่ให้ข้อมูลถูกแก้ไขเปลี่ยนแปลงโดยมิชอบ หรือโดยไม่ได้รับอนุญาต
A	Availability	การรักษาสภาพความพร้อมใช้ เพื่อให้ผู้มีสิทธิสามารถใช้งานได้เมื่อต้องการ
L	Compliance	การรักษากฎหมายและระเบียบที่เกี่ยวข้อง เพื่อให้การดำเนินงานสอดคล้องกับ กฎหมายและระเบียบที่เกี่ยวข้อง

2.5 Vulnerability

ช่องโหว่(Vulnerability) หมายความว่า จุดอ่อนของทรัพย์สิน หรือกลุ่มของทรัพย์สินที่สามารถนำมาเป็นประโยชน์ต่อภัยคุกคาม

2.5.1 วิธีประเมินช่องโหว่

การประเมินช่องโหว่จะดำเนินการต่อจากการประเมินภัยคุกคาม โดยคำว่า “ช่องโหว่” หมายความว่า “จุดอ่อนของทรัพย์สินหรือกลุ่มของทรัพย์สิน ซึ่งสามารถนำไปใช้เป็นประโยชน์ได้โดยภัยคุกคาม” หรือกล่าวได้อีกอย่างว่า ช่องโหว่คือจุดอ่อนของทรัพย์สินที่เป็นประโยชน์ต่อภัยคุกคาม ทั้งนี้ ช่องโหว่สามารถจำแนกได้ 3 ประเภท ดังนี้

ช่องโหว่ที่เกิดจากการบริหาร (Administrative Vulnerability) หมายถึง จุดอ่อนที่เกิดจากการบริหารจัดการ การควบคุมดูแล หรือการขาดความเข้าใจ เช่น ขาดการควบคุมการเปลี่ยนแปลง ที่มีประสิทธิผล ขาดการบำรุงดูแลรักษาอุปกรณ์ที่ได้ประสิทธิผล ขาดการทดสอบซอฟต์แวร์ที่เพียงพอ ไม่มีการควบคุมการทำสำเนา เป็นต้น

ช่องโหว่ที่เกิดจากเทคนิค (Technical Vulnerability) หมายถึง จุดอ่อนที่เกิดขึ้นทางเทคนิค ซึ่งอาจมาจากการตั้งค่าการทำงาน การไม่ได้บังคับใช้มาตรการควบคุมที่มีอยู่บนระบบ หรือบนอุปกรณ์ป้องกัน เช่น การตั้งค่าพารามิเตอร์ผิด การกำหนดสิทธิการเข้าถึงผิดพลาด ซอฟต์แวร์

มีข้อบกพร่องที่ได้รับการเปิดเผย ขาดความสามารถในการจัดเก็บหลักฐานการตรวจสอบที่เพียงพอ เป็นต้น

ช่องโหว่ที่เกิดจากคุณลักษณะทางกายภาพ หรือสิ่งแวดล้อม (Physical and Environmental Vulnerability) หมายถึง จุดอ่อนที่เกิดขึ้นจากคุณลักษณะทางกายภาพ หรือสิ่งแวดล้อมของทรัพย์สินนั้นเอง เช่น ความไว้ต่อความชื้น ฝุ่นหรือสิ่งสกปรก ความไวต่อคลื่นแม่เหล็กไฟฟ้า ความไวต่อแรงดันไฟฟ้าที่ผันผวน ขาดการป้องกันทางกายภาพสำหรับอาคาร ประตู และหน้าต่าง เป็นต้น

2.6 Risk

ภัยคุกคาม(Risk) หมายความว่า สาเหตุที่อาจเกิดขึ้น หรือก่อให้เกิดเหตุอันไม่พึงประสงค์ และเป็นอันตรายต่อทรัพย์สิน หรือสร้างความเสียหายต่อองค์กร

การประเมินภัยคุกคามจะกระทำภายหลังจากที่ได้ทำการประเมินความสำคัญของทรัพย์สินเสร็จสิ้น โดยคำว่า “ภัยคุกคาม” หมายความว่า “ปัจจัยของอุบัติการณ์ที่ไม่พึงประสงค์ที่มีศักยภาพ ซึ่งผลลัพธ์อาจสร้างความเสียหายต่อระบบหรือองค์กร” และอาจจำแนกลักษณะของภัยคุกคามได้ 4 ลักษณะ คือ (1) ภัยคุกคามที่เกิดจากสิ่งแวดล้อม (2) ภัยคุกคามที่เกิดจากธรรมชาติ (3) ภัยคุกคามที่เกิดความตั้งใจของมนุษย์ และ (4) ภัยคุกคามที่เกิดจากอุบัติเหตุ ดังมีตัวอย่างแสดงในตารางที่ 3

ทั้งนี้ การประเมินภัยคุกคามจะใช้ชื่อภัยคุกคามที่มีลักษณะเป็นกลาง ไม่จำเพาะเจาะจง โดยมีหลักว่าหากลักษณะภัยคุกคามเหมือนกัน คล้ายกัน มีรูปแบบในทำนองเดียวกันก็จัดให้เป็นภัยคุกคามเดียวกัน ตัวอย่างเช่น ภัยคุกคามที่เกิดจาก (1) พนักงานที่ไม่มีสิทธิเข้าถึงข้อมูล (2) แฮกเกอร์ และ (3) ลูกค้าเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต จะพบว่าต่างมีลักษณะเหมือนกันคือ การเข้าถึงนั้นไม่มีสิทธิ ดังนั้น จึงอาจเรียกภัยคุกคามนี้ว่า ผู้ไม่มีสิทธิเข้าถึงทรัพย์สิน เป็นต้น

ตารางที่ 3 ตัวอย่างภัยคุกคาม

ลำดับที่	ประเภท	หมวดทรัพย์สิน	ภัยคุกคาม	ช่องโหว่	มาตรการจัดการความเสี่ยงที่มีอยู่ในปัจจุบัน	ปัจจัยที่มีผลกระทบ			
ID No.	Type	Asset	Threat	Vulnerability	Existing Controls	C	I	A	L
1	Hardware	กลุ่ม server ที่ DC	ผู้ไม่มีสิทธิรบกวนการทำงานอุปกรณ์	การบริหารจัดการสิทธิ์ไม่มีประสิทธิผล	มีการกำหนดสิทธิ์	C	I	A	L
2	Hardware	กลุ่ม server ที่ DC	ผู้ไม่มีสิทธิรบกวนการทำงานอุปกรณ์	การควบคุมความมั่นคงปลอดภัยของสถานที่ไม่มีประสิทธิผล	DC มีการควบคุมตามมาตรฐาน ISO 27001	C	I	A	L
3	Hardware	กลุ่ม server ที่ DC	อุปกรณ์ล้มเหลวหรือไม่พร้อมให้บริการ	การบำรุงรักษาอุปกรณ์ไม่มีประสิทธิผล	มีการทำ MA สำหรับอุปกรณ์ทุกตัว	-	I	A	L
4	Hardware	กลุ่ม server ที่ DC	อุปกรณ์ล้มเหลวหรือไม่พร้อมให้บริการ	การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไม่มีประสิทธิผล	มีการจัดทำเอกสารที่เป็น flow การทำงานอยู่แล้วในปัจจุบัน แต่ไม่มีขั้นตอนการเก็บหลักฐานไม่ชัดเจน	-	I	A	L
5	Hardware	กลุ่ม server ที่ DR	ผู้ไม่มีสิทธิรบกวนการทำงานอุปกรณ์	การบริหารจัดการสิทธิ์ไม่มีประสิทธิผล	มีการกำหนดสิทธิ์	C	I	A	L
6	Hardware	กลุ่ม server ที่ DR	ผู้ไม่มีสิทธิรบกวนการทำงานอุปกรณ์	การควบคุมความมั่นคงปลอดภัยของสถานที่ไม่มีประสิทธิผล	มีการควบคุมโดยใช้ Access Control	C	I	A	L
7	Hardware	กลุ่ม server ที่ DR	อุปกรณ์ล้มเหลวหรือไม่พร้อมให้บริการ	การบำรุงรักษาอุปกรณ์ไม่มีประสิทธิผล	มีการทำ MA สำหรับอุปกรณ์ทุกตัว	-	I	A	L
8	Hardware	กลุ่ม server ที่ DR	อุปกรณ์ล้มเหลวหรือไม่พร้อมให้บริการ	การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไม่มีประสิทธิผล	มีการจัดทำเอกสารที่เป็น flow การทำงานอยู่แล้วในปัจจุบัน แต่ไม่มีขั้นตอนการเก็บหลักฐานไม่ชัดเจน	-	I	A	L

2.6.1 วิธีการประเมินผลกระทบความมั่นคงปลอดภัยสารสนเทศ

การประเมินผลกระทบความมั่นคงปลอดภัยสารสนเทศที่จะเกิดขึ้นกับทรัพย์สิน โดยต้องพิจารณามาตรการควบคุมที่มีปัจจุบันประกอบ ว่ามาตรการดังกล่าวสามารถลดความเสียหาย หรือผลกระทบที่เกิดขึ้นจากภัยคุกคาม และช่องโหว่ได้หรือไม่ หรือมาตรการดังกล่าวสามารถลดโอกาสเกิดเหตุการณ์ความเสี่ยงที่ได้ระบุไว้หรือไม่

สำหรับเกณฑ์ผลกระทบความมั่นคงปลอดภัยสารสนเทศพิจารณาได้ 2 ด้าน คือ ผลกระทบต่อการดำเนินงาน และผลกระทบต่อลูกค้าหรือผู้ใช้บริการ

ตารางที่ 4 การประเมินผลกระทบความมั่นคงปลอดภัยสารสนเทศ

เกณฑ์ผลกระทบความมั่นคงปลอดภัยสารสนเทศ 2 ด้าน		
O	Operation	ผลกระทบต่อการดำเนินงาน
C	Customer	ผลกระทบต่อลูกค้า หรือผู้ใช้บริการ

ตารางที่ 5 เกณฑ์การประเมินระดับของผลกระทบต่อการดำเนินงาน (Operation: Impact1)

ระดับ	หลักเกณฑ์การวัดระดับผลกระทบ
3	• ต้องใช้เวลาในการแก้ไขมากกว่า 6 ชั่วโมง
2	• ต้องใช้เวลาในการแก้ไขมากกว่า 4 – 6 ชั่วโมง
1	• ต้องใช้เวลาในการแก้ไขน้อยกว่า หรือเท่ากับ 4 ชั่วโมง

ตารางที่ 6 เกณฑ์การประเมินระดับของผลกระทบต่อลูกค้าหรือผู้ใช้บริการ (Customer: Impact2)

ระดับ	หลักเกณฑ์การวัดระดับความเสียหาย
3	• มีผลกระทบต่อลูกค้า หรือผู้ใช้บริการจำนวนตั้งแต่ 5 รายขึ้นไป
2	• มีผลกระทบต่อลูกค้า หรือผู้ใช้บริการจำนวน 2-4 ราย
1	• มีผลกระทบต่อลูกค้า หรือผู้ใช้บริการจำนวน 0-1 ราย

ตารางที่ 7 การคำนวณระดับผลกระทบ

Operation Impact	Customer Impact		
	1	2	3
1	1	1	2
2	3	4	5
3	5	5	5

ตารางที่ 8 ระดับผลกระทบ

Impact Level	ระดับความเสียหายที่มีผลกระทบต่อธุรกิจหรือการให้บริการของระบบ		ผลกระทบเชิงปริมาณ
5	ผลกระทบสูงมาก	ส่งผลกระทบซึ่งอาจนำไปสู่ความเสี่ยงสูงมากที่จะทำให้ บริษัทฯ จะไม่สามารถปฏิบัติตาม SLA ที่ได้ทำกับลูกค้าได้ และมีผลกับลูกค้าจำนวนหลายราย	ค่าความเสียหาย > 10,000,000 บาท
4	ผลกระทบสูง	ส่งผลกระทบซึ่งอาจนำไปสู่ความเสี่ยงสูงที่จะทำให้ บริษัทฯ จะไม่สามารถปฏิบัติตาม SLA ที่ได้ทำกับลูกค้าได้ หรือมีผลกับลูกค้าจำนวนหลายราย	5,000,000 < ค่าความเสียหาย <= 10,000,000 บาท
3	ผลกระทบปานกลาง	ส่งผลกระทบในด้านคุณภาพการให้บริการ	1,000,000 < ค่าความเสียหาย <= 5,000,000 บาท

