สารนิพนธ์เรื่อง การพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก

คำสำคัญ เฝ้าระวัง, การแจ้งเตือน, ความมั่นคงปลอดภัยไซเบอร์

นักศึกษา จ่าสิบเอก เกียรติศักดิ์ ลุยทอง

อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย

อาจารย์ที่ปรึกษาร่วม ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง

หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะ เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

พ.ศ. 2561

บทคัดย่อ

การศึกษาวิจัยนี้ เพื่อเป็นการพัฒนาวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยใช้เครื่องมือในการพัฒนาระบบได้แก่ภาษา PHP สำหรับการพัฒนาแอปพลิเคชัน และโปรแกรม MySQL สำหรับจัดการฐานข้อมูล กลุ่มตัวอย่างที่ใช้ ในการดำเนินการวิจัย มีจำนวน 2 กลุ่ม คือ กลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 ท่าน และกลุ่มผู้ใช้งานระบบ ซึ่งเป็นบุคลากรภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน

สรุปผลการประเมินด้านเหมาะสมของระบบ โดยกลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์อยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$=4.51, S.D.=0.54) และการประเมินด้านการประสิทธิภาพการใช้งานระบบ โดยกลุ่มผู้ใช้งาน ซึ่งอยู่ในระดับมีประสิทธิภาพมาก ($\overline{X}$=4.18, S.D.=0.78) แสดงให้เห็นว่าระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสม และสามารถตอบสนองการทำงานผู้ใช้งานได้ในทุกระดับ การตรวจสอบและการรายงานผลสถิติภัยคุกคามทางไซเบอร์เป็นไปอย่างรวดเร็ว ลดขั้นตอนการตรวจสอบภัยคุกคามของเจ้าหน้าที่และลดปริมาณการใช้กระดาษ รวมถึงเป็นการรักษาความลับของทางราชการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้อย่างมีประสิทธิภาพ

THEMATIC TITLE	DEVELOPMENT OF MONITORING , INTRUSION DETECTION AND ALERT SYSTEMS FOR CYBERSECURITY CONTROL IN ARMY CYBER CENTER
KEYWORDS	MONITORING, INTRUSION DETECTION, ALERT, CYBERSECURITY
STUDENT	SM.1 KEAITTISAK LUITHONG
ADVISOR	ASSIST. PROF. DR.NIVET CHIRAWIVHITCHAI
CO-ADVISOR	PROF.DR.PRASONG PRANEETPOLGRANG
LEVEL OF STUDY	MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
FACULTY	INFORMATION TECHNOLOGY SRIPATUM UNIVERSITY
YEAR	2018

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 2 groups: 6 Software professionals and 35 personnel from the Army Cyber Center who use the system.

The conclusion of the research shows that the software professionals' assessment of the system's suitability found it to be the most suitable ($\overline{X}$=4.51, S.D.=0.54). The efficiency assessment carried out by the system users found it to be the most efficient ($\overline{X}$=4.18, S.D.=0.78). This results show that the system that have been developed is suitable and responds to the needs and purposes of the users on every level. It also verifies the statistics reports on cyber threats immediately, reducing the reliance on personals, reduce the amount of paper and improves confidentiality of the government service.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้เกิดขึ้นและสำเร็จเป็นอย่างดีได้ เพราะได้รับการสนับสนุนและคำแนะนำทางด้านการศึกษา ค้นคว้าข้อมูล และแนวทางในการดำเนินการวิจัยที่เกี่ยวข้อง จากอาจารย์ที่ปรึกษางานสารนิพนธ์ จำนวน 2 ท่าน ได้แก่ ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง และผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย ที่คอยแนะนำ และให้คำปรึกษาทางด้านแนวทางในการทำงานนี้ จนสำเร็จลุล่วงไปด้วยดี และทันตามกรอบเวลาที่กำหนด ในโอกาสนี้ผู้จัดทำจึงขอขอบพระคุณท่านผู้ทรงคุณวุฒิ จำนวน 2 ท่านที่กล่าวมาแล้วอย่างสูง ที่คอยแนะนำให้คำปรึกษาและถ่ายทอดประสบการณ์ความรู้อันเป็นประโยชน์ต่อสารนิพนธ์ฉบับนี้ รวมถึงเพื่อนร่วมรุ่นที่คอยช่วยเหลือและให้กำลังใจมาโดยตลอด เจ้าหน้าที่ของมหาวิทยาลัยศรีปทุม ที่คอยอำนวยความสะดวกทางด้านการเรียนการสอน และงานวิจัย รวมถึงช่วยเหลือในช่วงที่ใช้ชีวิตอยู่ในมหาวิทยาลัยศรีปทุมในทุก ๆ ด้าน

ผู้วิจัยขอขอบพระคุณคณาจารย์ทุกท่านที่ประสิทธิ์ประสาทวิชาความรู้ให้ ขอขอบคุณผู้ทรงคุณวุฒิ ที่คอยให้คำปรึกษาทางด้านอื่น ๆ ที่เป็นประโยชน์ต่องานสารนิพนธ์ คุณพ่อ คุณแม่ครอบครัว โดยมีภรรยาที่อยู่ระหว่างตั้งครรภ์ ผู้ที่เป็นกำลังใจและอยู่เบื้องหลังความสำเร็จในครั้งนี้ด้วยประการทั้งปวง รวมถึงผู้เชี่ยวชาญทางด้านซอฟต์แวร์ ทั้ง 6 ท่านและบุคลากรภายในศูนย์ไซเบอร์กองทัพบก และผู้ที่ไม่ได้กล่าวถึงในที่นี้ ทุก ๆ ท่าน ที่มีส่วนทำให้งานวิจัยนี้ประสบความสำเร็จด้วยดี จึงขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

เกียรติศักดิ์ ลุยทอง

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีมีความเจริญก้าวหน้าเป็นอย่างมาก ซึ่งกล่าวได้ว่าเป็นส่วนหนึ่งของชีวิตประจำวัน ซึ่งการติดต่อสื่อสารนั้น จะรับรู้ได้อย่างรวดเร็วภายในระยะเวลาเสี้ยววินาที ซึ่งส่งผลให้การธุรกรรมต่าง ๆ ดำเนินการไปอย่างรวดเร็ว รวมถึงมีการนำเอาเทคโนโลยีมาใช้กันอย่างมากขึ้น อย่างไรก็ดี แม้ว่าเทคโนโลยีจะมีความเจริญก้าวหน้าเพียงใด แต่ถ้าหากรู้เท่าไม่ถึงการณ์ หรือว่ามีมาตรการป้องกันไม่ดีพอ ก็อาจจะก่อให้เกิดโทษอันมหันต์ โดยเฉพาะปัจจุบันมีการนำเทคโนโลยีมาช่วยในการพัฒนาระบบสารสนเทศในหลาย ๆ ด้าน เพื่อเพิ่มประสิทธิภาพการทำงานเพิ่มความรวดเร็ว ความถูกต้องแม่นยำของข้อมูลต่าง ๆ รวมถึงความรวดเร็วในการให้บริการ การแลกเปลี่ยนข้อมูล ซึ่งไม่ว่าจะเป็นองค์กรหน่วยงานภาครัฐขนาดเล็กหรือขนาดใหญ่ ย่อมมีความจำเป็นในการใช้ระบบเทคโนโลยีสารสนเทศในการดำเนินกิจการต่าง ๆ ด้วยกัน แต่ในการใช้เทคโนโลยีสารสนเทศนั้นมักพบปัญหาต่าง ๆ หลายด้าน ไม่ว่าจะด้านความมั่นคงปลอดภัยของระบบ การถูกโจมตีระบบเครือข่ายขององค์กรหน่วยงานภาครัฐ การใช้เทคโนโลยีสารสนเทศ ไปในทางที่ผิดการนำเอาเทคโนโลยีไปใช้เพื่อหาประโยชน์ส่วนบุคคล ทำให้องค์กรได้รับความเสียหาย

รัฐบาลได้ตระหนักถึงการรักษาความปลอดภัยของระบบสารสนเทศ จึงได้จัดตั้งกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศสมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รัฐบาลจึงได้กำหนดแนวทางการพัฒนายุทธศาสตร์ความมั่นคงไซเบอร์แห่งชาติ เพื่อเป็นแนวทางในการดำเนินการการวางยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติจนไปถึงการบริหารจัดการในระดับองค์กรทั้งแนวคิดทางด้านบริหารจัดการและทางเทคนิค

ภัยคุกคามด้านไซเบอร์ (Cyber Threat) นับวันจะทวีความความรุนแรงมากขึ้นตามลำดับ องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์ (Cyber Attack) ซึ่งหลายคนอาจมองว่าเป็นภัยที่ไกลตัว หรือจินตนาการมองเห็นได้ยาก แต่แท้จริงแล้วเป็นภัยคุกคามที่อยู่ใกล้ตัวที่ถูกมองข้าม และมีเกณฑ์เสี่ยงที่ค่อนข้างสูง ยิ่งถ้าทุกสิ่งทุกอย่างเราฝากไว้กับระบบเครือข่ายทั้งหมด ยิ่งเป็นที่ต้องการอย่างมากกับเหล่าโจรกรรมทางด้านไซเบอร์ ดังนั้น จึงมีความจำเป็นต้องมีการพัฒนาระบบเพื่อตรวจสอบ และเทคนิคในการรักษาความปลอดภัยไอทีให้ควบคู่กันไปด้วย

การรักษาความมั่นคง (Security) จึงมีความจำเป็นอย่างยิ่ง ที่หน่วยงานต่าง ๆ ต้องมีการบริหารจัดการ การรักษาความมั่นคงของระบบคอมพิวเตอร์ในหน่วยงานเพื่อไม่ให้เกิดปัญหาความเสี่ยง ที่ส่งผลกระทบร้ายแรงนี้ หน่วยงานต้องมีความรู้เท่าทันปัญหาความเสี่ยงต่าง ๆ ที่เกิดขึ้นจากเทคโนโลยีหรือจากตัวบุคคลรวมทั้งยังต้องรู้วิธีที่จะป้องกันการโจรกรรมจากผู้มุ่งร้ายรวมทั้งไซเบอร์

เพื่อเป็นการป้องกันการถูกโจมตีจากภัยคุกคามทางไซเบอร์ กองทัพบกจึงได้อนุมัติให้จัดตั้งศูนย์ไซเบอร์กองทัพบกเพื่อพัฒนากองทัพให้ทันสมัยโดยสามารถทำงานให้สอดคล้องกับหน่วยงานภาครัฐอื่น ๆ โดยจะเน้นการปกป้องงานของกองทัพบกเพื่อป้องกันการถูกแทรกแซงจากแฮกเกอร์ ต่าง ๆ รวมทั้งงานที่เกี่ยวข้องกับด้านการข่าว โดยเน้นหนักไปในเรื่องการพัฒนากำลังคนและเครื่องมือโดยเฉพาะที่กองทัพมีพื้นฐานรองรับงานต่าง ๆ ไว้แล้ว กองทัพบกได้มองเห็นปัญหาของภัยคุกคามทางไซเบอร์ ซึ่งมีการใช้เทคโนโลยีเข้ามาทำลายความมั่นคงของประเทศจึงได้เร่งพัฒนาเสริมศักยภาพของกองทัพไว้ให้พร้อมกับภัยที่กำลังเกิดขึ้น

การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบกจำเป็นต้องมีการจัดทำระบบเพื่อทำการจัดเก็บสถิติภัยคุกคามเพื่อศึกษาถึงสภาพปัญหาและสถิติภัยคุกคามที่เป็นเกณฑ์เสี่ยงต่อการรักษาความปลอดภัยของระบบสารสนเทศของกองทัพบก รวมถึงการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์นั้น ต้องสามารถแก้ปัญหาได้อย่างรวดเร็วและตรงประเด็น ดังนั้นผู้วิจัยจึงสนใจที่จะพัฒนาระบบแอปพลิเคชันสำหรับจัดเก็บสถิติภัยคุกคามของโปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ และการเก็บสถิติการบุกรุกของโปรแกรมไม่พึงประสงค์ เพื่อเป็นการยกระดับมาตรฐานเกณฑ์การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก รวมถึงการเพื่อประเมินระดับความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศของศูนย์ไซเบอร์กองทัพบก

วัตถุประสงค์ของการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยมีวัตถุประสงค์หลัก 4 ประการ ได้แก่

1. เพื่อศึกษาบริบท ปัญหาและสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ ภายในศูนย์ไซเบอร์กองทัพบก

2. เพื่อพัฒนาวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ ไซเบอร์กองทัพบก

3. เพื่อพัฒนาแอปพลิเคชันสำหรับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์

4. เพื่อทำการประเมินระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน สำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์

ขอบเขตของการวิจัย

งานวิจัยนี้ มีของเขตการพัฒนา เว็บแอปพลิเคชัน เพื่อการจัดเก็บสถิติภัยคุกคามของโปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ และการเก็บสถิติการบุกรุกของโปรแกรมไม่พึงประสงค์ เพื่อเป็นการยกระดับมาตรฐานเกณฑ์การตรวจสอบ เฝ้าระวังและแจ้งเตือน ความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ทราบถึง แนวทาง กระบวนการ และมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก

2. ทำให้ทราบถึงระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในศูนย์ไซเบอร์กองทัพบก

3. ทำให้ทราบถึงวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์ กองทัพบก

4. ทำให้ได้แอปพลิเคชัน สำหรับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์ กองทัพบก

นิยามศัพท์

1. ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน

2. ระบบเฝ้าระวังภัยคุกคาม หมายถึง ระบบที่ใช้สำหรับการตรวจสอบ และเฝ้าสังเกตภัยคุกคามทางไซเบอร์ ที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ ที่คาดว่าจะทำให้เกิดผลเสียต่อระบบสารสนเทศ

3. ระบบตรวจหาการบุกรุก หมายถึง ระบบที่ใช้ตรวจหาการใช้งานเครือข่ายภายในองค์กรในทางที่ผิดไปจากกฎ ข้อบังคับส่งผลต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต กลไกระบบตรวจหาการบุกรุกเป็นการวิเคราะห์กิจกรรมต่าง ๆ ที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ด้วยการตรวจสอบกับข้อกำหนดการใช้งานและการตรวจสอบจากสถิติการใช้งาน

4. ระบบแจ้งเตือน คือ ระบบที่ใช้สำหรับการบ่งบอกการบุกรุกของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์

บทที่ 2
แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การศึกษาและวิจัยในครั้งนี้เป็นการพัฒนาแอปพลิเคชันสำหรับบันทึกสถิติภัยคุกคามทางไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยผู้วิจัยได้ศึกษาเอกสาร แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องเพื่อเป็นพื้นฐานและแนวทางการในการพัฒนาระบบ ตามลำดับ ดังนี้

ความเป็นมาของศูนย์ไซเบอร์กองทัพบก
วัตถุประสงค์การจัดตั้งศูนย์ไซเบอร์กองทัพบก
ภารกิจของศูนย์ไซเบอร์กองทัพบก
แนวคิด ทฤษฎี และคำจำกัดความที่สำคัญ
นโยบายการรักษาความปลอดภัย
แนวโน้มความเสี่ยงด้านภัยคุกคามทางไซเบอร์
ความเสียหายหรือผลกระทบจากเหตุภัยคุกคามไซเบอร์
งานวิจัยที่เกี่ยวข้อง

ความเป็นมาของศูนย์ไซเบอร์กองทัพบก

กองทัพบก ได้เตรียมความพร้อมรับมือกับภัยคุกคามที่มองไม่เห็นตัวบนโลกไซเบอร์หรือบนเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งปัจจุบันนับวันจะทวีความเข้มข้นและมีความรุนแรงเพิ่มขึ้นตามลำดับ ก่อให้เกิดความเสียหาย และผลกระทบในวงกว้างทางด้านการเมือง เศรษฐกิจ และสังคมจิตวิทยา ซึ่งเป็นกำลังอำนาจแห่งชาติ (National Power) ในด้านความมั่นคงปลอดภัยของประเทศอย่าง ไร้พรมแดนในช่วงเวลาเพียงพริบตา ประเทศมหาอำนาจหลายประเทศได้กำหนดความสำคัญให้พื้นที่บนโลกไซเบอร์ (Cyber Space) เป็น 1 ใน 5 ของอาณาเขตในการปฏิบัติการทางหาร (Domain) นอกเหนือจาก พื้นดิน (Land Domain) พื้นน้ำ(Sea Domain) ห้วงอากาศ (Air Domain) และ ห้วงอวกาศ (Space Domain) ที่เรียกกันว่า ไซเบอร์โดเมน (Cyber Domain) จากเหตุผลดังกล่าว กองทัพบกจึงได้อนุมัติหลักการจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ขึ้นเพื่อปฏิบัติงาน โดยจะเริ่มทดลองปฏิบัติงาน ตั้งแต่ 1 ตุลาคม 2557 พร้อม ๆ กับเหล่าทัพอื่น กองบัญชาการกองทัพไทย และกระทรวงกลาโหม

วัตถุประสงค์การจัดตั้งศูนย์ไซเบอร์กองทัพบก

ศูนย์ไซเบอร์กองทัพบก ที่จะจัดตั้งขึ้นมาใหม่นี้ มิได้มีความแปลกกว่าหน่วยงานราชการอื่น ๆ ที่มีอยู่ในปัจจุบันแต่อย่างไร และในหลาย ๆ ประเทศก็มีหน่วยงานประเภทนี้ไว้ดูแลงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ส่วนของกองทัพบกมีวัตถุประสงค์เพื่อให้มีหน่วยงานรับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นการเฉพาะโดยตรงตามนโยบายรัฐบาลที่ผ่านมา และมีขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุกเมื่อจำเป็น รวมถึงการใช้ประโยชน์จากไซเบอร์ในการสนับสนุนการปฏิบัติการข่าวสาร โดยมีสถานะเป็นหน่วยขึ้นตรงกองทัพบก และปฏิบัติหน้าที่เป็นฝ่ายกิจการพิเศษ โดยมีภารกิจที่สำคัญ คือ การรักษาความมั่นคงปลอดภัยไซเบอร์ การปฏิบัติการไซเบอร์ การใช้ประโยชน์ไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร และการพัฒนาความพร้อมด้านไซเบอร์ของกองทัพบก ซึ่งการเตรียมการจัดตั้งศูนย์ไซเบอร์กองทัพบกที่ผ่านมาตั้งแต่กันยายน 2557 นับว่ามีความคืบหน้าไปพอสมควร มีการดำเนินการปรับโครงสร้างองค์กรและที่ตั้งสำนักงานใหม่ (Reorganization) โดยแตกกิ่งก้านสาขาหน่วยงาน และยุบรวมแผนก จาก ศูนย์เทคโนโลยีทางทหาร แบ่งออกเป็น 5 กลุ่มงาน คือ งานธุรการ งานแผนและฝึก งานการรักษาความปลอดภัยไซเบอร์ งานปฏิบัติการไซเบอร์ และงานสนับสนุนการปฏิบัติการข่าวสาร โดย ศูนย์เทคโนโลยีทางทหาร ยังคงปฏิบัติภารกิจด้านการบริการเทคโนโลยีสารสนเทศ (IT) ให้กับหน่วยต่าง ๆ ในกองทัพบกเช่นเดิม ยกเว้นภารกิจด้านการสงครามสารสนเทศ (IW) ได้แก่ การสนับสนุนด้านระบบคอมพิวเตอร์และคอมพิวเตอร์แม่ข่าย (Application Server / Web Server) ระบบฐานข้อมูล (Data Center) ระบบอินเทอร์เน็ต ระบบเครือข่ายภายใน องค์กรหรืออินเทอร์เน็ต ระบบเครือข่ายไร้สาย (Wifi) ภายในพื้นที่กองบัญชาการกองทัพบก (เริ่มให้การบริการ Free Wifi ตั้งแต่ มกราคม 2557 เป็นต้นไป) การสนับสนุนระบบควบคุมบังคับบัญชา (C^4I) ตลอดจนการพัฒนาและให้การบริการระบบงานด้านเทคโนโลยีสารสนเทศ เช่น ระบบการบริหารงานยามปกติ (MIS) ระบบจัดการองค์ความรู้กองทัพบก (KM) ระบบสารสนเทศระดับกองพัน (e-Army / e-Battalion) และระบบงานอื่น ๆ เป็นต้น

ภารกิจของศูนย์ไซเบอร์กองทัพบก

การจัดตั้งศูนย์ไซเบอร์กองทัพบก ได้ดำเนินการภายใต้หลักการบริหารงานเชิงกลยุทธ์ 4 ประการ (POLE) คือ การวางแผนงาน (Planning) การจัดการองค์กร (Organizing) การนำไปสู่การปฏิบัติ (Leading) และ การประเมินผล (Evaluating) โดยได้จัดการระดมความคิด (Brain Storming) ในการจัดทำแผนที่การทำงาน (Road Map) และกรอบตารางการปฏิบัติงาน

(Time Frame) การดำเนินการปรับปรุงโครงสร้างองค์กร (Reorganization) และที่ตั้งสำนักงานศูนย์ไซเบอร์กองทัพบก การปรับเปลี่ยนระบบกระบวนการทำงานใหม่ (Reengineering) เพื่อให้เกิดประสิทธิภาพ และประสิทธิผลในการทำงานขององค์กร โดยเน้นผลสัมฤทธิ์ (Outcome) และได้เริ่มทดลองปฏิบัติงานขั้นต้น เป็นการภายในมาตั้งแต่ กันยายน 2557 เช่น การสำรวจตรวจสอบทรัพย์สินที่เกี่ยวข้องกับไซเบอร์ (Asset Management) การตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ (Environmental Scanning) การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ (Risk Assessment) การประเมินช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) การปลูกฝังสร้างเสริมความสำนึก ความตระหนัก และการฝึกอบรม (Awareness and Training) การสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก (Army Cyber Communities) การเฝ้าระวังตรวจสอบ วิเคราะห์ไซเบอร์ และข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง การปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (CSOC) เป็นต้น โดยอาศัยเครื่องมืออุปกรณ์ที่มีอยู่เดิม ซอฟต์แวร์ Open Source และแสวงหาความร่วมมือจากหน่วยงานภายนอก โดยมีผลการปฏิบัติงานที่ผ่านมา ดังนี้

1. การสำรวจตรวจสอบทรัพย์สินที่เกี่ยวข้องกับไซเบอร์ (Asset Management) เพื่อจัดทำบัญชีคุมสถานภาพสิ่งอุปกรณ์ การจำหน่ายสิ่งอุปกรณ์ที่ชำรุดใช้การไม่ได้ และการนำอุปกรณ์ที่ไม่ใช้งานไปใช้เป็นเครื่องมือในการปฏิบัติงานเบื้องต้นของ ศูนย์ไซเบอร์ของกองทัพบก

2. การตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ (Environmental Scanning) เป็นการใช้เครื่องมือตรวจสอบ ป้องกันระบบ Network และ Application โดยสามารถตรวจสอบและดักจับความเคลื่อนไหวของภัยคุกคามไซเบอร์ในระบบเครือข่ายคอมพิวเตอร์ได้ตั้งแต่ระดับ Physical Layer (Layer 1) ไปจนถึงระดับ Application Layer (Layer 7) ตั้งแต่แหล่งที่มาของต้นทางไปยังอุปกรณ์คอมพิวเตอร์ปลายทางภายในระบบเครือข่าย โดยเฉพาะโปรแกรม BotNet, Trojan Horse, Backdoor, Virus และ Malware รวมถึงเส้นทางการจราจรบนเครือข่าย (Network Traffic) ที่ผิดปกติเพื่อแจ้งให้หน่วยที่เกี่ยวข้องทราบ และดำเนินการต่อไป

3. การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่งคงปลอดภัย3ไซเบอร์ (Risk Assessment) เป็นการประเมินตนเองด้านความเสี่ยงในการรักษาความมั่งคงปลอดภัยไซเบอร์ของกองทัพบก ผ่านระบบ Online ของ ACIS Professional Center เพื่อวิเคราะห์ ภาพจำลองความพร้อม และความไม่พร้อมในด้านต่าง ๆ ของกองทัพบก ซึ่งควรจะต้องเร่งดำเนินการพัฒนาปรับปรุงแก้ไขจุดอ่อนดังกล่าวต่อไปในอนาคต

4. การประเมินช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นการใช้เครื่องมือตรวจสอบช่องโหว่ระบบสารสนเทศ ด้วยซอฟต์แวร์ Open source เพื่อตรวจสอบและวิเคราะห์ช่องโหว่ของพอร์ตต่าง ๆ บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) รวมถึงการบุกรุก โจมตีผ่านช่องโหว่ดังกล่าว เพื่อแจ้งให้หน่วยที่เกี่ยวข้องทราบ และดำเนินการต่อไป

5. การปลุกฝังสร้างเสริมความสำนึก ความตระหนักและการฝึกอบรม (Awareness and Training) เป็นการจัดชุดนิเทศไซเบอร์เคลื่อนที่ไปชี้แจงระเบียบคำสั่ง ด้านการรักษาความปลอดภัยสารสนเทศ การสร้างความตระหนัก ความสำนึก และความระมัดระวังในการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร โดยได้ดำเนินการไปแล้วในพื้นที่ทั้ง 4 กองทัพภาค รวมถึงการเข้ารับฝึกอบรมฯ จากสถาบันและองค์กรต่าง ๆ ตามแนวทางการพัฒนาความร่วมมือจากหน่วยงานภายนอก ทั้งภาครัฐและเอกชน เพื่อพัฒนาขีดความสามารถของบุคลากรศูนย์ไซเบอร์ของกองทัพบก

6. การสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก (Army Cyber Communities) เป็นการจัดตั้งประชาคมเครือข่ายไซเบอร์ของกำลังพลในกองทัพบก โดยแสวงประโยชน์จากการดำเนินงาน

7. ปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (CSOC) เพื่อใช้เป็นศูนย์ปฏิบัติการฯ ในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการขออนุมัติโครงการปรับปรุงห้องฝึกอบรมศูนย์เทคโนโลยีทางทหาร เพื่อใช้เป็นห้องปฏิบัติการไซเบอร์ (War Room) ในขั้นต้น และโครงการปรับปรุงระบบการรักษาความมั่นคงปลอดภัยเครือข่ายภายใน

8. การดำเนินการเฝ้าระวัง ติดตาม ตรวจสอบ วิเคราะห์ไซเบอร์ และข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง เพื่อสนับสนุนการปฏิบัติการข่าวสารของกองทัพบก โดยดำเนินการเฝ้าระวัง สืบค้น ติดตาม ตรวจสอบ แหล่งที่มาของข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง อย่างต่อเนื่อง

คำจำกัดความที่สำคัญ

การรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรก็คือการรักษาความลับการรักษาความครบถ้วน และ การรักษาสภาพพร้อมใช้งาน ต่อทรัพย์สินด้านไซเบอร์ที่เป็นโครงสร้างพื้นฐานด้านไซเบอร์หรือไอซีทีสามารถพิจารณาได้ดังนี้ ด้านบุคลากร ด้านอุปกรณ์ ด้านโปรแกรม ด้านสารสนเทศ ด้านมาตรฐานของเครือข่ายและรหัสที่ใช้ในการส่งผ่าน โครงสร้างพื้นฐานเหล่านี้ถ้าขาดสภาพความมั่นคงปลอดภัยก็อาจก่อให้เกิดผลเสียต่อองค์กร

ความหมายของไซเบอร์ (Cyber) มีความหมายว่าเกี่ยวข้องกับคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ หรืออินเทอร์เน็ต หรือ ความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม

ความเสี่ยง (ISO/IEC TR 13335) เป็นโอกาสของความเป็นไปได้ที่ภัยคุกคามจะฉวยประโยชน์จากจุดอ่อน หรือช่องโหว่ในระบบ อันส่งผลให้สินทรัพย์ขององค์กรเกิดการสูญเสีย หรือถูกทำลายไม่ว่าในทางตรงหรือทางอ้อม

ความเสี่ยง หมายถึงโอกาสที่จะเกิดความผิดพลาด การสูญเสียความลับ การหยุดให้บริการหรือเหตุการณ์ที่ไม่พึงประสงค์กับเทคโนโลยีสารสนเทศและการสื่อสารเป็นผลให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

