การพัฒนาระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือน การรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก*

Development of Monitoring, Intrusion Detection and Alert Systems for Cybersecurity Control in Army Cyber Center

เกียรติศักดิ์ ลุยทอง (Keaittisak Luithong)**
เอกฉัตร บ่ายคล้อย (Ekkachat Baikloy)***
ประสงค์ ปราณีตพลกรัง (Prasong Praneetpolgrang)****

บทคัดย่อ

การศึกษาวิจัยนี้ เพื่อเป็นการพัฒนาวิธีการเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยใช้เครื่องมือในการพัฒนาระบบได้แก่ ภาษา PHP สำหรับการพัฒนาแอปพลิเคชัน และโปรแกรม MySQL สำหรับจัดการฐานข้อมูล กลุ่มตัวอย่างที่ใช้ในการดำเนินการวิจัย มีจำนวน 3 กลุ่ม คือ กลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์ กลุ่มผู้บังคับบัญชาภายในศูนย์ไซเบอร์ และกลุ่มผู้ใช้งานระบบภายในศูนย์ไซเบอร์กองทัพบก ผลการวิจัยพบว่า ได้ ระบบและแอปพลิเคชันสำหรับเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ในศูนย์ไซเบอร์กองทัพบก ทั้งนี้ การประเมินด้านความเหมาะสมของระบบที่ได้พัฒนาขึ้นโดยกลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์และเครือข่าย และการประเมินโดยผู้บังคับบัญชาพบว่ามีค่าความเหมาะสมเฉลี่ยอยู่ในระดับมากที่สุด ในขณะเดียวกันการประเมินประสิทธิภาพการใช้งานโดยกลุ่มผู้ใช้พบว่ามีค่าเฉลี่ยอยู่ในระดับมาก ทั้งนี้ แสดงให้เห็นว่าระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสม และสามารถตอบสนองการทำงานของผู้ใช้ได้ในทุกระดับ

คำสำคัญ : ระบบเฝ้าระวังภัยคุกคาม, ตรวจหาการบุกรุก, ความมั่นคงปลอดภัยไซเบอร์

---

* บทความวิจัยนี้นำเสนอวิธีการเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยทำการพัฒนาแอปพลิเคชันให้ผู้ที่ทำงานในศูนย์ไซเบอร์กองทัพบกได้ใช้ประโยชน์ เพื่อให้การทำงานมีประสิทธิภาพมากขึ้น ซึ่งระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสมต่อการใช้งานจริง อีกทั้งสามารถตอบสนองการทำงานของผู้ใช้ได้ในทุกระดับ

** นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตศึกษา มหาวิทยาลัยศรีปทุม
(Student, Master of Science in Information Technology, Sripatum University, email: keaittisuk@gmail.com)
*** นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตศึกษา มหาวิทยาลัยศรีปทุม
(Student, Doctor of Philosophy in Information Technology, Sripatum University, email: ekkachat@epit.co.th)
**** ศาสตราจารย์ ดร. ประจำบัณฑิตศึกษา คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีทุม
(Professor Dr., Graduate School, Faculty of Information Technology, Sripatum University, email: prasongspu@gmail.com)

Veridian E-Journal, Science and Technology Silpakorn University
Volume 5 Number 5 September – October 2018 ISSN 2408 - 1248

Abstract

The purpose of this research is to development of monitoring, intrusion detection and alert systems for cybersecurity control in Army Cyber Center. Tools used for developing the system are: PHP language to develop the duplication and MySQL program used to manage the database. The representative samples used as a base for the research are made up of 3 groups of people such as software professionals, commander in army cyber center and officers from the army cyber center who use the system. The system evaluation result from the software and network experts and the commander agree on the system with the most suitable. In addition, the efficiency assessment carried out by the users found it to be in high level. It shows that the system is suitable and responds to the needs and purposes of the users on every level.

Keywords: Threat Monitoring Systems, Intrusion Detection, Cybersecurity

บทนำ

ศูนย์ไซเบอร์กองทัพบก เป็นหน่วยขึ้นตรงกองทัพบก ปฏิบัติหน้าที่เป็นฝ่ายกิจการพิเศษ โดยมีภารกิจที่สำคัญ คือ การรักษาความมั่นคงปลอดภัยไซเบอร์ การปฏิบัติการไซเบอร์ การใช้ประโยชน์ไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร และการพัฒนาความพร้อมด้านไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ การประเมินช่องโหว่ของระบบสารสนเทศการเฝ้าระวัง ตรวจสอบ วิเคราะห์ด้านไซเบอร์และข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคงของหน่วยงานภายในกองทัพบก (ฤทธี อินทราวุธ, 2557)

การจัดเก็บสถิติภัยคุกคามทางไซเบอร์และรายงานผลสถิติภัยคุกคามทางไซเบอร์ ศูนย์ไซเบอร์กองทัพบกได้จัดเก็บสถิติภัยคุกคามเป็นเอกสาร ในการนำเสนอให้ผู้บังคับบัญชา เพื่อมอบนโยบายสั่งการตรวจสอบหาแหล่งที่มาของภัยคุกคามทางไซเบอร์ และเก็บเอกสารเข้าแฟ้มเอกสารเมื่อการดำเนินการแล้วเสร็จ โดยวิธีดังกล่าวอาจเป็นสาเหตุให้เอกสารสำคัญตกหล่น หรือชำรุดสูญหายได้ ด้วยการทำงานที่ซ้ำซ้อน อาจทำให้การตรวจสอบเป็นไปอย่างล่าช้า และผิดพลาดบ่อยครั้ง ทำให้ส่งผลเสียต่อระบบสารสนเทศของศูนย์ไซเบอร์กองทัพบกและกองทัพบกโดยภาพรวม เพื่อเป็นการแก้ปัญหาที่เกิดขึ้นผู้วิจัยจึงได้มีแนวคิดที่จะพัฒนาวิธีการเฝ้าระวังภัยคุกคาม และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก เพื่อเป็นมาตรการในการป้องกันภัยคุกคามทางไซเบอร์ และลดขั้นตอนการทำงานของผู้ปฏิบัติงานที่เกี่ยวข้อง ซึ่งจะช่วยอำนวยความสะดวกในการจัดเก็บสถิติภัยคุกคาม และการระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ อีกทั้งสามารถช่วยสนับสนุนการตัดสินใจของผู้บริหารของศูนย์ไซเบอร์กองทัพบก ทางด้านการจัดการภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้นต่อไป

วัตถุประสงค์ในการวิจัย

ผู้วิจัยได้กำหนดวัตถุประสงค์ในการวิจัยไว้จำนวน 4 ข้อ ดังนี้

1. เพื่อศึกษาบริบท ปัญหาและสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ ภายในศูนย์ไซเบอร์กองทัพบก

2. เพื่อพัฒนาวิธีการเฝ้าระวังภัยคุกคาม และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก

3. เพื่อพัฒนาแอปพลิเคชันสำหรับการเฝ้าระวังภัยคุกคาม และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก

4. เพื่อทำการประเมินระบบเฝ้าระวังภัยคุกคาม และแจ้งเตือน ระดับความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก

ขอบเขตในการวิจัย

1. ผู้วิจัยเน้นพัฒนาแอปพลิเคชันสำหรับการเฝ้าระวังภัยคุกคาม และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์กองทัพบก

2. กำหนดมาตรฐาน เกณฑ์การเฝ้าระวังภัยคุกคาม และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในกองทัพบก

ประโยชน์ที่ได้รับจากการวิจัย

1. ได้ทราบถึง แนวทาง และขั้นตอน การสร้างความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์
2. ได้ระบบที่ช่วยเพิ่มประสิทธิภาพในการเฝ้าระวังภัยคุกคามทางไซเบอร์ในศูนย์ไซเบอร์กองทัพบก
3. ทำให้ได้แอปพลิเคชันสำหรับทำการประเมินระดับความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์
4. ทำให้กำลังพลได้มีความรู้ด้านไซเบอร์และสามารถปฏิบัติภารกิจบนหลักการที่พึ่งพาตนเองได้

วิธีดำเนินการวิจัย

การพัฒนาระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก มีขั้นตอนในการดำเนินการวิจัย 4 ขั้นตอน ดังต่อไปนี้

1. ศึกษางานระบบงานเดิม

ผู้วิจัยได้ศึกษาปัญหาจากระบบที่มีอยู่เดิม พบว่า ศูนย์ไซเบอร์กองทัพบกได้จัดเก็บสถิติข้อมูลภัยคุกคามเป็นเอกสาร อาจทำให้เกิดความคลาดเคลื่อน ล่าช้า และซ้ำซ้อน อาจเป็นเหตุให้เอกสารเกิดการชำรุดหรือสูญหายขอเอกสารสำคัญได้ โดยวงจรการทำงานของระบบงานเดิมนั้น มีดังนี้