2	ผลกระทบต่ำ	ส่งผลกระทบต่อการดำเนินงานน้อย	50 < ค่าความเสียหาย <= 1,000,000 บาท
1	ผลกระทบต่ำมาก	ไม่ส่งผลกระทบต่อการดำเนินงาน	ไม่มีความเสียหาย หรือค่าความเสียหาย <= 50,000 บาท

ตารางที่ 9 ระดับโอกาสเกิดเหตุการณ์

Likelihood Level	ระดับโอกาสเกิดเหตุการณ์	
5	Weekly	มีโอกาสเกิดขึ้นบ่อยทุกสัปดาห์ (Frequently) (เกิดขึ้นบ่อย อย่างน้อย 52 ครั้งขึ้นไป)
4	Monthly	มีโอกาสเกิดขึ้นทุกเดือน (Likely) (เกิดขึ้นอย่างน้อย 12-51 ครั้ง ต่อปี)
3	Quarterly	มีโอกาสเกิดขึ้นทุกไตรมาส (Possibly) (เกิดขึ้นอย่างน้อย 4-11 ครั้ง ต่อปี)
2	Half-Yearly	มีโอกาสเกิดขึ้นทุกครึ่งปี (Unlikely) (เกิดขึ้นอย่างน้อย 2-3 ครั้ง ต่อปี)
1	Yearly	ปีละหนึ่งครั้ง/ไม่ค่อยได้เกิดขึ้นในรอบปี (Rarely) (อาจเกิดขึ้นได้ หรืออย่างน้อย 1 ครั้ง ต่อปี)
** ประเมิน "ระดับโอกาสเกิดเหตุการณ์" ตามปัจจัยเสี่ยง (ภัยคุกคามและช่องโหว่) ที่มีต่อทรัพย์สินสารสนเทศ		

2.6.2 วิธีการคำนวณระดับความเสี่ยง

เมื่อดำเนินการประเมินระดับผลกระทบ และระดับโอกาสเกิดเหตุการณ์ได้แล้ว ข้อมูลดังกล่าวจะถูกนำมาใช้ในการคำนวณระดับความเสี่ยง ทั้งนี้ การคำนวณจะใช้ข้อมูล 2 ด้าน คือ (1) ระดับผลกระทบ และ (2) โอกาสเกิดเหตุการณ์ ซึ่งสามารถอธิบายความสัมพันธ์ดังสมการ (1.2)

ระดับความเสี่ยง = ระดับผลกระทบ x ระดับโอกาสเกิดเหตุการณ์ ... (1.2)

ระดับความเสี่ยงเมื่อนำมาคำนวณอาจใช้ตารางแผนที่ความเสี่ยง (Risk map) เพื่อช่วยในการระบุตำแหน่งความเสี่ยง

ตารางที่ 10 แผนที่ความเสี่ยง (Risk map)

Risk Level			Likelihood Level				
			1	2	3	4	5
			Yearly	Half-Yearly	Quarterly	Monthly	Weekly
Impact Level	Very High	5	M5	H10	E15	E20	E25
	High	4	L4	H8	E12	E16	E20
	Medium	3	L3	M6	H9	E12	E15
	Low	2	L2	L4	M6	H8	H10
	Very Low	1	L1	L2	L3	L4	L5

การเลือกแนวทางตอบสนองความเสี่ยงเป็นขั้นตอนระยะสุดท้ายในการประเมินความเสี่ยง ซึ่งเกี่ยวข้องกับการพิจารณาว่าความเสี่ยงที่วิเคราะห์ได้อยู่ในระดับที่ยอมรับได้หรือไม่ และหากยอมรับไม่ได้ก็ต้องเลือกแนวทางในการควบคุมความเสี่ยง

แนวทางการตอบสนองต่อความเสี่ยงแบ่งเป็น 2 แนวทาง ซึ่งสัมพันธ์กับระดับความเสี่ยง ดังนี้

ตารางที่ 11 โดยแนวทางการตอบสนองต่อความเสี่ยง

Risk Rating Level	ระดับความเสี่ยง (Level)	เกณฑ์การยอมรับความเสี่ยง	เกณฑ์การตอบสนองต่อสภาพปัจจัยความเสี่ยง
Extremely	ระดับความเสี่ยงสูงมาก	ควบคุมความเสี่ยง	ควบคุมความเสี่ยง โดยเลือกมาตรการควบคุมความเสี่ยงที่เหมาะสม และจัดทำแผนจัดการความเสี่ยง เพื่อดำเนินการโดยทันที
High	ระดับความเสี่ยงสูง		ควบคุมความเสี่ยง โดยเลือกมาตรการควบคุมความเสี่ยงที่เหมาะสม และจัดทำแผนจัดการความเสี่ยง เพื่อดำเนินการโดยเร็ว
Moderate	ระดับความเสี่ยงปานกลาง	ยอมรับความเสี่ยง	ยอมรับความเสี่ยง โดยควรมีการเฝ้าระวัง
Low	ระดับความเสี่ยงต่ำ		ยอมรับความเสี่ยง เนื่องจากเป็นความเสี่ยงที่เกิดขึ้นเป็นปกติในการดำเนินงาน

2.6.3 แนวทางการควบคุมความเสี่ยง (Risk Treatment Options)

การเลือกแนวทางตอบสนองความเสี่ยง เกี่ยวข้องกับการพิจารณาว่าความเสี่ยงที่วิเคราะห์ได้อยู่ในระดับที่ยอมรับได้หรือไม่ และหากยอมรับไม่ได้ก็ต้องเลือกแนวทางในการตอบสนองความเสี่ยง โดยแนวทางการควบคุมความเสี่ยงแบ่งเป็น 4 แนวทาง คือ

2.6.3.1 ยอมรับความเสี่ยง (Accepting) หมายความว่า เป็นความเสี่ยงที่ยอมรับให้เกิดขึ้น

2.6.3.2 ควบคุมความเสี่ยง (Controlling) หมายความว่า เป็นความเสี่ยงที่ต้องทำการควบคุม โดยการควบคุมอาจเลือกมาตรการควบคุมที่ระบุไว้ท้ายมาตรฐาน ISO27001

2.6.3.3 ถ่ายโอนความเสี่ยง (Transferring) หมายความว่า เป็นความเสี่ยงที่อาจต้องถ่ายโอนให้หน่วยงานอื่นรับความเสี่ยงนั้นไป ปกติการเลือกถ่ายโอนความเสี่ยงจะกระทำต่อเมื่อผลกระทบของ ความเสี่ยงสูงแต่โอกาสเกิดความเสี่ยงนั้นน้อย

2.6.3.4หลีกเลี่ยงความเสี่ยง (Avoiding) หมายความว่า เป็นความเสี่ยงที่จะต้องหลีกเลี่ยง ไม่ให้มีการกระทำหรือการปฏิบัติที่จะนำไปสู่ความเสี่ยง ปกติการเลือกหลีกเลี่ยงความเสี่ยงจะกระทำต่อเมื่อผลกระทบของความเสี่ยงสูง มีโอกาสเกิดเหตุการณ์สูง

2.6.4 วิธีการปฏิบัติการประมาณระดับความเสี่ยงที่เหลือ (Residual Risks)

หลังจากพิจารณาแนวทางการตอบสนองความเสี่ยง หากทางเลือกในการตอบสนองความเสี่ยงเป็นการ ควบคุม หรือยอมรับความเสี่ยง ทีมงานผู้เกี่ยวข้องต้องดำเนินการประมาณระดับความเสี่ยงที่เหลือ ด้วยการประมาณผลกระทบ และโอกาสเกิดที่คาดว่าเมื่อเลือกแนวทางตอบสนองความเสี่ยงแล้ว จะมีผลกระทบ และโอกาสเกิดของความเสี่ยงอย่างไร

2.7 Elastic Stack

คือชุดของซอฟต์แวร์ เพื่อใช้ในการทำ Centralized Log โดยประกอบด้วย 3ส่วนหลักๆ

2.7.1 Shipping เป็นส่วนที่ใช้ในการส่งLogจากต้นทางเข้าระบบเพื่อใช้ต่อไปในการประมวลผล

- Software ที่จัดการเรื่องนี้ Beat, Logstash

2.7.2 Distributed search and analytics เป็นส่วนที่ใช้ในการประมวลผล Logที่ผ่านการindexingแล้ว

- Software ที่จัดการเรื่องนี้ Elasticsearch

2.7.3 Interface and display เป็นส่วนที่ใช้ในการแสดงผล โดยดึงข้อมูลจากส่วนประมวลผลมาแสดง

- Software ที่จัดการเรื่องนี้ Kibana

รูปที่ 2 รูปแบบการทำงานของ Elastic Stack

บทที่ 3

การออกแบบ

3.1 ความต้องการของระบบ

3.1.1. ใช้ระบบปฏิบัติการ Centos version 7

3.1.2. ใช้ Elastic Stack

3.1.3. ใช้ WordPress

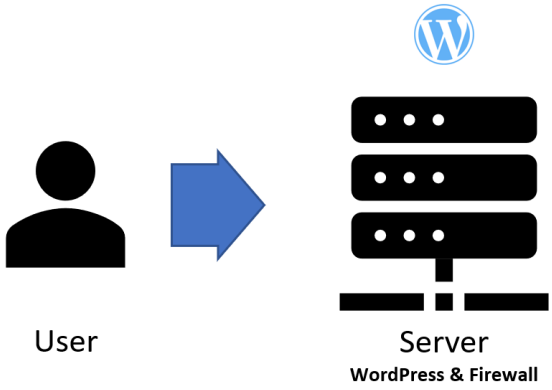
3.1.4. ใช้ Firewall iptables

3.2 ภาพรวมของระบบ

จากผู้ใช้งาน Web Page

ผู้ใช้งานสามารถเข้าถึงWeb Page โดยการเรียกURLเพื่อชี้เข้ามาผ่านFirewall ซึ่งมีFortinet ตรวจสอบ เมื่อคำร้องเข้าถึงส่วนWeb Server จะถูกตรวจสอบต่อด้วย Snort เพื่อดูว่ามีรูปแบบของคำร้องหรือมีลักษณะที่เกี่ยวข้องกับลักษณะจำเพาะของภัยคุกคามตามที่มีในข้อมูลหรือไม่ จากนั้นจึงเข้าถึงส่วนของSoftwareบริการ Web Pageเพื่อนำหน้า Web Page และข้อมูลไปแสดงตามคำร้องของผู้ใช้งาน

ซึ่งสามารถอธิบายการทำงานของระบบโดยรวมได้ดังรูปภาพ

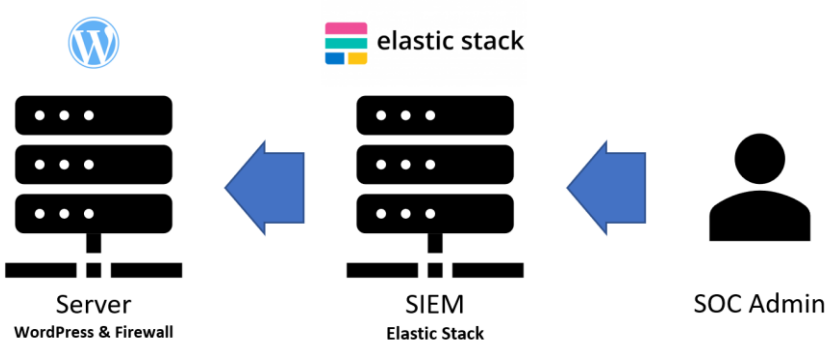


รูปที่ 3 ภาพรวมของระบบมุมมองผู้ใช้งานจากภายนอก

จากผู้ใช้ตรวจสอบระบบ

SIEMจะทำการเก็บlog จากServer, WordPress และ Snort มารวมแล้วทำการวิเคราะห์และแสดงผลโดยผู้ใช้งานสามารถเข้า consoleของ SIEM เพื่อดำเนินการตรวจสอบระบบได้