กล่าวโดยสรุป ความเสี่ยง คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และส่งผลกระทบหรือสร้างความเสียหาย หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจที่กำหนด ทั้งในด้านกลยุทธ์ การปฏิบัติงาน งบประมาณ และการบริหาร โดยวัดผลจากผลกระทบที่จะได้รับและโอกาสที่จะเกิดของเหตุการณ์

การบริหารความเสี่ยง หมายถึง กระบวนการ เบ็ดเสร็จที่พิสูจน์ทราบ ควบคุม และลดผลกระทบจากเหตุการณ์ที่ไม่แน่นอนให้ เหลือน้อยที่สุด จุดประสงค์หลักของการบริหารความเสี่ยง คือ การลดความเสี่ยง

ความลับ (Confidentiality) คือ การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

บูรณภาพ (Integrity) คือการรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

ความพร้อมใช้งาน(Availability) คือการรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

การพิสูจน์ฝ่าย (Authentication) คือการตรวจสอบและการพิสูจน์สิทธิของการขอเข้าใช้ระบบของผู้ใช้บริการจากรายชื่อผู้มีสิทธิสำหรับอุปกรณ์ไอที รวมถึงแอพพลิเคชั่นทั้งหลาย

การพิสูจน์สิทธิ์ (Authorization) หมายถึงการตรวจสอบว่า บุคคล อุปกรณ์ไอที หรือแอพพลิเคชั่นนั้น ๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

การเก็บสำรองข้อมูล (Data Backup) หมายถึง ในระหว่างการเก็บสำรอง สำเนาของชุดข้อมูลปัจจุบันจะถูกสร้างขึ้นมาเพื่อป้องกันการสูญหาย

การปกป้องข้อมูล (Data Protection) หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทนการรักษาความมั่นคงปลอดภัยของสารสนเทศได้

การประเมินความเสี่ยงหรือการวิเคราะห์ความเสี่ยง (Risk assessment or Analysis) ของระบบสารสนเทศ หมายถึง การตรวจสอบโอกาสของผลลัพธ์ใด ๆ ที่ไม่พึงประสงค์ ต่อระบบสารสนเทศและผลเสียที่อาจจะเกิดขึ้นตามมาได้

นโยบายด้านความมั่นคงปลอดภัย (Security Policy) หมายถึงนโยบายที่แสดงเป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบทของความต้องการอย่างเป็นทางการขององค์กร

การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security)

เป็นมาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตให้เข้าใช้เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตเพื่อทำลายข้อมูลหรือทำในสิ่งที่อาจก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูล มีองค์กรทางด้านการรักษาความมั่นคงปลอดภัยและผู้เชี่ยวชาญได้ให้ความหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศไว้ดังนี้ UK Office of Cyber Security and UK Cyber Security Operations Centre ให้ความหมายการรักษาความปลอดภัยสารสนเทศ หมายถึง การปกป้อง การป้องกันผลประโยชน์ของ สหราชอาณาจักร รวมถึงการแสวงหานโยบายการรักษาความมั่นคงปลอดภัยที่กว้างขึ้นจากการบุกรุกในโลกไซเบอร์ และ Gavigan ให้ความหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ว่า หมายถึง การปกป้องข้อมูลโดยการป้องกัน การตรวจหา และการตอบสนองต่อการโจมตี

สรุปได้ว่าการรักษาความมั่นคงปลอดภัยสารสนเทศ หมายถึง วิธีการในการปกป้อง ป้องกันข้อมูลบนเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต เพื่อนำมากำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและหาแนวทางในการปกป้อง ป้องกันข้อมูล

แนวคิดเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

การรักษาความมั่นคงปลอดภัยสารสนเทศ มีแนวคิดเกี่ยวกับการรักษาความมั่นคงปลอดภัยที่หน่วยงานควรคำนึงถึงดังนี้

1. ความเป็นส่วนบุคคล (Privacy) หมายถึงข้อมูลถูกใช้ตามวัตถุประสงค์ ที่เจ้าของข้อมูลระบุในช่วงที่เก็บรวบรวมเท่านั้น

2. การระบุตัวตน (Identification) หมายถึงระบบสามารถระบุตัวตนของผู้ใช้แต่ละคนที่ใช้งานระบบได้เพื่อให้สามารถเข้าถึงข้อมูลที่มีการกำหนดระดับความลับข้อมูลตัวอย่าง เช่น การระบุชื่อผู้ใช้

3. การพิสูจน์ทราบตัวตน (Authentication) หมายถึงระบบสามารถพิสูจน์ได้ว่าผู้ใช้คือผู้ที่ได้รับอนุญาตจริง ตัวอย่างเช่นป้อนรหัสผ่านที่ตรงกับการระบุชื่อผู้ใช้ได้ถูกต้องและสามารถผ่านเข้าใช้ข้อมูลได้

4. การอนุญาตให้ใช้งาน (Authorization) หมายถึงการตรวจสอบสิทธิของผู้ใช้ว่าสามารถใช้งานระบบได้ในระดับใดหลังจากระบุรายชื่อผู้ใช้และป้อนรหัสผ่านถูกต้องแล้ว เช่น การเข้าถึง การอ่าน การแก้ไข การลบข้อมูล การอนุญาตให้ใช้งานจะครอบคลุมถึงการจัดกลุ่มของผู้ใช้ในระบบ เช่น กลุ่มผู้ใช้ทั่วไป ผู้ดูแลระบบ

5. การตรวจสอบได้ (Accountability) หมายถึงความสามารถในการตรวจสอบการใช้งานระบบได้ว่าผู้ใช้แต่ละคนได้ทำกิจกรรมใดบ้างกับระบบ ตัวอย่างเช่นการจัดเก็บแฟ้มบันทึกข้อมูลการใช้เครือข่าย (Log File) เกี่ยวกับกิจกรรมต่าง ๆ ผู้ใช้แต่ละคนใช้งานระบบ

จุดมุ่งหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ

จุดมุ่งหมายของการรักษาความปลอดภัยสารสนเทศเพื่อให้คุณสมบัติของข้อมูลที่มีความสำคัญและถือว่าเป็นทรัพย์สินอันมีค่าขององค์กรคงความสำคัญ 3 ด้านคือ

1. ความลับ (Confidentiality) หมายถึงข้อมูลที่มีความสำคัญและเป็นทรัพย์สินอันมีค่าไม่ได้ถูกเปิดเผยให้ผู้ไม่หวังดีรับรู้

2. ความคงสภาพ (Integrity) หมายถึงข้อมูลไม่ได้ถูกเปลี่ยนแปลงไปจากสภาพเดิมยังคงมีความถูกต้องของเนื้อหาและแหล่งที่มา

3. ความพร้อมใช้งาน (Availability) หมายถึงข้อมูลและอุปกรณ์ของระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตสามารถใช้งานตามต้องการ

การรักษาความมั่นคงปลอดภัยข้อมูลในองค์กร

ถือเป็นหน้าที่ของบุคลากรภายในองค์กรทุกคน ที่ต้องตระหนักและปฏิบัติเป็นส่วนหนึ่งของการปฏิบัติงานทุกวัน เนื่องจากข้อมูลคือทรัพยากรที่มีความสำคัญช่วยให้องค์กรดำเนินงานได้จนประสบความสำเร็จตามเป้าหมาย กระบวนการรักษาความมั่นคงปลอดภัยข้อมูลในองค์กรประกอบด้วยขั้นตอน ดังนี้

1. การประเมินความเสี่ยง (Risk Assessment) หมายถึงการระบุความเสี่ยงที่จะเกิดต่อทรัพย์สินที่สำคัญเพื่อให้ทราบว่าองค์กรมีความเสี่ยงอยู่ในระดับใด รวมถึงการประมาณค่าความเสี่ยงเป็นการประเมินมูลค่าของทรัพย์สินข้อมูลขององค์กร และสามารถเลือกใช้เครื่องมือหรือระบบป้องกันที่เหมาะสมและมีประสิทธิภาพ มีขั้นตอนสำคัญในการปฏิบัติดังนี้

1) การระบุทรัพย์สิน (Assets Identification)
2) การประเมินช่องโหว่ (Vulnerability Assessment)
3) การประเมินภัยคุกคาม (Threat Assessment)
4) การประเมินความเสี่ยง (Risk Assessment)
5) การจัดการความเสี่ยง (Risk Treatment)

2. กำหนดนโยบาย (Policy) หมายถึงการกำหนดระเบียบ แนวปฏิบัติและหน้าที่ความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยในองค์กร ตามสภาพความเสี่ยงที่ได้รับจากการประเมินนโยบายที่เป็นพื้นฐานในการรักษาความมั่นคงปลอดภัยของข้อมูลประกอบด้วย

1) นโยบายข้อมูล (Information Policy)
2) นโยบายการรักษาความมั่นคงปลอดภัย (Security Policy)
3) นโยบายการใช้งาน (Usage Policy)
4) นโยบายการสำรอง (Backup Policy)
5) ระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการบัญชีผู้ใช้ (Account Management Procedure)
6) ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์ (Incident Handing Procedure)
7) การฟื้นฟูหลังภัยร้ายแรง (Disaster Recovery Plan)

3. การติดตั้งระบบป้องกัน (Implementation) หมายถึงการติดตั้งระบบที่ใช้รักษาความมั่นคงปลอดภัยด้วยการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตจากภายนอกและภายในเครือข่าย เช่นระบบตรวจหาการบุกรุก (Intrusion Detection System) ซึ่งมีทั้งฮาร์ดแวร์และซอฟต์แวร์ ระบบป้องกันจะเกี่ยวข้องกับผู้ดูแลระบบเครือข่ายในการตรวจสอบถึงผลกระทบจากการติดตั้งต่อสภาพแวดล้อมของเครือข่ายโดยรวม

4. การฝึกอบรม (Training) หมายถึงการจัดกิจกรรมฝึกอบรมทั้งในด้านทฤษฎีและปฏิบัติให้กับบุคลากรในองค์กรตามสิทธิและหน้าที่ที่ได้รับในการใช้ข้อมูลและเครือข่าย

5. การตรวจสอบ (Audit) หมายถึงการค้นหาว่ามีการฝ่าฝืนนโยบายและระเบียบปฏิบัติหรือไม่ เนื่องจากถ้าบุคลากรไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยที่กำหนดไว้จะก่อให้เกิดความเสียหายต่อเครือข่าย ข้อมูลและทรัพย์สินขององค์กรอย่างมากตามระดับความสำคัญ

สรุปได้ว่ากระบวนการรักษาความมั่นคงปลอดภัย ที่มีขั้นตอนการประเมินความเสี่ยง การกำหนดนโยบาย การติดตั้งระบบป้องกันมีความเกี่ยวข้องกับบุคลากรในองค์กรทั้งสิ้น โดยบุคลากรต้องมีความรู้ ความเข้าใจต่อกระบวนการประเมินความเสี่ยง การปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัย การดูแลบำรุงรักษาระบบป้องกัน ดังนั้นองค์กรจำเป็นต้องจัดการฝึกอบรม (Training) และสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยให้กับบุคลากร จากกระบวนการรักษาความมั่นคงปลอดภัยดังกล่าว ต้องได้รับการตรวจสอบ (Audit) เพื่อติดตามการให้ความร่วมมือในการประเมินความเสี่ยง ความรับผิดชอบต่อหน้าที่ที่ได้รับมอบหมาย การปฏิบัติตามนโยบายและกฎหมาย ระเบียบข้อบังคับ ความรู้ความชำนาญในการดูแลบำรุงรักษาระบบป้องกันต่าง ๆ เพื่อปรับปรุงแก้ไขเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อทรัพย์สินองค์กรน้อยที่สุด

รูปแบบของภัยคุกคามในสารสนเทศ

การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) ในองค์กรบุคลากรทุกคนต้องมีความเข้าใจ และตระหนักถึงความเสียหายที่ตามมา ดังนั้นองค์กรจึงต้องหาวิธีการในการป้องกันเหตุการณ์ต่าง ๆ โดยเฉพาะอย่างยิ่งบุคลากรด้านไอซีทีจะต้องรอบรู้ถึงวิธีการบุกรุกโจมตี วิธีการป้องกัน รูปแบบของการโจมตี เทคโนโลยีและความก้าวหน้าเป็นอย่างมาก รูปแบบภัยคุกคามถือว่ามีความสำคัญที่หน่วยงานต้องหาแนวทางในการป้องกัน โดยมีรูปแบบของภัยคุกคามที่มักจะเกิดขึ้นดังนี้

1. การปลอมตัว (Spoofing)
2. การเข้าไปยุ่ง (Tampering)
3. การไม่ยอมรับ (Repudiation)
4. การเปิดเผยข้อมูล (Information Disclosure)
5. การปฏิเสธการให้บริการ (Denial of Service)
6. การยกเลิกสิทธิพิเศษ (Elevation of Privilege)

หลักการพื้นฐานในการป้องกันภัยคุกคาม

1. การป้องกันทางกายภาพ (Phycical Security) หมายถึง มาตรการที่ใช้ป้องกันข้อมูลและทรัพย์สินจากภัยคุกคามทางกายภาพทั้งโดยเจตนาและไม่เจตนา ด้วยการจำกัดให้เฉพาะผู้ที่มีหน้าที่ในการใช้งานเท่านั้น

2. ระบบไฟร์วอลล์ (Firewall) หมายถึงระบบป้องกันอันตรายที่มาจากอินเทอร์เน็ตหรือเครือข่ายภายนอก มีหน้าที่ควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกที่ไม่ปลอดภัยกับเครือข่ายภายในขององค์กร

3. ระบบการตรวจหาการบุกรุก (Intrusion Detection System) หมายถึงระบบที่ใช้ตรวจหาการใช้งานเครือข่ายภายในองค์กรในทางที่ผิดไปจากกฎ ข้อบังคับส่งผลต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต กลไกระบบตรวจหาการบุกรุกเป็นการวิเคราะห์กิจกรรมต่าง ๆ ที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ด้วยการตรวจสอบกับข้อกำหนดการใช้งานและการตรวจสอบจากสถิติการใช้งาน

4. วิทยาการเข้ารหัสข้อมูล (Cryptography) หมายถึงกรรมวิธีที่ใช้สำหรับแปลงข้อความทั่วไปให้เป็นข้อความที่เข้ารหัสเพื่อส่งไปยังผู้รับ เมื่อผู้รับได้รับก็จะถอดรหัสข้อมูล (Decryption) เพื่อให้ได้ข้อมูลเดิม

5. การใช้ซอฟต์แวร์ป้องกันไวรัส โดยการติดตั้งโปรแกรมกำจัดไวรัสและตรวจสอบเป็นประจำ ปรับปรุงหรืออัพเดทโปรแกรมกำจัดไวรัส ตรวจสอบอุปกรณ์บันทึกข้อมูลจากการใช้งานร่วมกับผู้อื่น สังเกตความผิดปกติที่เกิดขึ้นในแต่ละวัน หลีกเลี่ยงการคัดลอกโปรแกรมจากภายนอก

สรุปได้ว่าภัยคุกคามคือสาเหตุที่ทำลายความมั่นคงปลอดภัยสารสนเทศขององค์กรวิธีป้องกันต้องได้รับความร่วมมือจากบุคลากรในองค์กรทุกคนในการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยขององค์กร ส่วนกระบวนการรักษาความมั่นคงปลอดภัยอื่น ๆ จึงเป็นหน้าที่ของฝ่ายบริหารต้องบริหารจัดการ จัดหาอุปกรณ์เครื่องมือเช่น ไฟล์วอลล์ ระบบตรวจหาการบุกรุก ซอฟต์แวร์ป้องกันไวรัส การเข้ารหัสข้อมูล เจ้าหน้าที่รักษาความปลอดภัยหรือกฎ ระเบียบการเปิดปิดและการเข้าออกสำนักงาน เพื่อให้เกิดความมั่นคงปลอดภัยต่อข้อมูลและทรัพย์สินทางด้านสารสนเทศขององค์กรมากที่สุด

มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Standard)

กระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศ นอกจากองค์กรจะกำหนดมาตรการต่าง ๆ เพื่อการป้องกันตนเองแล้ว รัฐบาลยังได้กำหนดกฎหมายและระเบียบต่าง ๆ เพื่อควบคุมความมั่นคงปลอดภัยของประเทศโดยรวมให้มีมาตรฐานในระดับเดียวกัน เช่น พระราชบัญญัติว่าด้วยการ

กระทำธุรกรรมทางอิเล็กทรอนิกส์และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกอบกับแนวคิด GRC (Governance Risk and Compliance) กำลังเป็นที่นิยมอยู่ในขณะนี้ ทำให้หลายองค์กรเกิดความตื่นตัวในเรื่อง การปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ (Regulatory Compliance) จากหน่วยงานที่เกี่ยวข้อง เช่น สถาบันการเงิน หน่วยงานรัฐบาล หน่วยงานเอกชน เป็นต้น

การนำมาตรฐานสากลมาเป็นแนวทางปฏิบัติภายในองค์กร ถือได้ว่าเป็นความต้องการของหน่วยงานที่ต้องปฏิบัติตามกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ บุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานมีความรู้ความเข้าใจแนวปฏิบัติ หลักการวิธีการของมาตรฐานนั้นเป็นอย่างดี เพื่อให้การนำมาประยุกต์ใช้ถูกต้อง เหมาะสมกับหน่วยงาน ก่อให้เกิดประสิทธิภาพและประสิทธิผลในองค์กร ในงานวิจัยนี้มีการประยุกต์ใช้มาตรฐานที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

นโยบายการรักษาความปลอดภัย

สิ่งสำคัญสำหรับการใช้งานไฟร์วอลล์ คือ การกำหนดนโยบายการรักษาความปลอดภัย (Security Policy) ถึงแม้ว่าไฟร์วอลล์จะมีประสิทธิภาพ แต่ถ้ามีนโยบายการรักษาความปลอดภัยที่ไม่เพียงพอ ไฟร์วอลล์ก็จะไม่มีประโยชน์มากนัก ดังนั้น ก่อนที่จะติดตั้งไฟร์วอลล์ควรกำหนดนโยบายการรักษาความปลอดภัยที่สามารถควบคุมหรือป้องกันทราฟฟิก ที่อาจมีผลกระทบต่อเครือข่ายให้มากที่สุด เมื่อกำหนดนโยบายแล้ว ต่อไปคือ นำนโยบายไปบังคับใช้ในไฟร์วอลล์ กฎในความปลอดภัยนั้นเรียกว่า ACL (Access Control List) หรือไฟร์วอลล์รูจ (Firewall Rule)

1. Intrusion Detection System (IDS) เป็นระบบตรวจจับการบุกรุก หรือ IDS เป็นเครื่องมือสำหรับการรักษาความปลอดภัยประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อมีรการบุกรุก หรือมีการพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ป้องกันการบุกรุก แต่ว่าเป็นเครื่องมือในการแจ้งเตือนเท่านั้น เปรียบเหมือนสัญญาณกันขโมยของรถยนต์ ซึ่งจะทำงานโดยการส่งสัญญาณ เมื่อมีการบุกรุก พวกแฮกเกอร์ก็อาจจะหลีกเลี่ยงการบุกรุกเครือข่ายนี้ เพราะเกรงว่าจะถูกจับได้

หน้าที่หลักของ IDS คือการแจ้งเตือนการเข้าถึงเครือข่ายที่ผิดปกติ สิ่งที่เป็นประเด็นสำคัญในการออกแบบ IDS คือ เหตุการณ์ใดคือส่งที่ถือว่าผิดปกติ ดังนั้น การใช้ IDS ขึ้นอยู่กับว่าอะไรที่จะแจ้งให้ทราบ

ปัญหาของ IDS คือ บางครั้ง ไม่สามารถตรวจจับการบุกรุกได้ เนื่องจากปัญหาเรื่องการทำงานกับเครือข่ายที่ใช้ระบบ สวิตซ์ชิ่ง (Swiching) เนื่องจากทราฟฟิกที่วิ่งบนเครือข่ายนั้นจะไม่กระจายไปทั่ว ทำให้ยากต่อการตรวจจับ นอกจากนั้นยังมีปัญหาอื่น ๆ เช่น ในกรณีของการใช้ IDS

แบบซิกเนเจอร์เบส นั้น บางทีซิกเนเจอร์ในรูปแบบต่าง ๆ ของการบุกรุกที่ IDS รู้จักไม่ได้ถูกอัพเดทอย่างสม่ำเสมอ ทำให้ IDS ไม่สามารถตรวจจับการบุกรุกใหม่ๆ ได้

2. ขีดความสามารถของ IDS

1) มอนิเตอร์และวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบและพฤติกรรมของผู้ใช้

2) ทดสอบระดับความปลอดภัยของระบบ

3) บอกถึงระดับมาตรฐานความปลอดภัยของระบบ และเฝ้าติดตามการเปลี่ยนแปลง

4) เรียนรู้ลำดับเหตุการณ์ของระบบที่เกิดจากการโจมตีที่รู้ล่วงหน้า

5) เรียนรู้ลำดับเหตุการณ์ของระบบที่แตกต่างจากเหตุการณ์ปกติ

6) จัดการข้อมูลเกี่ยวกับอีเวนท์ล็อก (Event Log) และออดิทล็อก (Audit Log) ของระบบปฏิบัติการ

7) รายงานข้อมูลเกี่ยวกับนโยบายการรักษาความปลอดภัยพื้นฐาน

8) อนุญาตให้ผู้ที่ยังไม่มีความชำนาญด้านการรักษาความปลอดภัย สามารถมอนิเตอร์ความปลอดภัยได้

3. IDS ไม่สามารถทำหน้าที่ต่อไปนี้ได้

1) ไม่สามารถปิดช่องโหว่ หรือจุดอ่อนของระบบที่ไม่ได้ป้องกันโดยระบบการรักษาความปลอดภัยอื่น ๆ เช่น ไฟร์วอลล์ การพิสูจน์ทราบตัวตน การเข้ารหัสข้อมูล การควบคุมการเข้าถึง และการป้องกันไวรัส

2) ไม่สามารถตรวจจับ รายงาน และตอบโต้การโจมตีได้ในช่วงเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น หรือโหลดของเครือข่ายมากเกินไป

3) ไม่สามารถตรวจจับการโจมตีแบบใหม่ หรือการโจมตีเก่าที่ได้ปรับเปลี่ยนรูปแบบการโจมตี

4) ไม่สามารถตอบโต้การโจมตีได้อย่างมีประสิทธิภาพ

5) ไม่สามารถสืบหาผู้บุกรุกได้อย่างอัตโนมัติ

6) ไม่สามารถขัดขวางไม่ให้โจมตี IDS เอง

7) ไม่สามารถป้องกันปัญหาเกี่ยวกับความถูกต้องของแหล่งข้อมูล

8) ไม่สามารถทำงานได้ดีในระบบเครือข่ายที่ใช้สวิทซ์

แนวโน้มความเสี่ยงด้านภัยคุกคามทางไซเบอร์

1. ระดับการเปลี่ยนแปลงทางเทคโนโลยีและผลกระทบจากเทคโนโลยี ก็ได้ปรากฏให้เห็นชัด โดยมีเทคโนโลยีใหม่ ๆ เกิดขึ้นมากมาย และการที่มีเทคโนโลยีอินเทอร์เน็ตแพร่หลายทั่วโลก โดยเฉพาะอย่างยิ่ง ในประเทศกำลังพัฒนา ยิ่งเพิ่มโอกาสที่สำคัญต่อสังคมมากขึ้น การพัฒนาเหล่านี้ได้นำมาซึ่งข้อได้เปรียบที่สำคัญที่มีการเชื่อมต่อในทุกวันนี้ แต่จากการที่ประเทศไทยยังคงต้องพึ่งพาเครือข่ายในต่างประเทศ จึงเป็นโอกาสสำหรับผู้ที่พยายามจะละเมิด ต่อระบบและข้อมูลของประเทศ ซึ่งการกระทำทางไซเบอร์ที่อันตรายนั้น ไม่มีขอบเขตระหว่างประเทศ ผู้บุกรุกที่เป็นภาครัฐกำลังทดลองใช้ขีดความสามารถในการโจมตีทางไซเบอร์ โดยอาชญากรไซเบอร์ ได้มีความพยายามขยายแนวทางการดำเนินงานเชิงกลยุทธของตนเพื่อให้ได้ผลประโยชน์มากขึ้นจากพลเมือง องค์กร และสถาบันต่าง ๆ ของประเทศ ผู้ก่อการร้ายและผู้สนับสนุนต่าง ๆ กำลังดำเนินการโจมตีในระดับต่ำอย่างต่อเนื่อง และต้องการที่จะทำในสิ่งที่มีผลกระทบมากยิ่งขึ้น

2. อาชญากรรมทางไซเบอร์มีความผิดทางอาญาสองรูปแบบ ได้แก่:

2.1 อาชญากรรมที่ขึ้นกับไซเบอร์ (cyber-dependent crimes) คือ อาชญากรรมที่เกิดขึ้นจากการใช้อุปกรณ์ทางเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งอุปกรณ์ดังกล่าวเป็นทั้งเครื่องมือในการก่ออาชญากรรมและเป้าหมายของอาชญากรรม (เช่น การพัฒนาและแพร่กระจายมัลแวร์สำหรับหวังผลทางการเงิน, การแฮกเพื่อโจรกรรมข้อมูลและทำให้เกิดความเสียหาย, การบิดเบือนหรือทำลายข้อมูลและ / หรือเครือข่ายหรือกิจกรรม)

2.2 อาชญากรรมแบบที่ใช้ไซเบอร์ (cyber-enabled crimes) เป็นอาชญากรรมแบบดั้งเดิมที่สามารถเพิ่มขนาดหรือเข้าถึงได้โดยใช้คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์หรือ ICT รูปแบบอื่น ๆ (เช่น การฉ้อโกงบนโลกไซเบอร์และการโจรกรรมข้อมูล)

3. อาชญากรรมทางไซเบอร์ที่ร้ายแรงที่สุดที่เกิดขึ้นในประเทศไทยส่วนใหญ่ คือ การหลอกลวง, การขโมย และการขูดรีดเงิน (fraud, theft and extortion) อย่างไรก็ตามภัยคุกคามนี้ก็เกิดจากประเทศและภูมิภาคอื่น ๆ เช่นกัน

4. ถึงแม้ว่าจะสามารถระบุผู้ที่ต้องรับผิดชอบต่อการกระทำทางอาชญากรรมไซเบอร์ที่สร้างความเสียหายต่อประเทศได้นั้น แต่ก็มีความยากลำบากสำหรับประเทศและหน่วยงานบังคับใช้กฎหมายระหว่างประเทศในการฟ้องร้องเมื่อบุคคลเหล่านั้นอยู่ในเขตอำนาจศาลที่มีข้อจำกัดหรือไม่มีข้อตกลงในเรื่องการส่งผู้ร้ายข้ามแดน

5. กลุ่มแฮกเกอร์หลักๆ จากทั่วทุกมุมโลกได้ทำการพัฒนาและใช้งานมัลแวร์ขั้นสูงที่เผยแพร่ต่อคอมพิวเตอร์และเครือขายของประชากรโลก, อุตสาหกรรม และรัฐบาลของประเทศต่าง ๆ ซึ่งผลกระทบได้กระจายไปทั่วรวมทั้งประเทศไทย โดยการโจมตีเหล่านี้มีความก้าวร้าวและ

เผชิญหน้ามาก Distributed denial of service (DDoS) ขึ้นซึ่งเห็นได้จากการใช้ Ransomware เพิ่มมากขึ้นและภัยคุกคามจากการโจมตีระบบเครือข่ายแบบ Distributed denial of service (DDoS)

6. ขณะที่กลุ่มแฮกเกอร์หลัก ๆ ในระดับโลกอาจก่อให้เกิดภัยคุกคามที่สำคัญต่อการเติบโตและความมั่นคง แต่เรื่องที่น่าห่วงใยไม่แพ้กันคือภัยคุกคามจากการกระทำของอาชญากรรมไซเบอร์ที่มีความซับซ้อนน้อยกว่า แต่แพร่กระจายในกลุ่มบุคคลหรือองค์กรขนาดเล็ก