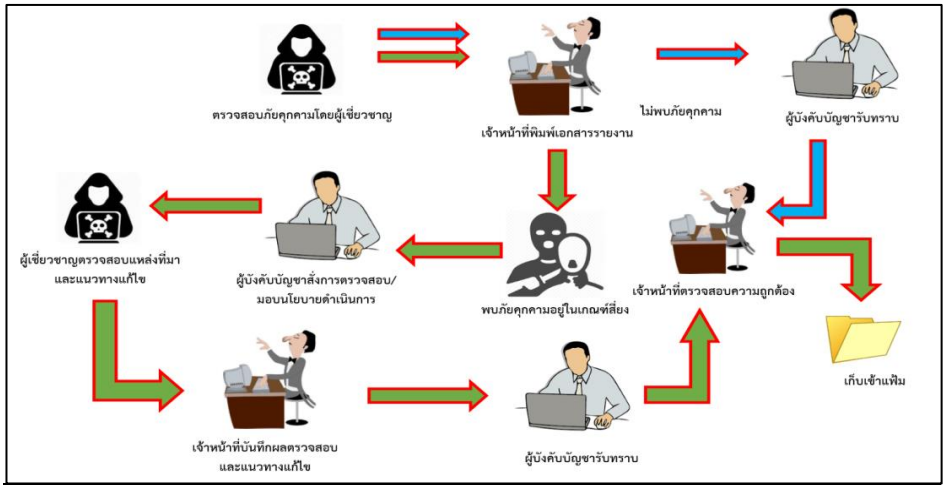
1) การตรวจสอบภัยคุกคาม จะมีผู้เชี่ยวชาญทางด้านไซเบอร์มาทำการตรวจสอบ และส่งผลการตรวจสอบให้เจ้าหน้าที่เพื่อรวบรวมสถิติ พิมพ์รายงาน นำเสนอผู้บังคับบัญชา เพื่อรับทราบและสั่งการเมื่อจบกระบวนการจึงเก็บเข้าแฟ้มเอกสาร ซึ่งกระบวนดังกล่าว อาจทำให้เกิดความผิดพลาดหรือตกหล่นสูญหายของเอกสารสำคัญได้

Veridian E-Journal, Science and Technology Silpakorn University
Volume 5 Number 5 September – October 2018 ISSN 2408 - 1248

2) เอกสารการตรวจสอบภัยคุกคามทางไซเบอร์นั้น ถือเป็นเอกสารที่มีอยู่ในชั้นลับที่สุด หากเอกสารหรือรั่วไหลออกไป อาจจะทำให้เกิดความเสียหายต่อศูนย์ไซเบอร์กองทัพบก และกองทัพบกโดยภาพรวม

3) การเก็บสถิติแบบเดิม ไม่สามารถสนับสนุนการตัดสินใจของผู้บังคับบัญชาทางด้านการตรวจสอบภัยคุกคามทางไซเบอร์ของศูนย์ไซเบอร์กองทัพบกได้

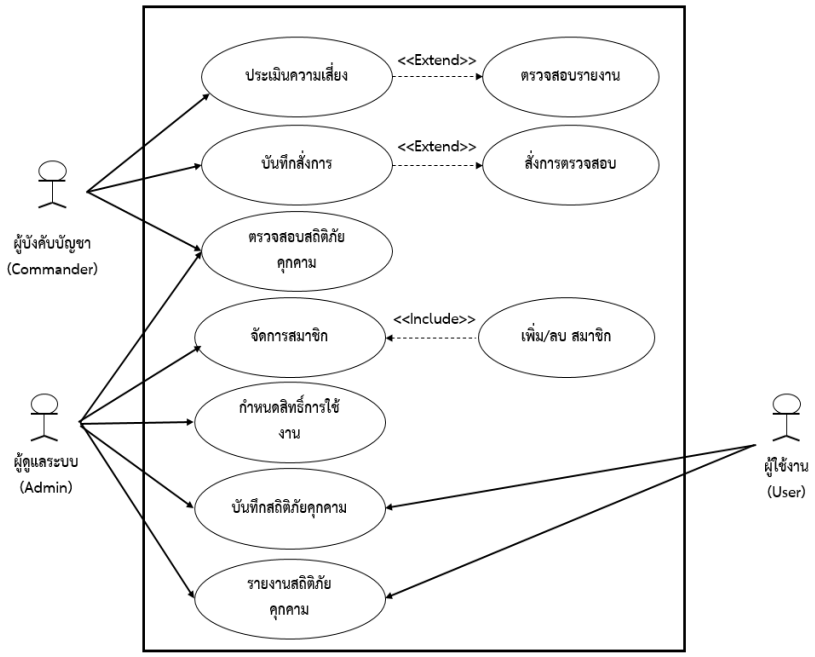
4) การตรวจสอบชนิด ประเภท แหล่งที่มาของภัยคุกคามโดยผู้เชี่ยวชาญ หากมีการตรวจพบภัยคุกคามทางไซเบอร์ซึ่งอาจทำให้ระบบสารสนเทศเกิดความเสียหายแล้วนั้น ผู้บังคับบัญชาจะต้องมีการแจ้งให้ผู้เชี่ยวชาญได้ทำการตรวจสอบ และส่งให้เจ้าหน้าที่ได้ทำการบันทึกรายงานให้ผู้บังคับบัญชาได้รับทราบและแนวทางในการแก้ไข หากเจ้าหน้าที่ไม่สามารถปฏิบัติงานได้ในขณะนั้น หรือไม่สามารถทำงานทดแทนกันได้ หรือขาดความชำนาญในการปฏิบัติงาน จะทำให้เอกสารล่าช้าออกไป ซึ่งอาจจะเกิดผลเสียต่อระบบสารสนเทศที่ต้องมีการแก้ไขอย่างเร่งด่วนได้ วงจรการทำงานของระบบงานเดิม ตามภาพที่ 1



ภาพที่ 1 วงจรการทำงานของระบบงานเดิม

2. การวิเคราะห์และออกแบบระบบ

ผู้วิจัยจึงได้ทำการวิเคราะห์และออกแบบระบบงานใหม่ เพื่อให้สอดคล้องกับการใช้งาน และภารกิจของศูนย์ไซเบอร์กองทัพบกโดยระบบงานใหม่ที่ได้ออกแบบนั้น ใช้หลักการวิเคราะห์และออกแบบเชิงวัตถุด้วยภาษา UML (Unified Modeling Language) ในการออกแบบระบบ ซึ่งประกอบด้วย 1) ผู้บังคับบัญชา (Commander) 2) ผู้ดูแลระบบ (Admin) 3) ผู้ใช้งาน (User) ดังภาพที่ 2



ภาพที่ 2 การออกแบบยูสเคสไดอะแกรมของระบบงานใหม่

จากการออกแบบระบบ ผู้วิจัยได้ทำการแบ่งสิทธิ์การใช้งานของผู้ใช้งานระบบเป็น 3 ระดับ ดังนี้

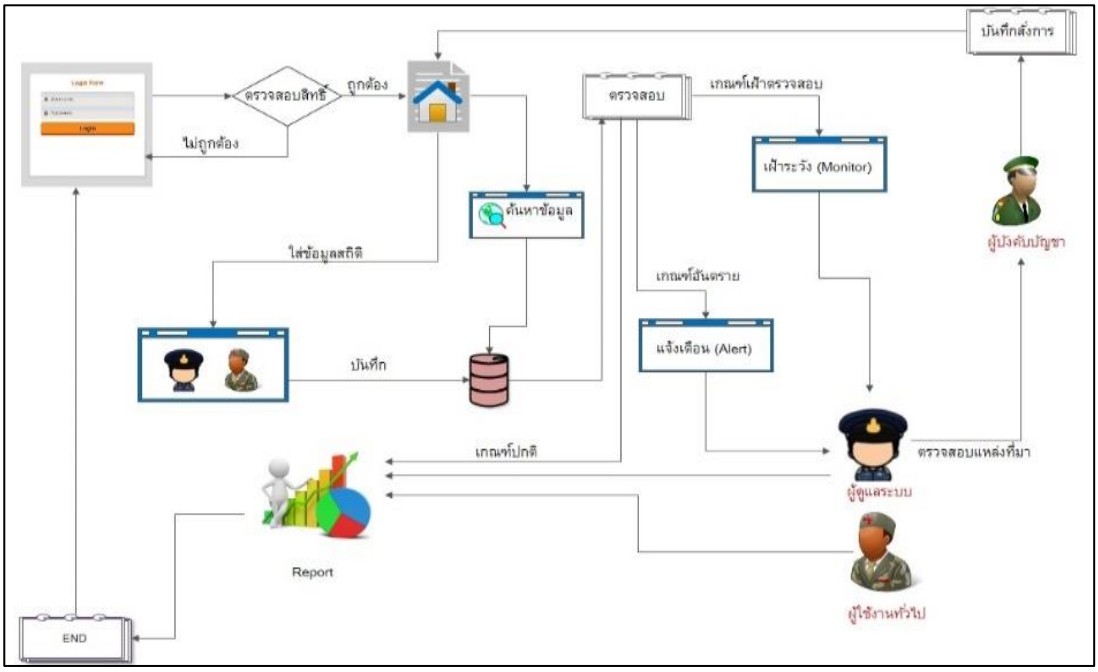
1) ผู้บังคับบัญชา (**Commander**) จะมีสิทธิ์ในการทำหน้าที่ ประเมินความเสี่ยงของภัยคุกคาม ตรวจสอบสถิติภัยคุกคาม และบันทึกสั่งการ/สั่งการตรวจสอบ