ซึ่งสามารถอธิบายการทำงานของระบบโดยรวมได้ดังรูปภาพ

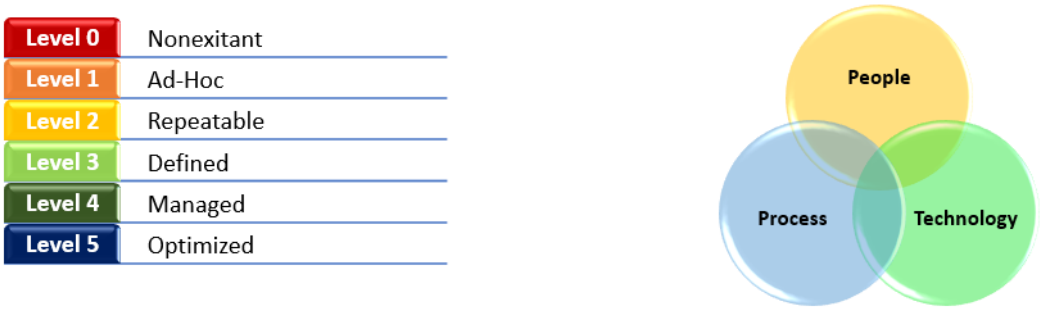


รูปที่ 4 ภาพรวมของระบบมุมมองผู้ใช้งานจากผู้ตรวจสอบ

3.3 SOC Maturity Model

การทำ Maturity Model คือการประเมินระดับความพร้อมใช้ของ SOCว่าอยู่ในระดับใด เหมาะสมกับความต้องการของระบบหรือไม่ ทำให้ผู้ประเมินสามารถทราบได้ว่าจำเป็นต้องมีการพัฒนาด้านใด ต้องมีการบริการSOCในรูปแบบใดบ้าง เพื่อที่จะพัฒนาSOCให้อยู่ในจุดที่เหมาะสม โดยระบบที่จำลองขึ้นมาได้มีการจัดระดับMaturity ไว้ที่ระดับ Level0 หรือยังไม่มีการดำเนินงานเกี่ยวกับการทำSOC และกำหนดเป้าหมายที่ต้องการคือ Level3 หรือมีรูปแบบการดำเนินงานSOCที่ชัดเจน โดยสามารถยึดหลักจาก SOC Capability assessment model ได้ โดยการวิเคราะห์ต้องวิเคราห์ 3ส่วน

- People: มีทรัพยากรบุคคลที่มีความสามารถเพียงพอหรือไม่
- Process: มีระบบตรวจสอบครอบและนโยบายครอบคลุมถึงส่วนการดูแลระบบหรือไม่
- Technology: มีเทคโนโลยีที่ช่วยเหลืองานส่วนนี้หรือไม่ สามารถใช้งานได้อย่างมีประสิทธิภาพหรือไม่



รูปที่ 5 SOC Maturity Model

รูปที่ 6 SOC Capability Assessment Model

โดยสามารถแบ่งวิเคราะห์จำแนกตามDomain ของ Capability Assessment Model ได้ดังนี้

- Service Continuity

  กล่าวถึงความพร้อมในการดูแลระบบให้สามารถใช้งานได้อยู่เสมอ

ตารางที่ 12 Service Continuity Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรและไม่มีแผน	มีผู้รู้และสามารถปฏิบัติงานด้านความต่อเนื่องในการให้บริการเพียงบางส่วน	มีคนปฏิบัติงานเป็นประจำด้วยทักษะที่เหมาะสม แต่ยังคงเป็นแบบไม่เต็มเวลา JD / บทบาทที่กำหนดไว้บางส่วน	มีบุคคลที่มีความรู้ความสามารถเฉพาะด้านที่รับผิดชอบ มีบทบาทและความรับผิดชอบที่ชัดเจน	Lv3 + ประสิทธิภาพและทักษะจะได้รับการตรวจสอบและประเมินผลเป็นระยะและมีการปรับปรุงในเชิงรุกและแบ่งปันความรู้กับผู้ใช้	Lv4 + มีทักษะสำหรับการจัดหาและความต้องการ ไม่เคยมีปัญหาด้านทักษะ หรือขาดบุคลากร

Process	ไม่มีกระบวนการในการให้บริการ	มีการแก้ไขแบบเฉพาะกิจในการแก้ปัญหาระบบล่ม	มีกิจกรรมที่ทำซ้ำได้ แต่ไม่ได้กำหนดหรือกำหนดบางส่วน / ไม่มีเอกสารอย่างเป็นทางการ ไม่มีการสนับสนุนจากผู้บริหาร	มีนโยบายและกระบวนการกำหนดและจัดทำเป็นเอกสาร	Lv3 + มีการทบทวนและทดสอบเป็นระยะ ๆ	Lv4 + มีขั้นตอนการรักษาการให้บริการต่อเนื่องครบวงจร เป็นส่วนหนึ่งของกระบวนการทางธุรกิจ
Technology	ไม่มีเทคโนโลยีในการให้บริการ	มีการกู้คืนในบางระบบหรือบางปัญหา	มีเครื่องมือสำหรับการกู้คืนระบบอย่างสม่ำเสมอ มีการตรวจจับและการแจ้งเตือนความเสี่ยงที่เกิดขึ้นใหม่ๆ	มีการใช้เครื่องมือที่มีมาตรฐาน อุปกรณ์ที่ติดตั้งมาจากพื้นฐานความเสี่ยง	Lv3 + เครื่องมือจะได้รับการตรวจทานเป็นระยะ ๆ และทดสอบประสิทธิภาพเพื่อตรวจสอบภัยคุกคามที่เกิดขึ้นใหม่ ที่เป็นกระบวนการ	Lv4 + ใช้เครื่องมือการตรวจสอบคาดการณ์ไม่เคยมีปัญหาด้านเทคโนโลยี

- Physical Security

กล่าวถึงความพร้อมด้านความปลอดภัยทางกายภาพ

ตารางที่ 13 Physical Security Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากร	มีบุคลากรที่มีความสามารถบางส่วน	มีบุคลากรที่มีทักษะมีความสามารถที่เหมาะสม	มีบุคลากรที่มีทักษะมีความสามารถที่เหมาะสมเฉพาะด้าน	L3+ มีบุคลกรจะได้รับการตรวจสอบปรับปรุงอยู่เป็นระยะ	L4+ บุคลการสามารถแก้ไขจัดการปัญหาได้เอง ไม่มีปัญหาด้านความสามารถ
Process	ไม่มีกระบวนการ	มีการแก้ไขปัญหาแบบเฉพาะหน้า	มีการกำหนดแผนอย่างไม่เป็นทางการ	มีแผนเป็นเอกสารชัดเจน	L3+ มีการกำหนดนโยบายเพื่อดูแลรักษาอุปกรณ์ชัดเจน	L4+ มีการทดสอบปรับปรุงนโยบายด้านความปลอดภัยอยู่เสมอ
Technology	ไม่มีเทคโนโลยี	จัดหาอุปกรณ์เมื่อมีปัญหา	มีบางระบบที่มีการเตรียมความพร้อมใช้อยู่ตลอดเวลา	มีการเตรียมอุปกรณ์สำรองไว้	L3+ มีอุปกรณ์เพื่อลดผลกระทบเมื่อเกิดความเสียหายต่ออุปกรณ์	L4+ อุปกรณ์ทุกตัวมีความพร้อมใช้อยู่ตลอดเวลา

- Policy Process & Procedure

  กล่าวถึงความพร้อมในด้านนโยบาย ระเบียบ และแผนงานต่างๆ

ตารางที่ 14 Policy Process & Procedure Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากร	มีบุคลากรเฉพาะกิจ	มีบุคลากรปฏิบัติหน้าที่ประจำ	มีบุคลากรที่มีความรู้และทักษะที่เหมาะสม	L3+ มีบุคลากรที่มีประสิทธิภาพ มีความรู้และทักษะที่เหมาะสมเฉพาะด้าน	L4+ มีบุคลากรที่มีทักษะตามความต้องการ ไม่มีปัญหาด้านทักษะ หรือขาดบุคลากร
Process	ไม่มีกระบวนการ	มีขั้นตอนปฏิบัติเมื่อเกิดเหตุหรือมีภัยคุกคาม	มีขั้นตอนปฏิบัติ แต่ไม่มีเอกสารอย่างเป็นทางการ ไม่มีการสนับสนุนจากผู้บริหาร	มีนโยบายและขั้นตอนปฏิบัติชัดเจน	L3+ มีการทบทวนแผนและขั้นตอนปฏิบัติเป็นระยะ	L4+ มีการพัฒนาแผนและขั้นตอนปฏิบัติ
Technology	ไม่มีเทคโนโลยี	มีอุปกรณ์ในการจัดการเมื่อเกิดภัยคุกคาม	มีอุปกรณ์ที่ตรวจดูภัยคุกคาม	มีแผนและอุปกรณ์ที่มีมาตรฐาน สามารถรวบรวมข้อมูลมาวิเคราะห์ได้	L3+ อุปกรณ์ที่มีจะได้รับการตรวจทานและทดสอบเป็นระยะ เพื่อตรวจสอบภัยคุกคามใหม่ๆ	L4+ ใช้เครื่องมือการตรวจสอบคาดการณ์ ไม่เคยมีปัญหาด้านเทคโนโลยีภายในองค์กรเป็นไปตาม policy ที่กำหนดไว้หรือไม่

- Asset Management

  กล่าวถึงการจัดการสินทรัพย์ควบคุม

ตารางที่ 15 Asset Management Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรจัดการงานด้าน Asset	มีบุคลากรในบางส่วนหรือจัดการเมื่อมีทรัพย์สินสูญหาย	มีบุคลากรปฏิบัติหน้าที่ประจำ	มีบุคลากรที่มีความรู้และทักษะที่เหมาะสม	L3+ มีบุคลากรที่มีประสิทธิภาพ มีความรู้และทักษะที่เหมาะสมเฉพาะด้าน	L4+ มีบุคลากรที่มีทักษะตามความต้องการ ไม่มีปัญหาด้านทักษะ หรือขาดบุคลากร

Process	ไม่มีกระบวนการจัดการงานด้าน Asset	มีขั้นตอนปฏิบัติเมื่อเกิดเหตุทรัพย์สินสูญหาย	มีขั้นตอนปฏิบัติ แต่ไม่มีเอกสารอย่างเป็นทางการ ไม่มีการสนับสนุนจากผู้บริหาร	มีนโยบายและขั้นตอนปฏิบัติชัดเจน	L3+ มีการทบทวนแผนและขั้นตอนปฏิบัติเป็นระยะ	L4+ มีการพัฒนาแผนและขั้นตอนปฏิบัติ
Technology	ไม่มีเครื่องมือช่วย	มีอุปกรณ์ในการจัดการทรัพย์สินเมื่อมีปัญหา	มีอุปกรณ์จัดการเรื่องสินทรัพย์บางรายการ	มีอุปกรณ์ที่มีมาตรฐาน	L3+ อุปกรณ์ที่มีจะได้รับการตรวจทานและทดสอบเป็นระยะ เพื่อตรวจสอบภัยคุกคามใหม่ๆ	L4+ ใช้เครื่องมือการตรวจสอบคาดการณ์ ไม่เคยมีปัญหาด้านเทคโนโลยี