7. เรามักเห็นความพยายามของรัฐและกลุ่มที่ได้รับการสนับสนุนจากรัฐ ในการเจาะเครือข่ายของประเทศเพื่อประโยชน์ทางด้านการเมือง การทูต การจารกรรมเทคโนโลยี การค้าและผลประโยชน์ทางยุทธศาสตร์ โดยมุ่งเน้นไปที่รัฐบาลและการป้องกันประเทศ การเงิน พลังงานและโทรคมนาคม

8. ความสามารถและผลกระทบของโครงการไซเบอร์ของรัฐในแต่ละประเทศแตกต่างกัน ประเทศที่ก้าวหน้าที่สุดยังคงเพิ่มขีดความสามารถในการรวมการเข้ารหัสและการให้บริการการระบุตัวตนลงในเครื่องมือของตนเพื่อที่จะรักษาข้อมูลที่เป็นความลับ แม้ว่าจะมีขีดความสามารถทางเทคนิคในการใช้การโจมตีที่ซับซ้อน แต่ก็มักจะสามารถบรรลุเป้าหมายได้โดยใช้เครื่องมือและเทคนิคขั้นพื้นฐานต่อเป้าหมาย

9. มีหลายประเทศที่มีขีดความสามารถทางเทคนิคที่ก่อให้เกิดภัยคุกคามอย่างร้ายแรงต่อความมั่นคงและการเติบโตโดยรวมของประเทศไทยได้ และมีอีกหลายประเทศกำลังพัฒนาโปรแกรมทางไซเบอร์ที่มีความซับซ้อนซึ่งอาจเป็นภัยคกคาม ต่อประเทศไทยในอนาคตอันใกล้นี้ หลายประเทศที่มีความพยายามในการพัฒนา ขีดความสามารถในการสอดแนมทางไซเบอร์สามารถซื้อเครื่องมือที่หาซื้อได้ ทั่วไปสำหรับหาประโยชนจากเครือข่ายคอมพิวเตอร์เช่นใช้ในการโจรกรรมทางไซเบอร์

10. นอกจากภัยคุกคามจากการโจรกรรมแล้ว ยังมีกลุ่มแฮกเกอร์ที่เป็นภัยคุกคามจากต่างประเทศจนวันหนึ่งที่มีการพัฒนาและใช้ขีดความสามารถทาง ไซเบอร์ที่ไม่เหมาะสม รวมทั้งใช้ไปในทางมุ่งทำลายด้วย ซึ่งขีดความสามารถ เหล่านี่คุกคามต่อความมั่นคงของโครงสร้างพื้นฐานสำคัญและระบบการควบคุมอุตสาหกรรมที่สำคัญของประเทศ บางประเทศอาจใช้ขีดความสามารถเหล่านี้ในการฝ่าฝืนกฎหมายระหว่างประเทศโดยเชื่อว่า พวกเขาสามารถทำเช่นนั้นได้โดยได้รับการยกเว้นโทษ

11. กลุ่มผู้ก่อการร้ายยังคงมุ่งมั่นที่จะสร้างความเสียหายจากการกระทำทางไซเบอร์ที่เป็นอันตรายต่อประเทศและผลประโยชน์ของประเทศ โดยมีแนวโน้มว่า ผลกระทบของกิจกรรมที่ใช้ขีดความสามารถต่ำต่อประเทศในปัจจุบันนั้นถือเป็นอัตราส่วนที่สูงมาก เพียงการเปลี่ยนข้อมูล (Defacements) และการแฮกข้อมูลส่วน ตัวที่รั่วไหลทางออนไลน์ ช่วยให้กลุ่มผู้ก่อการร้ายได้รับความสนใจจากสื่อมวลชนและข่มขู่ผู้ที่ตกเป็นเหยื่อได้

12. การประเมินผลในปัจจุบันคือการโจมตีทางกายภาพยังเป็นการโจมตีที่ผู้ก่อการร้ายจะยังคงให้ความสำคัญมากกว่าการโจมตีทางไซเบอร์ในช่วงเวลานี้โดยมีการคาดว่าในอนาคตอันใกล้ศักยภาพของผู้มีความเชี่ยวชาญและทักษะในด้านไซเบอร์จำนวนมากจะปรากฏออกมาให้เห็นมากขึ้น เช่นเดียวกับความเสี่ยงที่องค์กรผู้ก่อการร้ายจะพยายามแสวงหาแหล่งข้อมูลภายใน ผู้ก่อการร้ายอาจใช้ขีดความสามารถในโลกไซเบอร์ใด ๆ เพื่อให้บรรลุผลสูงสุด ดังนั้นแม้การเพิ่มขึ้นของขีดความสามารถในการก่อการร้ายในระดับปานกลางอาจเป็นภัยคุกคามที่สำคัญต่อประเทศและผลประโยชน์ของประเทศได้

13. กลุ่ม Hacktivist จะขับเคลื่อนตามวาระหรือประเด็นต่าง ๆ ที่มี ด้วยการสร้างและเลือกเป้าหมาย โดยกิจกรรมทางไซเบอร์ของ Hacktivist ส่วนใหญ่จะก่อกวนในรูปแบบของ Defacement หรือ DDoS

ภัยคุกคามจากอินไซเดอร์หรือคนภายใน ยังคงเป็นความเสี่ยงด้านไซเบอร์ต่อองค์กรในประเทศ คนภายในที่เป็นบุคลากรที่น่าเชื่อถือขององค์กรและมีสิทธิ์เขาถึงระบบและข้อมูลที่สำคัญถือเป็นภัยคุกคามที่น่ากลัวที่สุด ซึ่งอาจทำให้เกิดความ เสียหายทางการเงินและชื่อเสียงขององค์กรจากการขโมยข้อมูลสำคัญและทรัพย์สินทางปัญญาสิ่งที่น่ากังวลไม่นอยกว่ากันคือ บุคคลภายในหรือพนักงานที่ทำให้เกิดอันตรายทางไซเบอร์โดยไม่ตั้งใจจากการเปิดอีเมล์ฟิชชิ่ง หรือใช้ USB ที่ติดไวรัส หรือละเลยขั้นตอนด้านความปลอดภัยและดาวน์โหลดเนื้อหาที่ไม่ปลอดภัยจากอินเทอรเน็ต ถึงแม้พวกเขาจะมิได้ตั้งใจทำให้เกิดความเสียหายทางไซเบอร์ต่อองค์กร แต่การมีสิทธิ์ในการเข้าถึงระบบและข้อมลหมายความว่าการกระทำของพวกเขาอาจก่อให้เกิดความเสียหายเช่นเดียวกับอินไซเดอร์ ซึ่งบุคคลเหล่านี่มักตกเป็นเหยื่อที่สามารถเข้าถึงเครือข่ายขององค์กรหรือที่ตามคำแนะนำโดยบริสุทธิ์ใจแต่สร้างประโยชน์ให้แก่ผู้หลอกลวงความเสี่ยงทางไซเบอร์โดยรวมต่อองค์กรจากภัยคุกคามจากอินไซเดอร์ไม่ได้เป็นเพียงเรื่องเกี่ยวกับการเข้าถึงระบบสารสนเทศและเนื้อหาโดยไม่ได้รับอนุญาตเท่านั้น การควบคุมความปลอดภัยทางกายภาพเพื่อปกป้องระบบจากการเขาถึงทำไม่เหมาะสมหรือการลบ ข้อมูลสำคัญหรือข้อมูลที่มีเจ้าของในรูปแบบต่าง ๆ ต่างมีความสำคัญเท่าเทียมกัน

14. กลุ่มแฮกเกอร์มือใหม่ที่ยังขาดความชำนาญในการเจาะระบบคอมพิวเตอร์ โดยใช้โปรแกรมที่พัฒนาโดยคนอื่นมาใช้โจมตีทางไซเบอร์ ซึ่งไม่ได้เป็นภัยคุกคามที่สำคัญต่อเศรษฐกิจหรือสังคมในวงกว้าง แต่พวกเขามีสิทธิ์เข้าถึงคู่มือการเจาะข้อมูลและเครื่องมือต่าง ๆ บนอินเทอร์เน็ต เนื่องจากช่องโหว่ที่พบในระบบที่ใช้อินเทอรเน็ตซึ่งถูกนำมาใช้โดยองค์กรหลายแห่งซึ่งบางครั้งการกระทำของ "Script Kiddies" อาจทำให้เกิดผลเสียหายร้ายแรงต่อองค์กรได้

15. ประชาชนส่วนใหญ่เข้าใจเรื่องความมั่นคงปลอดภัยทางไซเบอร์ในมุมมองของการปกป้องอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ เดสก์ทอป หรือแลปทอป เป็นต้น ตั้งแต่นั้นมา อินเทอรเน็ตก็ได้เข้ามามีบทบาทในชีวิตประจำวันมากขึ้น แต่แนวโน้ม เทคโนโลยี Internet of Things กำลังสร้างโอกาสใหม่ๆ รวมทั้งผลกระทบที่อาจเกิดขึ้นตามมาจากการโจมตีที่ทำให้เกิดความเสียหายได้

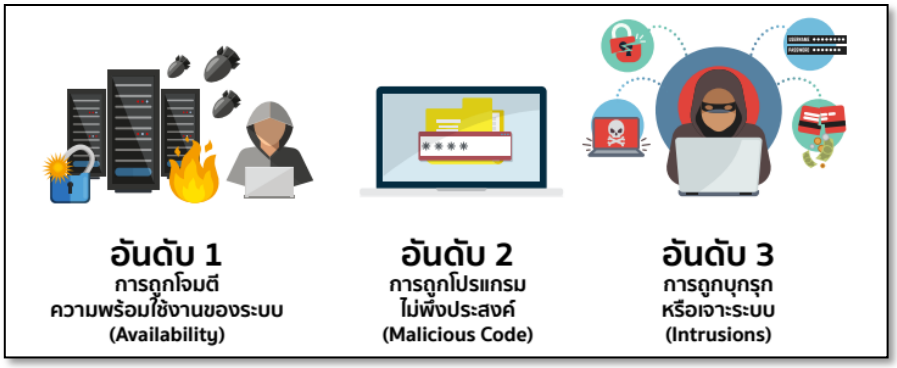
16. การใช้การเชื่อมต่อในกระบวนการควบคุมอุตสาหกรรมในระบบที่สำคัญได้เพิ่มขึ้นอย่างรวดเร็วในหลากหลายอุตสาหกรรมไม่วาจะเป็นพลังงาน การทำเหมืองแร่ เกษตรกรรม และการบิน เพิ่มความเสี่ยงให้สูงขึ้นโดยอาจจะถูกแฮกและดัดแปลงจนมีผลกระทบร้ายแรงตามมา

17. ดังนั้นประชาชนจึงไม่เพียงแต่เสี่ยงต่ออันตรายจากโลกไซเบอร์ที่เกิดจากอุปกรณ์ที่ขาดความปลอดภัยทางไซเบอร์เท่านั้น แต่ยังมความเสี่ยงจากภัยคุกคามต่อระบบที่มีการเชื่อมต่อ ซึ่งเป็นพื้นฐานของสังคม สุขภาพ และสวัสดิการของประชาชนในทุกวันนี้

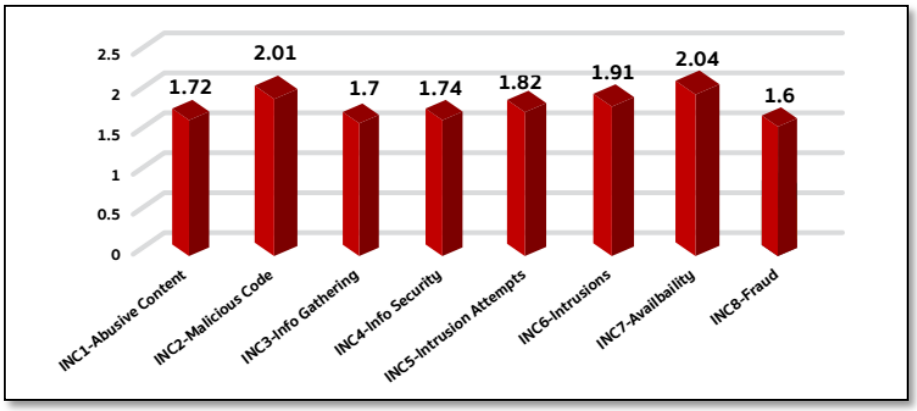
18. การตระหนักถึงช่องโหว่ทางเทคนิคทั้งในซอฟต์แวร์และเครือข่าย และความต้องการสำหรับการใช้ไซเบอร์ที่ถูกต้องในประเทศได้เพิ่มขึ้นตลอดในช่วงห้าปีที่ผ่านมา ส่วนหนึ่งเป็นผลมาจากการริเริ่มของรัฐบาลในเรื่องความมั่นคงปลอดภัยไซเบอร์และยังเกิดจากการเพิ่มขึ้นของเหตุการณ์สำคัญทางไซเบอร์ที่ส่งผลต่อรัฐบาล และบริษัทต่าง ๆ ด้วย ซึ่งการโจมตีทางไซเบอร์ไม่ได้ซับซ้อนหรือหลีกเลี่ยงไม่ได้เสมอไปแต่มักเป็นผลมาจากการใช้ประโยชน์ที่ไม่ถูกต้องซึ่งสามารถแก้ไขได้ไม่ยากและบ่อยครั้งที่สามารถป้องกันช่องโหว่ได้

ความเสียหายหรือผลกระทบจากเหตุภัยคุกคามไซเบอร์

จากการสำรวจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) พบว่า ในระยะเวลา 12 เดือนที่ผ่านมา มีจำนวนหน่วยงานที่เคยประสบเหตุภัยคุกคามไซเบอร์ เป็นสัดส่วนสูงถึงประมาณร้อยละ 90 เหตุภัยคุกคามที่สร้างความเสียหายหรือผลกระทบต่อหน่วยงานมากที่สุด 3 อันดับแรก พิจารณาเปรียบเทียบจากค่าเฉลี่ยของระดับผลกระทบโดยรวมของหน่วยงานทั้งหมด ได้แก่ เหตุจากการถูกโจมตีความพร้อมใช้งานของระบบ (Availabillity) เหตุจากการถูกโปรแกรมไม่พึงประสงค์ (Malicious Code) และเหตุจากการถูกบุกรุกหรือเจาะระบบ (Intrutions) รายละเอียดดังในภาพประกอบที่ 2.1 และภาพประกอบที่ 2.2



ภาพประกอบที่ 2.1 ภัยคุกคามที่สร้างความเสียหายหรือผลกระทบต่อหน่วยงานมากที่สุดใน 3 อันดับแรก (แหล่งที่มา https://www.thaicert.or.th/index.html)



ภาพประกอบที่ 2.2 ความเสียหายหรือผลกระทบจากเหตุภัยคุกคามไซเบอร์ที่หน่วยงานได้รับ (แหล่งที่มา https://www.thaicert.or.th/index.html)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ได้ระบุถึงการตรวจพบภัยคุกคามในส่วนของภาครัฐ ที่พบว่า เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดต่อหน่วยงานอิสระ ได้แก่ ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) หน่วยงานของศาล ได้แก่ การบุกรุกหรือถูกเจาะระบบ (Intrusion) กระทรวงได้แก่ โปรแกรมไม่พึงประสงค์ (Malicious Code) สำนักนายกรัฐมนตรี ได้แก่ เนื้อหาที่เป็นภัย (Abusive Content) องค์ประกอบวิชาชีพ องค์การมหาชน รัฐวิสาหกิจ และมหาวิทยาลัยของรัฐ ได้แก่ ความพร้อมใช้งานของระบบ (Availability) รายละเอียดดังในตารางที่ 2.1

ตารางที่ 2.1 เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดต่อหน่วยงานภาครัฐ

(แหล่งที่มา https://www.thaicert.or.th/index.html)

ภาครัฐ	เหตุภัยคุกคามที่สร้างความเสียหายให้สูงสุด
หน่วยงานอิสระ	Intrusion Attempts (ความพยายามบุกรุกเข้าระบบ)
หน่วยงานของศาล	Intrusions (การถูกบุกรุกหรือเจาะระบบ)
กระทรวง	Malicious Code (โปรแกรมไม่พึงประสงค์)
สำนักนายกรัฐมนตรี	Abusive Content (เนื้อหาที่เป็นภัย)
องค์กรประกอบวิชาชีพ	Availability (ความพร้อมใช้งานของระบบ)
องค์การมหาชน	
รัฐวิสาหกิจ	
มหาวิทยาลัยของรัฐ	

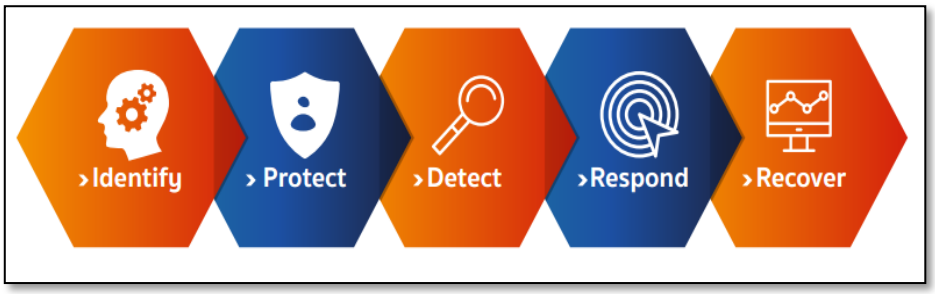
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ได้ระบุถึงการตรวจพบภัยคุกคามในส่วนของภาคเอกชน ที่พบว่า เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดต่อธุรกิจการเงิน (Bank) ได้แก่ การฉ้อโกง หรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ธุรกิจหลักทรัพย์ ได้แก่ การบุกรุก หรือเจาะระบบ (Intrusions) และ การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ธุรกิจชำระเงินและประกันภัย ความพร้อมใช้งานของระบบ (Availability) พลังงาน ได้แก่ เนื้อหาที่เป็นภัย (Abusive Content) โรงพยาบาล เทคโนโลยีสารสนเทศและการสื่อสาร และขนส่งและโลจิสติกส์ ได้แก่ โปรแกรมไม่พึงประสงค์ (Malicious Code) ดังรายละเอียดในตารางที่ 2.2

ตารางที่ 2.2 เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดต่อหน่วยงานภาคเอกชน

(แหล่งที่มา https://www.thaicert.or.th/index.html)

กลุ่มธุรกิจเอกชน	เหตุภัยคุกคามที่สร้างความเสียหายให้สูงสุด
ธุรกิจการเงิน (Bank)	Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์)
ธุรกิจหลักทรัพย์	Intrusions (การบุกรุกหรือเจาะระบบ) และ Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์)
ธุรกิจชำระเงิน (e-Payment)	Availability (ความพร้อมใช้งานของระบบ)
ธุรกิจประกันภัย	
พลังงาน	Abusive Content (เนื้อหาที่เป็นภัย)
โรงพยาบาล	Malicious Code (โปรแกรมไม่พึงประสงค์)
เทคโนโลยีสารสนเทศและการสื่อสาร	
ขนส่งและโลจิสติกส์	

กรอบการทำงาน และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ เมื่อพิจารณากรอบการทำงาน (Framework) และการดำเนินงาน (Implementation) ด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานในประเทศไทย ตามแนวคิดแบบจำลองของ NIST (National Institute of Standard and Technology) หรือสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา 5 กรอบการทำงานดังภาพประกอบที่ 2.3



ภาพประกอบที่ 2.3 กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์

งานวิจัยที่เกี่ยวข้อง

วิภารัตน์ ปทักขินัง และ ประสงค์ ปราณีตพลกรัง (2557) ศึกษาเรื่อง การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ขององค์กร พบว่า องค์ประกอบความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ จะประกอบไปด้วย 7 ส่วน ได้แก่ 1) ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ 2) ด้านกฎระเบียบที่เกี่ยวข้อง 3) ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ 4) ด้านการป้องกันอาชญากรรมไซเบอร์ 5) การพัฒนากำลังพลด้านไซเบอร์ 6) ด้านงบประมาณการวิจัย และ 7) ด้านความร่วมมือกับหน่วยงานอื่น

ณัฐวี อุตกฤษฎ์ (2555) ศึกษาเรื่อง การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร พบว่า การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงของสารสนเทศในองค์กรคือการเตรียมการรับเหตุการณ์ฉุกเฉินที่คุกคามต่อสารสนเทศซึ่งองค์กรควรให้ความสำคัญเพราะบางครั้งองค์กรอาจอยู่ในสภาวะที่ไม่สามารถรองรับและตอบสนองเหตุการณ์ดังกล่าวได้ด้วยการปฏิบัติตามแผนปกติบทความนี้จึงมุ่งเน้นให้เห็นถึงความสำคัญของการวางแผนรองรับสำหรับเหตุการณ์ฉุกเฉินในองค์กรและยังอธิบายถึงขั้นตอนของการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินโดยพิจารณาตามแนวทางปฏิบัติของ NIST SP 800-34 และส่วนประกอบหลัก 4 ประการของแผนรองรับเหตุการณ์ฉุกเฉินได้แก่1) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 2) การวางแผนเพื่อตอบสนองต่อเหตุการณ์ที่ไม่คาดคิด (Incident Response

Plan: IRP) 3) การวางแผนฟื้นฟูเหตุการณ์จากความเสียหายที่รุนแรง (Disaster Recovery Plan: DRP) และ 4) การวางแผนเพื่อดำาเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง (Business Continuity Plan: BCP)

ศิวลีย์ สิริโรจน์บริรักษ์ (2558) ศึกษาเรื่อง การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัย ไซเบอร์ของกระทรวงกลาโหม พบว่า 1) กรอบนโยบาย ยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ได้แก่ พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของ กห. พ.ศ. 2551, นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กห. พ.ศ. 2554, ยุทธศาสตร์ กห. อิเล็กทรอนิกส์ (e-Defence), แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของ กห. ฉบับที่ 3 พ.ศ. 2557-2561, การจัดตั้งศูนย์บัญชาการไซเบอร์ กห. 2) มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และมาตรฐาน IT BPM 3) แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานในระดับสากล เชิงนโยบาย ได้แก่ ส่วนบังคับการ ต้องเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อปัญหา/เหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงได้อย่างรวดเร็ว ส่วนนโยบายและแผน ต้องมีการบรรจุข้อกำหนดในกระบวนการจัดซื้อจัดจ้าง อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้อุปกรณ์มีความปลอดภัยในระดับสากล ส่วนปฏิบัติการไซเบอร์ จะต้องมีหน่วยปฏิบัติการเชิงรับและเชิงรุก สงครามข้อมูลข่าวสาร ส่วนวิจัยและพัฒนาไซเบอร์จะต้องจัดตั้งส่วนงานวิจัยระบบสงครามข้อมูลข่าวสารเพื่อพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และต้องบรรจุอัตราจเรทหารที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อดำเนินการตรวจสอบตามหลักการICT Audit เชิงปฏิบัติ ได้แก่ 1) ควรจัดทำหลักสูตร CyberTraining เพื่ออบรมความรู้เกี่ยวกับการใช้งานซอฟต์แวร์ และฮาร์ดแวร์รวมทั้งการให้ทุนการศึกษาต่อในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับ 2) ควรมีการจัดการองค์ความรู้ด้านไซเบอร์ ในหน่วยงาน และควรนำ E-Document มาใช้ในการปฏิบัติราชการมากยิ่งขึ้น

สมชาย บุญเจิม (2557) ศึกษาเรื่อง การพัฒนาระบบตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศภายในกองทัพบก พบว่า แนวทางการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศที่มีอยู่ ศึกษาจุดเด่นและข้อจำกัดของแต่ละแนวทาง เพื่อพิจารณาคัดเลือกแนวทางการตรวจสอบความมั่นคงปลอดภัยที่เหมาะสมสำหรับกองทัพบก ซึ่งขอบเขตของการตรวจสอบนั้นครอบคลุมเครื่องแม่ข่าย

J. Ryoo และคณะ (2009) ได้วิจัยเพื่อประเมินความพร้อมระบบรักษาความมั่นคงปลอดภัยข้อมูลในเทศบาลของรัฐเพนซิลเวเนีย เป็นการประเมินโครงสร้างพื้นฐาน ประเมินการใช้คอมพิวเตอร์ ประเมินความรู้ในการวางแผนการรักษาความมั่นคงปลอดภัย สถานะของภัยคุกคามภายใน ประเมินผลการปฏิบัติงานประจำวัน ผลการวิจัยพบว่า จุดแข็งคือด้านโครงสร้างพื้นฐานของเทศบาลที่เกี่ยวกับความมั่นคงปลอดภัย จุดอ่อนคือ การฝึกอบรมและองค์ความรู้ด้านความมั่นคงปลอดภัย

T. Sommestad และคณะ (2009) วิจัยเรื่อง Cybersecurity Risks Assessment with Bayesian Defense Graphs and Architectural Models เป็นการนำเสนอตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยไซเบอร์ ตามสถานการณ์ที่แตกต่างกันโดยใช้สถิติแบบเบส์เพื่อแสดงกราฟการโจมตี ผลการวิจัยพบว่า ตัวแบบนี้ช่วยให้การคำนวณโอกาสที่จะถูกโจมตีถูกต้องตามที่คาดการณ์ไว้

บทที่ 3
วิธีดำเนินการวิจัย

การศึกษาและวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาแอปพลิเคชันสำหรับจัดเก็บสถิติและรายงานภัยคุกคามทางไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก โดยผู้วิจัยได้ดำเนินการดำเนินการขั้นตอนการวิจัยดังนี้

รูปแบบในการดำเนินการวิจัย
ประชากรและกลุ่มตัวอย่าง
ขั้นตอนในการดำเนินการวิจัย
เครื่องมือที่ใช้ในการพัฒนาระบบ
คำจำกัดความของ ผู้ใช้งานระบบ
วงจรการทำงานโดยรวมของระบบ
เครื่องมือที่ใช้ในการวิจัย
การเก็บรวบรวม
สถิติที่ใช้ในการวิเคราะห์ข้อมูล
ระยะเวลาในการดำเนินงาน

รูปแบบในการดำเนินการวิจัย

1. ศึกษากระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์ การรักษาความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ภายในศูนย์ไซเบอร์กองทัพบก

2. วิเคราะห์และออกแบบระบบเชิงวัตถุโดยใช้หลักการของ ยูสเคสไดอะแกรม (Use case Diagram) โดยในการออกแบบได้พิจารณาจากความต้องการของผู้ใช้ในศูนย์ไซเบอร์กองทัพบกเป็นหลัก รวมทั้งความสัมพันธ์ของผู้ที่เกี่ยวข้องในระบบ

3. ศึกษาการพัฒนาระบบตรวจสอบ เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก ทางด้านการจัดเก็บสถิติภัยคุกคาม และการรายงานผล

4. ทำการพัฒนาแอปพลิเคชัน สำหรับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก

5. ทำการประเมินประสิทธิภาพและความเหมาะสมของระบบโดยผู้ใช้งานระบบ และผู้บังคับบัญชา

ประชากรและกลุ่มตัวอย่าง

1. ประชากรที่ใช้ในการวิจัยครั้งนี้กำหนดกลุ่มตัวอย่างเป็นกำลังที่ปฏิบัติงานอยู่ภายในหน่วยงานศูนย์ไซเบอร์กองทัพบก เป็นเพศชายจำนวน 35 คน ส่วนใหญ่มีอายุมากกว่า 30 ปี ร้อยละ 72 เป็นนายทหารสัญญาบัตรร้อยละ 57 การศึกษาระดับปริญญาตรีขึ้นไป ร้อยละ 86 และมีอายุงานมากกว่า 10 ปีขึ้นไปร้อยละ 72 เป็นตัวแทนในการตอบแบบสอบถาม

2. ผู้วิจัยได้ใช้เครื่องมือทางสถิติ (Statistic) เพื่อการวิเคราะห์ข้อมูล แปลผลและสรุปผล โดยค่าสถิติที่วิเคราะห์ได้ดำเนินการเป็นสถิติสำหรับการประเมินความเหมาะสมของโมเดลการจัดการเรียนรู้ และประเมินสถิติเชิงบรรยายและสรุปผลการวิจัย ประกอบด้วยส่วนเบี่ยงเบนมาตรฐาน (S.D) และค่าเฉลี่ย ($\overline{X}$) โดยใช้มาตรวัดตามมาตราส่วนประมาณค่ากำหนดระดับค่าคะแนนในการตอบแบบสอบถามระดับความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศใช้ 5 ระดับ ดังนี้