2) ผู้ดูแลระบบ (**Admin**) จะมีสิทธิ์และหน้าที่ ตรวจสอบสถิติภัยคุกคาม จัดการสมาชิก กำหนดสิทธิ์ผู้ใช้งาน บันทึกสถิติภัยคุกคาม และรายงานสถิติภัยคุกคาม

3) ผู้ใช้งาน **(User)** จะมีสิทธิ์และหน้าที่ บันทึกสถิติภัยคุกคาม รายงานผลการบันทึกสถิติภัยคุกคาม

เพื่อให้เกิดความเข้าใจในภาพรวมของระบบ ผู้วิจัยจึงแสดงออกแบบวงจรการทำงานของระบบงานใหม่ ดังภาพที่ 3

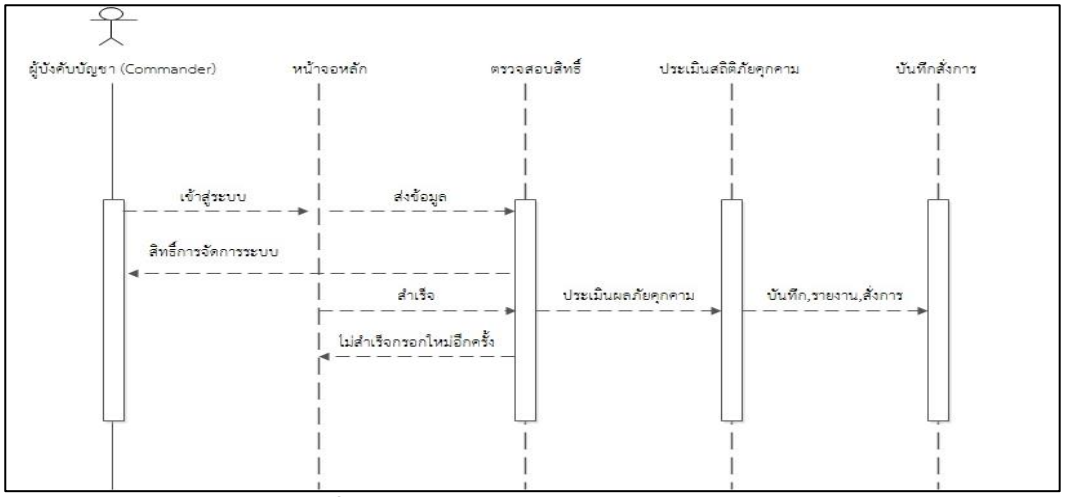
Veridian E-Journal, Science and Technology Silpakorn University
Volume 5 Number 5 September – October 2018 ISSN 2408 - 1248



ภาพที่ 3 ภาพวงจรการทำงานของระบบงานใหม่

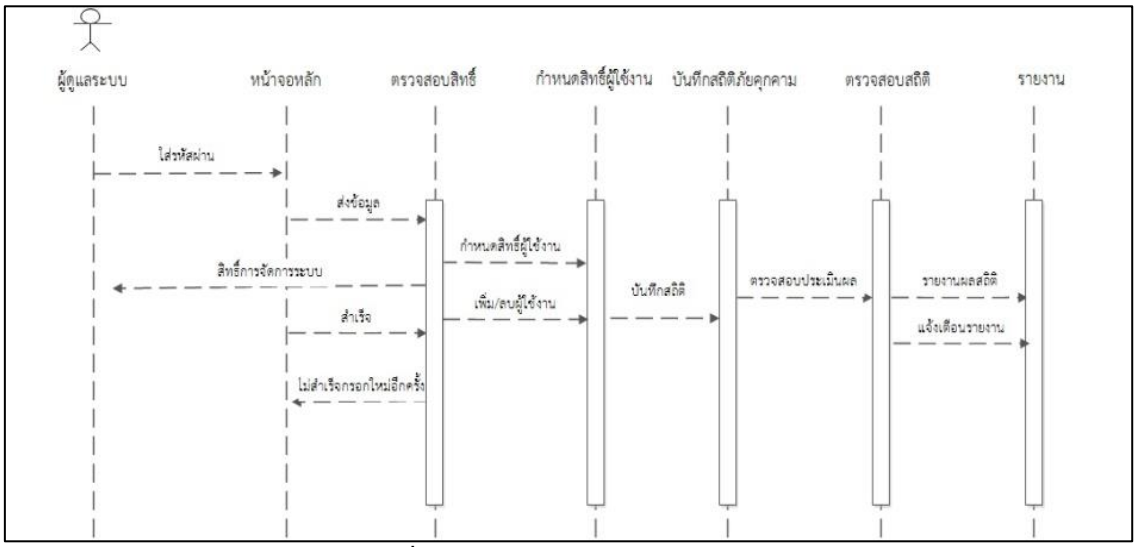
โดยการจัดการข้อมูลในแต่ละระดับสิทธิ์นั้น สามารถดำเนินการได้ดังนี้

1) ผู้บังคับบัญชา (Commander) จะสามารถตรวจสอบความเสี่ยง การประเมินความเสี่ยงของภัยคุกคามการบันทึกสั่งการตามภัยคุกคามที่ตรวจพบ และ มอบนโยบายการตรวจสอบ ดังภาพที่ 4



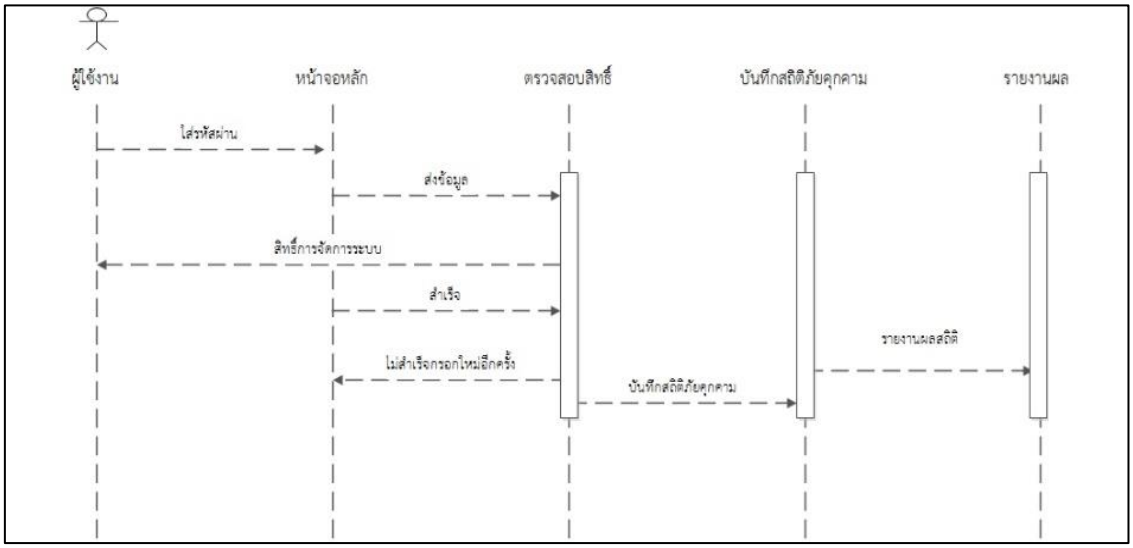
ภาพที่ 4 การจัดการข้อมูลของผู้บังคับบัญชา

2) ผู้ดูแลระบบ (Admin) จะสามารถจัดการระบบ กำหนดสิทธิ์ผู้ใช้งาน เพิ่ม/ลบสมาชิก ตรวจสอบสถิติ ภัยคุกคาม และรายงานสถิติภัยคุกคามให้ผู้บังคับบัญชารับทราบ ดังภาพที่ 5



ภาพที่ 5 การจัดการข้อมูลของผู้ดูแลระบบ

3) ผู้ใช้งาน (USER) จะสามารถ บันทึกสถิติภัยคุกคาม รายงานผลการบันทึกสถิติภัยคุกคาม ดังภาพที่ 6