- Vulnerability Management

กล่าวถึงการจัดการช่องโหว่ของระบบ

ตารางที่ 16 Vulnerability Management Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรในการจัดการช่องโหว่	บุคลากรแก้ไขช่องโหว่เมื่อมีปัญหาเกิดขึ้น	มีบุคลากรเฉพาะตำแหน่งที่เกี่ยวข้องและมีทักษะในการวิเคราะห์ช่องโหว่	มีบุคลากรที่มีความรู้และทักษะที่เหมาะสม และมีการใช้อุปกรณ์ตรวจสอบ	L3+ บุคลากรมีการใช้อุปกรณ์ตรวจสอบช่องโหว่ และนำผลที่ได้มาทำรายงานและแจ้งเตือน	L4+ บุคลากรสามารถวิเคราะห์และสามารถนำผลจากการวิเคราะห์มาแก้ไขช่องโหว่ที่เกิดขึ้นได้
Process	ไม่มีกระบวนการ	มีแผนงานหรือกระบวนการตรวจสอบช่องโหว่เมื่อเกิดภัยคุกคาม	มีขั้นตอนปฏิบัติ แต่ไม่มีเอกสารอย่างเป็นทางการ ไม่มีการสนับสนุนจากผู้บริหาร	มีแผนนโยบายและขั้นตอนปฏิบัติชัดเจน	L3+ มีขั้นตอนการปฏิบัติชัดเจนและมีการทบทวนอยู่เสมอ	L4+ มีขั้นตอนการปฏิบัติชัดเจนและมีแผนรับมือเมื่อเกิดช่องโหว่ใหม่ๆ
Technology	ไม่มีเทคโนโลยี	ไม่มีอุปกรณ์เฉพาะด้าน	มีอุปกรณ์เฉพาะด้านในบางส่วนของระบบ	มีอุปกรณ์เฉพาะด้าน แต่อาจจะไม่มีการแจ้งเตือนอยู่ตลอดเวลา	L3+ มีอุปกรณ์เฉพาะด้านที่มีการแจ้งเตือนอยู่ตลอดเวลา	L4+ ใช้เครื่องมือการตรวจสอบคาดการณ์ ไม่เคยมีปัญหาด้านเทคโนโลยี

- Risk Management

กล่าวถึงการจัดการความเสี่ยงของระบบ

ตารางที่ 17 Risk Management Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรด้านการบริหารจัดการความเสี่ยง	มีบุคลากรดำเนินการประเมินความเสี่ยงแต่ตั้งเฉพาะกิจ	มีบุคลากรด้านการบริหารจัดการความเสี่ยง	บุคลากรที่มีทักษะเหมาะสมในเฉพาะด้าน	L3 + บุคลากรมีประสิทธิภาพและทักษะจะได้รับการตรวจสอบและประเมินผลเป็นระยะ	L4 + มีทักษะสำหรับการจัดหาและความต้องการไม่เคยมีปัญหาด้านทักษะหรือขาดบุคลากร
Process	ไม่มีกระบวนการด้านการบริหารจัดการความเสี่ยง	มีการประเมินความเสี่ยงในบางระบบ	ดำเนินการประเมินความเสี่ยงของระบบทั้งหมดอยู่เป็นระยะ	กำหนดให้มีการประเมินความเสี่ยงของระบบที่ให้บริการ	L3 + ผู้บริหารกำหนดระดับความเสี่ยงขั้นต่ำของระบบที่ใช้งานจริงหากไม่ได้ตามเกณฑ์จะไม่สามารถนำขึ้นให้บริการได้	L4 + หาแนวทางเพื่อมาช่วยลดความเสี่ยงของระบบให้ได้มากที่สุด
Technology	ไม่มีเทคโนโลยีด้านการวิเคราะห์ความเสี่ยง	มีการนำเครื่องมือภายนอกมาวิเคราะห์ความเสี่ยง	มีเครื่องมือที่เป็นของตนเองในการวิเคราะห์ความเสี่ยง	มีการใช้เครื่องมือที่มีมาตรฐาน อุปกรณ์ที่ติดตั้งมาจากพื้นฐานความเสี่ยง	L3 + เครื่องมือจะได้รับการตรวจทานและทดสอบประสิทธิภาพเพื่อตรวจสอบภัยคุกคามที่เกิดขึ้นใหม่	L4 + ใช้เครื่องมือการตรวจสอบคาดการณ์ ไม่เคยมีปัญหาด้านเทคโนโลยี

- Incident Response

กล่าวถึงการตอบสนองต่อข้อผิดพลาด

ตารางที่ 18 Incident Response Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรในด้านการจัดการเหตุการณ์ภัยคุกคาม	ผู้ทำงานเป็นแบบ Part time หรืออาจใช้ทีมเดียวกับ IT ทำงานตามความต้องการเท่านั้น ผู้ทำงานไม่ได้เป็นผู้เชี่ยวชาญ	มีผู้ทำงาน 8 x 5 เหตุการณ์ และภัยคุกคามในโลกไซเบอร์บางอย่างได้รับการจัดหมวดหมู่และบันทึก	มีผู้ทำงานและผู้จัดการ SOC เป็นแบบแบบเต็มเวลา แผนจะใช้ผู้ให้บริการเฉพาะทางด้าน SOC มีการรวบรวมเหตุการณ์และภัยคุกคามในโลกไซเบอร์ไว้ที่ศูนย์กลาง และเป็นส่วนหนึ่งของงานประจำ	Lv3 + มีขั้นตอนละเอียดยิ่งขึ้นในการตรวจสอบเหตุการณ์ มีการรายงานเหตุการณ์ไปยังผู้มีส่วนได้เสียที่เกี่ยวข้อง มีการทบทวนเหตุการณ์ที่เกิดขึ้น	Lv4 + มีการปรับปรุงการควบคุมข้อมูลสำคัญและกระบวนการดำเนินการวิเคราะห์แนวโน้มภัยคุกคามที่จะเกิดขึ้น มีการสื่อสารและการสร้างบทเรียนและทำการป้องกันภัยคุกคามใหม่ๆได้ทันเวลา

Process	ไม่มีการจัดการเหตุการณ์ภัยคุกคาม	มีการดำเนินการประเมินความเสี่ยงที่มีผลกระทบสำคัญสำหรับองค์กร แต่ไม่มีขั้นตอนการดำเนินการการจัดการ	มีการดำเนินการวิเคราะห์เหตุการณ์ภัยคุกคาม และความปลอดภัยในโลกไซเบอร์ และจัดการภัยคุกคามที่เกิดขึ้นจริง และมีการฝึกซ้อมการรับมือ	มีการกำหนดขั้นตอนในการระบุเหตุการณ์ด้านความปลอดภัยในโลกไซเบอร์กำหนดวัตถุประสงค์และตรวจสอบสถานการณ์ดำเนินการที่เหมาะสม	Lv3 + มีขั้นตอนละเอียดยิ่งขึ้นในการตรวจสอบเหตุการณ์ มีการรายงานเหตุการณ์ไปยังผู้มีส่วนได้เสียที่เกี่ยวข้อง มีการทบทวนเหตุการณ์ที่เกิดขึ้น	Lv4 + มีการปรับปรุงการควบคุมข้อมูลสำคัญและกระบวนการดำเนินการวิเคราะห์แนวโน้มภัยคุกคามที่จะเกิดขึ้น มีการสื่อสารและการสร้างบทเรียนที่ได้เรียนรู้
Technology	ไม่มีเทคโนโลยี	ใช้การตรวจสอบการควบคุมความปลอดภัยแบบ Signature based เครื่องมือรักษาความปลอดภัยที่ซื้อมาเพื่อป้องกันการโจมตีแบบเฉพาะ	มีเครื่องมือ SIEM ไม่ได้ใช้อย่างมีประสิทธิภาพ สำหรับการตรวจจับหรือตรวจสอบภัยคุกคาม ไม่มีมาตรฐานในการใช้เครื่องมือในการตอบสนองต่อเหตุการณ์	มีการใช้ SIEM + เครื่องมือตรวจสอบเครือข่ายในส่วนของเครือข่ายหลักเพื่อเพิ่มทัศนวิสัยในการตอบสนองภัยคุกคาม มีการสร้างขั้นตอนการตอบสนองต่อเหตุการณ์ที่ระบุไว้เป็นเอกสาร	Lv3 + มีการประเมินการใช้งานเทคโนโลยีและวางแผนปรับปรุงระบบการตรวจจับและการตอบสนองต่อเหตุการณ์	Lv4 + มีการประเมินแนวโน้มสถานการณ์และเลือกใช้งานเครื่องมือในการตอบสนองต่อเหตุการณ์ที่เหมาะสมกับภัยคุกคาม

- Incident Management

  กล่าวถึงการจัดการกับข้อผิดพลาด

ตารางที่ 19 Incident Management Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรทราบเหตุการณ์ที่เกิดขึ้นและไม่มีแผนงาน	ทราบเหตุการณ์จากการรับแจ้ง ไม่มีแผนการจัดการ	มีตำแหน่งที่เกี่ยวข้องเฉพาะ แต่ขึ้นอยู่กับตัวบุคคลถ้าบุคคลนี้ไม่อยู่ไม่มีคนรู้ มีการจัดการเหตุการณ์ที่เกิดขึ้น ไม่มีแผนที่เป็นทางการ	มีตำแหน่งที่เกี่ยวข้องเฉพาะและมีเอกสารเกี่ยวกับแผนงานที่ต้องทำ	มีตำแหน่งผู้ทำหน้าที่ทราบเกี่ยวกับแผนงานที่ถูกกำหนดเป็นนโยบาย	ทุกคนรับทราบเกี่ยวกับนโยบายและสามารถทำตามแผนงานได้เอง

Process	ไม่มีกระบวนการ	มีจัดการเหตุการณ์แบบเฉพาะกิจเป็นครั้งๆไป	มีการทำซ้ำ กำหนดขั้นตอนไว้บางส่วน / ไม่มีเอกสารอย่างเป็นทางการไม่มีการสนับสนุนจากผู้บริหาร	มีการกำหนดนโยบาย ขั้นตอนของกระบวนการและจัดทำเป็นเอกสาร	Lv3 + มีการทบทวนนโยบายขั้นตอนและทดสอบเป็นระยะๆ	Lv4 + มีการจัดการอย่างครบวงจร เป็นส่วนหนึ่งของกระบวนการทางธุรกิจ มีประสิทธิภาพในการจัดการกับเหตุการณ์
Technology	ไม่มีเทคโนโลยี	มี Log บันทึกการรักษาความปลอดภัยบางส่วนสำหรับการตรวจสอบในแบบเฉพาะกิจ	มีเครื่องมือสำหรับการตรวจสอบอย่างสม่ำเสมอที่ตรวจพบและแจ้งเตือนอยู่แล้ว อุปกรณ์ที่ติดตั้งอยู่ไม่ได้ขึ้นอยู่กับความเสี่ยง	มีการใช้เครื่องมือที่มีมาตรฐานอุปกรณ์ที่ติดตั้งอยู่บนพื้นฐานความเสี่ยง	Lv3 + เครื่องมือที่ใช้งานจะได้รับการตรวจทานเป็นระยะๆ และมีการทดสอบประสิทธิภาพเพื่อตรวจสอบภัยคุกคามที่เกิดขึ้นใหม่ เพิ่มรวมไปในกระบวนการ	Lv4 + มีการใช้เครื่องมือการตรวจสอบคาดการณ์ไม่เคยมีปัญหาด้านเทคโนโลยี

- Reporting

กล่าวถึงกระบวนการทำรายงานต่างๆ

ตารางที่ 20 Reporting Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคคลากรที่รับผิดชอบในการทำ Report	มีบุคลากรที่ทำ report เป็นครั้งคราวไป เมื่อมีความต้องการ Report	มีการกำหนดใน Role ของการทำงาน แต่ยังไม่มีคนทำประจำ Ad Hoc การทำ Report เพิ่มจากงานประจำที่ตนเองรับผิดชอบอยู่	มีเจ้าหน้าที่รับผิดชอบในการทำรายงานที่ชัดเจน กำหนดประเภทของ Report ที่จะต้องทำ Daily, Weekly, Monthly Report	L3 + มีบุคลากรที่มีประสิทธิภาพ มีความรู้และมีทักษะที่เหมาะสม	L4 + มีบุคลากรที่สามารถทำ Report แทนกันได้ ไม่ขาดแคลนบุคลากรที่รับผิดชอบการทำ Report
Process	ไม่มีกระบวนการรองรับ	มีกระบวนการทำ Report เป็นครั้งคราว ไม่มีการกำหนด Template ในการทำ Report	มีการกำหนด Template ขึ้นมาใช้ในการทำ Report กำหนดรูปแบบเนื้อหาในการนำเสนอ Report แต่ก็ยังไม่เป็นทางการ	Template Report ถูกประกาศใช้อย่างเป็นทางการ กำหนดรูปแบบ เนื้อหาของ Report อย่างชัดเจน	L3 + มีการทบทวนปรับปรุง Template ที่ใช้ในการทำ Report ทบทวนเนื้อหาและข้อมูลในการนำเสนอ Report อยู่เป็นระยะ	L4 + มีการทบทวนปรับปรุง Template ที่ใช้ในการทำ Report ทบทวนเนื้อหาและข้อมูลในการนำเสนอ Report อยู่อย่างสม่ำเสมอ