5	หมายถึง	มีความพร้อมมากที่สุด
4	หมายถึง	มีความพร้อมมาก
3	หมายถึง	มีความพร้อมปานกลาง
2	หมายถึง	มีความพร้อมน้อย
1	หมายถึง	มีความพร้อมน้อยที่สุด

3. การแปลความหมายระดับค่าคะแนนเฉลี่ย ข้อมูลวัดมาตราส่วนประมาณค่าพิจารณาตามเกณฑ์ ระดับค่าคะแนนดัชนีความสอดคล้อง (Index of Item Objective Conguence : IOC) ของข้อคำถามระดับค่าคะแนนเป็น 2 ระดับดังนี้

ระดับคะแนนเฉลี่ย -1.00 - 0.49 หมายถึง มีระดับความสอดคล้องไม่เหมาะสม

ระดับคะแนนเฉลี่ย 0.50 – 1.00 หมายถึง มีระดับความสอดคล้องเหมาะสม

4. การแปลความหมายระดับค่าคะแนนเฉลี่ย ข้อมูลวัดมาตราส่วนประมาณค่าพิจารณาตามเกณฑ์การวิเคราะห์ของเบสท์ แบ่งช่วงคะแนนสำหรับการแปลผลดังนี้

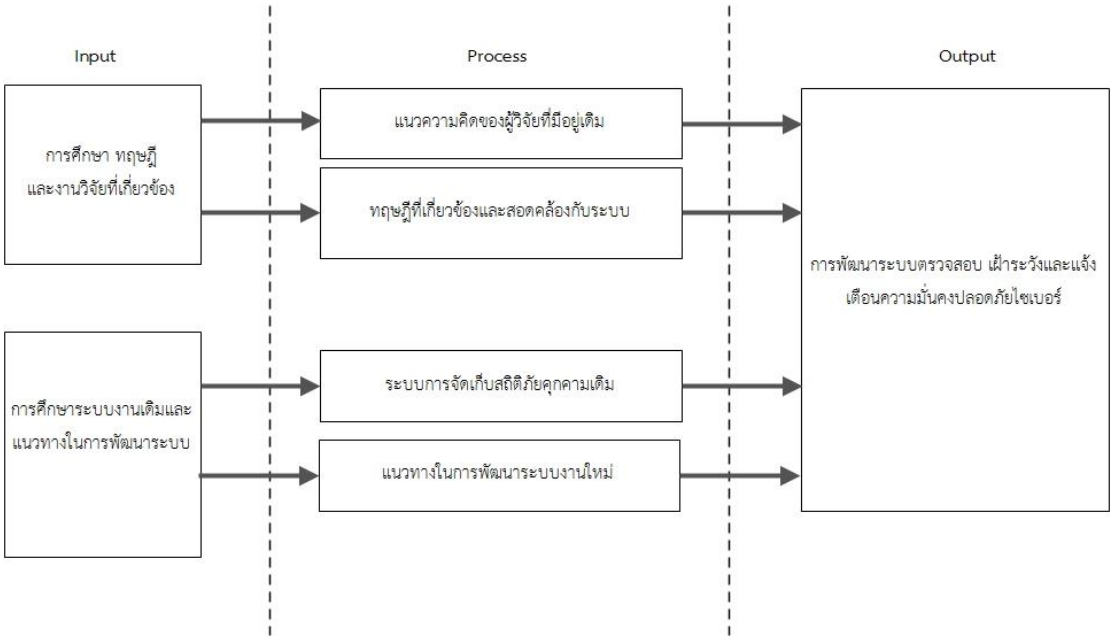
ระดับคะแนนเฉลี่ย 4.51- 5.00	หมายถึง	มีความพร้อมมากที่สุด
ระดับคะแนนเฉลี่ย 3.51- 4.50	หมายถึง	มีความพร้อมมาก
ระดับคะแนนเฉลี่ย 2.51- 3.50	หมายถึง	มีความพร้อมปานกลาง
ระดับคะแนนเฉลี่ย 1.51- 2.50	หมายถึง	มีความพร้อมน้อย
ระดับคะแนนเฉลี่ย 1.00- 1.50	หมายถึง	มีความพร้อมน้อยที่สุด

ขั้นตอนในการดำเนินการวิจัย

1. ศึกษาเอกสาร และงานวิจัยที่เกี่ยวข้อง แนวคิดเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ภารกิจ หน้าที่ ของศูนย์ไซเบอร์กองทัพบก และจุดมุ่งหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งศึกษาทางด้านแนวทางในการพัฒนาระบบ

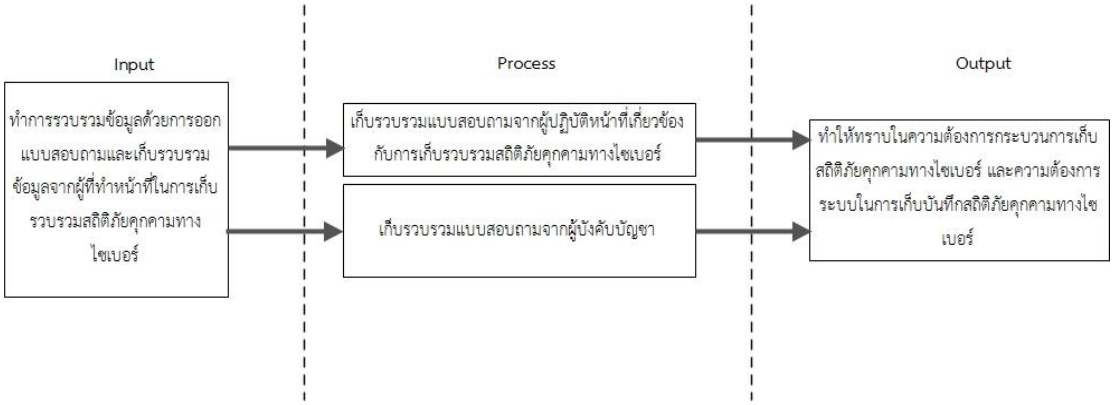
2. การพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ผู้วิจัยได้ศึกษาการดำเนินการตามกรอบแนวคิด ในการพัฒนาระบบจัดเก็บสถิติภัยคุกคามทางไซเบอร์ และการรายงานผล โดยกระบวนการและแนวทางในการพัฒนาระบบนั้น ผู้วิจัยได้กำหนดขั้นตอนในการดำเนินการ ออกเป็น 3 ขั้นตอน ดังนี้

1) ศึกษาทฤษฎี,งานวิจัย และระบบงาน เพื่อเป็นแนวทางในการพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน ความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก ดังภาพประกอบที่ 3.1



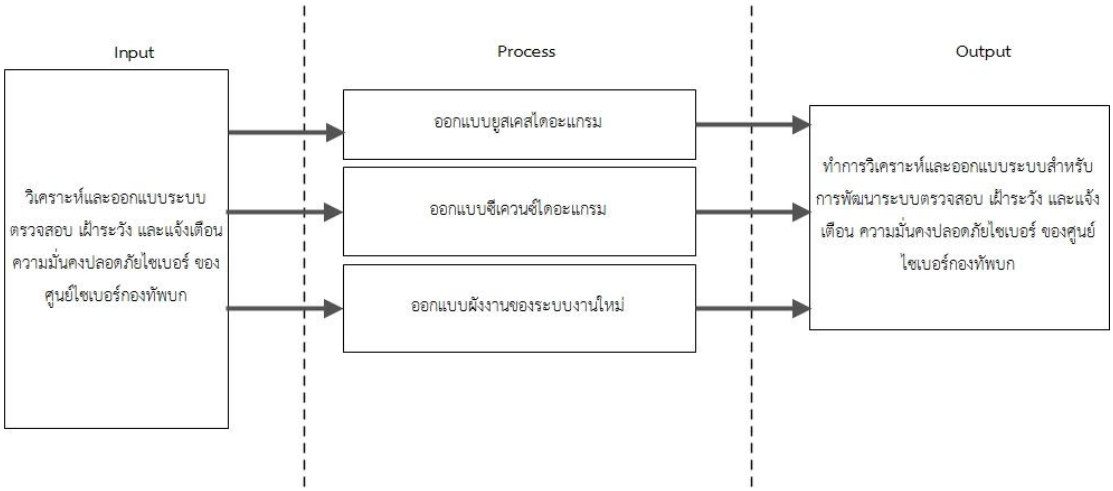
ภาพประกอบที่ 3.1 ขั้นตอนการศึกษาทฤษฎี,งานวิจัยและระบบงาน

2) เก็บรวบรวมข้อมูล โดยการทำแบบสอบถามความคิดเห็นของผู้ที่ปฏิบัติหน้าที่ทางด้านการรวบรวมข้อมูล การเก็บสถิติภัยคุกคาม ทางด้านความพร้อมและประสิทธิภาพของระบบงาน เพื่อให้สอดคล้องกับภารกิจของหน่วยงาน ดังภาพประกอบที่ 3.2



ภาพประกอบที่ 3.2 ขั้นตอนการเก็บรวบรวมข้อมูล

3) วิเคราะห์และออกแบบระบบ ทำการออกแบบระบบการจัดเก็บสถิติภัยคุกคามทางไซเบอร์ และการรายงานการประเมินผลภัยคุกคามทางไซเบอร์ ดังภาพประกอบที่ 3.3



ภาพประกอบที่ 3.3 ขั้นตอนการวิเคราะห์และออกแบบระบบ

เครื่องมือที่ใช้ในการพัฒนาระบบ

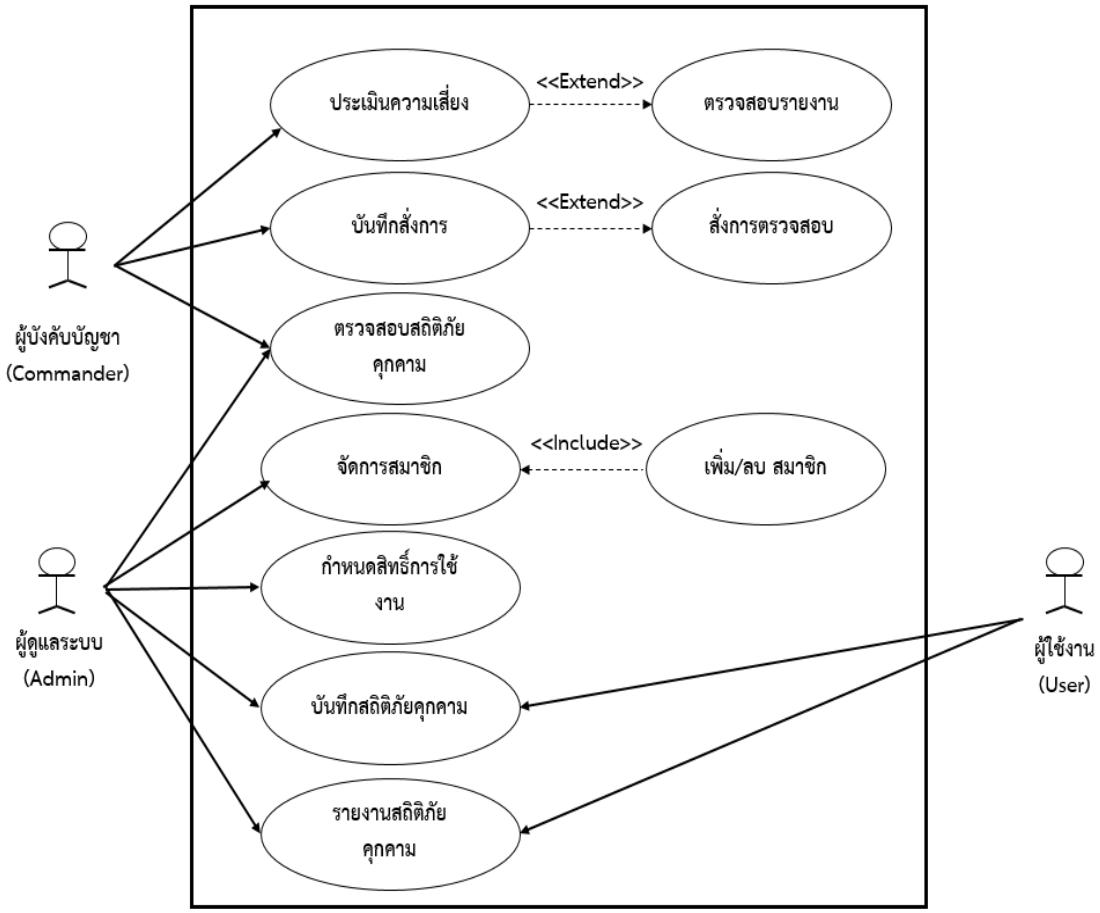
1) ฮาร์ดแวร์ที่ใช้ในการวิจัยประกอบด้วย

- คอมพิวเตอร์ Notebook
- ซีพียู Intel Core i7 Duo
- ฮาร์ดดิสก์ความจุ 1 TB
- หน่วยความจำ 16 GB
- การ์ดแสดงผล NVIDIA GEFORCE GTX 950 M

2) ซอฟต์แวร์ที่ใช้ในการวิจัยประกอบด้วย

- ระบบปฏิบัติการ Microsoft Windows 10
- ระบบการจำลอง Server ด้วยโปรแกรม Xampp
- ระบบจัดการฐานข้อมูล MySQL
- โปรแกรมภาษา PHP, C++
- โปรแกรม Macromedia Dreamweaver CS6

ในการพัฒนาระบบ ผู้วิจัยได้ทำการวิเคราะห์และออกแบบระบบในเชิงวัตถุ โดยใช้หลักของยูสเคสไดอะแกรม ในการออกแบบการสร้างระบบ เพื่อหาความต้องการของผู้ใช้ในศูนย์ไซเบอร์กองทัพบก รวมทั้งความสัมพันธ์ของผู้ที่เกี่ยวข้องในระบบ สำหรับนำไปพัฒนาระบบจริง ให้เป็นไปตามวัตถุประสงค์ ซึ่งรายละเอียดการแสดงความสัมพันธ์ระหว่างผู้บังคับบัญชา ผู้ดูแลระบบ และผู้ใช้งาน ที่มีส่วนเกี่ยวข้องในการใช้งานระบบ ดังภาพประกอบที่ 3.4



ภาพประกอบที่ 3.4 ยูสเคส (Use Case) แสดงความสัมพันธ์ของผู้ใช้งานระบบ

จากภาพประกอบที่ 3.4 ในการพัฒนาระบบจะแสดงให้เห็นถึงความสัมพันธ์ของผู้ใช้งาน ซึ่งจะประกอบด้วย 3 ระดับได้แก่

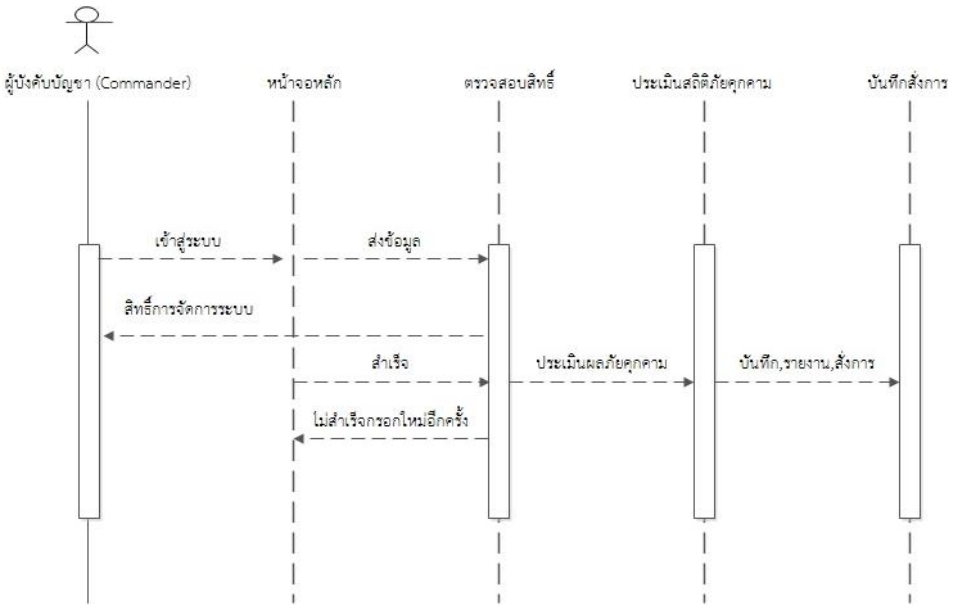
1) ผู้บังคับบัญชา (Commander)

2) ผู้รับผิดชอบระบบหลัก (Admin) และ

3) ผู้ใช้งานทั่วไป (User)

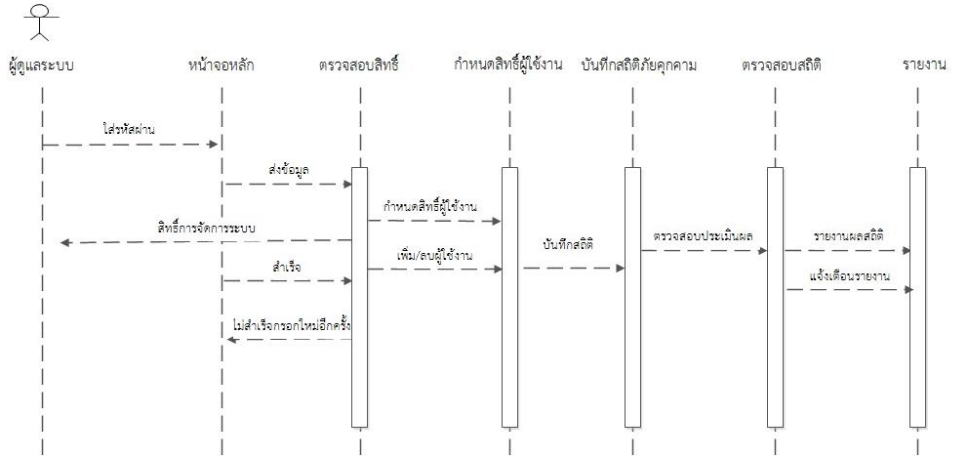
โดยการจัดการข้อมูลในแต่ละระดับสิทธิ์นั้น สามารถดำเนินการได้ดังนี้

1) ผู้บังคับบัญชา (Commander) จะสามารถตรวจสอบความเสี่ยง การประเมินความเสี่ยงของภัยคุกคาม การบันทึกสั่งการตามภัยคุกคามที่ตรวจพบ และ มอบนโยบายการตรวจสอบ ดังภาพประกอบที่ 3.5



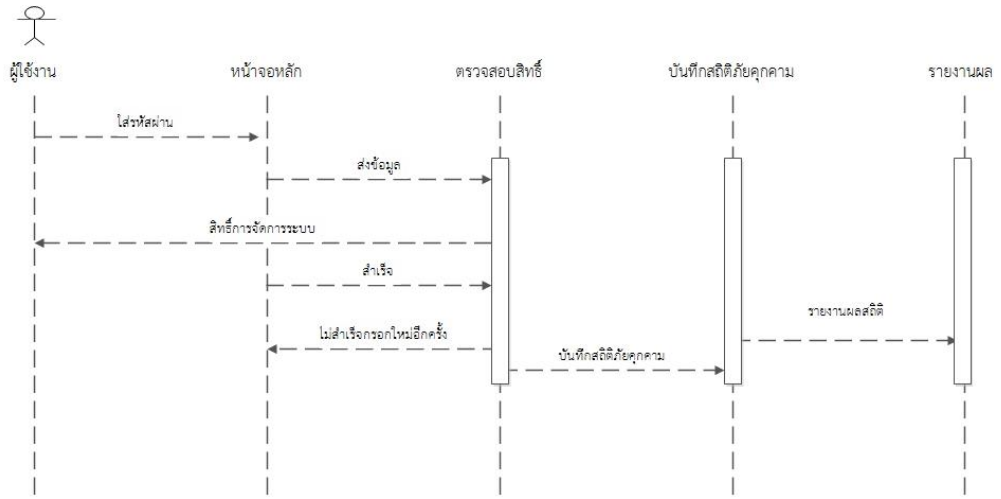
ภาพประกอบที่ 3.5 การจัดการข้อมูลของผู้บังคับบัญชา

2) ผู้ดูแลระบบ (Admin) จะสามารถจัดการระบบ กำหนดสิทธิ์ผู้ใช้งาน เพิ่ม/ลบสมาชิก ตรวจสอบสถิติภัยคุกคาม และ รายงานสถิติภัยคุกคามให้ผู้บังคับบัญชารับทราบ ดังภาพประกอบที่ 3.6



ภาพประกอบที่ 3.6 การจัดการข้อมูลของผู้ดูแลระบบ

3) ผู้ใช้งาน (Admin) จะสามารถ บันทึกสถิติภัยคุกคาม รายงานผลการบันทึกสถิติภัยคุกคาม ดังภาพประกอบที่ 3.7



ภาพประกอบที่ 3.7 การจัดการข้อมูลของผู้ใช้งาน

ผู้วิจัยได้ดำเนินการพัฒนาแอปพลิเคชันสำหรับการเก็บสถิติภัยคุกคามทางไซเบอร์ โดยจำแนกออกเป็น 3 ระบบงาน และเพื่อให้เป็นไปตามวัตถุประสงค์ดังที่กล่าวมาแล้ว ในบทที่ 1 ผู้วิจัยจึงได้กำหนดการทำงานของระบบที่พัฒนาขึ้นมานั้น ต้องสามารถแก้ปัญหาที่ผู้วิจัยได้ตั้งสมมุติฐานการวิจัยเอาไว้ ดังนี้

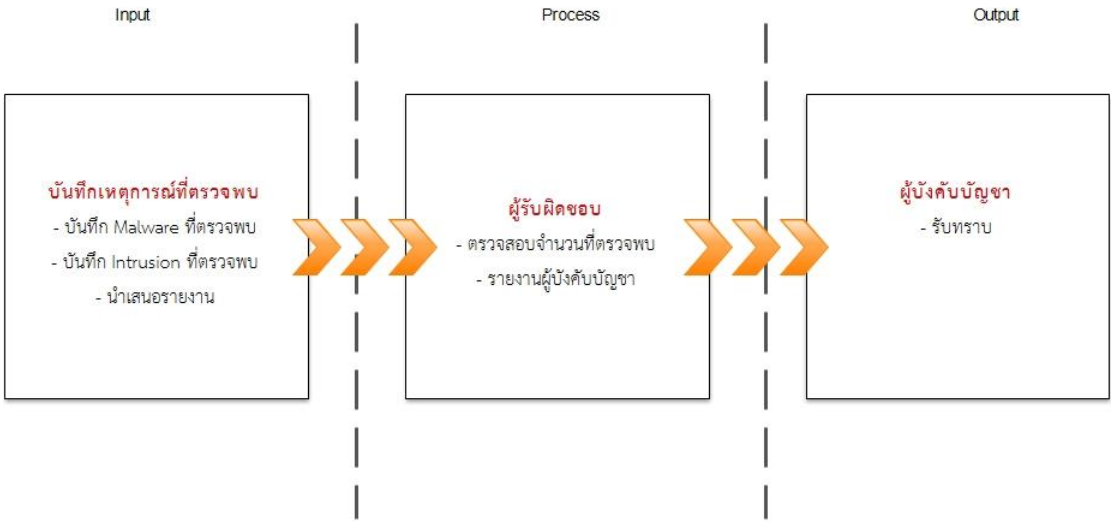
1) ระบบที่พัฒนาขึ้นมานั้นจะต้องสามารถบันทึกสถิติภัยคุกคามได้และตรวจสอบภัยคุกคามได้

2) ระบบที่พัฒนาขึ้นมานั้นจะต้องสามารถใช้เป็นการป้องกันภัยคุกคาม และเฝ้าระวังภัยคุกคามได้

3) ระบบที่พัฒนาขึ้นมานั้นสามารถแจ้งเตือนผู้ที่เกี่ยวข้องต่อความมั่นคง ปลอดภัยไซเบอร์ของศูนย์ไซเบอร์ได้

ความต้องการของระบบ

1) บันทึกและตรวจสอบภัยคุกคามตามแผนของงานวิจัยที่ได้พัฒนาขึ้นเพื่อทำการตรวจสอบและเก็บสถิติภัยคุกคามที่เกิดขึ้นภายในองค์กร ดังภาพประกอบที่ 3.8



ภาพประกอบที่ 3.8 ผังการบันทึกสถิติภัยคุกคามของศูนย์ไซเบอร์กองทัพบก

การจำแนก ภัยคุกคามที่ได้ทำการเก็บสถิติภัยคุกคามที่ตรวจพบ 2 ประเภท ดังนี้

- Malware ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น

ม้าโทรจัน (Trojan horse) คือ โปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่รันโดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับ E-mail และเมื่อดูเผิน ๆ ก็เป็นโปรแกรมอรรถประโยชน์ทั่ว ๆ ไป แต่จริง ๆ แล้วข้างในจะแฝงส่วนที่เป็นอันตรายต่อระบบเมื่อรันโปรแกรมนี้

เวิร์ม (Worm) คุณสมบัติพิเศษของเวิร์ม คือ สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่น ๆ ผ่านทางเครือข่าย เวิร์ม สามารถทำอันตรายให้กับระบบ เวิร์มบางประเภทสามารถแพร่กระจายตัวเองโดยที่ไม่ต้องอาศัยการช่วยเหลือจากผู้ใช้เลย หรือบางตัวก็อาจแพร่กระจายเมื่อผู้ใช้รันโปรแกรมบางโปรแกรม นอกจากความสามารถในการแพร่กระจายด้วยตัวเองแล้ว เวิร์มยังสามารถทำลายระบบได้อีกด้วย

ไวรัส (Virus) ไวรัสเป็นโปรแกรมที่สามารถติดต่อจากอีกไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น มันสามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เมื่อโฮสต์รันโปรแกรมที่ติดไวรัสส่วนที่เป็นไวรัสก็จะถูกรันด้วยและทำให้แพร่กระจายไปยังเครื่องอื่นหรือบางทีก็สร้างโค้ดใหม่

- Intrusion หรือ พฤติกรรมหรือความพยายามที่จะบุกรุกเครือข่าย โดยทั่วไปแล้ว Intrusion นั้นจะถูกดักจับ หรือถูกตรวจจับโดย ระบบตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) โดยระบบจะแจ้งให้ทราบว่ามีผู้พยายามที่จะบุกรุกเครือข่าย แต่ระบบ IDS ไม่ใช่ระบบการป้องกันการโจรกรรมหรือว่าป้องกันการบุกรุก แต่เป็นเพียงระบบที่คอยแจ้งเตือนภัยเท่านั้น ซึ่งระบบ IDS จะทำงานด้วยการส่งสัญญาณ เมื่อมีการตรวจพบความพยายามที่จะถูกบุกรุกด้วยวิธีการต่าง ๆ ซึ่งวิธีการนั้น มีหลายประเภท โดยส่วนใหญ่ที่ตรวจพบ จะมีอยู่หลายประการดังนี้