ภาพที่ 6 การจัดการข้อมูลของผู้ใช้งาน

3. การพัฒนาระบบงานใหม่

จากการวิเคราะห์และออกแบบระบบงานใหม่ ผู้วิจัยจึงได้ทำการพัฒนาระบบงานขึ้นตามการวิเคราะห์และออกแบบระบบงาน โดยจะมีส่วนประกอบหลักๆ ที่สำคัญได้แก่ 1) ส่วนของการบันทึกสถิติภัยคุกคามทางไซเบอร์ และ 2) ส่วนการรายงานสถิติภัยคุกคามทางไซเบอร์ และ 3) ส่วนการแจ้งเตือนภัยคุกคามทางไซเบอร์ โดยการออกแบบระบบผู้วิจัยได้ใช้ภาษา PHP และ MySQL เป็นเครื่องมือในการพัฒนาระบบ

Veridian E-Journal, Science and Technology Silpakorn University
Volume 5 Number 5 September – October 2018 ISSN 2408 - 1248

4. การประเมินผลระบบ

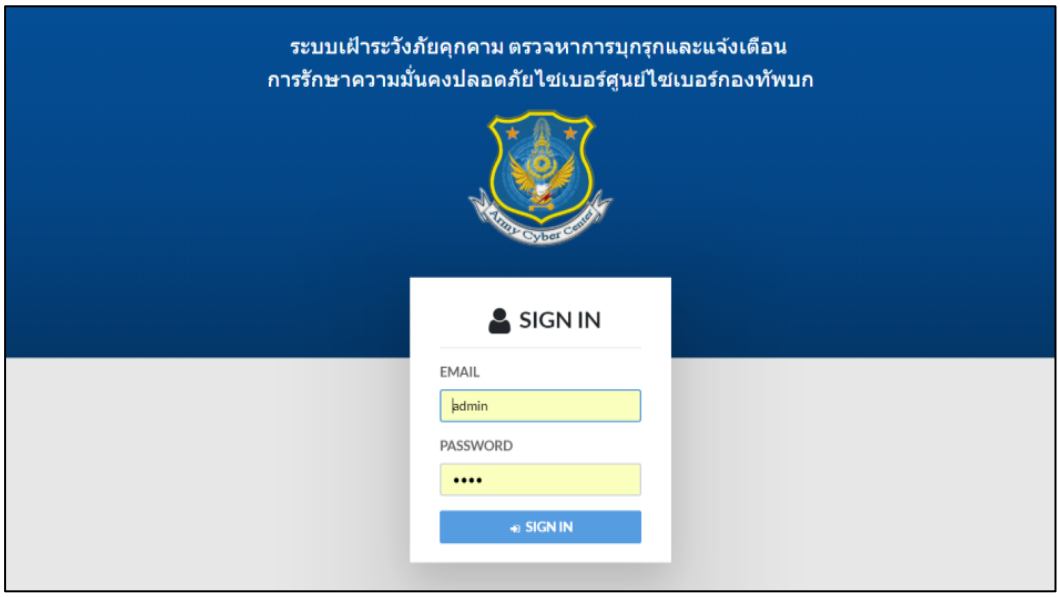
เพื่อให้เกิดการสมบูรณ์ของระบบ ผู้วิจัยจึงนำระบบนี้ไปทดสอบความเหมาะสมของระบบโดยผู้เชี่ยวชาญซอฟต์แวร์ และประสิทธิภาพการใช้งานโดยผู้บังคับบัญชาของศูนย์ไซเบอร์กองทัพบก และผู้ใช้งานระบบ โดยการทดสอบความเหมาะสมของระบบโดยผู้เชี่ยวชาญซอฟต์แวร์นั้น จะประเมิน 5 ด้าน ได้แก่ 1) ความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งาน 2) ความเหมาะสมด้านความถูกต้องของการออกแบบระบบ 3) ความเหมาะสมในการใช้งานของระบบ 4) ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย 5) ความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้การประเมินประสิทธิภาพการใช้งานระบบโดยผู้บังคับบัญชา จะมีการประเมิน 5 ด้าน ได้แก่ 1) ด้านการออกแบบการใช้งาน 2) ด้านการบันทึกและการแก้ไขข้อมูล 3) ด้านการประมวลผลและการแสดงผล 4) ด้านการสืบค้นข้อมูล และการรายงาน 5) ด้านประสิทธิภาพการใช้งานของระบบ และการประเมินประสิทธิภาพการใช้งานระบบโดยผู้ใช้งาน จะมีการประเมิน 5 ด้าน ได้แก่ 1) ด้านการออกแบบการใช้งาน 2) ด้านการบันทึกและการแก้ไขข้อมูล 3) ด้านการประมวลผลและการแสดงผล 4) ด้านการสืบค้นข้อมูล และการรายงาน และ 5) ด้านประสิทธิภาพการใช้งานของระบบ

ผลการวิจัย

จากการพัฒนาระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุกแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก เพื่อเป็นการศึกษาปัญหา และสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก และพัฒนาการเฝ้าระวังภัยคุกคาม และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก พบว่าเป็นไปตามวัตถุประสงค์หลักของงานวิจัย และสอดคล้องกับภารกิจของศูนย์ไซเบอร์กองทัพบก โดยผลการวิจัยนั้นผู้วิจัยจะนำเสนอ เป็น 2 ส่วน คือ 1) ผลจากการพัฒนาระบบ และ 2) ผลจากการประเมินผลระบบดังนี้

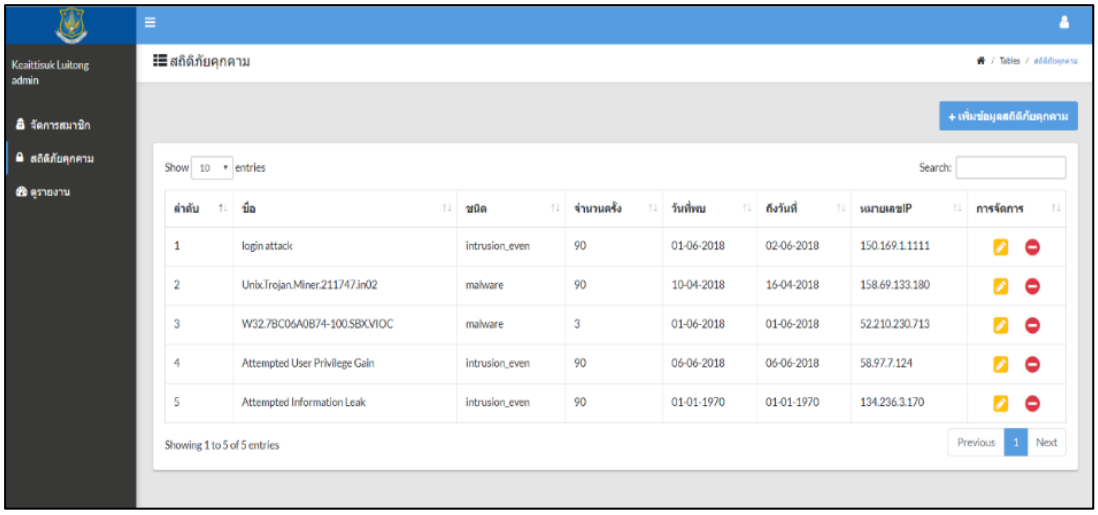
1. ผลจากการพัฒนาระบบ ระบบที่พัฒนาขึ้นมานั้น มีการทำงานหลายส่วน ซึ่งจะแสดงในขั้นตอนกระบวนการทำงานที่สำคัญ ดังนี้

1.1 การเข้าสู่ระบบ เป็นหน้าแรกในการเข้าใช้งานระบบเฝ้าสังเกต ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยผู้วิจัยได้แบ่งสิทธิ์การใช้งานออกเป็น 3 ระดับ ได้แก่ 1) ผู้บังคับบัญชา (Commander) 2) ผู้ดูแลระบบ (Admin) และ 3) ผู้ใช้งาน (User) ดังภาพที่ 7