Technology	ไม่มี Technology ที่ใช้สำหรับการทำ Report	มีการใช้โปรแกรมประยุกต์ เช่น Word, Excel เข้ามาช่วยในการ Report	มีการนำ Opensource มาพัฒนาเพื่อใช้ในการทำ Report	มีการ Integrate tool ที่ใช้ในการทำ Report เข้ากับระบบที่ต้องดึงข้อมูลมาทำ Report	L3 + พัฒนา tool ที่ใช้ในการทำ Report ให้เป็น Automate	L4 + ปรับปรุง tool ที่ใช้ในการทำ Report อย่างสม่ำเสมอเพื่อให้เกิดข้อผิดพลาดในการทำ Report น้อยที่สุด

- Logging & Analysis

  กล่าวถึงการจัดการและวิเคราะห์ข้อมูลจาก Log

ตารางที่ 21 Logging & Analysis Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มี จนท. คอย monitor ระบบ	เมื่อเกิดเหตุค่อยมอบหมาย หรือแต่งตั้งชั่วคราว	จนท. ดำเนินการตรวจสอบกันเอง ไม่มีใครมอบหมาย สั่งการ	กำหนด จนท. เพื่อตรวจสอบอย่างชัดเจนตลอด 24x7	Lv3+ มีการประเมินและวัดผลการปฏิบัติหน้าที่ของ จนท.	Lv4+ มีการพัฒนาและจัดเตรียมกาลังพลทดแทนอย่างต่อเนื่อง
Process	ไม่มีกระบวนการใดๆ สนับสนุน	มีขั้นตอนการทำงานยึดตามเจ้าหน้าที่ที่ปฏิบัติงานในตอนนั้น	นำขั้นตอนการทำงานจากที่เคยทำมากำหนดใช้ภายในกันเอง	กำหนดกระบวนการตรวจสอบ แหล่งข้อมูลไว้อย่างชัดเจน	Lv3+ มีการประเมินกระบวนการและแหล่งข้อมูลเพื่อให้เห็นภัยคุกคามได้อย่างทั่วถึง	Lv4+ พิจารณานาเข้าระบบและอุปกรณ์ใหม่ๆ ในระบบเพื่อตรวจสอบทันที
Technology	ไม่มีเทคโนโลยีสนับสนุน	เมื่อเกิดเหตุก็ใช้ Log ที่เก็บไว้ในอุปกรณ์นั้นๆ มาทำการวิเคราะห์ แต่ไม่ได้กำหนดให้มีการเก็บ Log	กำหนดให้มีการเก็บ Log ตามพรบ. เพื่อใช้ในการตรวจสอบย้อนหลัง	มีการใช้ SIEM เข้ามาใช้งานในการเก็บ Log มารวมไว้เป็น centralized logging	Lv3+ ทบทวนเครื่องมือและเทคโนโลยีที่ใช้อยู่เป็นระยะ	Lv4+ พิจารณาเครื่องมือและเทคโนโลยีที่ใช้เพื่อประสิทธิภาพที่ดีขึ้นอย่างต่อเนื่อง

- Use case Hunting

  กล่าวถึงกระบวนการจัดทำ Use Case

ตารางที่ 22 Use case Hunting Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีบุคลากรในการทำ Use case และไม่สามารถ Hunting case เพื่อวิเคราะห์สาเหตุได้	สรรหาบุคลากรภายนอกที่สามารถทำหน้าที่ตรวจสอบและวิเคราะห์สาเหตุได้ แต่ไม่ได้มีความรับผิดชอบหลัก	กำหนดให้มีบุคลากรที่รับผิดชอบในการทำ Use case และ Hunting case แต่อาจจะไม่ได้มีทักษะเฉพาะด้าน	บุคลากรที่รับผิดชอบมีทักษะตามรูปแบบที่ได้มีการกำหนดไว้เป็นทางการ	L3 + มีการพัฒนาทักษะของบุคลากรและประเมินผลการทำงานของบุคลากรประจำปี	L4 + มีบุคลากรทดแทน สามารถทำงานได้อย่างต่อเนื่อง
Process	ไม่มีกระบวนการในการทำ Use case และ Hunting case	ใช้แผนงานจากที่อื่นนำมาปรับใช้เป็นครั้งคราว	มีการกำหนดรูปแบบออกเป็นเอกสารแบบไม่เป็นทางการ	มีการกำหนดรูปแบบออกเป็นเอกสารแบบเป็นทางการ	L3 + มีการประเมินผลกระบวนการทำงานตรวจสอบ เพื่อปรับปรุงแผนใหม่	L4 + มีการพัฒนานโยบาย เพื่อเพิ่มขีดความสามารถของบุคลากร
Technology	ไม่มีเครื่องมือใดๆ เข้ามาช่วยในการทำ Use case และ Hunting case	เมื่อเกิดเหตุดการณ์ใช้วิธีการหาข้อมูล หา tool ที่ใช้ในการทำจาก Internet	มีการใช้ tool ที่ใช้สำหรับการทำ Use case Hunting case	มีเครื่องมือสำรอง พร้อมเปลี่ยนและมีการเตรียมทำ Replacement ภายใน SLA ที่กำหนด	L3 + มีอุปกรณ์หรือเครื่องมือเพื่อลดผลกระทบ Single Point of Failure	L4 + มีการรักษาอุปกรณ์และระบบทุกตัวพร้อมใช้ตลอดเวลา

- Role & People

กล่าวถึงการจัดการคนและหน้าที่รวมถึงขอบเขตการเข้าถึงของข้อมูล

ตารางที่ 23 Role & People Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีการจัด Organization ที่เกี่ยวกับ SOC เลย	มีการกำหนดความรับผิดชอบในลักษณะเฉพาะกิจ เป็นครั้งๆหรือ เป็น Project เสร็จแล้วจบไปไม่มีการดำเนินการต่อ	มีคนทำหน้าที่แต่ไม่มีระบุไว้ชัดเจน รู้กันได้เองว่าใครทำหน้าที่นั้น หากคนๆ นั้นไม่อยู่ไม่มีคนทำหน้าที่แทน	: มีการกำหนดหน้าที่/โครงสร้างไว้ชัดเจน ใน Organization Chart มี Job Description สำหรับตำแหน่งงาน	Level 3 + มีการทำแผนพัฒนาบุคลากรประจำปี ตามความรู้ความสามารถที่ต้องใช้ในงาน SOC	Lv4+ มีการประเมินและพัฒนา ฝึกอบรม จนท. เพื่อเพิ่มความชำนาญ และจัดหากาลังสำรองเพื่อทดแทน
Process	ไม่มีการจัด Organization ที่เกี่ยวกับ SOC เลย	มีการสรรหาบุคลากรมาทำหน้าที่เป็นครั้งคราว ไม่มีผู้รับผิดชอบชัดเจน	มีการสรรหาบุคลากรมาทำหน้าที่แทนหาก หากผู้รับผิดชอบเดิมไม่อยู่หรือไม่มีคนทำ	มีการกำหนดนโยบายขั้นตอน ในการสรรหาบุคลากรในตำแหน่งนี้ มีการกำหนด JD กำหนด Skill ของตำแหน่งอย่างชัดเจน	Lv3+ มีการกำหนดระยะเวลาในการสรรหาบุคลากรให้ทันต่อความต้องการ	Lv4+ สามารถหาบุคลากรมาทดแทนได้ทันทีเมื่อขาดแคลน
Technology	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A

- Education & Expertise

กล่าวถึงการจัดการพัฒนาทักษะองค์รวมภายในองค์กร

ตารางที่ 24 Education & Expertise Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีการอบรมให้ความรู้ จนท.	เมื่อมีเทคโนโลยีใหม่ๆ จึงค่อยพิจารณาส่ง จนท. เข้ารับการอบรม	จนท. ฝึกและศึกษาด้วยตัวเองเพื่อนามาใช้ปฏิบัติงาน	กำหนดการฝึกและศึกษาของ จนท. ที่ชัดเจน	Lv3+ มีการประเมินทักษะและความสามารถของ จนท. เพื่อรองรับการทดแทนและเติบโตในอนาคต	Lv4+ พัฒนาทักษะและความชานาญของ จนท. อย่างต่อเนื่อง จัดหาขึ้นทะเบียนกำลังพลทดแทน

Process	ไม่มีการกำหนดแนวทางการอบรมหรือฝึกทักษะของ จนท.	เมื่อเกิดเหตุค่อยไปหาวิธีจากอินเตอร์เน็ตมาใช้	มีการกำหนดแนวทางการอบรมหรือทักษะของ จนท. ไว้แต่ยังไม่สามารถดำเนินการได้จริง	กำหนดลำดับการอบรมและทักษะที่ต้องการของ จนท. ไว้ชัดเจน	Lv3+ มีการประเมินผลการอบรมหรือทักษะ จนท. เพื่อให้ตรงตามคุณสมบัติที่กำหนดไว้	Lv4+ พัฒนาลำดับและขั้นตอนในการศึกษาของ จนท. เพื่อให้พร้อมต่อการปฏิบัติงานทดแทน
Technology	ไม่มีระบบช่วยการฝึกหรือให้ความรู้ จนท.	เมื่อมีเทคโนโลยีใหม่ๆ ให้ จนท. ไปหาศึกษาจากอินเตอร์เน็ตด้วยตัวเอง	จนท. หาเครื่องมือมาใช้ในการเรียนรู้ภายในด้วยตัวเอง	กำหนดเครื่องมือและสนับสนุนการเรียนรู้ของ จนท.	Lv3+ มีเครื่องมือช่วยฝึกและประเมินทักษะของ จนท.	Lv4+ พัฒนาเครื่องมือช่วยฝึกและประเมินทักษะของ จนท. อย่างต่อเนื่อง

- Security Framework & Strategy

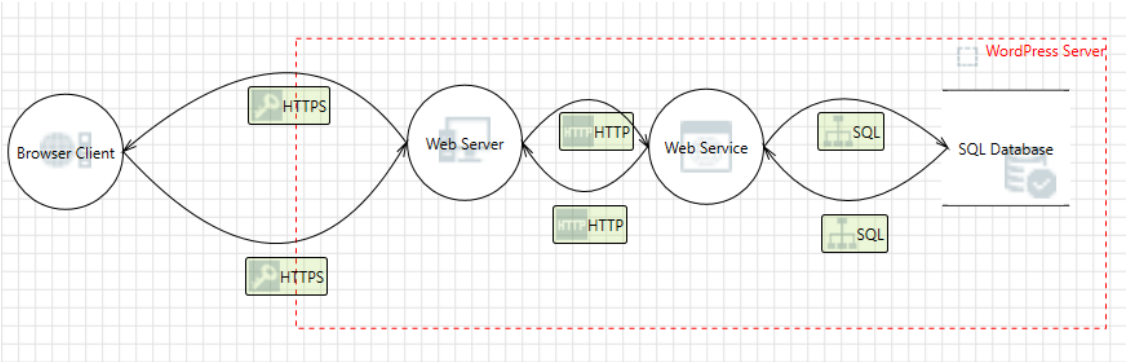
  กล่าวถึงการนำ Framework มาประยุกต์ใช้ภายในองค์กร

ตารางที่ 25 Security Framework & Strategy Maturity Model

Maturity Level	Level 0 Nonexistent	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
People	ไม่มีผู้กำหนด	หาคนมาทำเป็นครั้งๆ ไป	ผู้ดูแลระบบหา framework มาเพื่อดูแลระบบของตัวเอง	กำหนดให้ จนท. ทุกคนต้องปฏิบัติงานตามframework และมีผู้กากับดูแลผลการดำเนินงานอย่างชัดเจน	Lv3+ นำผลการปฏิบัติงานของ จนท. มาเป็นเครื่องมือในการประเมินผลการปฏิบัติงาน	Lv4+ มีแผนการพัฒนา จนท. เพื่อให้สามารถปฏิบัติงานตาม framework และสามารถทดแทนกันได้
Process	ไม่ได้กำหนด	เมื่อจะทำจึงหาแนวทางการดำเนินงาน	นำกระบวนการขั้นตอนตาม framework มาใช้กันเองไม่มีผู้กำหนด/สั่งการ	กำหนดขั้นตอนการปฏิบัติงานตาม framework ไว้อย่างชัดเจน	Lv3+ นำขั้นตอนการปฏิบัติงานที่ใช้มาทบทวนเพื่อให้เหมาะสมกับหน่วยงาน	Lv4+ ทบทวนและปรับปรุงกระบวนการการปฏิบัติงานทุกๆ 4 เดือน
Technology	ไม่ได้นำมาใช้	เมื่อจะทำจึงจัดหาอุปกรณ์เครื่องมือมาสนับสนุน	หาเทคโนโลยีเครื่องมือมาใช้กันเองไม่ได้กำหนดไว้	กำหนดเทคโนโลยีและเครื่องมือเพื่อใช้ในการปฏิบัติงานไว้อย่างชัดเจน	Lv3+ ทบทวนประเมินผลเทคโนโลยีเครื่องมือที่ใช้ว่าเพียงพอครบถ้วนสำหรับการปฏิบัติงานหรือยัง	Lv4+ ทบทวนและปรับปรุงเทคโนโลยีเครื่องมือที่ใช้ทุกๆ 6 เดือน