1. Web Application Attack หมายถึง ความพยายามที่จะเปลี่ยนแปลงหน้าเว็บเพจ

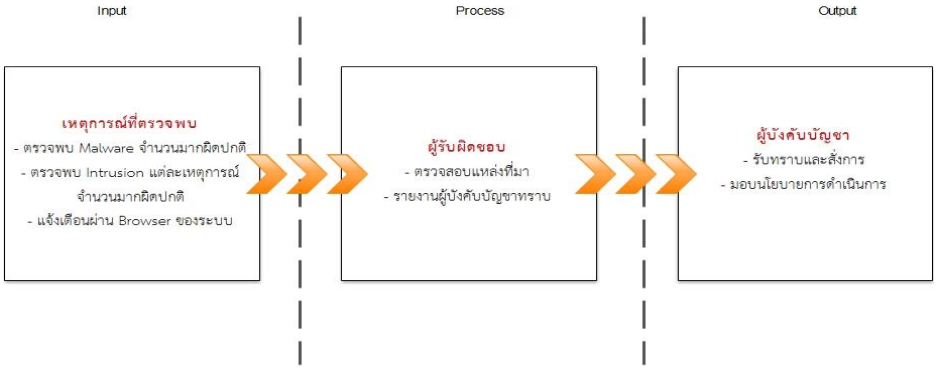
2. Scanning Attack การโจมตีแบบสแกนระบบ หมายถึงการทดสอบระบบว่าใช้งานอะไรได้บ้าง โดยทำการส่งแพคเก็ตประเภทต่าง ๆ ไปยังระบบ การโจมตีจะคล้ายกับการสแกนเพื่อหาจุดอ่อนหรือช่องโหว่ของระบบ แต่ต่างกันตรงที่ว่าข้อมูลที่ได้จะใช้ข้อมูลไปทางด้านการศึกษาเรียนรู้

3. Attempted Denial of Service หมายถึง ความพยายามที่จะปฏิเสธการให้บริการหรือทำให้ระบบทำงานช้าลงหรือทำงานไม่ได้เลย

4. A Network Trojan was Detected การแจ้งเตือนการพบ Trojan ในระบบเครือข่าย

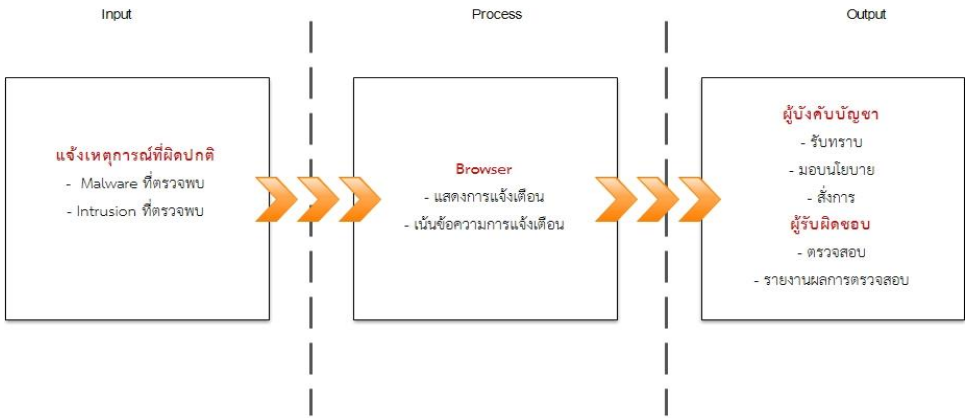
5. Penetration Attacks จะเป็นการตรวจพบการลักลอบเข้ามาโดยไม่ได้รับอนุญาตเพื่อทำการเปลี่ยนแปลงสิทธิ์ รีซอร์ส และข้อมูลที่อยู่ภายในระบบ

2) ระบบต้องทำการเฝ้าระวังการโจมตี หรือบุกรุก ที่ตรวจพบ จากพฤติกรรมการบุกรุก หรือ โปรแกรมประสงค์ร้ายที่เข้ามาเป็นจำนวนมากผิดปกติ โดยการแจ้งเตือนจำนวนที่ตรวจพบมากผิดปกติผ่าน Browser ของระบบ เพื่อให้ผู้ที่รับผิดชอบ ทำการตรวจแหล่งที่มา และทำการรายงานให้ผู้บังคับบัญชาได้รับทราบถึงผลการตรวจสอบ และแหล่งที่มาของ พฤติกรรมการบุกรุก หรือ โปรแกรมประสงค์ร้ายที่ตรวจพบ ดังภาพประกอบที่ 3.9



ภาพประกอบที่ 3.9 ผังการตรวจสอบการเฝ้าระวังการโจมตีหรือบุกรุก

3) ระบบจะต้องมีการแจ้งเตือนเพื่อให้ผู้ที่มีส่วนเกี่ยวข้องในการตรวจสอบ และผู้บังคับบัญชาได้ทราบถึงการโจมตีหรือบุกรุก ระบบจะแจ้งการตรวจพบพฤติกรรมดังกล่าวที่เข้ามาเป็นจำนวนมากผิดปกติ โดยการแจ้งเตือนจะเตือนผ่าน Browser ของระบบทันทีที่ระบบได้บันทึก โดยจะเน้นข้อความเพื่อให้เกิดความชัดเจน เป็นจุดสังเกตุที่จะให้มีการเร่งรีบในการตรวจสอบ ดังภาพประกอบที่ 3.10



ภาพประกอบที่ 3.10 ผังการแจ้งเตือนเมื่อระบบตรวจพบภัยคุกคามมากผิดปกติ

คำจำกัดความของ ผู้ใช้งานระบบ

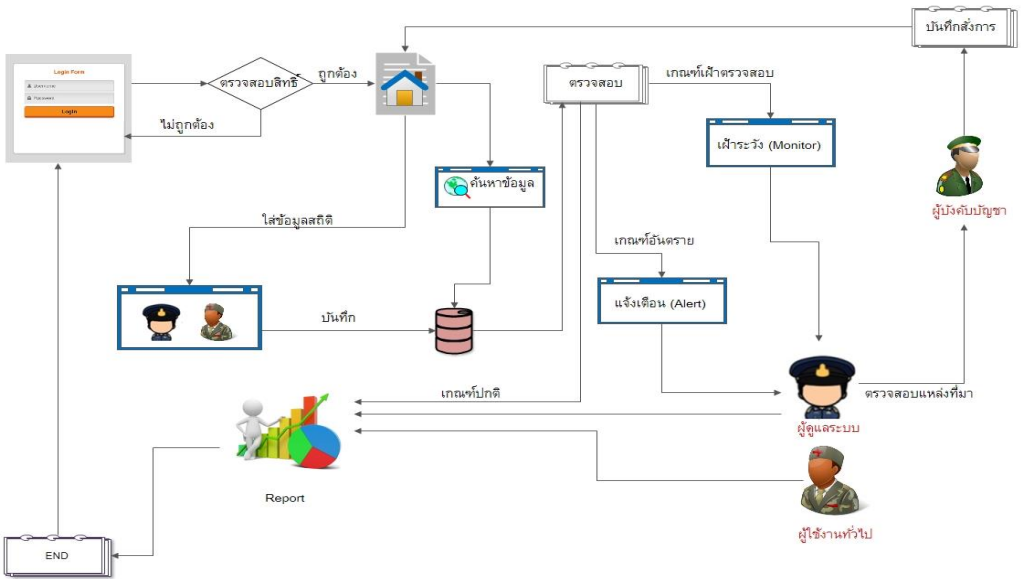
- ผู้บังคับบัญชา (Commander) (ผู้ใช้งานระดับที่ 3 (Tier3)) หมายถึง ผู้บังคับบัญชาระดับสูง ชั้นยศ พันเอก (พิเศษ) ถึง พลตรี ที่มีอำนาจในการตัดสินใจ, ตกลงใจในการสั่งตรวจสอบภัยคุกคาม และมอบนโยบาย

- ผู้ดูแลระบบ (Admin) (เจ้าหน้าที่ผู้ใช้งานระดับที่ 2 (Tier2)) หมายถึง ผู้บังคับบัญชาระดับรับคำสั่ง (ชั้นยศ พันตรี ถึง พันเอก) เจ้าหน้าที่ระดับตรวจสอบสถิติภัยคุกคามทางไซเบอร์ , ผู้ที่ทำหน้าที่นำเสนอข้อมูลทางด้านภัยคุกคามทางไซเบอร์ ในระดับสูง

- ผู้ใช้งาน (User) (เจ้าหน้าที่ผู้ใช้งานระดับที่ 1 (Tier1)) หมายถึง เจ้าหน้าที่ผู้ปฏิบัติงาน (ชั้นยศ สิบตรี ถึง จ่าสิบเอก) และหัวหน้าเจ้าหน้าที่ผู้ปฏิบัติงาน (ชั้นยศ ร้อยตรี ถึง ร้อยเอก) ที่มีหน้าที่ในการตรวจสอบภัยคุกคามชั้นต้น

วงจรการทำงานของระบบงานใหม่โดยรวม

จากการที่ได้รวบรวมปัญหา และศึกษาความเป็นไปได้ในการพัฒนาระบบ ทำให้สามารถสรุปเป็นภาพรวมของระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ดังภาพประกอบที่ 3.11



ภาพประกอบที่ 3.11 ผังสรุปภาพรวมของระบบใหม่

เครื่องมือที่ใช้ในการวิจัย

การวิเคราะห์ข้อมูลในการวิจัยในครั้งนี้ เพื่อตอบวัตถุประสงค์และทดสอบสมมุติฐานการวิจัยคือการวิเคราะห์ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก สถิติที่ใช้ในการวิเคราะห์ข้อมูลประกอบด้วย ค่าความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) ด้านความมั่นคงปลอดภัยสารสนเทศในศูนย์ไซเบอร์กองทัพบก สถิติที่ใช้ในการวิเคราะห์ข้อมูลประกอบด้วย ค่าความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

การเก็บรวบรวมข้อมูล

การดำเนินการวิจัยใช้กับกลุ่มตัวอย่าง คือผู้ที่ปฏิบัติงานภายในหน่วยศูนย์ไซเบอร์กองทัพบก และมีส่วนเกี่ยวข้องกับการเก็บสถิติภัยคุกคาม จำนวน 35 คน เพื่อทำการประเมินประสิทธิภาพและความเหมาะสมต่อระบบการบันทึกสถิติภัยคุกคามทางไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก โดยทำการจัดพิมพ์แบบประเมินความเหมาะสมการใช้งานระบบการบันทึกสถิติภัยคุกคามทางไซเบอร์ และนำไปทำการประเมินประสิทธิภาพกับกลุ่มตัวอย่าง เพื่อหาข้อเปรียบเทียบข้อดี และข้อเสียของระบบที่ได้พัฒนาขึ้นมา ตามแบบในการวิจัยในครั้งนี้

กลุ่มผู้ใช้งานระบบ เป็นผู้ที่มีส่วนเกี่ยวข้องกับการบันทึกสถิติภัยคุกคามทางไซเบอร์ของศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน ดำเนินการทดสอบระบบและทำการประเมินการใช้งานของระบบ แล้วทำการปรับปรุงระบบตามคำแนะนำที่ได้รับจากการประเมินระบบ ก่อนที่จะใช้งานจริงต่อไป เพื่อให้เกิดความสมบูรณ์ของระบบ

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลการวิจัย ข้อมูลดำเนินการโดยนำผลการประเมินแบบประเมินผลมาวิเคราะห์แล้วประเมินผลข้อมูลโดยใช้โปรแกรมสำเร็จรูป SPSS (Statistics Package for the Social Sciences : SPSS) เพื่อใช้ในการวิเคราะห์และรายงานผลค่าทางสถิติ และประมวลผลหาความสัมพันธ์ทางสถิติด้วยระดับความเชื่อมั่น 95 เปอร์เซ็นต์ และมีความคลาดเคลื่อนที่ยอมรับได้ 0.05 เปอร์เซ็นต์ เป็นเกณฑ์ในการยอมรับหรือปฏิเสธสมมติฐานในการศึกษา สำหรับบทที่ 3 นั้นจะเป็นการนำเสนอวิธีดำเนินการวิจัย ที่ประกอบด้วย การออกแบบการวิจัย ขั้นตอนการวิจัย เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย ประชากรและกลุ่มตัวอย่าง การเก็บรวบรวมข้อมูลการวิเคราะห์ข้อมูล การกำหนดเกณฑ์พิจารณาระดับค่าคะแนน พร้อมทั้งนำเสนอวิธีการประเมินระดับ

ประสิทธิภาพและความเหมาะสมของโมเดลระบบ และระยะเวลาในการดำเนินงาน พร้อมตอบคำถามตามวัตถุประสงค์และสมมติฐานที่กำหนดไว้ สถิติที่ใช้ในการวิเคราะห์มีรายละเอียด อาทิ ค่าเฉลี่ย (Mean) และค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation)

ระยะเวลาในการดำเนินการ

การดำเนินงานวิจัยใช้ระยะเวลารวมทั้งสิ้น 9 เดือน ตั้งแต่เดือน พฤศจิกายน พ.ศ. 2560 ถึงเดือน กรกฎาคม พ.ศ. 2561 ดังตารางที่ 3.1

ตารางที่ 3.1 แสดงระยะเวลาที่ใช้ในการดำเนินการ

ขั้นตอนการดำเนินการ	ระยะเวลาที่ใช้ในการดำเนินการ								
	ปี 2560		ปี 2561						
	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.
1.ศึกษาปัญหา,ทฤษฎีและงานวิจัย	←→ / ←- - →	←→ / ←- - →							
2.วิเคราะห์และออกแบบระบบ			←→ / ←- - →	←→ / ←- - →	←→				
3.พัฒนาระบบ				←→ / ←- - →	←→ / ←- - →	←→			
4.ทดสอบและใช้งานจริง							←→ / ←- - →	←→ / ←- - →	
5. ประเมินผลระบบ								←→ / ←- - →	←→ / ←- - →

←——→ ระยะเวลาที่กำหนด

←- - - - - - - -→ ระยะเวลาใช้จริง

บทที่ 4
ผลการวิจัย

งานวิจัยในครั้งนี้ ผู้วิจัยได้ทำการพัฒนาระบบเพื่อการเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก พร้อมทั้งขอคำแนะนำจากผู้เชี่ยวชาญ และได้รวบรวมปัญหาของระบบงานเดิม เพื่อเป็นแนวทางในการพัฒนาระบบตามแนวคิดที่ได้วางแผนงานไว้ก่อนหน้านี้แล้ว ภายหลังจากที่ได้ทำการพัฒนาระบบเรียบร้อยแล้ว จึงได้นำไปให้ผู้เชี่ยวชาญและผู้ใช้ระบบเข้าทำการประเมินประสิทธิภาพและระดับความเหมาะสมของระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยการวิจัยครั้งนี้ผู้วิจัยได้กำหนดผลการวิจัยเอาไว้ ดังนี้

การตรวจสอบและใช้งานระบบ

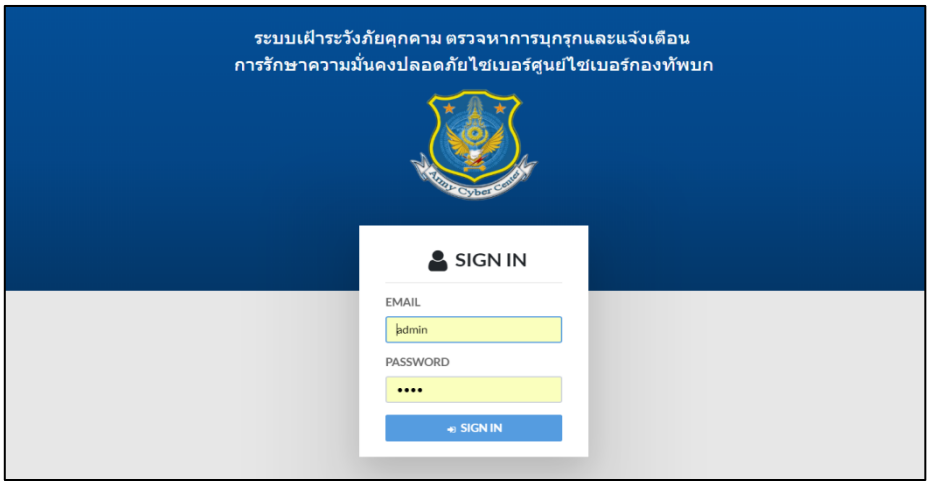
การตรวจสอบภัยคุกคามทางไซเบอร์ของศูนย์ไซเบอร์กองทัพบก มีการดำเนินการออกเป็น 2 ขั้นตอน ได้แก่

1. ขั้นตอนการตรวจสอบภัยคุกคามทางไซเบอร์ ศูนย์ไซเบอร์กองทัพบกได้มีการตรวจสอบภัยคุกคามทางไซเบอร์ โดยใช้ซอฟต์แวร์ ประเภทมัลแวร์ชั้นสูง (Advance Malware) สำหรับการตรวจจับภัยคุกคามทางไซเบอร์ประเภทมัลแวร์ และ ระบบการตรวจจับการบุกรุกเครือข่าย (Intrusion Detection System : IDS) สำหรับการตรวจจับภัยคุกคามทางไซเบอร์ประเภท Intrusion ด้วยวิธีการทำงานของระบบตรวจสอบภัยคุกคามดังกล่าวนั้น จะทำให้การดำเนินการตรวจสอบภัยคุกคามทางไซเบอร์ภายในระบบ มีสเถียรภาพมากยิ่งขึ้น ซึ่งจากการทำงานของระบบทั้ง 2 ชนิดนั้น จะอยู่ภายใต้ Splunk หรือซอฟต์แวร์ ที่ช่วย ค้นหา แสดงรายงาน ตรวจสอบ และวิเคราะห์ ข้อมูล แบบ Live Streaming หรือ ดูข้อมูลในลักษณะข้อมูลทางสถิติได้

2. ขั้นการบันทึกสถิติ การเฝ้าระวัง และแจ้งเตือน ระดับความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ในการบันทึกสถิติภัยคุกคามที่ตรวจพบจากระบบตรวจสอบภัยคุกคามทางไซเบอร์นั้น ผู้เชี่ยวชาญจะส่งผลการตรวจสอบที่ได้จากการตรวจสอบด้วยซอฟต์แวร์ สำหรับการตรวจสอบภัยคุกคาม ในข้อที่ 1 ให้เจ้าหน้าที่ได้ทำการบันทึกสถิติภัยคุกคาม ลงในระบบการเฝ้าระวัง และแจ้งเตือน ระดับความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบกที่ผู้วิจัย

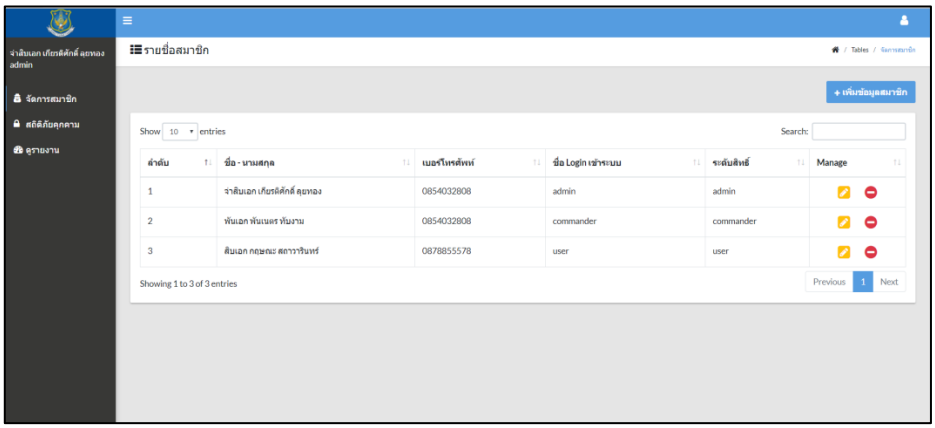
ได้ทำการพัฒนาระบบขึ้น เพื่อทำการประเมินเกณฑ์การเฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ดังกล่าว ซึ่งผลที่ได้จากการพัฒนาระบบตรวจสอบเฝ้าระวังและแจ้งเตือนรักษาความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก มีดังนี้

การเข้าสู่ระบบ เป็นหน้าแรกในการเข้าใช้งานระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยผู้วิจัยได้แบ่งสิทธิ์การใช้งานออกเป็น 3 ระดับ ได้แก่ 1) ผู้บังคับบัญชา (Commander) 2) ผู้ดูแลระบบ (Admin) และ 3) ผู้ใช้งาน (User) ดังภาพประกอบที่ 4.1



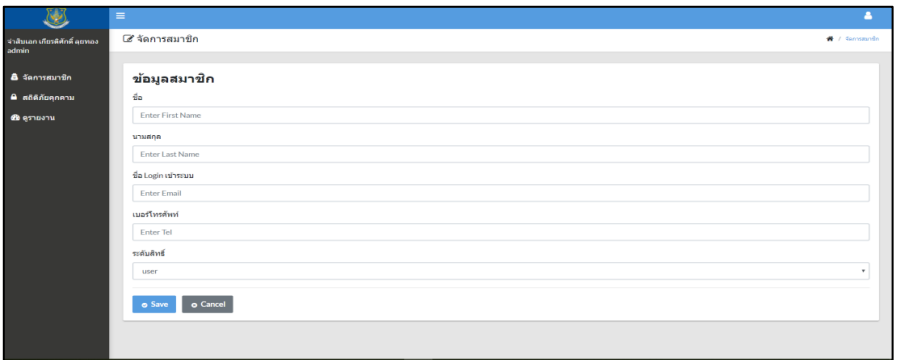
ภาพประกอบที่ 4.1 หน้า Log-in เพื่อเข้าสู่ระบบ

การจัดการสมาชิก เป็นเมนูการทำงานในส่วนของผู้ดูแลระบบ ที่จะแจกสิทธิ์การใช้งานให้กับบุคลากรของศูนย์ไซเบอร์กองทัพบก ซึ่งการสมัครสมาชิกนั้น ผู้วิจัยได้ออกแบบมาให้สิทธิ์การสมัครสมาชิกโดยผู้ดูแลระบบเพียงอย่างเดียวเท่านั้น ดังภาพประกอบที่ 4.2



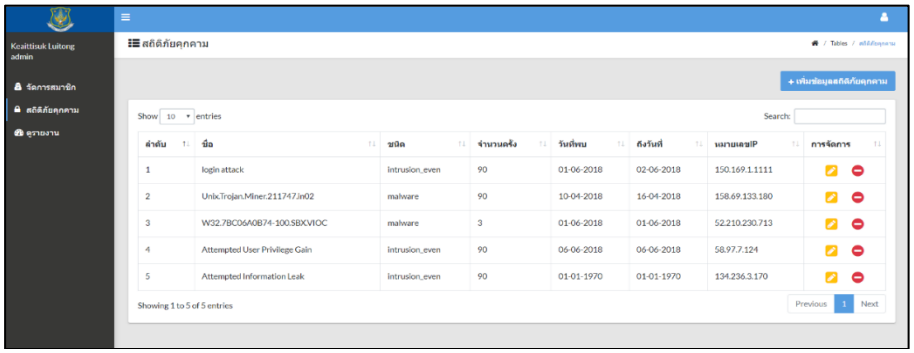
ภาพประกอบที่ 4.2 หน้าการจัดการสมาชิก

การสมัครสมาชิก เป็นขั้นตอนการทำงานโดยผู้พัฒนาระบบได้ออกแบบไว้สำหรับการสมัครสมาชิก โดยอนุญาตให้สมัครสมาชิกผ่านผู้ดูแลระบบเท่านั้น ดังภาพประกอบที่ 4.3



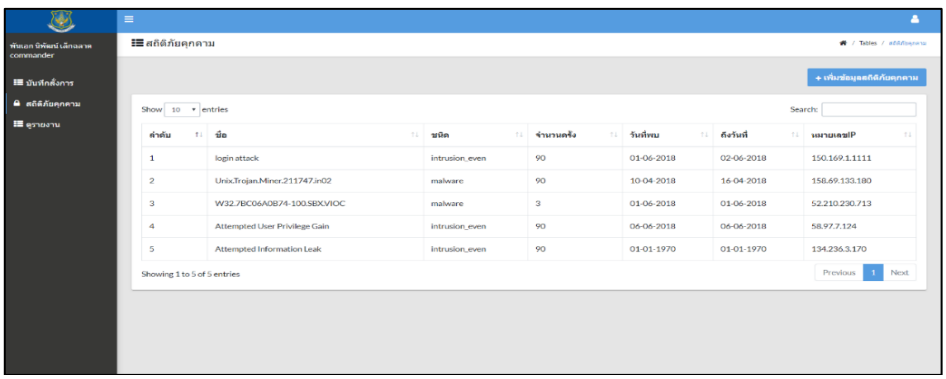
ภาพประกอบที่ 4.3 การจัดการสมาชิกโดยผู้ดูแลระบบ

การใช้งานระบบ การใช้งานระบบนั้น ผู้วิจัยได้ทำการแยกสิทธิ์การใช้งาน ได้แก่ 1) ผู้ดูแลระบบ จะมีสิทธิ์ในการเพิ่ม/ลบ และแก้ไขภัยคุกคามได้



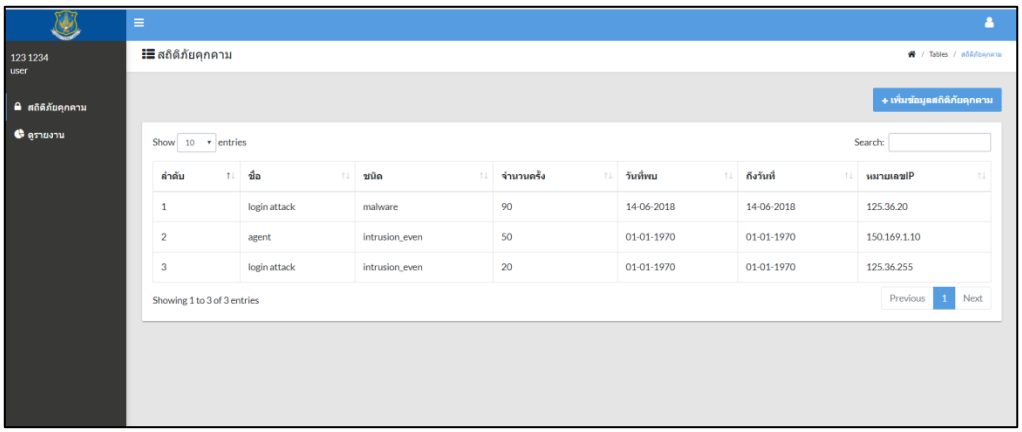
ภาพประกอบที่ 4.4 การเข้าใช้งานของผู้ดูแลระบบ (Admin)

ผู้บังคับบัญชา (Commander) จะสามารถเพิ่มข้อมูลภัยคุกคามเพียงอย่างเดียว โดยไม่มีสิทธิ์ในการลบและแก้ไขข้อมูลสถิติภัยคุกคามได้ ดังภาพประกอบที่ 4.5



ภาพประกอบที่ 4.5 การเข้าใช้งานของผู้บังคับบัญชา (Commander)

ผู้ใช้งาน (User) จะสามารถเพิ่มข้อมูลภัยคุกคามเพียงอย่างเดียว โดยไม่มีสิทธิ์ในการลบและแก้ไขข้อมูลสถิติภัยคุกคามได้ ดังภาพประกอบที่ 4.6



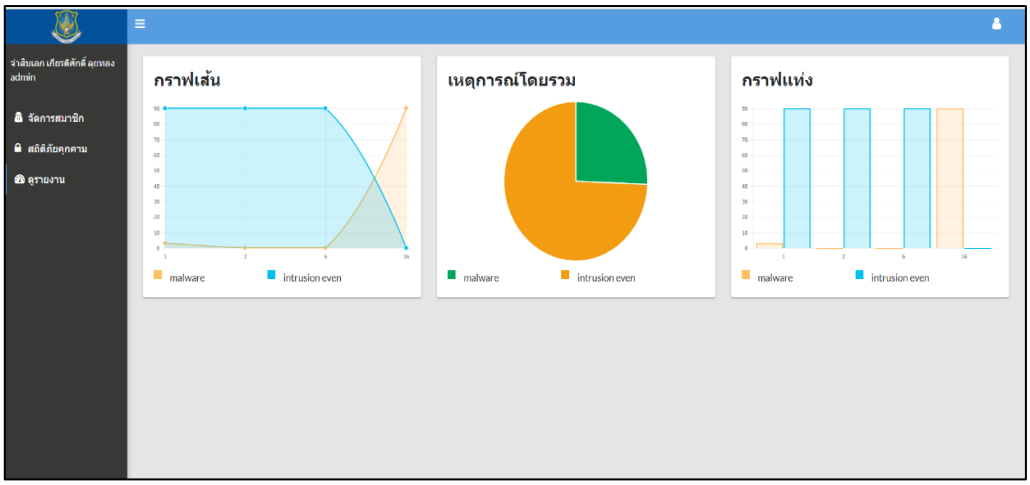
ภาพประกอบที่ 4.6 การเข้าใช้งานของผู้ใช้งานทั่วไป (User)