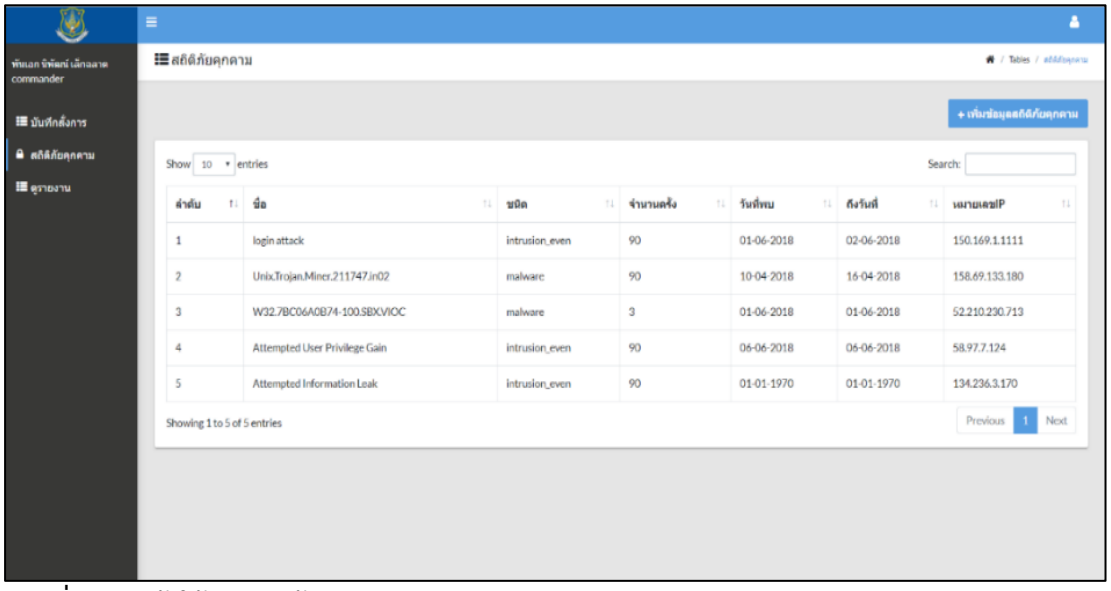
ภาพที่ 7 หน้า Log-in เพื่อเข้าสู่ระบบ

1.2 การใช้งานระบบของแต่ละสิทธิ์การใช้งาน ได้แก่ 1) ผู้ดูแลระบบ มีสิทธิ์ในการเพิ่ม/ลบ และแก้ไขภัยคุกคาม และ 2) ผู้บังคับบัญชา (Commander) และผู้ใช้งาน (User) จะสามารถเพิ่มข้อมูลภัยคุกคามเพียงอย่างเดียว ไม่มีสิทธิ์ในการลบและแก้ไขข้อมูลสถิติภัยคุกคาม ดังภาพที่ 8-10

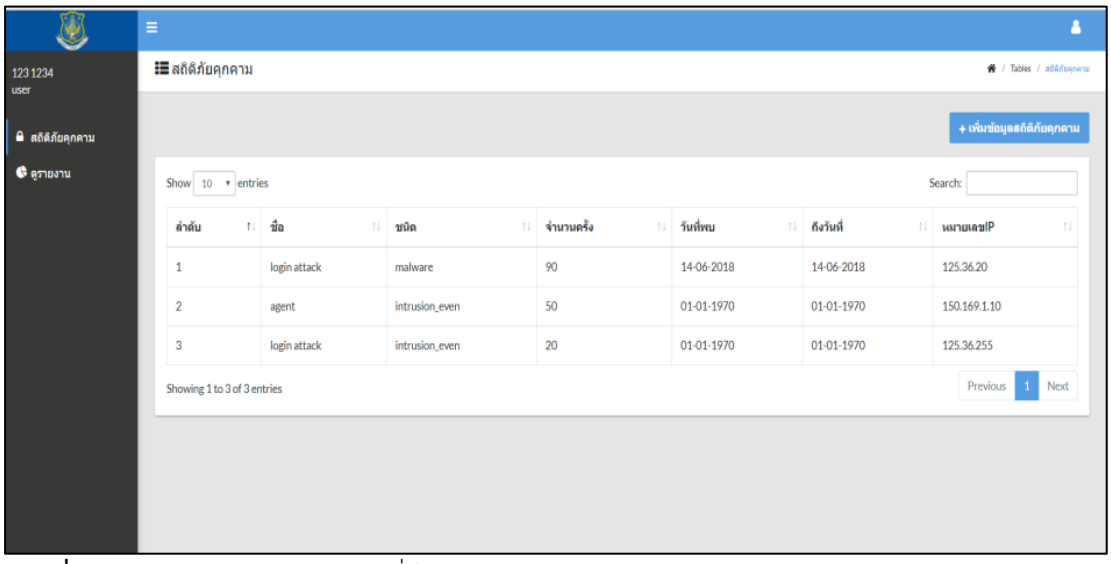


ภาพที่ 8 การเข้าใช้งานของผู้ดูแลระบบ (Admin)

Veridian E-Journal, Science and Technology Silpakorn University
Volume 5 Number 5 September – October 2018 ISSN 2408 - 1248



ภาพที่ 9 การเข้าใช้งานของผู้บังคับบัญชา (Commander)



ภาพที่ 10 การเข้าใช้งานของผู้ใช้งานทั่วไป (User)

1.3 การตรวจจับภัยคุกคามทางไซเบอร์และการแสดงผลภัยคุกคามทางไซเบอร์

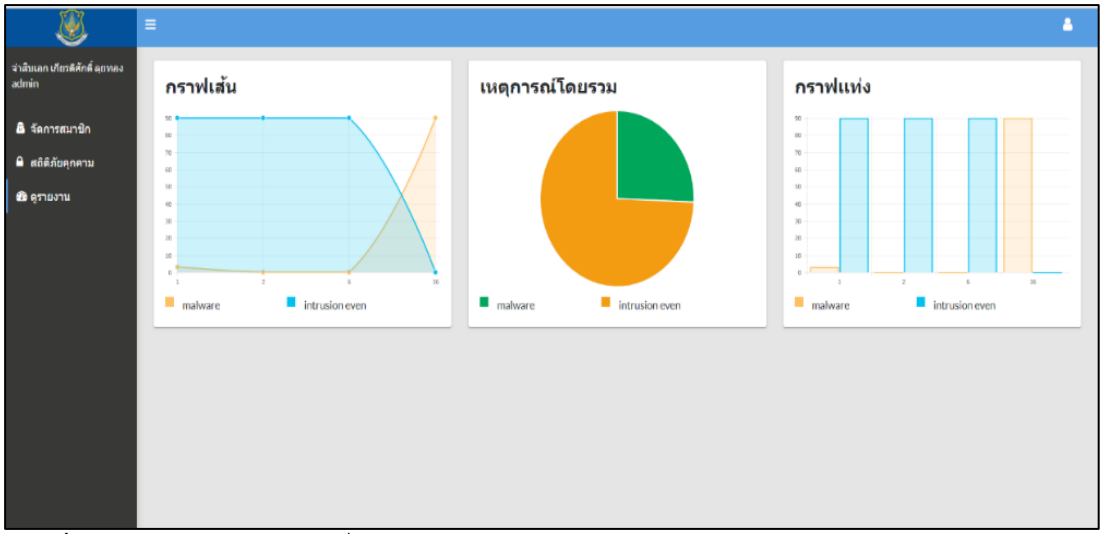
1.3.1 การตรวจจับภัยคุกคามทางไซเบอร์ ระบบจะทำการตรวจจับภัยคุกคามทางไซเบอร์ 2 ชนิด ได้แก่

1.3.1.1) Malware หรือ Malicious Software โปรแกรมประสงค์ร้ายต่างๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล

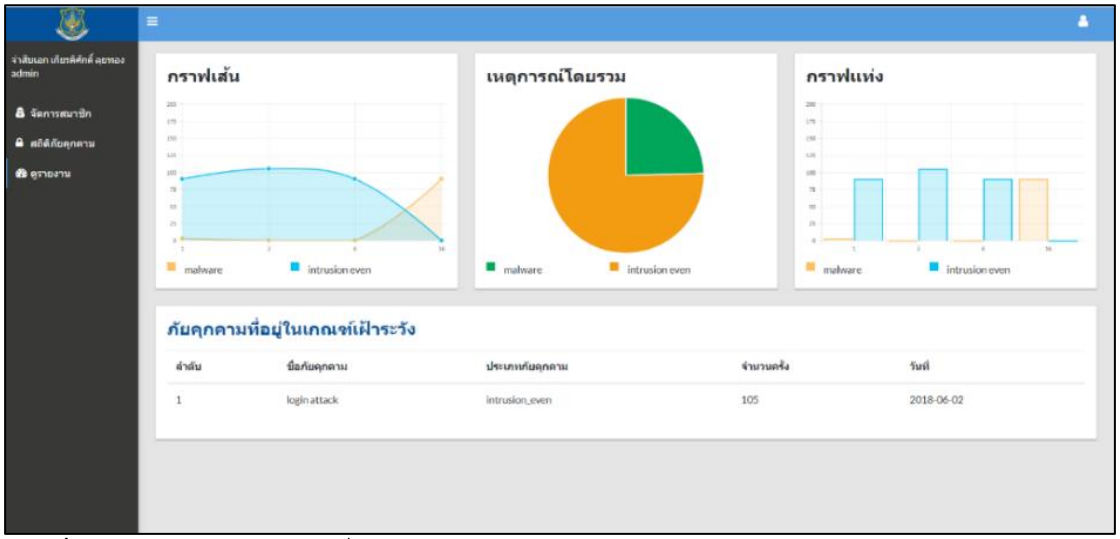
1.3.1.2) Intrusion หรือ พฤติกรรมหรือความพยายามที่จะบุกรุกเครือข่าย