3.4 Threat Modeling

การสร้างแบบจำลองภัยคุกคามเป็นขั้นตอนสำหรับการเพิ่มประสิทธิภาพความปลอดภัยของเครือข่ายโดยการระบุวัตถุประสงค์และจุดอ่อนจากนั้นกำหนดวิธีการรับมือเพื่อป้องกันหรือบรรเทาผลกระทบของภัยคุกคามต่อระบบ ในบริบทนี้ภัยคุกคามเป็นเหตุการณ์ที่อาจเกิดขึ้นหรือเกิดขึ้นจริงและอาจเป็นอันตราย (เช่นการโจมตีแบบDDoS) หรืออื่นๆ และอาจทำให้เกิดความเสียหายต่อองค์กร



รูปที่ 7 Threat Modeling Architecture Design

3.5 Use Case development

หมวดที่ 1 การเข้าถึงและการพิสูจน์ตัวตน (Access and Authentication)

ประเภท	กรณีศึกษา	แหล่งที่มาของข้อมูล Log	แนวทางการตรวจจับ/รับมือ
Identity Management	มีการใช้งาน user ที่ไม่ได้รับอนุญาต หรือ user ที่ disabled มีการใช้งาน root, admin/มีการ add privilege user/ SU	Databases, Applications, Event log, HR Data	Correlation rules
Password Brute force	มีการ Brute Force สำเร็จที่ asset สำคัญ	Event log	Correlation rules
Access Management	จำนวนการ logon failure ของ Privilege User เพิ่มขึ้น	Event log	Correlation rules
	มีการพยายามเข้าถึงโดยใช้ Default user ของอุปกรณ์	Host, Server & Security devices	Correlation rules
	มีการเปลี่ยน Password ของ Privilege account	Event log, IDS Database, Firewall,	Rule Alert
	มีความผิดปกติหรือเพิ่มจำนวนของจำนวน Failed remote login attempt, RDP Attempt จาก Local admin	Event log, Firewalls, IDS	Correlation rules

หมวดที่ 2 การปฏิบัติการ/การให้บริการ (Service Continuity)

ประเภท	กรณีศึกษา	แหล่งที่มาของข้อมูล Log	แนวทางการตรวจจับ/รับมือ
System Health	มีอุปกรณ์ไม่ส่ง log หรือหยุดทำงาน	System log, Report	Health Check,

หมวดที่ 3 การเปลี่ยนแปลงการตั้งค่า (Configuration Change)

ประเภท	กรณีศึกษา	แหล่งที่มาของข้อมูล Log	แนวทางการตรวจจับ/รับมือ
Unauthorized change	Configuration ของอุปกรณ์มีการเปลี่ยนแปลง	IDS, Firewall, System log	Correlation rules

หมวดที่ 4 พฤติกรรมการใช้งานที่ผิดปกติ (Abnormal Traffic)

ประเภท	กรณีศึกษา	แหล่งที่มาของข้อมูล Log	แนวทางการตรวจจับ/รับมือ
Network Security	มีความผิดปกติหรือเพิ่มจำนวนของจำนวน มี Traffic การใช้งาน	Event log, Firewalls, IDS, Access Controls	Correlation rules
	มีการพยายามเข้าถึง server จากหมายเลข IP ต้องสงสัย หรือไม่ได้รับอนุญาต	Firewall, IDS	Correlation rules
	มี server พยายามเข้า internet โดยไม่ได้รับอนุญาต	Firewall, IDS	Correlation rules

หมวดที่ 5 การโจมตีที่รู้จัก (Known Threat)

ประเภท	กรณีศึกษา	แหล่งที่มาของข้อมูล Log	แนวทางการตรวจจับ/รับมือ
OWASP Top 10	Default	IDS, Firewall, System log, Event log	Security controls/ Correlation rules/Alerts
Callback C&C			
Scan port			

บทที่ 4

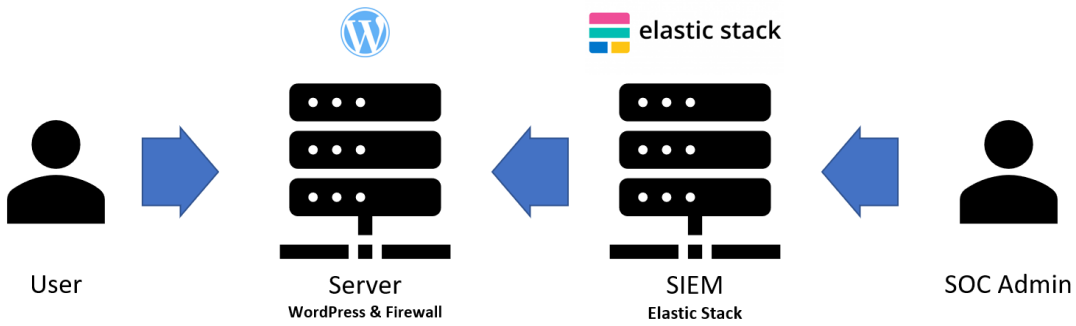
ผลการดำเนินงาน

4.1 หลักการและเหตุผล

ในบทนี้จะกล่าวถึงวิธีการดำเนินโครงการ ผลการพัฒนาและทดสอบระบบการเฝ้าระวังและตรวจจับภัยคุกคามเว็บเซิร์ฟเวอร์ ซึ่งข้อมูลที่ได้จากการศึกษาระบบ การออกแบบระบบและการดำเนินการสร้างโดยมีผล การดำเนินงานดังนี้

4.2 ขั้นตอนการดำเนินงาน

การดำเนินงานจะทำการจำลองระบบที่มีผู้ใช้งานทั่วไป (User) โดยผู้ใช้งานจะมีการเข้าถึงเว็บเซิร์ฟเวอร์ผ่านทางWebpage โดยในเครื่องของเว็บเซิร์ฟเวอร์จะมีการรันService Log Shipping เพื่อใช้ในการส่งข้อมูลของเว็บเซิร์ฟเวอร์ไปที่เครื่อง SIEMเพื่อทำLog Management และแสดงผลผ่านเครื่องของ SOC Admin



รูปที่ 8 แสดงภาพรวมการทำงานของระบบ

4.3 ความต้องการพื้นฐานในการพัฒนาระบบ

4.3.1 ฮาร์ดแวร์

4.3.1.1 เครื่องคอมพิวเตอร์ สำหรับทำการทดสอบใช้งานWeb Server

4.3.1.2 เครื่องคอมพิวเตอร์ สำหรับติดตั้งโปรแกรม Log Management

4.3.1.3 เครื่องคอมพิวเตอร์ สำหรับSOC Admin

4.3.2 ซอฟต์แวร์

4.3.2.1 ระบบปฏิบัติการ CentOS7 สำหรับเครื่อง Service

4.3.2.2 WordPress Components (Apache, MariaDB, PHP)

4.3.2.3 ระบบปฏิบัติการ Windows 10 สำหรับ SOC Admin

4.3.2.4 โปรแกรม Kibana Version7.4

4.3.2.5 โปรแกรม Elasticsearch Version 7.4

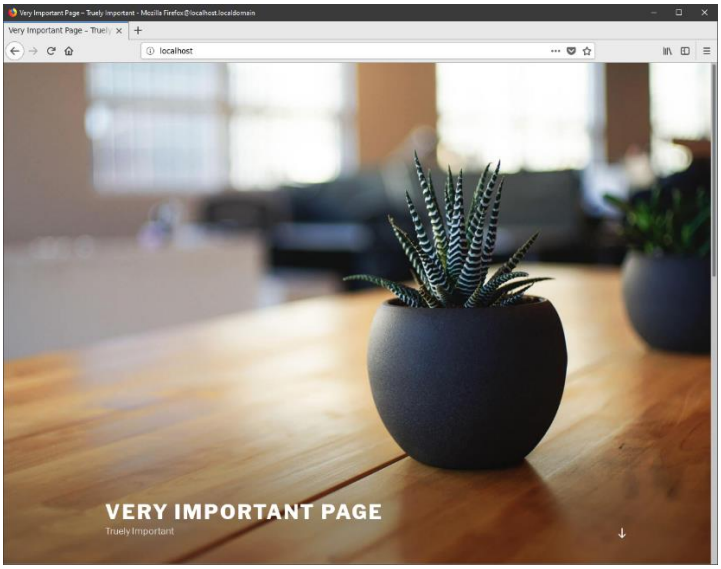
4.3.2.6 โปรแกรม Beat

4.3.2.7 โปรแกรม Logstash

4.4 ผลการดำเนินงาน

4.4.1 ฝั่งผู้ใช้งาน (Client)

ในการดำเนินการทดสอบนั้นการทดสอบจะเริ่มจากขั้นตอนในสร้างส่วนติดต่อผู้ใช้งานภายนอก Webpage WordPress มีการใช้งาน process ทั้งหมดสามส่วนทำงานร่วมกัน ได้แก่ httpd, MariaDB และ php โดย MariaDB และphp เป็นส่วนของWebpage และhttpd เป็นส่วน service เพื่อรองรับrequestจากภายนอก



รูปที่ 9 แสดงหน้า Webpage WordPress

4.4.2 ฝั่ง Log Management และ Monitoring

ซอฟต์แวร์ที่เลือกใช้งาน คือElastic stack ซึ่งเป็น opensource ประกอบด้วย Softwareที่ทำงานร่วมกันได้แก่ Beat, Logstash, Elasticsearch และ Kibana

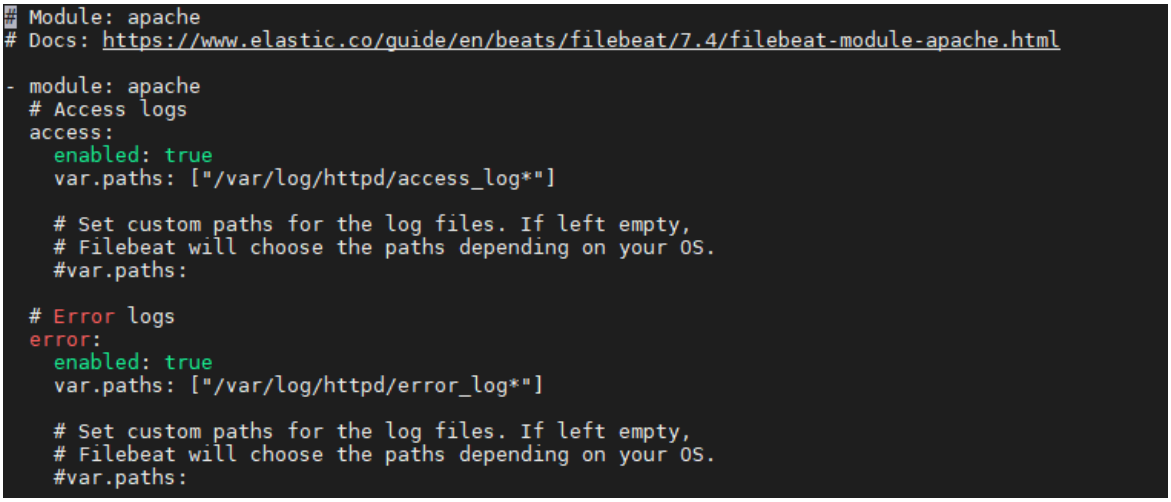
Beat (Log Shipper)