การตรวจจับและการแสดงผลภัยคุกคามทางไซเบอร์

1. ภัยคุกคามที่ระบบทำการตรวจจับ การตรวจจับภัยคุกคามทางไซเบอร์ของระบบที่ผู้วิจัยได้ทำการพัฒนาระบบขึ้นมาเพื่อการตรวจจับภัยคุกคาม 2 ประเภท ได้แก่ 1) Malware หรือ Malicious Software โปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล และ 2) Intrusion หรือ พฤติกรรมหรือความพยายามที่จะบุกรุกเครือข่าย ซึ่งผู้วิจัยได้ทำการออกแบบ โดยให้ระบบทำการตรวจจับภัยคุกคาม 2 ประเภทนี้ที่มีพฤติรรมกระทำซ้ำ ๆ กัน ในแต่ละเหตุการณ์ อยู่ที่ 100 – 149 ครั้ง/วัน/เหตุการณ์ ระบบจะทำการเฝ้าระวัง และ ตั้งแต่ 150 ครั้ง/วัน/เหตุการณ์ ระบบจะทำการแจ้งเตือนเพื่อให้ทำการตรวจสอบภัยคุกคามนี้ในทันที

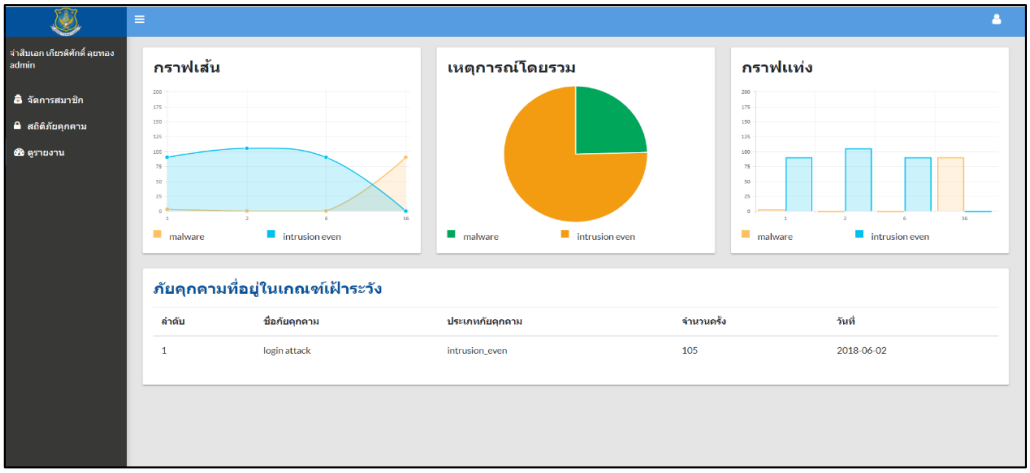
2. การแสดงผลภัยคุกคามทางไซเบอร์ ผู้วิจัย ได้ทำการพัฒนาระบบโดยได้ออกแบบให้รายงานแบบกราฟแสดงสถิติ โดยจะแสดงผลภัยคุกคามใน 3 ระดับ ได้แก่

1) ภัยคุกคามที่อยู่ในเกณฑ์ปกติ จะไม่มีการแจ้งเตือนการตรวจพบเกณฑ์เสี่ยงของภัยคุกคามที่เกิดขึ้นในระบบ ดังภาพประกอบที่ 4.8



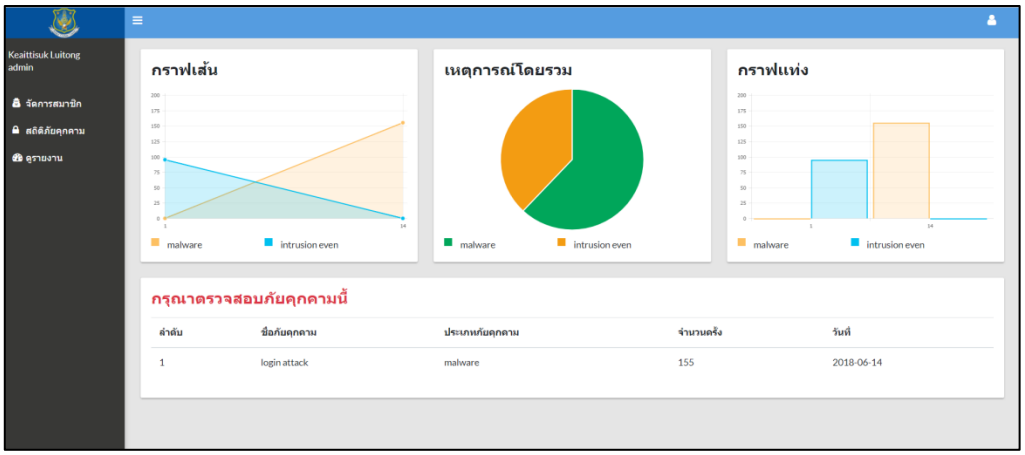
ภาพประกอบที่ 4.7 ภาพแสดงภัยคุกคามที่อยู่ในเกณฑ์ปกติ

2) ภัยคุกคามที่อยู่ในเกณฑ์เฝ้าระวัง ระบบจะแสดงข้อความแจ้งเตือนในระบบว่า “ภัยคุกคามที่อยู่ในเกณฑ์เฝ้าระวัง” เพื่อให้ผู้ที่เกี่ยวข้องทำการเฝ้าระวังภัยคุกคามในชนิดนั้น ดังภาพประกอบที่ 4.9



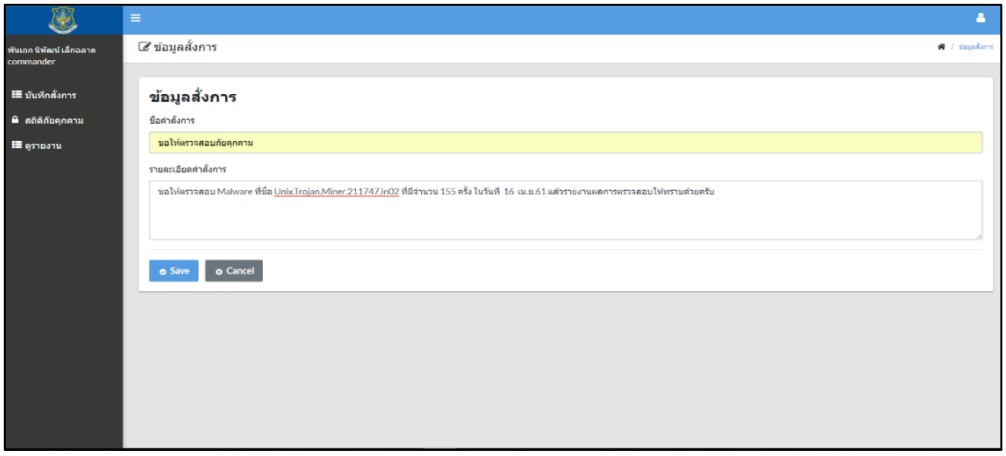
ภาพประกอบที่ 4.8 ภาพแสดงภัยคุกคามที่อยู่ในเกณฑ์เฝ้าระวัง

3) ภัยคุกคามที่อยู่ในเกณฑ์เสี่ยงต่อความปลอดภัยของระบบสารสนเทศ ระบบจะทำการแจ้งเตือนด้วยข้อความแจ้งเตือนในระบบว่า “กรุณาตรวจสอบภัยคุกคามนี้” เพื่อให้ผู้ที่เกี่ยวข้องได้ทำการตรวจสอบภัยคุกคามที่ตรวจพบเพื่อหาแหล่งที่มาและแนวทางในการแก้ไข ดังภาพประกอบที่ 4.10



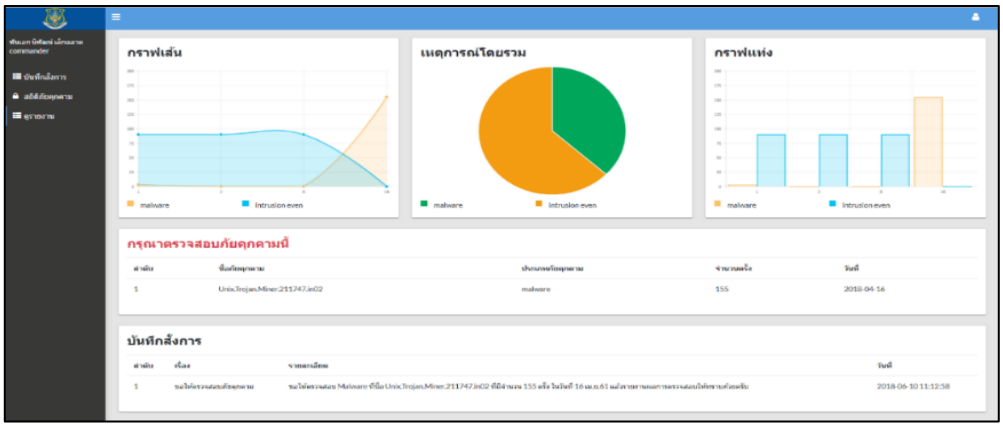
ภาพประกอบที่ 4.9 ภาพแสดงการตรวจพบภัยคุกคามที่อยู่ในเกณฑ์เสี่ยง

การบันทึกสั่งการ ผู้บังคับบัญชาจะทำการบันทึกสั่งการในกรณีที่มีการตรวจพบภัยคุกคามที่อยู่ในเกณฑ์เสี่ยง หรือสั่งการเรื่องอื่น ๆ ที่เกี่ยวข้องกับระบบ โดยผู้พัฒนาระบบได้ออกแบบการบันทึกสั่งการของผู้บังคับบัญชา เพื่อให้สามารถสั่งการผ่านเว็บแอปพลิเคชัน และแสดงผลการบันทึกสั่งการผ่านระบบ ดังภาพประกอบที่ 4.11



ภาพประกอบที่ 4.10 ภาพแสดงการบันทึกสั่งการของผู้บังคับบัญชาผ่านทางระบบ

การแสดงผลการบันทึกสั่งการ จะเป็นการแสดงการสั่งการของผู้บังคับบัญชาในระบบการรีพอร์ต เพื่อให้ผู้ที่เกี่ยวข้องในการตรวจสอบภัยคุกคามทางไซเบอร์ หรือตรวจสอบเรื่องอื่น ๆ ตามที่ผู้บังคับบัญชาได้สั่งการผ่านแอปพลิเคชัน ดังภาพประกอบที่ 4.12



ภาพประกอบที่ 4.11 ภาพแสดงการสั่งการของผู้บังคับบัญชาผ่านทางระบบ

ผลการประเมิน

การประเมินประสิทธิภาพการใช้งานและความเหมาะสมของระบบ ผู้วิจัยได้ทำการประเมินประสิทธิภาพและความเหมาะสมการใช้งานระบบ เฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยมีรายละเอียดในการประเมินดังนี้

2.1 การประเมินความเหมาะสมของระบบโดยผู้เชี่ยวชาญ ผู้วิจัยได้ขอรับคำแนะนำจากผู้เชี่ยวชาญ จำนวน 6 ท่าน เพื่อประเมินด้านความเหมาะสมของการพัฒนาระบบ โดยมีรายละเอียดการประเมิน ดังนี้

ส่วนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบสอบถาม เป็นเพศชายจำนวน 6 ท่าน คิดเป็นร้อยละ 100 มีอายุระหว่าง 41 - 50 ปี จำนวน 4 ท่าน คิดเป็นร้อยละ 66 และอายุมากกว่า 50 ปีขึ้นไป จำนวน 2 ท่าน คิดเป็นร้อยละ 34 ตำแหน่งงาน เป็นผู้บริหาร จำนวน 3 ท่าน คิดเป็นร้อยละ 50 เป็นผู้ดูแลระบบเครือข่าย จำนวน 1 ท่าน คิดเป็นร้อยละ 16 และเป็นผู้เชี่ยวชาญทางด้านไอที จำนวน 2 ท่าน คิดเป็นร้อยละ 34 และระยะเวลาในการทำงาน 11 – 15 ปี จำนวน 4 ท่าน คิดเป็นร้อยละ 66 ระยะเวลาในการทำงาน 16 - 20 ปี จำนวน 1 ท่าน คิดเป็นร้อยละ 16 และมากกว่า 20 ปี จำนวน 2 ท่าน คิดเป็นร้อยละ 34

ส่วนที่ 2 ความคิดเห็นทางด้านความเหมาะสมของระบบ ผู้วิจัยได้ทำแบบสอบถามความคิดเห็นจากผู้เชี่ยวชาญ เพื่อประเมินความเหมาะสมของระบบ โดยมีผลการประเมินความเหมาะสมของระบบโดยผู้เชี่ยวชาญ โดยสรุปการประเมินดังนี้

ตารางที่ 4.1 ความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งาน

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
ความเหมาะสมทางด้านการจัดการข้อมูลผู้ใช้งาน	4.67	0.52	มากที่สุด
ความเหมาะสมทางด้านการจัดเก็บสถิติภัยคุกคาม	4.50	0.55	มากที่สุด
ความเหมาะสมทางด้านการนำเสนอรายงานภัยคุกคาม	4.33	0.52	มาก
ระดับความคิดเห็นเฉลี่ย	**4.50**	**0.51**	**มากที่สุด**

จากตารางที่ 4.1 ด้านความสามารถตรงตามความต้องการของผู้ใช้งาน ซึ่งประกอบด้วย ความเหมาะสมทางด้านการจัดการข้อมูลผู้ใช้งาน มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.67, S.D. = 0.52) ความเหมาะสมทางด้านการจัดเก็บสถิติภัยคุกคาม มีความเหมาะสม อยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.50, S.D. = 0.55) และความเหมาะสมทางด้านการนำเสนอรายงานภัยคุกคาม มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.33, S.D. = 0.52) ความคิดเห็นโดยรวม มีความเหมาะสม อยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.51)

ตารางที่ 4.2 ความเหมาะสมด้านความถูกต้องของการออกแบบระบบ

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
การใช้งานมีความง่ายในการเข้าถึงข้อมูล	4.33	0.52	มาก
มีความรวดเร็วในการใช้บริการ	4.50	0.55	มากที่สุด
มีความเหมาะสมในการจัดวางตำแหน่งของส่วนประกอบระบบ	4.67	0.52	มากที่สุด
มีเทคนิคในการนำเสนอที่ทันสมัย	4.33	0.52	มาก
ระดับความคิดเห็นเฉลี่ย	**4.46**	**0.51**	**มาก**

จากตารางที่ 4.2 ด้านความถูกต้องของการออกแบบระบบ ซึ่งประกอบด้วยความเหมาะสม การใช้งานมีความง่ายในการเข้าถึงข้อมูล มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.33, S.D. = 0.52) ความเหมาะสมทางด้านมีความรวดเร็วในการใช้บริการ มีความเหมาะสม อยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.55) ความเหมาะสมทางด้านการจัดวางตำแหน่งของส่วนประกอบระบบ มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.67, S.D. = 0.52) และความเหมาะสมทางด้านเทคนิคในการนำเสนอที่ทันสมัย มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.33, S.D. = 0.52) ความคิดเห็นโดยรวม มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.46, S.D. = 0.51)

ตารางที่ 4.3 ความเหมาะสมในการใช้งานของระบบ

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
ระบบใช้งานง่าย ไม่ซับซ้อน	4.50	0.55	มากที่สุด
ข้อมูลมีความถูกต้อง ครบถ้วนและสมบูรณ์	4.17	0.75	มาก
ข้อมูลในระบบสามารถช่วยการตัดสินใจให้แก่ผู้ใช้	4.33	0.52	มาก
ระบบมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลอย่างเหมาะสม	4.00	0.89	มาก
ระดับความคิดเห็นเฉลี่ย	**4.25**	**0.95**	**มาก**

จากตารางที่ 4.3 ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย ซึ่งประกอบด้วยระบบใช้งานง่าย ไม่ซับซ้อน มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.55) ข้อมูลมีความถูกต้อง ครบถ้วนและสมบูรณ์ มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.17, S.D.= 0.75) ข้อมูลในระบบสามารถช่วยการตัดสินใจให้แก่ผู้ใช้ มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.33, S.D. = 0.52) และระบบมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลอย่างเหมาะสม มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.00, S.D. = 0.89) ความคิดเห็นโดยรวมมีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.25, S.D. = 0.95)

ตารางที่ 4.4 ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
มีการตรวจสอบสิทธิ์การใช้งานในแต่ละระดับ	4.83	0.41	มาก
มีการแบ่งแยกรายการของแต่ละระดับการเข้าถึง	4.50	0.55	มาก
มีการรักษาความปลอดภัยข้อมูลในระบบฐานข้อมูล	4.33	0.52	มาก
มีการตรวจหาและแจ้งเตือนภัยคุกคามอย่างทันท่วงที	4.67	0.52	มากที่สุด
ระดับความคิดเห็นเฉลี่ย	**4.58**	**0.50**	**มาก**

จากตารางที่ 4.4 ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย ซึ่งประกอบด้วยมีการตรวจสอบสิทธิ์การใช้งานในแต่ละระดับ มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.83, S.D. = 0.41) มีการแบ่งแยกรายการของแต่ละระดับการเข้าถึง มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.50, S.D. = 0.55) มีการรักษาความปลอดภัยข้อมูลในระบบฐานข้อมูลมีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.33, S.D. = 0.52) และมีการตรวจหาและ

แจ้งเตือนภัยคุกคามอย่างทันท่วงที มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\overline{X}$ = 4.67, S.D. = 0.52) ความคิดเห็นโดยรวม มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$ = 4.58, S.D. = 0.50)

ตารางที่ 4.5 ความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้

ข้อคำถาม	$\overline{X}$	S.D.	แปลความหมาย
การจัดหน้าจอ และตำแหน่งการจัดวางส่วนต่าง ๆ มีความเหมาะสม	4.33	0.52	มาก
ความชัดเจนของรายการและข้อความบนหน้าจอ มีความเหมาะสม	4.50	0.55	มากที่สุด
ภาษาที่ใช้ในส่วนต่างๆ มีความชัดเจน เข้าใจง่าย	4.50	0.52	มากที่สุด
รูปแบบของตัวอักษร ขนาด สี พื้นหลัง และรูปภาพ มีความเหมาะสม	4.67	0.52	มากที่สุด
ระดับความคิดเห็นเฉลี่ย	**4.50**	**0.51**	**มากที่สุด**

จากตารางที่ 4.5 ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย ซึ่งประกอบด้วยการจัดหน้าจอ และตำแหน่งการจัดวางส่วนต่าง ๆ มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\overline{X}$ = 4.33, S.D. = 0.52) ความชัดเจนของรายการและข้อความบนหน้าจอ มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$ = 4.50, S.D. = 0.55) ภาษาที่ใช้ในส่วนต่างๆ มีความชัดเจน เข้าใจง่าย มีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$ = 4.50, S.D. = 0.52) และรูปแบบของตัวอักษร ขนาด สี พื้นหลัง และรูปภาพมีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$ = 4.67, S.D. = 0.52) ความคิดเห็นโดยรวมมีความเหมาะสมอยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$ = 4.50, S.D. = 0.51)

ตารางที่ 4.6 สรุปการประเมินความเหมาะสมของผู้เชี่ยวชาญระบบ

ข้อคำถาม	$\overline{X}$	S.D.	แปลความหมาย
ความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งาน	4.50	0.51	เหมาะสมมากที่สุด
ความเหมาะสมด้านความถูกต้องของการออกแบบระบบ	4.46	0.51	เหมาะสมมาก
ความเหมาะสมในการใช้งานของระบบ	4.25	0.95	เหมาะสมมาก
ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย	4.25	0.95	เหมาะสมมาก
ความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้	4.50	0.51	เหมาะสมมากที่สุด
ระดับความคิดเห็นเฉลี่ย	**4.46**	**0.54**	**เหมาะสมมาก**

จากตารางที่ 4.6 พบว่า ระดับความคิดเห็นเฉลี่ยของความเหมาะสมของระบบ ซึ่งทำการประเมินโดยผู้เชี่ยวชาญ นั้น มีความเหมาะสมอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.46, S.D. = 0.54) ทำให้สามารถสรุปได้ว่า การพัฒนาระบบสามารถออกแบบได้ตรงตามความต้องการของผู้ใช้งาน และความถูกต้องในการทำงานและการประเมินความเสี่ยง รวมทั้งการใช้งานของระบบที่สอดคล้องกับความต้องการ และมีการรักษาความปลอดภัยของข้อมูลภายในระบบ และการติดต่อสื่อสารได้ตรงกับผู้ใช้งาน โดยรวมแล้วพบว่า ระบบที่ออกแบบมานั้นสามารถพัฒนาวิธีการตรวจสอบเฝ้าระวังและแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบกได้ เป็นอย่างดี

2.2 การประเมินประสิทธิภาพของระบบโดยผู้ใช้งาน ผู้วิจัยได้ทำการประเมินประสิทธิภาพของระบบโดยผู้ใช้งาน เพื่อประเมินประสิทธิภาพของการใช้งานระบบ รายละเอียดการประเมิน ดังนี้

- ประชากรและกลุ่มตัวอย่างที่ใช้ในงานวิจัย คือ บุคลากรที่ปฏิบัติงานอยู่ภายในศูนย์ไซเบอร์กองทัพบก กลุ่มตัวอย่างที่ใช้ในการวิจัยคือ บุคลากรที่ปฏิบัติงานอยู่ภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน โดยใช้วิธีการคัดเลือกกลุ่มตัวอย่างแบบง่าย ด้วยวิธีการจับสลากเลือกผู้ตอบแบบสอบถาม

- เครื่องมือที่ใช้ในการวิจัย ใช้แบบสอบถามเก็บรวบรวมข้อมูล โดยการแจกแบบสอบถามให้กลุ่มตัวอย่าง จำนวน 35 ชุด

- ผลการวิจัย พบว่า

ส่วนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบสอบถาม เป็นเพศชายจำนวน 30 คน คิดเป็นร้อยละ 85 เป็นเพศหญิง จำนวน 5 คน คิดเป็นร้อยละ 15 มีอายุน้อยกว่า 30 ปี จำนวน 7 คน คิดเป็นร้อยละ 20 มีอายุระหว่าง 30 - 40 ปี จำนวน 8 คน คิดเป็นร้อยละ 23 มีอายุระหว่าง 41 - 50 ปี จำนวน 15 คน คิดเป็นร้อยละ 42 และอายุมากกว่า 50 ปีขึ้นไป จำนวน 5 คน คิดเป็นร้อยละ 15 ระดับการศึกษาต่ำกว่าระดับปริญญาตรี จำนวน 10 คน คิดเป็นร้อยละ 28 ระดับปริญญาตรี จำนวน 20 คน คิดเป็นร้อยละ 57 และปริญญาโท จำนวน 5 คน คิดเป็นร้อยละ 15 ตำแหน่งงาน เป็นผู้บริหาร จำนวน 5 คน คิดเป็นร้อยละ 14 เป็นผู้ดูแลระบบเครือข่าย จำนวน 5 ท่าน คิดเป็นร้อยละ 14 และเป็นเจ้าหน้าที่ปฏิบัติงาน 25 คน คิดเป็นร้อยละ 72 และระยะเวลาในการทำงานน้อยกว่า 10 ปี จำนวน 5 คน คิดเป็นร้อยละ 15 ระยะเวลาในการทำงาน 11 - 15 ปี จำนวน 10 คน คิดเป็นร้อยละ 28 ระยะเวลาในการทำงาน 16 - 20 ปี จำนวน 20 คน คิดเป็นร้อยละ 57

ส่วนที่ 2 ความคิดเห็นทางด้านประสิทธิภาพในการใช้งานของระบบ ผู้วิจัยได้ทำแบบสอบถามความคิดเห็นจากผู้ใช้งาน โดยมีประเมินประสิทธิภาพของระบบโดยผู้ใช้งาน ดังแสดงตามตาราง

ตารางที่ 4.7 ประสิทธิภาพของระบบด้านการออกแบบการใช้งาน

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
การใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล	4.72	0.59	มากที่สุด
มีความสะดวก รวดเร็วในการเรียกใช้งานในเมนูต่างๆ	4.61	0.63	มากที่สุด
การวางตำแหน่งเมนูบนจอภาพ ทำให้สามารถเรียกใช้งานได้ง่าย	4.47	0.64	มาก
มีความสะดวกในการสรุปและนำเสนอข้อมูล	4.42	0.67	มาก
การใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล	4.31	0.66	มาก
ระดับความคิดเห็นเฉลี่ย	**4.51**	**0.61**	**มากที่สุด**

จากตารางที่ 4.7 ประสิทธิภาพของระบบด้านการออกแบบการใช้งาน ซึ่งประกอบด้วย การใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.72, S.D. = 0.59) มีความสะดวก รวดเร็วในการเรียกใช้งานในเมนูต่าง ๆ มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.61, S.D. = 0.63) การวางตำแหน่งเมนูบนจอภาพ ทำให้สามารถเรียกใช้งานได้ง่าย มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.47, S.D.= 0.64) มีความสะดวกในการสรุปและนำเสนอข้อมูล มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.42, S.D. = 0.67) และการใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.31, S.D. = 0.66) ความคิดเห็นโดยรวม มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.51, S.D. = 0.61)

ตารางที่ 4.8 ประสิทธิภาพของระบบด้านการบันทึกและการแก้ไขข้อมูล

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
แบบฟอร์มบันทึกและแก้ไขข้อมูลมีความเหมาะสม ใช้งานง่าย	4.44	0.65	มาก
แบบฟอร์มสำหรับบันทึกข้อมูลมีความเหมาะสม ครบถ้วน	4.47	0.61	มาก
การแก้ไขข้อมูล ทำได้สะดวก รวดเร็ว ใช้งานง่าย และถูกต้อง	4.33	0.72	มาก
ระดับความคิดเห็นเฉลี่ย	**4.42**	**0.66**	**มาก**

จากตารางที่ 4.8 ประสิทธิภาพของระบบด้านการบันทึกและการแก้ไขข้อมูล ซึ่งประกอบด้วยแบบฟอร์มบันทึกและแก้ไขข้อมูลมีความเหมาะสม ใช้งานง่าย มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.44, S.D. = 0.62) แบบฟอร์มสำหรับบันทึกข้อมูลมีความเหมาะสม ครบถ้วน มีประสิทธิภาพอยู่ในระดับเหมาะสมมาก ($\bar{X}$ = 4.47, S.D. = 0.61) และการแก้ไขข้อมูล ทำได้

สะดวก รวดเร็ว ใช้งานง่าย และถูกต้อง มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.33, S.D. = 0.72) ความคิดเห็นโดยรวมมีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.42, S.D. = 0.66)

ตารางที่ 4.9 ประสิทธิภาพของระบบด้านการประมวลผลและการแสดงผล

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
หน้าจอการสืบค้นและรายงานมีความเหมาะสม	4.50	0.51	มากที่สุด
สืบค้นข้อมูลได้สะดวก และใช้งานได้ง่าย	4.47	0.65	มาก
การสืบค้นข้อมูลมีความถูกต้อง	4.72	0.45	มากที่สุด
ตัวอักษร ขนาด สี ในการแสดงผลข้อมูล มีความเหมาะสม	4.50	0.70	มากที่สุด
การรายงานสามารถทำได้ง่าย สะดวก และถูกต้อง	4.64	0.59	มากที่สุด
ระดับความคิดเห็นเฉลี่ย	**4.57**	**0.59**	**มากที่สุด**

จากตารางที่ 4.99 ประสิทธิภาพของระบบด้านการประมวลผลและการแสดงผล ซึ่งประกอบด้วยหน้าจอการสืบค้นและรายงานมีความเหมาะสม มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.51) สืบค้นข้อมูลได้สะดวก และใช้งานได้ง่าย มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.47, S.D.= 0.65) การสืบค้นข้อมูลมีความถูกต้อง มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.72, S.D. = 0.45) ตัวอักษร ขนาด สี ในการแสดงผลข้อมูล มีความเหมาะสม มีประสิทธิภาพอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.70) และการรายงานสามารถทำได้ง่าย สะดวก และถูกต้อง มีประสิทธิภาพอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.64, S.D. = 0.59) ความคิดเห็นโดยรวมมีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.57, S.D. = 0.59)