1.3.2 การแจ้งเตือนและการแสดงผลภัยคุกคาม ระบบได้มีการแจ้งเตือนและแสดงผลภัยคุกคามทางไซเบอร์ เป็นกราฟสถิติ แสดงผลใน 3 ระดับ ได้แก่ 1) ภัยคุกคามที่อยู่ในเกณฑ์ปกติ 2) ภัยคุกคามที่

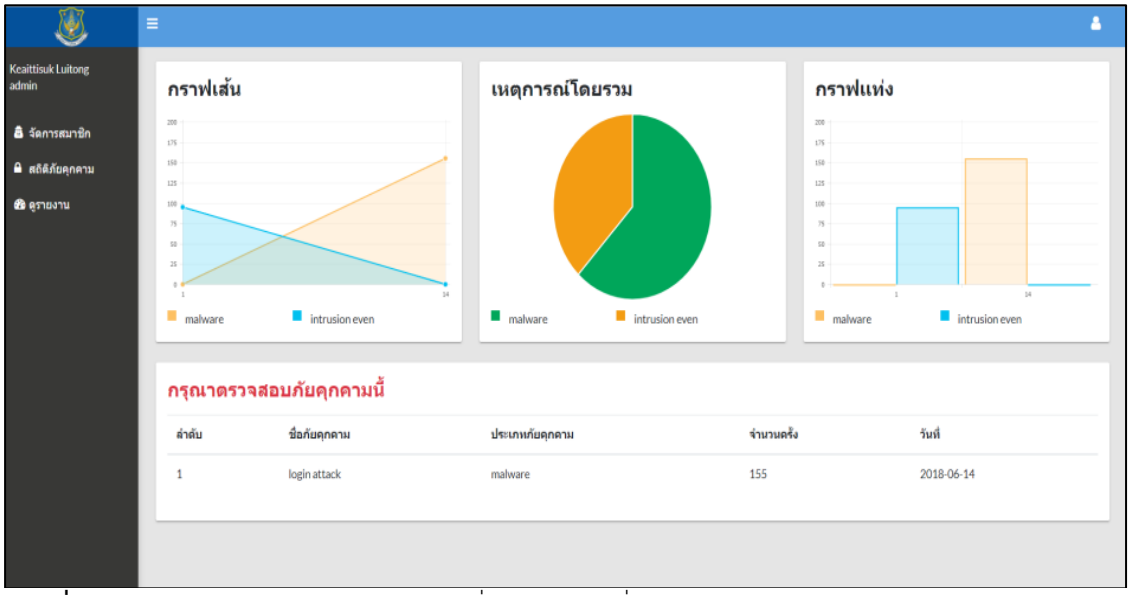
อยู่ในเกณฑ์เฝ้าระวัง หรือภัยคุกคามที่ตรวจพบ แต่อาจอยู่ในเกณฑ์ที่จะเพิ่มปริมาณถึงขั้นก่อให้เกิดผลเสียต่อระบบจะมีการแจ้งเตือนเป็นเกณฑ์ภัยคุกคามที่อยู่ในเกณฑ์เฝ้าระวัง เพื่อให้ผู้ที่เกี่ยวข้องทำการเฝ้าระวังภัยคุกคามในชนิดนั้น และ 3) ภัยคุกคามที่มีปริมาณมาก อาจส่งผลเสียต่อความปลอดภัยของระบบสารสนเทศ จะแจ้งเตือนว่ากรุณาตรวจสอบภัยคุกคามนี้ เพื่อให้ผู้ที่เกี่ยวข้องได้ทำการตรวจสอบภัยคุกคามที่พบเพื่อตรวจสอบแหล่งที่มาของภัยคุกคามและแนวทางแก้ไข เพื่อนำเสนอให้ผู้บังคับบัญชาทราบและสั่งการโดยผู้วิจัยได้ทำการออกแบบระบบเพื่อให้ระบบทำการบันทึกภัยคุกคามที่ตรวจพบ ทั้ง 2 ประเภท ที่มีพฤติกรรมกระทำซ้ำๆ กัน ในแต่ละเหตุการณ์ อยู่ที่ 100 – 149 ครั้ง/วัน/เหตุการณ์ ระบบจะทำการเฝ้าระวัง และตั้งแต่ 150 ครั้ง/วัน/เหตุการณ์ขึ้นไป ระบบจะทำการแจ้งเตือนภัยคุกคามทันที ดังภาพที่ 11 - 13



ภาพที่ 11 ภาพแสดงภัยคุกคามที่อยู่ในเกณฑ์ปกติ

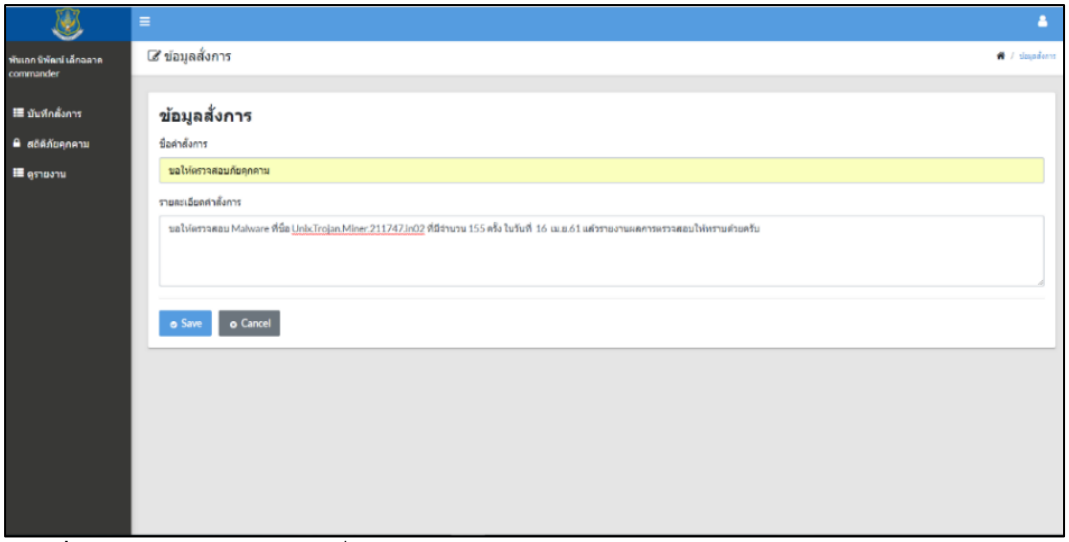


ภาพที่ 12 ภาพแสดงภัยคุกคามที่อยู่ในเกณฑ์เฝ้าระวัง

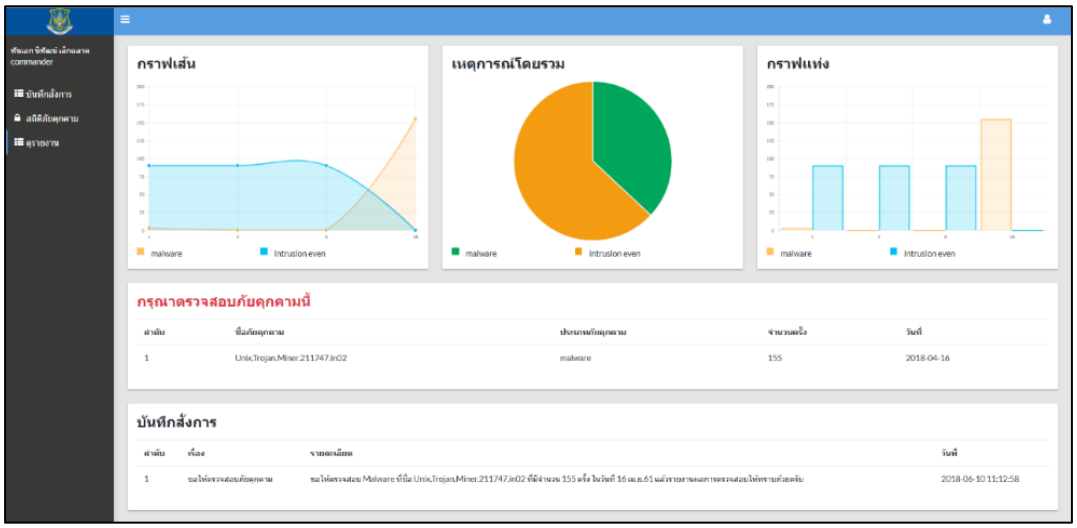


ภาพที่ 13 ภาพแสดงการตรวจพบภัยคุกคามที่อยู่ในเกณฑ์เสี่ยงต่อความปลอดภัยของระบบสารสนเทศ