เป็น Software ที่ทำหน้าที่หลักในการส่ง Logจาก Hostไปทำการประมวลผลต่อ โดยหลักการทำงานของ software คือมีรอบการเช็ค log update ที่มีการconfigไว้ว่าต้องมีการ Ship จาก File ใด เมื่อ Fileมีการเปลี่ยนแปลงจะทำการ ส่ง data streamไปยังendpoint ที่configไว้ ซึ่งในที่นี้จะมีสองกรณีคือส่งไปที่ Logstash ซึ่งเป็น Log Parser หรือส่งตรงไปที่ Elasticsearch ซึ่งเป็นหน่วยประมวลผล ข้อแตกต่างของทั้งสองแบบคือ การส่งไปLogstash จะสามารถจัดการกับLogที่ไม่ได้เป็น Default Pattern ได้หลากหลายกว่า แต่ในทางกลับกัน ข้อเสียคือ การ configจะซับซ้อนกว่าและต้องใช้Knowledge Baseทั้งในด้าน GROK และ Regular expressionในการจัดการ หากเป็นการส่งโดยตรงไปที่ Elasticsearch จำเป็นที่จะต้องลงPlug-inเฉพาะและรูปแบบLogจำเป็นต้องเข้ากันกับ Plug-inนั้นๆ ทำให้การจัดการLogรูปแบบนี้ มีข้อจำกัดในการใช้งานค่อนข้างมาก

```
#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["logstash_host:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

#----------------------------- Logstash output --------------------------------
#output.logstash:
  # The Logstash hosts
  #hosts: ["logstash_host:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

รูปที่ 10 แสดงConfigurationในการส่งLogทั้ง2รูปแบบ

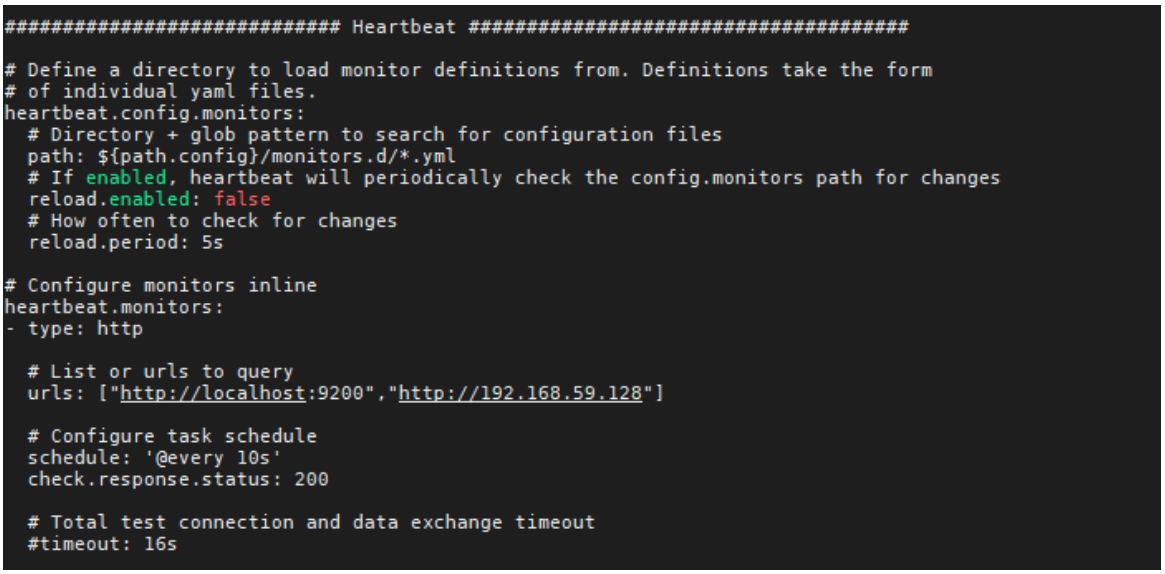
ในโครงงานนี้Logไฟล์ที่ทำการส่งจะเป็น Apache Access log และ Apache Error log ซึ่ง Log Pattern ตรงกันกับ Plug-inของBeat จึงสามารถใช้วิธีการส่งโดยไป Elasticsearchได้โดยผ่าน Plug-in โดยเมื่อมีการ Enable Plug-inแล้ว ต้องทำการ configในส่วนของModule Plug-inนั้นด้วย



```
# Module: apache
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.4/filebeat-module-apache.html

- module: apache
  # Access logs
  access:
    enabled: true
    var.paths: ["/var/log/httpd/access_log*"]

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

  # Error logs
  error:
    enabled: true
    var.paths: ["/var/log/httpd/error_log*"]

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:
```

รูปที่ 11 แสดงConfiguration Apache Plug-in Module

นอกจากการส่งData Streamจากไฟล์แล้ว ยังมีBeat รูปแบบอื่นๆ เช่น Metric Beat, Audit Beat, Heart Beat เพื่อใช้ในการส่งข้อมูลเพิ่มเติมอื่นๆโดยจะเป็นการยึดPathการShipตาม Operating System เป็นหลัก หรือเป็นข้อมูลการMonitorด้านอื่นๆ เช่น Heart Beatที่ส่งข้อมูลผลการPINGไปที่URLเพื่อเช็คAvailability ของระบบ



```
############################ Heartbeat ######################################

# Define a directory to load monitor definitions from. Definitions take the form
# of individual yaml files.
heartbeat.config.monitors:
  # Directory + glob pattern to search for configuration files
  path: ${path.config}/monitors.d/*.yml
  # If enabled, heartbeat will periodically check the config.monitors path for changes
  reload.enabled: false
  # How often to check for changes
  reload.period: 5s

# Configure monitors inline
heartbeat.monitors:
- type: http

  # List or urls to query
  urls: ["http://localhost:9200","http://192.168.59.128"]

  # Configure task schedule
  schedule: '@every 10s'
  check.response.status: 200

  # Total test connection and data exchange timeout
  #timeout: 16s
```

รูปที่ 12 แสดงConfiguration Heart Beat

Logstash (Log Parser)

เป็น Software ที่ทำหน้าที่ในการ Indexing ให้เหมาะสมกับการใช้งานในการวิเคราะห์ การรับLogมานั้นสามารถมาได้จากทั้ง รับมาจาก Beat ผ่าน Pipeline หรือ สามารถ Pullโดยตรงได้หากอยู่บนเครื่องเดียวกัน

```
# This file is where you define your pipelines. You can define multiple.
# For more information on multiple pipelines, see the documentation:
#   https://www.elastic.co/guide/en/logstash/current/multiple-pipelines.html

- pipeline.id: main
  path.config: "/etc/logstash/conf.d/*.conf"
```

รูปที่ 13 แสดงConfiguration Pipeline

หลักการทำงานของ Logstashนั้นจะเป็นการจัดแยกประเภทข้อมูลLog และระบุประเภทของDataที่สามารถเก็บได้จากLogนั้นๆ โดยการทำงานเหล่านี้จะยึดจากConfigเป็นหลัก

```
input {
  beats {
    port => 5044
  }
}
filter {
  if [fileset][module] == "apache" {
    if [fileset][name] == "access" {
      grok {
        match => { "message" => ["%{IPORHOST:[apache][access][remote_ip]} - %{DATA:[apache][access][user_name]} \[%{HTTPDATE:[apache][access][time]}\] \"%{WORD:[apache][access][method]} %{DATA:[apache][access][url]} HTTP/%{NUMBER:[apach
e][access][http_version]}\" %{DATA:[apache][access][response_code]} %{NUMBER:[apache][access][body_sent][bytes]}( \"%{DATA:[apache][access][referrer]}\")?( \"%{DATA:[apache][access][agent]}\")?",
          "%{IPORHOST:[apache][access][remote_ip]} - %{DATA:[apache][access][user_name]} \\[%{HTTPDATE:[apache][access][time]}\\] \"-\" %{DATA:[apache][access][response_code]} -" ] }
        remove_field => "message"
      }
      mutate {
        add_field => { "read_timestamp" => "%{@timestamp}" }
      }
      date {
        match => [ "[apache][access][time]", "dd/MMM/YYYY:H:m:s Z" ]
        remove_field => "[apache][access][time]"
      }
      useragent {
        source => "[apache][access][agent]"
        target => "[apache][access][user_agent]"
        remove_field => "[apache][access][agent]"
      }
      geoip {
        source => "[apache][access][remote_ip]"
        target => "[apache][access][geoip]"
      }
    }
    else if [fileset][name] == "error" {
      grok {
        match => { "message" => ["\[%{APACHE_TIME:[apache][error][timestamp]}\] \[%{LOGLEVEL:[apache][error][level]}\]( \[client %{IPORHOST:[apache][error][client]}\])? %{GREEDYDATA:[apache][error][message]}",
          "\[%{APACHE_TIME:[apache][error][timestamp]}\] \[%{DATA:[apache][error][module]}:%{LOGLEVEL:[apache][error][level]}\] \[pid %{NUMBER:[apache][error][pid]}(:tid %{NUMBER:[apache][error][tid]})?\]( \[client %{IPORHOST:[apache][e
rror][client]}\])? %{GREEDYDATA:[apache][error][message1]}" ] }
        pattern_definitions => {
          "APACHE_TIME" => "%{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{YEAR}"
        }
        remove_field => "message"
      }
      mutate {
        rename => { "[apache][error][message1]" => "[apache][error][message]" }
      }
      date {
        match => [ "[apache][error][timestamp]", "EEE MMM dd H:m:s YYYY", "EEE MMM dd H:m:s.SSSSSS YYYY" ]
        remove_field => "[apache][error][timestamp]"
      }
    }
  }
}
output {
  elasticsearch {
    hosts => localhost
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  }
}
```

รูปที่ 14 แสดงConfiguration Logstash for Apache

Elasticsearch

เป็น Software ที่ทำหน้าที่ในการ ประมวลผล จัดการข้อมูลต่างๆที่มีการจัดหมวดหมู่มาแล้ว รวมถึงการQuery ผลลัพท์ต่างๆ ด้วยเนื่องจากเป็นส่วนประมวลผล การใช้งานทรัพยากรณ์ของ Softwareนี้จะมากกว่าส่วนอื่นๆ และหากService มีปัญหาจะส่งผลกับทั้งระบบทำให้อาจมีความจำเป็นต้องทำRedundant ให้กับ Serviceนี้ และการตั้งค่าส่วนของการใช้งาน Memory(Heap Usage) เป็นส่วนสำคัญที่จะส่งผลโดยตรงกับ Performance ของ Service

```
# JVM configuration

################################################################
## IMPORTANT: JVM heap size
################################################################
##
## You should always set the min and max JVM heap
## size to the same value. For example, to set
## the heap to 4 GB, set:
##
## -Xms4g
## -Xmx4g
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/current/heap-size.html
## for more information
##
################################################################

# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space

-Xms256m
-Xmx512m
```

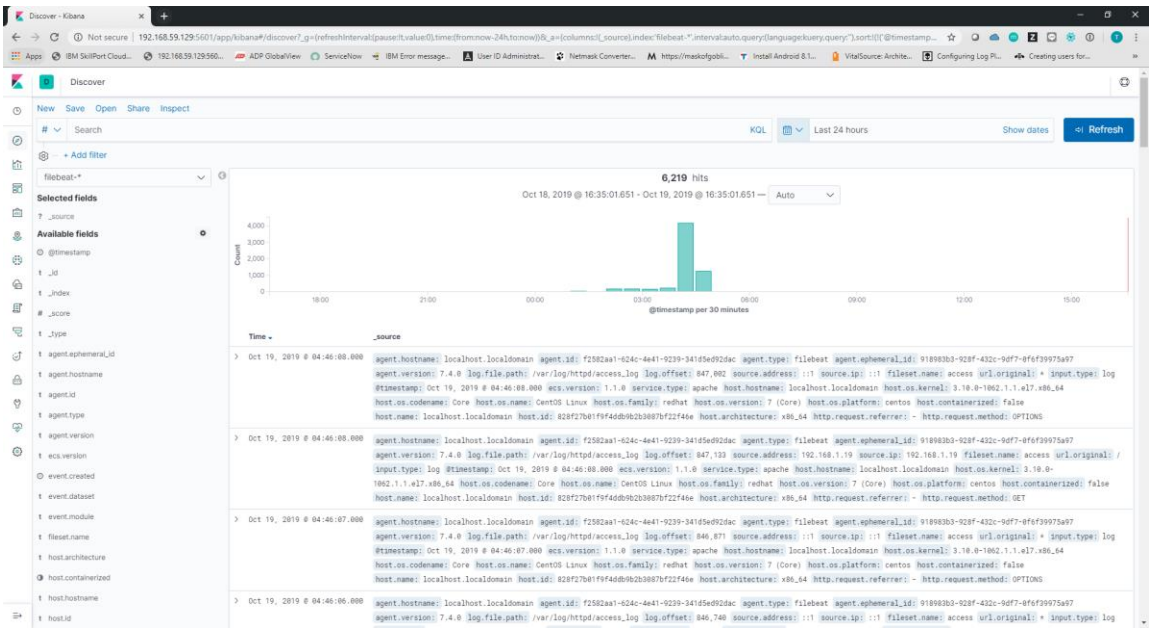
รูปที่ 15 แสดงConfiguration Heap Usage