ตารางที่ 4.10 ประสิทธิภาพของระบบด้านการสืบค้นข้อมูล และการรายงาน

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
การสืบค้น และการรายงานผล สะดวก ใช้งานง่าย	4.67	0.48	มากที่สุด
การประมวลผลแต่ละขั้นตอนมีความรวดเร็ว	4.72	0.45	มากที่สุด
ข้อมูลที่ได้ มีความแม่นยำ	4.58	0.50	มากที่สุด
ระดับความคิดเห็นเฉลี่ย	**4.66**	**0.48**	**มากที่สุด**

จากตารางที่ 4.10 ประสิทธิภาพของระบบด้านการสืบค้นข้อมูล และการรายงาน ซึ่งประกอบด้วยการสืบค้น และการรายงานผล สะดวก ใช้งานง่าย มีประสิทธิภาพอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.67, S.D. = 0.48) การประมวลผลแต่ละขั้นตอนมีความรวดเร็ว

มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.72, S.D. = 0.45) และข้อมูลที่ได้ มีความแม่นยำมีประสิทธิภาพอยู่ในระดับเหมาะสมมากที่สุด ($\bar{X}$ = 4.58, S.D. = 0.50) ความคิดเห็นโดยรวมมีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.66, S.D. = 0.48)

ตารางที่ 4.11 ประสิทธิภาพด้านการใช้งานของระบบ

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
สามารถตอบสนองความต้องการของผู้ใช้ได้รวดเร็ว	4.28	0.57	มาก
สามารถช่วยลดระยะเวลาในการประมวลผล	4.53	0.56	มากที่สุด
มีการตรวจสอบสิทธิ์การใช้งานในระดับต่าง ๆ	4.58	0.60	มากที่สุด
มีการเชื่อมโยงข้อมูลในแต่ละส่วนมาแสดงผลได้อย่างรวดเร็ว	4.44	0.65	มาก
ระดับความคิดเห็นเฉลี่ย	**4.46**	**0.60**	**มาก**

จากตารางที่ 4.11 ประสิทธิภาพด้านการใช้งานของระบบ ซึ่งประกอบด้วยสามารถตอบสนองความต้องการของผู้ใช้ได้รวดเร็ว มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.28, S.D. = 0.57) สามารถช่วยลดระยะเวลาในการประมวลผล มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.53, S.D. = 0.56) มีการตรวจสอบสิทธิ์การใช้งานในระดับต่าง ๆ มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.58, S.D. = 0.60) และมีการเชื่อมโยงข้อมูลในแต่ละส่วนมาแสดงผลได้อย่างรวดเร็ว มีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.44, S.D. = 0.65) ความคิดเห็นโดยรวมมีประสิทธิภาพอยู่ในระดับมาก ($\bar{X}$ = 4.46, S.D. = 0.60)

ตารางที่ 4.12 สรุปการประเมินประสิทธิภาพการใช้งานระบบโดยผู้ใช้งาน

ข้อคำถาม	$\bar{X}$	S.D.	แปลความหมาย
ประสิทธิภาพของระบบด้านการออกแบบการใช้งาน	4.51	0.61	มากที่สุด
ประสิทธิภาพของระบบด้านการบันทึกและการแก้ไขข้อมูล	4.42	0.66	มาก
ประสิทธิภาพของระบบด้านการประมวลผลและการแสดงผล	4.57	0.59	มากที่สุด
ประสิทธิภาพของระบบด้านการสืบค้นข้อมูล และการรายงาน	4.66	0.48	มากที่สุด
ประสิทธิภาพด้านการใช้งานของระบบ	4.46	0.60	มาก
ระดับความคิดเห็นเฉลี่ย	**4.52**	**0.59**	**มากที่สุด**

จากตารางที่ 4.12 พบว่า ระดับความคิดเห็นเฉลี่ยของประสิทธิภาพการใช้งานระบบโดยผู้ใช้งาน จำนวน 35 คน นั้น พบว่า มีประสิทธิภาพอยู่ในระดับมีประสิทธิภาพมากที่สุด ($\overline{X}$ = 4.52, S.D. = 0.59) ทำให้สามารถสรุปผลการประเมินประสิทธิภาพการใช้งานระบบโดยผู้ใช้งาน วิจัยในครั้งนี้ได้ว่า ประสิทธิภาพของระบบด้านการออกแบบการใช้งานได้ตรงตามความต้องการของผู้ใช้งาน การบันทึกและการแก้ไขข้อมูลสามารถทำได้ง่าย และมีความสะดวกในการประมวลผลและการแสดงผล รวมถึงความสะดวกในการสืบค้นข้อมูลและการรายงาน และสามารถตอบสนองการทำงานผู้ใช้งานได้ในทุกระดับ การตรวจสอบและการรายงานผลสถิติภัยคุกคามทางไซเบอร์เป็นไปอย่างรวดเร็ว ลดขั้นตอนการตรวจสอบภัยคุกคามด้านไซเบอร์ของเจ้าหน้าที่ และลดปริมาณการใช้กระดาษ รวมถึงเป็นการรักษาความลับของทางราชการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

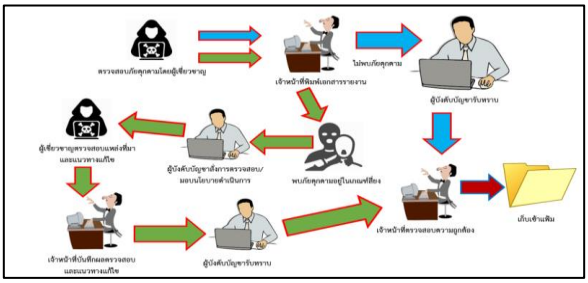
บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาและวิจัยครั้งนี้ เป็นการพัฒนาระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยมีวัตถุประสงค์ 1) เพื่อศึกษาบริบท ปัญหาและสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ ภายในศูนย์ไซเบอร์กองทัพบก 2) เพื่อพัฒนาวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก 3) เพื่อพัฒนาแอปพลิเคชันสำหรับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ 4) เพื่อทำการประเมินระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน สำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสรุปผลการวิจัยนั้น ผู้วิจัยจะนำเสนอตามลำดับต่อไปนี้

สรุปผลการวิจัย

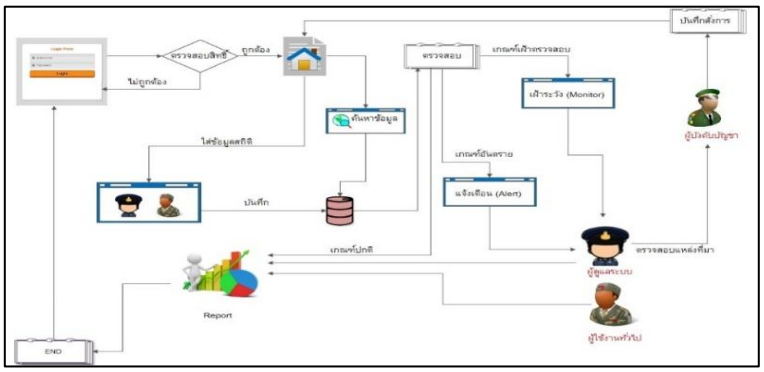
1. เพื่อศึกษาบริบท ปัญหาและสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ ภายในศูนย์ไซเบอร์กองทัพบก ผู้วิจัยได้ทำงานวิจัยนี้เพื่อเป็นการศึกษาความพร้อมทางด้านความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก เพื่อให้สอดคล้องกับภารกิจ ของศูนย์ไซเบอร์กองทัพบก และความต้องการของผู้บังคับบัญชา โดยการศึกษาวิจัยครั้งนี้ เพื่อเป็นการอำนวยความสะดวกให้แก่บุคลากรที่ทำหน้าที่ตรวจสอบภัยคุกคามทางทางด้านไซเบอร์ของศูนย์ไซเบอร์กองทัพบก และสนับสนุนการตัดสินใจของผู้บังคับบัญชาภายในศูนย์ไซเบอร์กองทัพบก

2. เพื่อพัฒนาวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ภายในศูนย์ไซเบอร์กองทัพบก ผู้วิจัยได้ทำการพัฒนาวิธีการตรวจสอบ วิธีการเฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยการทำเอาเทคโนโลยีมาประยุกต์ใช้แทนระบบเดิม ที่ใช้การดำเนินการทางด้านเอกสารเป็นหลัก ดังภาพประกอบที่ 5.1



ภาพประกอบที่ 5.1 วงจรการทำงานของระบบงานเดิม

3. เพื่อพัฒนาแอปพลิเคชันสำหรับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยได้ทำการพัฒนาแอปพลิเคชัน เพื่อการตรวจสอบ เฝ้าระวัง และแจ้งเตือน สำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ โดยได้ทำการออกแบบระบบเชิงวัตถุด้วยการใช้หลักการของ Use Case Diagram และได้ทำการพัฒนาระบบตามที่ได้ออกแบบไว้ก่อนหน้าแล้ว โดยมีวงจรการทำงานของระบบงานใหม่ ดังภาพประกอบที่ 5.2



ภาพประกอบที่ 5.2 วงจรการทำงานของระบบงานใหม่

4. เพื่อทำการประเมินระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน สำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยได้ทำการออกแบบระบบ พร้อมขอรับคำแนะนำจากผู้เชี่ยวชาญและโดยให้มีการประเมินความเหมาะสมของระบบ โดยผู้เชี่ยวชาญ และประเมินประสิทธิภาพระบบโดยผู้ใช้งาน ซึ่งผลการประเมินพบว่า การประเมินความเหมาะสมของระบบโดยผู้เชี่ยวชาญ จำนวน 6 ท่าน โดยมีหัวข้อในการประเมินรวม 5 ด้าน พบว่าด้านที่มีความเหมาะสมมากที่สุด 2 ด้าน ได้แก่ด้านความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งาน และ ด้านความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้ ด้านที่มีความเหมาะสมมาก 3 ด้าน ได้แก่ด้านความเหมาะสมด้านความถูกต้องของการออกแบบระบบ ด้านความเหมาะสมในการใช้งานของระบบ และด้านความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย แสดงว่าผู้เชี่ยวชาญยอมรับในความเหมาะสมของระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน สำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีความเหมาะสมในระดับที่มีความเหมาะสมมาก และการประเมินประสิทธิภาพการใช้งานของระบบโดยผู้ใช้งาน จำนวน 35 คน โดยมีหัวข้อในการประเมินรวม 5 ด้าน พบว่า ด้านที่มีประสิทธิภาพมากที่สุด 2 ด้าน ได้แก่การใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล และ ด้านมีความสะดวก รวดเร็วในการเรียกใช้งานในเมนูต่าง ๆ ด้านที่มีประสิทธิภาพมาก 3 ด้าน ได้แก่ด้านการวางตำแหน่งเมนูบนจอภาพ ทำให้สามารถเรียกใช้งานได้ง่าย ด้านมีความสะดวกในการสรุปและนำเสนอข้อมูล และด้านการใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล

แสดงว่าผู้ใช้งานยอมรับในประสิทธิภาพของระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน สำหรับการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ โดยรวมแล้วจะมีความพึงพอใจอยู่ในระดับที่มีประสิทธิภาพการใช้งานมากที่สุด

การพัฒนาระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก เพื่อเป็นการอำนวยความสะดวกให้แก่ผู้ใช้งานทางด้านการตรวจสอบเฝ้าระวังและแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ซึ่งจากผลการประเมินความเหมาะสมของระบบจากทั้งผู้เชี่ยวชาญและการประเมินประสิทธิภาพการใช้งานของระบบโดยผู้ใช้งาน บ่งบอกได้ว่าระบบมีความเหมาะสมและมีประสิทธิภาพในการใช้งาน ซึ่งสามารถนำมาใช้งานทางด้านการตรวจสอบเฝ้าระวัง และแจ้งเตือนการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ได้อย่างมีประสิทธิภาพ

อภิปรายผล

งานวิจัยนี้เพื่อเป็นการพัฒนาระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก จากผลการประเมิน แสดงให้เห็นว่าระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสม และสามารถตอบสนองการทำงานผู้ใช้งานได้ในทุกระดับ การตรวจสอบและการรายงานผลสถิติภัยคุกคามทางไซเบอร์เป็นไปอย่างรวดเร็ว ทำให้ลดขั้นตอนการตรวจสอบภัยคุกคามของเจ้าหน้าที่ รวมถึงเป็นการลดปริมาณการใช้กระดาษ และรักษาความลับของทางราชการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับงานวิจัยของ ธนกร มีหินกอง, ประสงค์ ปราณีตพลกรัง, นิเวศ จิระวิชิตชัย (2558) ศึกษาเรื่อง สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวด้วยเทคนิคกฎความสัมพันธ์ พบว่า ระบบตรวจหาการบุกรุก ที่ได้พัฒนาขึ้นมานั้น สามารถรายงานผลได้อย่างรวดเร็ว และสามารถนำไปใช้วิเคราะห์และทำนายผลการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ต่อไป

ปัญหาและอุปสรรค

การวิจัยเรื่อง การพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ได้พบปัญหาและอุปสรรคดังนี้

1. ปัญหาจากการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง ซึ่งจำเป็นต้องใช้เวลาที่ค่อนข้างมาก เพื่อให้งานวิจัยมีประสิทธิภาพสูงสุด และเพื่อเป็นการเข้าใจในหลักแนวคิด และทฤษฎี รวมถึงการแนวทางในการต่อยอดของงานวิจัย เพื่อประโยชน์ของงานวิจัยต่อไปในอนาคต

2. การทดสอบระบบของผู้ใช้ระบบ ทำได้ล้าช้ากว่ากำหนดเนื่องจากต้องใช้เวลาในการอธิบายถึงวิธีในการทำงานของระบบเพื่อให้เกิดประโยชน์ในการใช้งานมากที่สุด

ข้อเสนอแนะ

1. ข้อเสนอแนะสำหรับการใช้งานจริง

จากผลการวิจัย พบว่าการพัฒนาระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก นั้น ยังสามารถพัฒนาต่อยอดทำเป็นแอปพลิเคชันสำหรับการเฝ้าระวังภัยคุกคาม ประเมินความเสี่ยงด้านไซเบอร์บนอุปกรณ์สื่อสารเคลื่อนที่ได้ ซึ่งจะทำให้การใช้งานมีความง่ายและสะดวกมากยิ่งขึ้น

2. ข้อเสนอแนะสำหรับการนำงานวิจัยไปใช้ในอนาคต

นอกจากนั้น งานวิจัยนี้ยังสามารถขยายผลไปสู่การพัฒนาระบบเฝ้าระวังภัยคุกคามและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบกแบบเรียลไทม์อย่างอัตโนมัติในอนาคต ด้วยการทำเอาเทคโนโลยีสมัยใหม่เข้ามาใช้ร่วม ได้แก่

1) การนำเอาเทคโนโลยี AI มาใช้ในการตรวจสอบและแยกประเภทภัยคุกคามทางไซเบอร์เพื่อให้การวิเคราะห์และการแยกประเภทภัยคุกคามมีความสะดวกและแม่นยำมากยิ่งขึ้น

2) การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เพื่อทำให้สามารถรองรับสถิติภัยคุกคามที่มีแนวโน้มว่าจะมีการโจมตีสูงเพิ่มมากขึ้นต่อไปในอนาคต ซึ่งจะทำให้สามารถ รองรับการเข้าถึงการใช้งาน ข้อมูลจำนวนมาก ๆ ได้อย่างง่ายดาย

3) การใช้ Data Mining เพื่อหาความสัมพันธ์ของข้อมูลที่มีความเสี่ยงอันอาจเป็นภัยคุกคามทางไซเบอร์ ทั้งนี้ จะเป็นการทำนายแนวโน้มที่จะเกิดการเสี่ยงต่อระบบสารสนเทศในกองทัพบกในภาพรวม

4) การเพิ่มความพร้อมทางด้านการคืนสภาพได้อย่างรวดเร็วของระบบ (Cyber Resilience) เพื่อรับมือกับภัยคุกคามและทำให้องค์กรมีความทนทานต่อการบุกรุก การโจมตี รวมถึงความสามารถในการคืนสภาพของระบบ ไม่ว่าจะเป็นการโจมตีที่เกิดจากปัจจัยภายในหรือภายนอก เพื่อตอบสนองทางด้านการฟื้นฟูหรือการคืนสภาพของระบบสารสนเทศในกรณีที่ถูกภัยคุกคามทางไซเบอร์ต่อหน่วยงานของกองทัพบกได้ในอนาคต

บรรณานุกรม

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

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

ราชกิจจานุเบกษา. (2560). **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560.** เล่ม 134 ตอนที่ 10 ก ลงวันที่ 24 มกราคม 2560

ราชกิจจานุเบกษา. (2560). **ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560.** เล่ม 134 ตอนพิเศษ 259 ง ลงวันที่ 20 ตุลาคม 2560.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2555) **มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555**. ประกาศในราชกิจจานุเบกษา เล่ม 129. ตอนพิเศษ 191 ง. หน้า 42 . วันที่ 19 ธันวาคม 2555.

บัญชา ปะสีละเตสัง. (2557) **พัฒนาเว็บแอปพลิเคชันด้วย PHP ร่วมกับ MySQL และ JQuery.** บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน).

ปริญญา หอมเอนก. (2558) **Strategy to Cybersecurity 4.0.** บริษัท เอซิส โฟรเฟสชั่นนัลเซ็นเตอร์ จำกัด.

ฤทธี อินทราวุธ, พลโท. (2557). **ศูนย์ไซเบอร์กองทัพบก (Army Cyber Center).** วันที่สืบค้น 16 ต.ค.2560. จากเว็บไซต์ : http://rittee1834.blogspot.com/2014/10/army-cyber-center.html.

สำนักงานสภาความมั่นคงแห่งชาติ. (2560). **นโยบายความมั่นคงแห่งชาติ พ.ศ.2558 – 2564.** วันที่สืบค้น 22 ต.ค.2560. จากเว็บไซต์ : http://www.cabinet.soc.go.th/soc/Program23.jsp?top_serl=99313080.

สุธีร์ กิจเจริญการกุล. (2560) **5 ภัยคุกคามไซเบอร์ที่ต้องพึงระวังในปี 2018**. วันที่สืบค้น 22 ต.ค.2560. จากเว็บไซต์ : https://www.catcyfence.com/it-security/article/top-5-cyber-security-in-2018/

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). (2561) **สถิติภัยคุกคาม 2561.** วันที่สืบค้น 3 มี.ค.2561 จากเว็บไซต์ https://www.thaicert.or.th/statistics/statistics.html.

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). **การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม.** บทความวิชาการสถาบันวิชาการป้องกันประเทศ.

สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน. (2559). **โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล**. วารสารวิชาการมหาวิทยาลัยจอมเกล้าพระนครเหนือ ปีที่ 8 ฉบับที่ 2 กรกฎาคม ถึง ธันวาคม 2555.

ณัฐวี อุตกฤษฎ์. (2557). **การวางแผนรองรับเหตุการณ์ ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร.** วารสารเทคโนโลยีสารสนเทศ มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ ปีที่ 8 ฉบับที่ 2 กรกฎาคม - ธันวาคม 2555.

วิภารัตน์ ปทักขินัง และ ประสงค์ ปราณีตพลกรัง มหาวิทยาลัยศรีปทุม. (2557). **การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร.**

นรังสรรค์ วิไลสกุลยง และวรรณชัย วรรณสวัสดิ์. (2560). **“การพัฒนารูปแบบการจัดการห้องเรียนไซเบอร์บนระบบประมวลผลกลุ่มเมฆด้วยหลักจัดการเรียนแบบร่วมมือ”**. วารสารพัฒนาเทคนิคศึกษา มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ปีที่ 2017. ฉบับที่ 101.

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

T. Sommestad, M. Ekstedt and P. Johnson. **Cyber Security Risks Assessment with Bayesian** on System Sciences (HICSS). pp. 1–10, 2009.

Jose Palala, Martin Helmich. (2016) **PHP 7 Programming Blueprints**: on October 2016. 7-12 35 – 80. Production reference 2061016. ISBN 978-78588971-4.

Dinesh priyankara, Robert C. Cain. (2016). **SQL Server 2016 Reporting Service Cookbook**. First published: November 2016. 65 – 80 Production reference: 1211116 ISBN 978-78646-181.0.

Stoyan Stefanov, Kumar Chetan Sharma. (2008) **Object-Oriented JavaScript Second Edition.** First published: July 2008 Second edition: July 2013. 35 – 37 Ltd. ISBN 978-1-84969-312-7.

ภาคผนวก

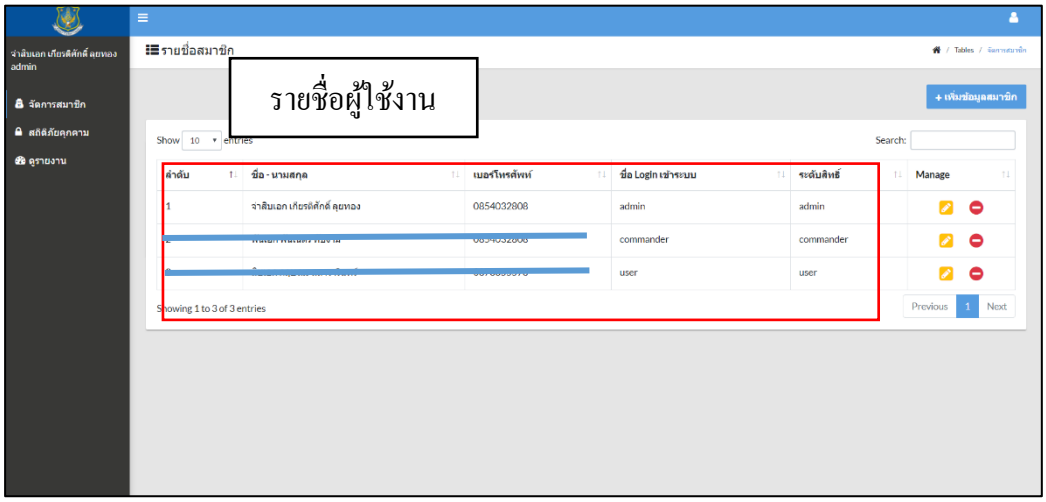
ภาคผนวก ก

คู่มือการใช้งาน ระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก

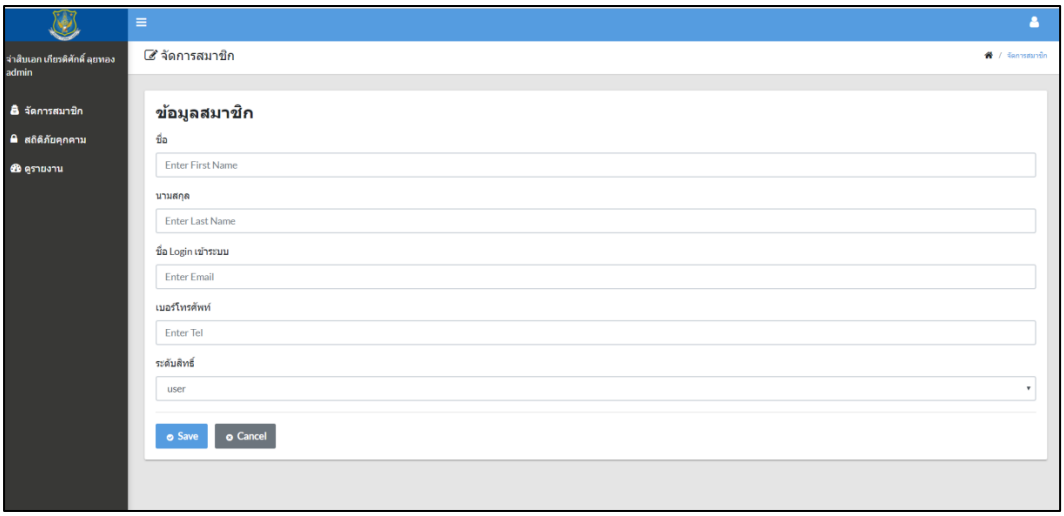
คู่มือและการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือน การรักษาความมั่นคงปลอดภัยไซเบอร์ศูนย์ไซเบอร์กองทัพบก

การเข้าสู่ระบบ : ให้ทำการเข้าสู่ระบบตามสิทธิ์ที่ตัวเองได้รับ ในที่นี้ ไม่อนุญาตให้ทำการสมัครด้วยตนเอง วิธีการสมัคร ต้องทำการสมัครผ่านแอดมินของระบบ เท่านั้น เพื่อเป็นการรักษาความลับของทางราชการ

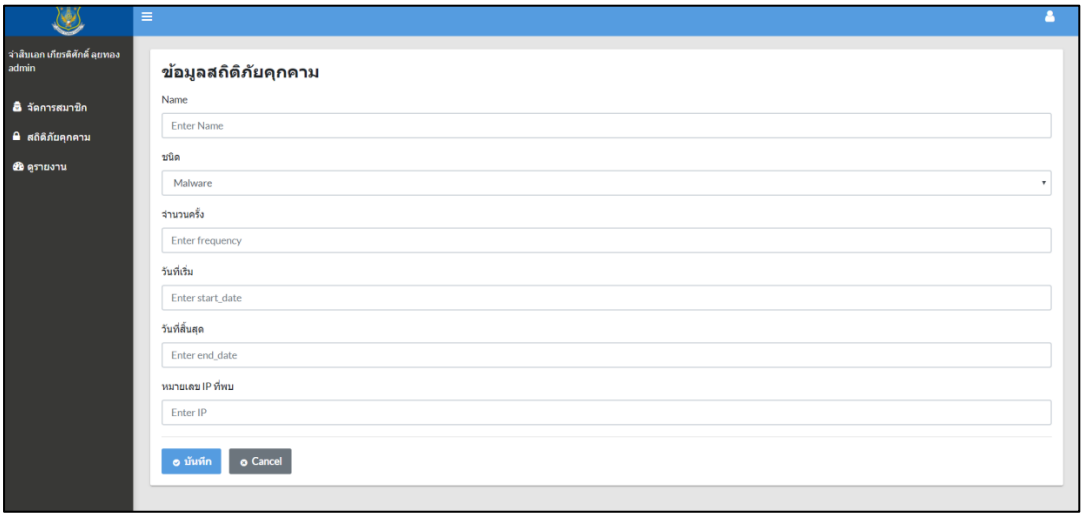
การจัดการสมาชิก : เป็นการบริหารจัดการสมาชิก ซึ่งจะอนุญาตให้ผู้ดูแลระบบได้ทำการบริหารจัดการสมาชิก เพื่อง่ายต่อการควบคุมและการดูแลบริหารสมาชิกพร้อมกำหนดสิทธิ์การใช้งาน ซึ่งจะสามารถ เพิ่มและลบสมาชิกได้โดยผู้ดูแลระบบ



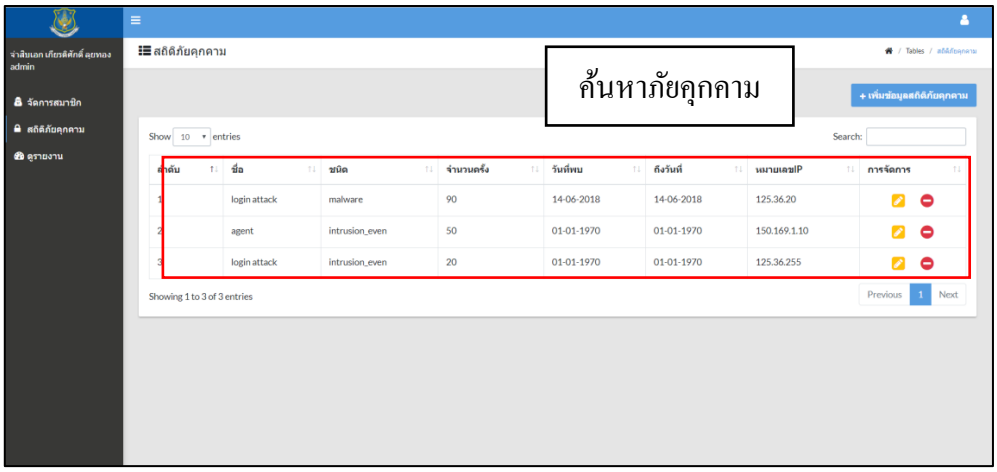
การเพิ่มสมาชิกใหม่ ให้ผู้ดูแลระบบได้ทำการเพิ่มข้อมูลสมาชิกใหม่ โดยมีรายละเอียดในการใช้งาน พื้นฐาน ได้แก่ ชื่อ นามสกุล ชื่อ Login เข้าระบบ เบอร์โทรศัพท์ ระดับสิทธิ์การใช้งาน