1.4 การบันทึกสั่งการของผู้บังคับบัญชา จะทำการบันทึกสั่งการในกรณีที่มีการตรวจพบภัยคุกคามที่อยู่ในเกณฑ์เสี่ยง หรือสั่งการเรื่องอื่นๆ ที่เกี่ยวข้องกับระบบ ผู้พัฒนาระบบได้ออกแบบการบันทึกสั่งการของผู้บังคับบัญชา ให้สามารถสั่งการและแสดงผลผ่านเว็บแอปพลิเคชัน ดังภาพที่ 14-15



ภาพที่ 14 ภาพแสดงการบันทึกสั่งการของผู้บังคับบัญชาผ่านทางระบบ



ภาพที่ 15 ภาพแสดงการสั่งการของผู้บังคับบัญชาผ่านทางระบบ

2. การประเมินระบบ ผู้วิจัยได้ทำการประเมินระบบ โดยมีวิธีการประเมินดังนี้

2.1 ประชากรและกลุ่มตัวอย่าง

2.1.1) ผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 ท่าน สำหรับการประเมินความเหมาะสมของระบบ โดยผู้เชี่ยวชาญทางด้านซอฟต์แวร์

2.1.2) ผู้บังคับบัญชาภายในศูนย์ไซเบอร์กองทัพบก จำนวน 10 ท่าน สำหรับการประเมินประสิทธิภาพการใช้งานของระบบโดยผู้บังคับบัญชา

2.1.3) บุคลากรภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน สำหรับการประเมินผลประสิทธิภาพการใช้งานของระบบโดยผู้ใช้งาน

2.2 การวิเคราะห์ข้อมูล ใช้การวิเคราะห์ข้อมูลด้วยวิธีทางสถิติได้แก่ ค่าเฉลี่ย (Mean) และค่าเบี่ยงเบนมาตรฐาน (Standard Deviation)

2.3 ผลการประเมินความเหมาะสมของระบบ ที่ประเมินโดยผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 ท่าน ดังสรุปไว้ในตารางที่ 1 ดังนี้

Veridian E-Journal, Science and Technology Silpakorn University
Volume 5 Number 5 September – October 2018 ISSN 2408 - 1248

ตารางที่ 1 การประเมินความเหมาะสมของระบบโดยผู้เชี่ยวชาญทางด้านซอฟต์แวร์

ลำดับ	รายการประเมิน	ค่าเฉลี่ย ($\overline{X}$)	ค่าเบี่ยงเบนมาตรฐาน	ระดับความเหมาะสม
1	ความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งาน	4.67	0.49	มากที่สุด
2	ความเหมาะสมด้านความถูกต้องของการออกแบบระบบ	4.21	0.72	มาก
3	ความเหมาะสมในการใช้งานของระบบ	4.54	0.51	มากที่สุด
4	ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย	4.46	0.51	มากที่สุด
5	ความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้	4.67	0.48	มากที่สุด
	ผลรวม	**4.51**	**0.54**	**มากที่สุด**

จากตารางที่ 1 ผลการประเมินความเหมาะสมของระบบที่ประเมินโดยผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 คน สรุปได้ว่า ด้านความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งานอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.67, S.D. = 0.49) ความเหมาะสมด้านความถูกต้องของการออกแบบระบบ อยู่ในระดับมาก ($\overline{X}$ = 4.21, S.D. = 0.72) ด้านความเหมาะสมในการใช้งานของระบบ อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.54, S.D. = 0.51) ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.46, S.D. = 0.51) และ ด้านความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้ อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.67, S.D. = 0.48) สรุปผลรวมอยู่ในระดับที่มีความเหมาะสมมากที่สุด ($\overline{X}$ = 4.51, S.D. = 0.54)

2.4 ผลการประเมินประสิทธิภาพการใช้งานระบบโดยผู้บังคับบัญชาภายในศูนย์ไซเบอร์กองทัพบก จำนวน 10 ท่าน ดังสรุปไว้ในตารางที่ 2 ดังนี้

ตารางที่ 2 การประเมินประสิทธิภาพการใช้งานระบบโดยผู้บังคับบัญชาภายในศูนย์ไซเบอร์กองทัพบก

ลำดับ	รายการประเมิน	ค่าเฉลี่ย ($\overline{X}$)	ค่าเบี่ยงเบนมาตรฐาน	ระดับความเหมาะสม
1	ด้านการออกแบบการใช้งาน	4.54	0.57	มากที่สุด
2	ด้านการบันทึกและการแก้ไขข้อมูล	4.44	0.73	มากที่สุด
3	ด้านการประมวลผลและการแสดงผล	4.46	0.61	มากที่สุด
4	ด้านการสืบค้นข้อมูล และการรายงาน	4.52	0.64	มากที่สุด
5	ด้านประสิทธิภาพการใช้งานของระบบ	4.54	0.57	มากที่สุด
	ผลรวม	**4.50**	**0.63**	**มากที่สุด**

จากตารางที่ 2 ผลการประเมินประสิทธิภาพการใช้งานของระบบ ที่ทำการประเมินโดยผู้บังคับบัญชาภายในศูนย์ไซเบอร์กองทัพบก จำนวน 10 ท่าน สรุปได้ว่า ด้านการออกแบบการใช้งาน อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.54,S.D. = 0.57) ด้านการบันทึกและการแก้ไขข้อมูล อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.44, S.D. = 0.73) ด้านการประมวลผลและการแสดงผล อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.46, S.D.= 0.61) ด้านการสืบค้นข้อมูล และการรายงาน อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.52, S.D. = 0.64) และ ด้านประสิทธิภาพการใช้งานของระบบอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.54, S.D. = 0.57) สรุปผลรวมอยู่ในระดับที่มีประสิทธิภาพมากที่สุด ($\overline{X}$ = 4.50, S.D. = 0.63)

2.5 ผลการประเมินประสิทธิภาพการใช้งานระบบโดยผู้ใช้งานภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน ดังสรุปไว้ในตารางที่ 3 ดังนี้

ตารางที่ 3 การประเมินประสิทธิภาพการใช้งานระบบโดยผู้ใช้งานภายในศูนย์ไซเบอร์กองทัพบก

ลำดับ	รายการประเมิน	ค่าเฉลี่ย ($\overline{X}$)	ค่าเบี่ยงเบนมาตรฐาน	ระดับความเหมาะสม
1	ด้านการออกแบบการใช้งาน	4.35	0.73	มากที่สุด
2	ด้านการบันทึกและการแก้ไขข้อมูล	4.21	0.75	มาก
3	ด้านการประมวลผลและการแสดงผล	4.12	0.85	มาก
4	ด้านการสืบค้นข้อมูล และการรายงาน	4.17	0.75	มาก
5	ด้านประสิทธิภาพการใช้งานของระบบ	4.08	0.81	มาก
	ผลรวม	**4.18**	**0.78**	**มาก**

จากตารางที่ 3 ผลการประเมินประสิทธิภาพการใช้งานของระบบ ที่ทำการประเมินโดยผู้ใช้งานทั่วไปภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน สรุปได้ว่า ด้านการออกแบบการใช้งาน อยู่ในระดับมากที่สุด ($\overline{X}$ = 4.35, S.D. = 0.73) ด้านการบันทึกและการแก้ไขข้อมูล อยู่ในระดับมาก ($\overline{X}$ = 4.21, S.D. = 0.75) ด้านการประมวลผลและการแสดงผล อยู่ในระดับมาก ($\overline{X}$ = 4.12, S.D.= 0.85) ด้านการสืบค้นข้อมูล และการรายงาน อยู่ในระดับมาก ($\overline{X}$ = 4.17, S.D. = 0.75) และ ด้านประสิทธิภาพการใช้งานของระบบ อยู่ในระดับมาก ($\overline{X}$ = 4.08, S.D. = 0.81) สรุปผลรวมอยู่ในระดับที่มีประสิทธิภาพมาก ($\overline{X}$ = 4.18,S.D. = 0.78)

สรุปผลการวิจัย

ผลการวิจัยครั้งนี้ทำให้ทราบถึงปัญหา สถานการณ์ และ ความพร้อมทางด้านความมั่นคงปลอดภัย ไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก อีกทั้งผู้วิจัยได้พัฒนาวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบกให้ดีกว่าระบบเดิม นอกจากนั้น ยังได้พัฒนาแอปพลิเคชันสำหรับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ ซึ่งผลการประเมินระดับความเหมาะสมของระบบจากทั้งผู้ที่เกี่ยวข้องพบว่าระบบมีความเหมาะสมและมีประสิทธิภาพในการใช้งานอยู่ในระดับมากที่สุด ทั้งนี้ เป็นการ

อำนวยความสะดวกให้แก่บุคลากรที่ทำหน้าที่ตรวจสอบภัยคุกคามทางไซเบอร์ และสามารถสนับสนุนการตัดสินใจของผู้บังคับบัญชาภายในศูนย์ไซเบอร์กองทัพบกได้อีกด้วย