```
## heap dumps

# generate a heap dump when an allocation from the Java heap fails
# heap dumps are created in the working directory of the JVM
-XX:+HeapDumpOnOutOfMemoryError

# specify an alternative path for heap dumps; ensure the directory exists and
# has sufficient space
-XX:HeapDumpPath=/var/lib/elasticsearch

# specify an alternative path for JVM fatal error logs
-XX:ErrorFile=/var/log/elasticsearch/hs_err_pid%p.log
```

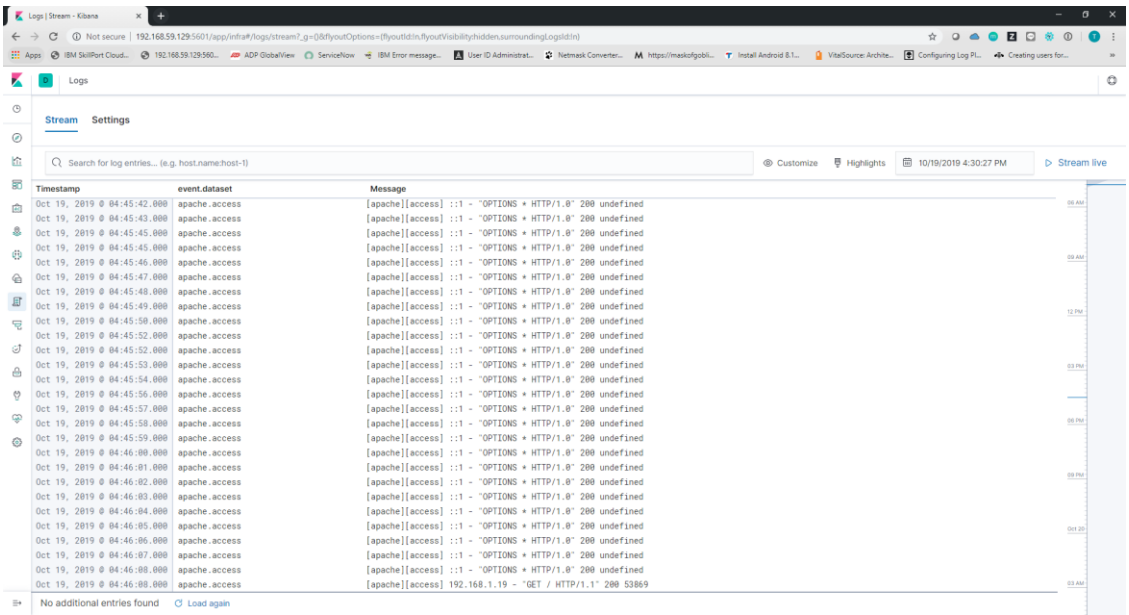
รูปที่ 16 แสดงConfiguration Heap Dump

Kibana

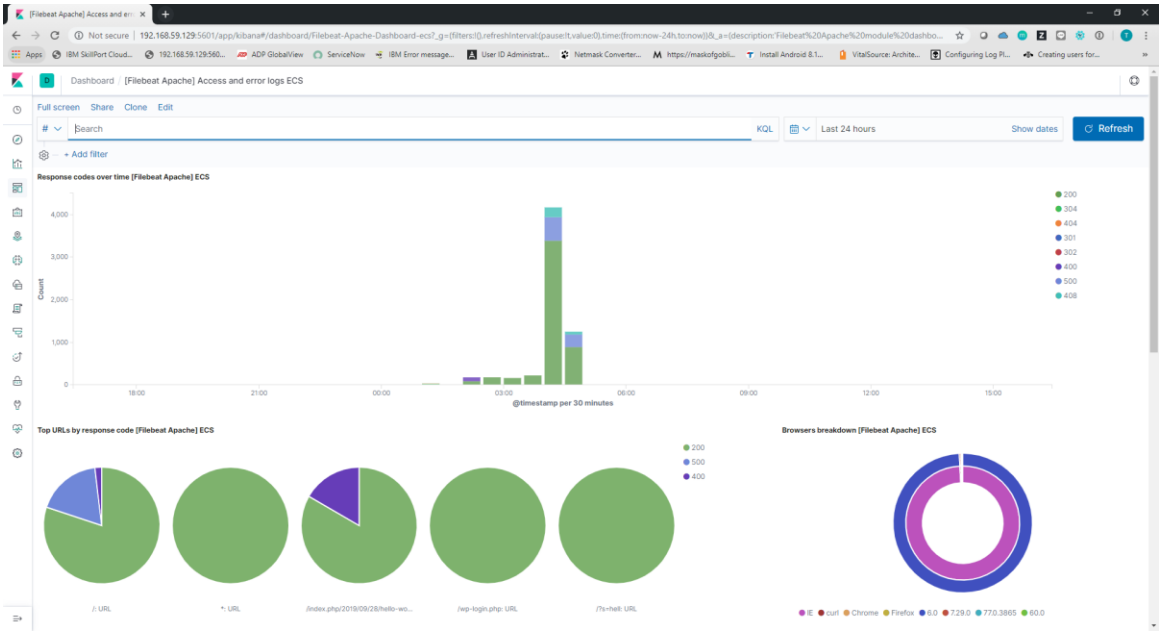
เป็น Software ส่วนที่ใช้แสดงผล และติดต่อกับผู้ใช้งานเป็นหลัก จำเป็นต้องทำงานควบคู่กับ Elasticsearch เพื่อใช้ในการรันQueryจากผู้ใช้งาน แสดงผลในรูปแบบกราฟต่างๆ การทำReport และ การทำAlertอีกด้วย



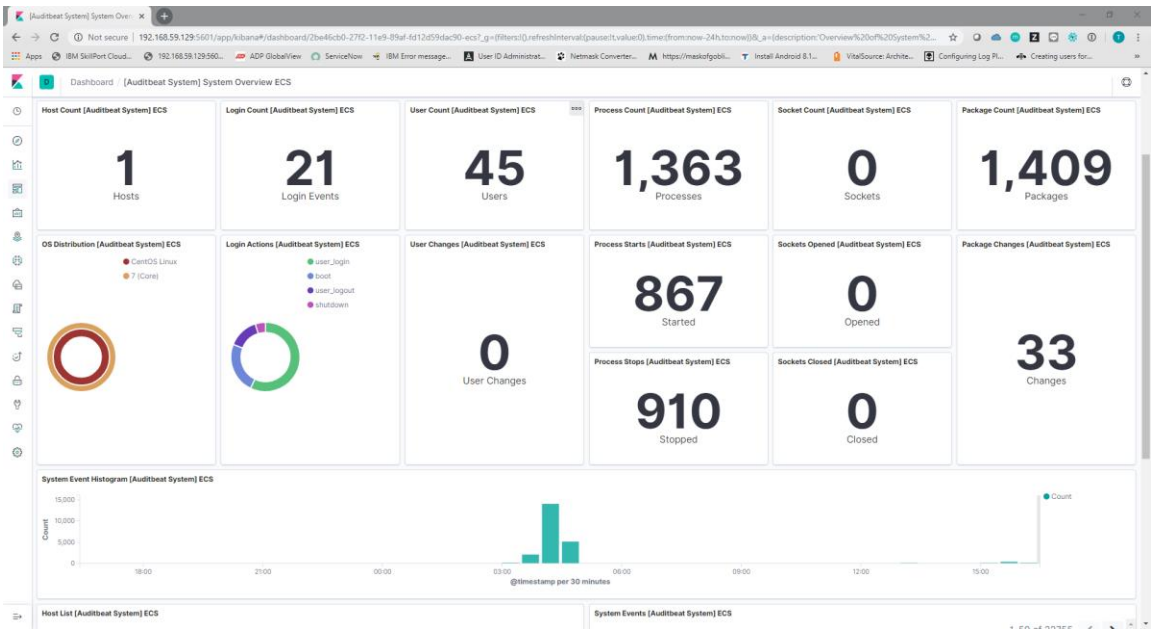
รูปที่ 17 แสดง Discover Dashboard



รูปที่ 18 แสดง Log Stream Page



รูปที่ 19 แสดง Apache Access and Error Dashboard



รูปที่ 20 แสดง Audit Dashboard

บทที่ 5

สรุปผลดำเนินโครงการ

5.1 กล่าวนำ

ในการดำเนินงานระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บเซิร์ฟเวอร์ ได้พัฒนาขึ้นเพื่อช่วยองค์กรที่ขาดความพร้อมในด้านอุปกรณ์หรือบุคลากรในการดำเนินงานเฝ้าระวังภัยคุกคาม สามารถเห็นภาพรวมการใช้งานของระบบทำให้สามารถพัฒนาการใช้งานทรัพยากรณ์ได้อย่างคุ้มค่า และสามารถป้องกันเหตุไม่ปกติต่างๆได้อย่างทันท่วงที รวมถึงนำข้อมูลต่างๆเหล่านี้ไปใช้งานต่อเพื่อการวาง Security Policy, Best Practice หรือ Hardening ระบบเพื่อปิดช่องโหว่ต่างๆที่พบ

5.2 สรุปผลการดำเนินโครงการ

โครงงานนี้ได้จัดทำเพื่อเฝ้าระวังและตรวจจับภัยคุกคาม เพื่อให้ผู้ดูแลระบบภายในองค์กรสามารถมองเห็นภาพรวมเกี่ยวกับใช้งานต่างๆของระบบในภาพรวมได้ รวมถึงประหยัดค่าใช้จ่ายเนื่องจากมีการนำ Software Open source ต่างๆมาประยุกต์ใช้งาน โดยสามารถสรุปได้ดังนี้

5.2.1 สามารถตรวจสอบการใช้งานของ Service Web Server ได้

5.2.2 สามารถตรวจสอบการใช้งานของ Host Web Server ได้

5.2.3 สามารถตรวจสอบการใช้งานของ Service Monitor ได้

5.2.4 สามารถจัดเก็บ ค้นหา และแสดงข้อมูลการใช้งานได้

5.3 แนวทางการพัฒนาในอนาคต

การพัฒนาระบบในอนาคตนั้นจะเน้นในเรื่องของการขยายการรองรับไปยัง Service รวมถึง Operating System อื่นๆ เนื่องด้วยองค์กรอาจมีการใช้งาน Service นอกเหนือจากWeb Server

ดังนั้นการพัฒนารูปแบบการส่งLog เก็บLog และแสดงผลให้เข้ากับองค์กรจึงเป็นเรื่องที่สำคัญ

เอกสารอ้างอิง

[1] Threat Modeling Concept [Online] Available:
https://www.owasp.org/index.php/Category:Threat_Modeling

[2] Security Operation center concept [Online] Available:
https://www.varonis.com/blog/security-operations-center-soc/

[3] Maturity Model concept [Online] Available:
https://www.pmi.org/learning/library/maturity-model-implementation-case-study-8882

[4] Learn Grok and working with Regular expression [Online] Available:
https://grokconstructor.appspot.com/

[5] Steps to install WordPress [Online] Available:
https://www.digitalocean.com/community/tutorials/how-to-install-wordpress-on-centos-7

[6] Elastic Stack SIEM Full Details provide [Online] Available:
https://www.elastic.co/products/siem