อภิปรายผลการวิจัย

ผู้วิจัยได้ทำการการพัฒนาระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ระบบนี้สามารถลดระยะเวลาในการประเมินความเสี่ยง การตรวจสอบ และการเฝ้าระวังการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบกได้ ทันต่อเหตุการณ์ ทำให้ลดความเสี่ยงที่จะส่งผลกระทบต่อระบบสารสนเทศของกองทัพบกได้ ระบบที่ผู้วิจัยได้พัฒนาขึ้นมานั้นมีความเหมาะสม และตอบสนองการทำงานของผู้ใช้งานได้ในทุกระดับ ซึ่งสอดคล้องกับงานวิจัยของ ธนกร มีหินกอง และคณะ (2558) ที่ได้ทำการศึกษาเรื่องสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวด้วยเทคนิคกฎความสัมพันธ์ที่การวิจัยพบว่า ระบบตรวจหาการบุกรุก ที่ได้พัฒนาขึ้นมานั้น สามารถรายงานผลการบุกรุกได้อย่างรวดเร็ว และนำไปใช้วิเคราะห์และทำนายผลการรักษาความมั่นคงปลอดภัยไซเบอร์ได้

ข้อเสนอแนะสำหรับการวิจัยในอนาคต

งานวิจัยนี้ยังสามารถขยายผลไปสู่การพัฒนาระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบกแบบเรียลไทม์อย่างอัตโนมัติได้ในอนาคต ด้วยการทำเอาเทคโนโลยีสมัยใหม่เข้ามาใช้ร่วม ได้แก่ ปัญญาประดิษฐ์ (Artificial intelligence : AI) สำหรับใช้ในการตรวจสอบและแยกประเภทภัยคุกคามทางไซเบอร์ รวมทั้งการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เพื่อวิเคราะห์สถิติภัยคุกคามที่มีแนวโน้มว่าจะมีการโจมตีมากขึ้นหรือน้อยลง รวมทั้ง การเพิ่มขีดความสามารถทางด้านการคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) เพื่อรับมือกับภัยคุกคามและทำให้หน่วยงานมีความแข็งแกร่งทนทานต่อการบุกรุกทางไซเบอร์ในอนาคต

เอกสารอ้างอิง

ภาษาไทย

Royal Thai Army . (2012) . rabīap kǭngthap bok wādūai kān raksā khwāmmankhong plǭtphai rabop sārasonthēt khǭng kǭngthap bok 2012. long sāmsip ʻet Mīnākhom 2012. Rātchakitchānubēksā . (2017) .

กองทัพบก. (2555). **ระเบียบกองทัพบกว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก พ.ศ. 2555**. ลง 31 มีนาคม 2555. ราชกิจจานุเบกษา. (2560).

Phæng chan .J (2015) . [Master in Security]. 3rd Edition . Phim khrang thī nưng nonthaburī : IDC Primere Co.Ltd.

จตุชัย แพงจันทร์. (2558). **Master in Security**. 3rd Edition. พิมพ์ครั้งที่ 1 นนทบุรี : บริษัทไอดีซี พรีเมียร์ จำกัด.

Phānitkun.P. [khwāmmankhong plǭtphai khǭng sārasonthēt læ kānchatkān (Information Security and Management)] . KPT Comp and Consault company Co.Ltd. 2010.

พนิดา พานิชกุล. **ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ (Information Security and Management)**. บริษัท เคพีที คอมพ์ แอนด์ คอนซัลท์ จำกัด. 2553.

Bun chœm.S, kangphitdān.S.atc (2014).[kānwichai læ phatthanā rabop truat sop khwāmmankhong plǭtphai khǭng rabop sārasonthēt In Royal Thai Army] . saphāwichai hæng chāt.

สมชาย บุญเจิม, ศุภกร กังพิศดาร และคณะ. (2557) **การวิจัยและพัฒนาระบบตรวจสอบ ความมั่นคงปลอดภัยของระบบสารสนเทศภายในกองทัพบก**. สภาวิจัยแห่งชาติ.

Kitcharœnkānkun.S (2017) . hā phai khukkhām sai bœ thī tǭng phưng rawang nai pī sǭngphansippæt . supkhon chāk : https : / / www . catcyfence . com / it - security / article / top - hā - cyber - security - in - sǭngphansippæt / .

สุธีร์ กิจเจริญการกุล. (2560). **“5 ภัยคุกคามไซเบอร์ที่ต้องพึงระวังในปี 2018”.** สืบค้นจาก : https://www.catcyfence.com/it-security/article/top-5-cyber-security-in-2018/.

Sirirotborirak.S. (2015) . [kānphatthanā māttrathān kān raksā khwāmmankhong plǭtphai sai bœ (Cyber Security) khǭng krasūang Kalāhom] . botkhwām wichākān sathāban wichākān pǭngkan prathēt . pī thī 6 chabap thī 3 (June To August 2015) .

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). **“การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม”**.บทความวิชาการสถาบันวิชาการป้องกันประเทศ.ปีที่ 6 ฉบับที่ 3 (พฤษภาคม ถึง สิงหาคม 2558).

Utkrit.N. (2014) . [kānwāngphæn rong rap hetkān chukchœn phūa khwāmmankhong sārasonthet nai ʻongkon] . wārasān theknōloyī sārasonthet mahāwitthayālai phrachǒmklao phranakhonnūa . pī thī pæt chabap thī song (Karakadākhom thưng Thanwākhom) .

ณัฐวี อุตกฤษฎ์. (2557). **“การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร”.** วารสารเทคโนโลยีสารสนเทศ มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ”. ปีที่ 8 ฉบับที่ 2 (กรกฎาคม ถึง ธันวาคม).

Mī hin kong.T., Prānitphonlakarang.P., Amd Chirawichitchai.(2015). [sathāpattayakam khwāmrū dān khwāmmankhong plotphai sai bœ phūa sanapsanun rabop truat hāka rabu kruk bæp prap tūa dūai theknik kot khwāmsamphan] . wārasān wichākān phrachǒmklao phranakhonnūa pī thī yīsipha chabap thī song (Phrutsaphākhom Singhākhom).

ธนกร มีหินกอง. ประสงค์ ปราณีตพลกรัง และ นิเวศ จิระวิชิตชัย. (2558) **“สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวด้วยเทคนิคกฎความสัมพันธ์”.** วารสารวิชาการพระจอมเกล้าพระนครเหนือ ปีที่ 25 ฉบับที่ 2 (พฤษภาคม – สิงหาคม).

Intharāwut , phon thō . (2014) . sūn sai bœ kongthap bok (Army Cyber Center) . supkhon chǎk : http : / / rittee 1834. blogspot . com / songphansipsī / sip / army - cyber - center. html.

ฤทธี อินทราวุธ, พลโท. (2557). **“ศูนย์ไซเบอร์กองทัพบก (Army Cyber Center)”.** สืบค้นจาก: http://rittee1834.blogspot.com/2014/10/army-cyber-center.html.

ภาษาต่างประเทศ

J. Ryoo, T. Girard and C. E. McConn. (2009). **An Information Systems Security Readiness Assessment for Municipalities in Rural Pennsylvania**. Center for Rural Pennsylvania.

T. Sommestad, M. Ekstedt and P. Johnson. (2009). **Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models**. in 42nd Hawaii International Conference on System Sciences (HICSS). pp. 1–10.

B. J. Colfer. **The Science of Cybersecurity and a Roadmap to Research.** Nova Science Publishers, Inc. 2011.

ISO/IEC 27001:2013 - Information Technology - Security Techniques Information Security Management Systems - Requirements. Switzerland. 2013.

J. R. Westby. **Legal Guide to Cybersecurity Research**. American Bar Association. 2014.

K. J. Andreasson. **Cybersecurity: Public Sector Threats and Responses**. CRC Press. 2011.

M. Douglas, W. D. Newhouse, and V.Tomas. "**Introducing the Federal Cybersecurity R&D Strategic Plan**". The Next Wave. Vol. 19. No. 4. 2012.

Subcommittee on Technology Subcommittee on Research and Committee on Science, Space, and Technology House of Representatives. **Cybersecurity Research and Development**. The U.S. Government Printing Office. 2013.

T. J. MowbrayWiley. **Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions**. John Wiley & Sons, Inc. 2013.

The U.S. Homeland Security. **A Roadmap for Cybersecurity Research**. [Online]. 2009. Available from: http://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf [2014, January 12].

J. R. Vacca. **Computer and Information Security Handbook**, 2nd Edition, Morgan Kaufmann Publishing Inc. 2013.

M. R. Ousley, **Information Security** (Complete Reference Series). 2nd Edition. McGraw- Hill Publishing Inc. 2013.

N. M. Ulsch. **Cyber Threat How to Manage the Growing Risk of Cyber Attacks**. John Willey & Sons, Inc. 2014.

P. W. Singer, and A. Friedman. **Cybersecurity and Cyberwar: What Everyone Needs to Know**. Oxford University Press. 2014.