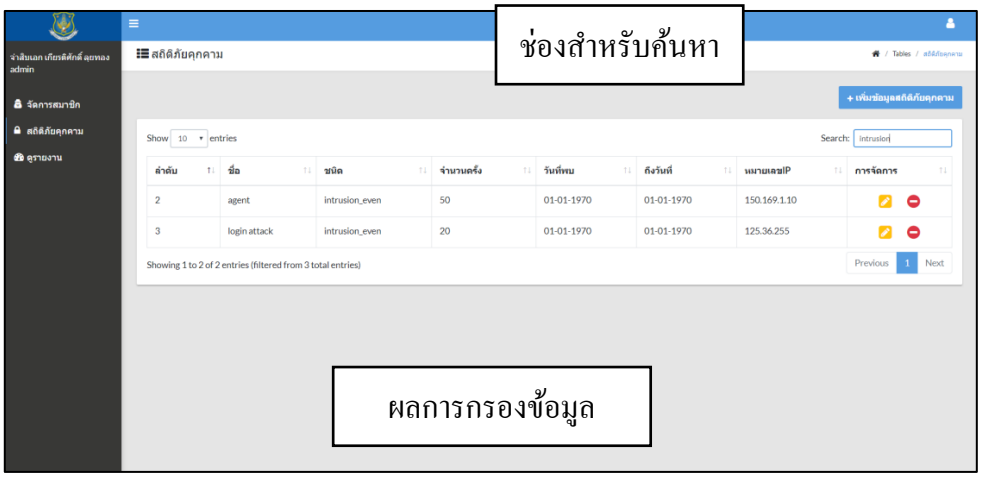


การบันทึกสถิติภัยคุกคาม : การบันทึกสถิติภัยคุกคามทั้ง 2 ประเภท ระบบจะให้ทำการบันทึก ในหน้าการบันทึกสถิติภัยคุกคาม เพื่อความง่ายในการบันทึก ระบบจะให้ทำการบันทึกเป็นส่วนรวม โดยการบันทึกให้ทำการบันทึกชื่อ ชนิด จำนวนครั้ง วันที่ พบ ถึงวันที่ หมายเลข IP ที่พบ

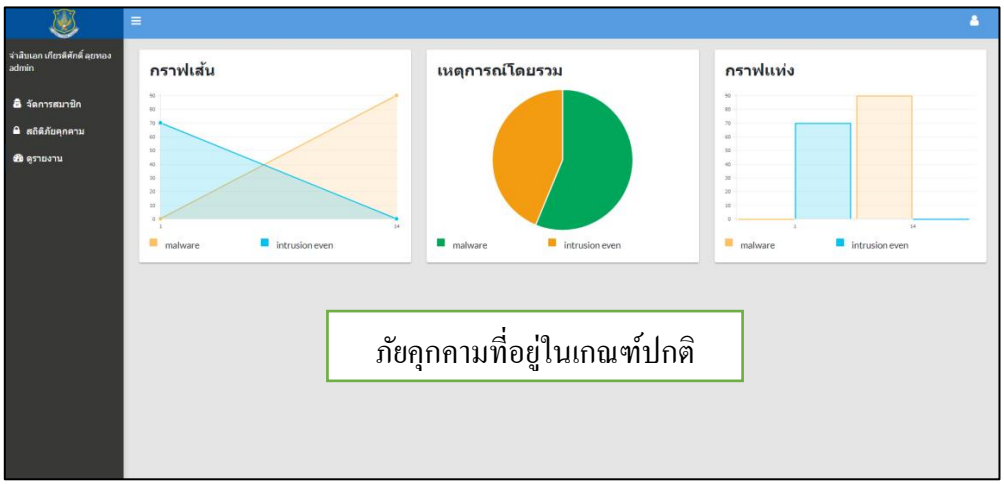


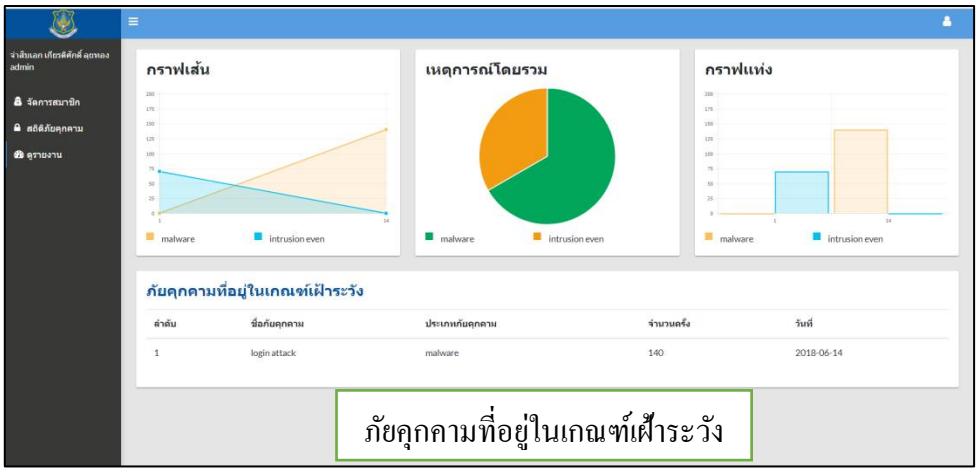
การรายงานผลการบันทึกสถิติภัยคุกคาม : การบันทึกสถิติภัยคุกคามทั้ง 2 ประเภท ระบบจะทำการรายงานผลการบันทึกสถิติภัยคุกคาม เพื่อความง่ายในการตรวจสอบ ระบบจะให้ทำการรายงานผลการบันทึกเป็นส่วนรวม โดยไม่ได้แยกประเภทของภัยคุกคาม เพื่อความสะดวกจะมีการค้นหาชื่อของภัยคุกคามเพื่อทำการตรวจสอบเพื่อทำการประเมินสถิติภัยคุกคาม

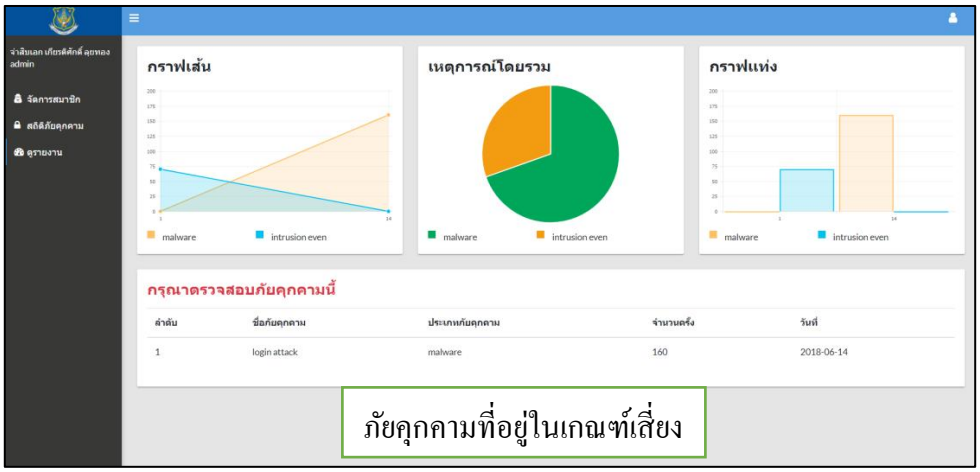




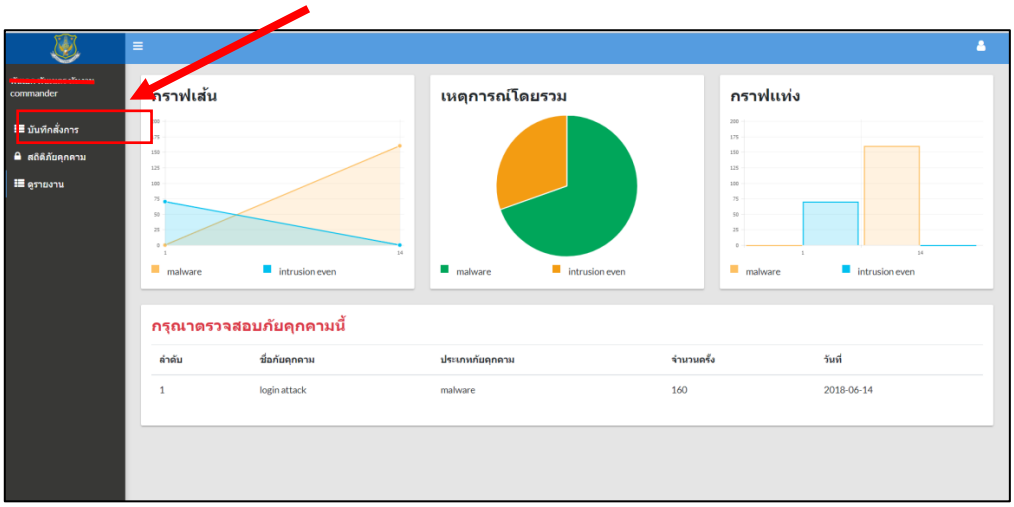
การนำเสนอรายงาน: เป็นการนำเสนอรายงานภัยคุกคามทางไซเบอร์ที่ตรวจพบ โดยจะแสดงออกมาเป็นรูปแบบของ Dash Board จะแบ่งออกเป็น 3 ระดับได้แก่ ภัยคุกคามที่อยู่ในเกณฑ์ปกติ ภัยคุกคามที่อยู่ในเกณฑ์เฝ้าระวัง และภัยคุกคามที่อยู่ในเกณฑ์เสี่ยง





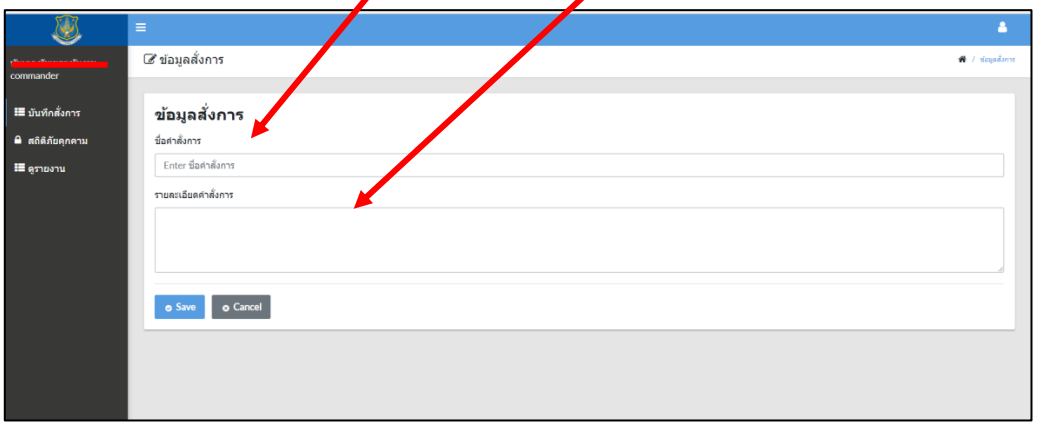


การบันทึกสั่งการ : เป็นการสั่งการในกรณีที่พบเห็นภัยคุกคามที่ผิดปกติ โดยทำการบันทึกเฉพาะสิทธิ์ของผู้บังคับบัญชา โดยเข้าไปในเมนูการบันทึกสั่งการนี้

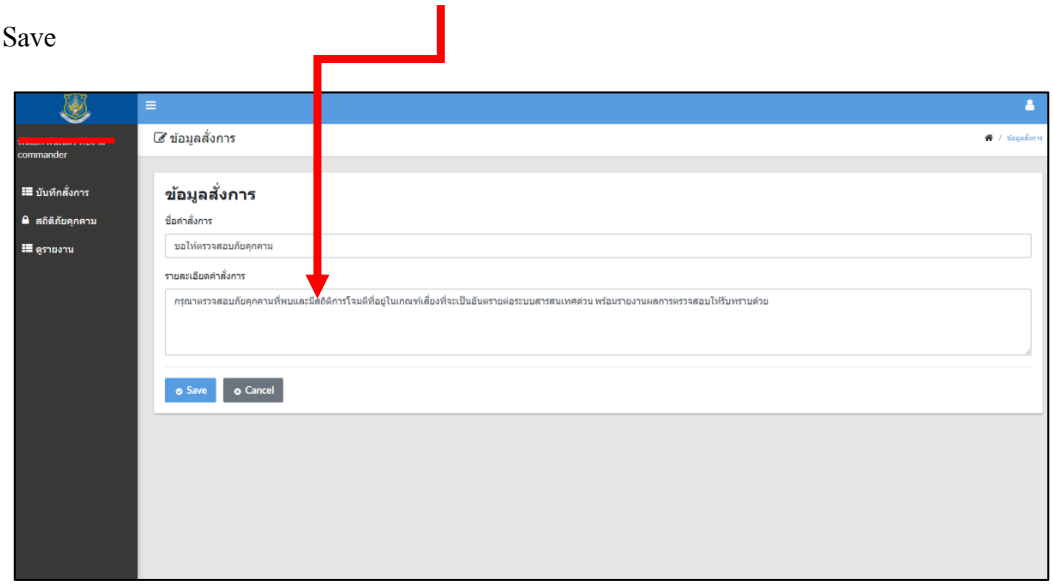


หัวข้อการบันทึกสั่งการ : ทำการคลิ๊ก Button เพื่อเข้าทำการบันทึกสั่งการ

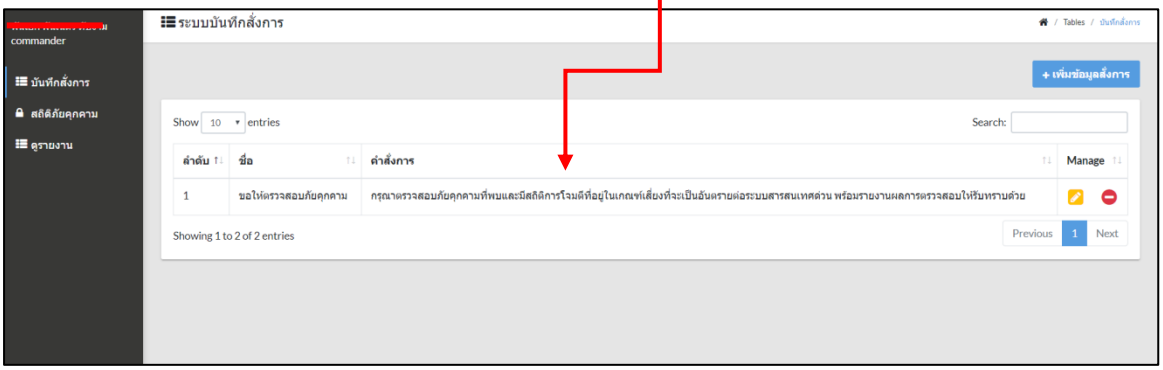
เพิ่มข้อมูลการสั่งการ : ทำการเพิ่มชื่อคำสั่ง และ รายละเอียดในการสั่งการ



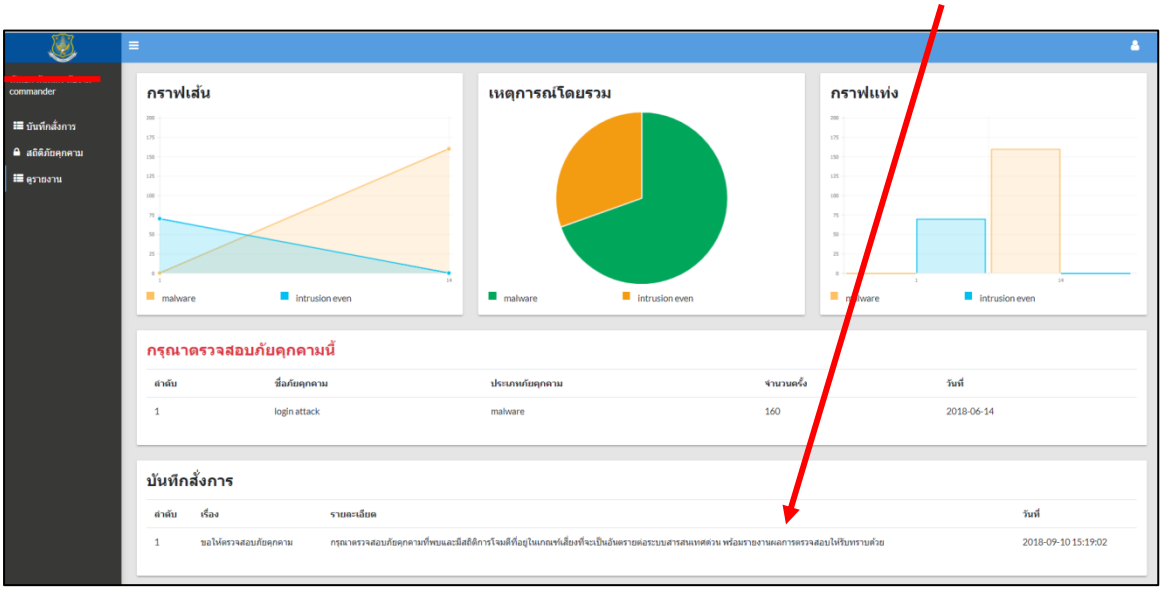
การบันทึกข้อมูลการสั่งการ : หลังจากตั้งหัวข้อพร้อมคำสั่งการเรียบร้อยแล้ว ให้ทำการกดปุ่ม Save



การแสดงผลการบันทึกข้อมูลการสั่งการ : จากการที่ได้ทำการบันทึกคำสั่งการแล้ว ระบบจะทำการบันทึกข้อมูลการสั่งการ ในส่วนของการบันทึกในระบบ



การแสดงผลการบันทึกข้อมูลการสั่งการ : ระบบจะทำการรายงานผลการสั่งการออกมาทางหน้าการรายงานข้อมูล เพื่อให้ผู้เกี่ยวข้องได้ทำตามคำสั่งการที่ผู้บังคับบัญชาได้สั่งการลงมา



ภาคผนวก ข

แบบประเมินความเหมาะสมของระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการควบคุมและรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก โดยผู้เชี่ยวชาญ

แบบประเมินความเหมาะสมของ ระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุกและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก (ประเมินโดยผู้เชี่ยวชาญ)

<u>คำชี้แจง</u>

แบบสอบถามชุดนี้ มีวัตถุประสงค์เพื่อทำการประเมินความเหมาะสมของระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ที่ผู้วิจัยได้พัฒนาขึ้น ผู้วิจัยใคร่ขอความอนุเคราะห์จากท่านได้โปรดประเมินความเหมาะสมระบบดังกล่าว รวมทั้งกรุณาให้ข้อเสนอแนะในสิ่งที่ต้องปรับปรุงให้ดีและสมบูรณ์มากยิ่งขึ้นต่อไป

<u>แบบสอบถามแบ่งออกเป็น 3 ตอน คือ</u>

ตอนที่ 1 แบบสอบถามสถานภาพทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 แบบประเมินความเหมาะสมของระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุกและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก

ตอนที่ 3 แบบสอบถามความคิดเห็นและข้อเสนอแนะ

การแปลค่าความหมาย แบ่งเป็น 5 ระดับ ดังต่อไปนี้

5	หมายถึง	มีความเหมาะสมมากที่สุด
4	หมายถึง	มีความเหมาะสมมาก
3	หมายถึง	มีความเหมาะสมปานกลาง
2	หมายถึง	มีความเหมาะสมน้อย
1	หมายถึง	มีความเหมาะสมน้อยที่สุด

ผู้วิจัย ขอขอบพระคุณเป็นอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

จ่าสิบเอก เกียรติศักดิ์ ลุยทอง โทรศัพท์ 080-934-9887 อีเมล ; Keaittisuk@gmail.com

นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ตอนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบสอบถาม

โปรดทำเครื่องหมาย ✓ ในช่อง ☐ ที่ตรงกับข้อมูลของท่าน เพียงช่องเดียว

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 - 40 ปี

☐ 41 - 50 ปี ☐ มากกว่า 50 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี

☐ ปริญญาโท ☐ ปริญญาเอก

4. ตำแหน่งหรือลักษณะงานที่ทำ

☐ ผู้บริหาร ☐ ผู้ดูแลระบบเครือข่าย

☐ เจ้าหน้าที่ปฏิบัติงาน ☐ ผู้เชี่ยวชาญด้านไอที

5. ระยะเวลาที่ปฏิบัติงานในหน่วยงาน

☐ น้อยกว่า 10 ปี ☐ 11 - 15 ปี

☐ 16 - 20 ปี ☐ มากกว่า 20 ปี

ตอนที่ 2 ความเหมาะสมของระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก

โปรดทำเครื่องหมาย ✓ ในช่องที่ตรงกับระดับความคิดเห็นของท่านที่มีต่อระบบฯ

ข้อคำถาม	ระดับความเหมาะสม				
	1	2	3	4	5
1.ความเหมาะสมด้านความสามารถตรงตามความต้องการของผู้ใช้งาน					
1.1 ความเหมาะสมทางด้านการจัดการข้อมูลผู้ใช้งาน					
1.2 ความเหมาะสมทางด้านการจัดเก็บสถิติภัยคุกคาม					
1.3 ความเหมาะสมทางด้านการนำเสนอรายงานภัยคุกคาม					

ข้อคำถาม	ระดับความเหมาะสม				
	1	2	3	4	5
2. ความเหมาะสมด้านความถูกต้องของการออกแบบระบบ					
2.1 การใช้งานมีความง่ายในการเข้าถึงข้อมูล					
2.2 มีความรวดเร็วในการใช้บริการ					
2.3 มีความเหมาะสมในการจัดวางตำแหน่งของส่วนประกอบระบบ					
2.4 มีเทคนิคในการนำเสนอที่ทันสมัย					
3. ความเหมาะสมในการใช้งานของระบบ					
3.1 ระบบใช้งานง่าย ไม่ซับซ้อน					
3.2 ข้อมูลมีความถูกต้อง ครบถ้วนและสมบูรณ์					
3.3 ข้อมูลในระบบสามารถช่วยการตัดสินใจให้แก่ผู้ใช้					
3.4 ระบบมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลอย่างเหมาะสม					
4. ความเหมาะสมด้านการรักษาความมั่นคงปลอดภัย					
4.1 มีการตรวจสอบสิทธิ์การใช้งานในแต่ละระดับ					
4.2 มีการแบ่งแยกรายการของแต่ละระดับการเข้าถึง					
4.3 มีการรักษาความปลอดภัยข้อมูลในระบบฐานข้อมูล					
4.4 มีการตรวจหาและแจ้งเตือนภัยคุกคามอย่างทันท่วงที					
5. ความเหมาะสมด้านการติดต่อระหว่างระบบกับผู้ใช้					
5.1 การจัดหน้าจอ และตำแหน่งการจัดวางส่วนต่าง ๆ มีความเหมาะสม					
5.2 ความชัดเจนของรายการและข้อความบนหน้าจอ มีความเหมาะสม					
5.3 ภาษาที่ใช้ในส่วนต่าง ๆ มีความชัดเจน เข้าใจง่าย					
5.4 รูปแบบของตัวอักษร ขนาด สี พื้นหลัง และรูปภาพ มีความเหมาะสม					

ตอนที่ 3 ความคิดเห็นและข้อเสนอแนะ **:** กรุณาให้ข้อเสนอแนะเกี่ยวกับระบบที่ผู้วิจัยได้พัฒนาขึ้น

……

……

……

ผู้วิจัย ขอกราบขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการประมินระบบฯ

ภาคผนวก ค

แบบประเมินประสิทธิภาพการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุกและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ใช้งาน

แบบประเมินประสิทธิภาพการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุกและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ (ประเมินโดยผู้ใช้งาน)

<u>คำชี้แจง</u>

แบบสอบถามชุดนี้ มีวัตถุประสงค์เพื่อทำการประเมินประสิทธิภาพการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผู้วิจัยได้พัฒนาขึ้น ผู้วิจัยใคร่ขอความอนุเคราะห์จากท่านได้โปรดพิจารณาตอบแบบสอบถามอันเป็นผลมาจากการที่ท่านได้ใช้ระบบดังกล่าว ทั้งนี้ เพื่อจะได้ทราบถึงประสิทธิภาพของการใช้งานระบบ รวมทั้งข้อเสนอแนะในสิ่งที่ต้องปรับปรุงให้ดีและสมบูรณ์มากยิ่งขึ้นต่อไป

<u>แบบสอบถามแบ่งออกเป็น 3 ตอน คือ</u>

ตอนที่ 1 แบบสอบถามสถานภาพทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 แบบประเมินประสิทธิภาพการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์

ตอนที่ 3 แบบสอบถามความคิดเห็นและข้อเสนอแนะที่มีต่อประสิทธิภาพการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์

การแปลค่าความหมาย แบ่งเป็น 5 ระดับ ดังต่อไปนี้

5	หมายถึง	มีประสิทธิภาพมากที่สุด
4	หมายถึง	มีประสิทธิภาพมาก
3	หมายถึง	มีประสิทธิภาพปานกลาง
2	หมายถึง	มีประสิทธิภาพน้อย
1	หมายถึง	มีประสิทธิภาพน้อยที่สุด

ประสิทธิภาพ (Efficiency) หมายถึง กระบวนการดำเนินงานที่มีลักษณะดังนี้ (1) ประหยัด ได้แก่ การประหยัดต้นทุน การประหยัดทรัพยากร การประหยัดเวลา (2) เสร็จทันตามกำหนดเวลา (3) คุณภาพโดยพิจารณาจากปัจจัยนำเข้า กระบวนการ และผลผลิตที่ดี ซึ่งวัดจากระดับความพึงพอใจและระดับการยอมรับของผู้ใช้ระบบ

ผู้วิจัย ขอขอบพระคุณเป็นอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

ตอนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบสอบถาม

โปรดทำเครื่องหมาย ✓ ในช่อง ☐ ที่ตรงกับข้อมูลของท่าน เพียงช่องเดียว

6. เพศ

☐ ชาย ☐ หญิง

7. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 - 40 ปี

☐ 41 - 50 ปี ☐ มากกว่า 50 ปี

8. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี

☐ ปริญญาโท ☐ ปริญญาเอก

9. ตำแหน่งงาน

☐ ผู้บริหาร ☐ ผู้ดูแลระบบเครือข่าย

☐ เจ้าหน้าที่ปฏิบัติงาน ☐ ผู้เชี่ยวชาญ

10. ระยะเวลาที่ปฏิบัติงานในหน่วยงาน

☐ น้อยกว่า 10 ปี ☐ 11 - 15 ปี

☐ 16 - 20 ปี ☐ มากกว่า 20 ปี

ตอนที่ 2 ความคิดเห็นประสิทธิภาพการใช้งานระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก โปรดทำเครื่องหมาย ✓ ในช่องที่ตรงกับระดับความพร้อมในหน่วยงานของท่านมากที่สุด

ข้อคำถาม	ระดับประสิทธิภาพ				
	1	2	3	4	5
1.ด้านการออกแบบการใช้งาน					
1.1 การใช้งานระบบ มีความง่ายในการเข้าถึงข้อมูล					
1.2 มีความสะดวก รวดเร็วในการเรียกใช้งานในเมนูต่างๆ					
1.3 การวางตำแหน่งเมนูบนจอภาพ ทำให้สามารถเรียกใช้งานได้ง่าย					
1.4 มีความสะดวกในการสรุปและนำเสนอข้อมูล					

ข้อคำถาม	ระดับประสิทธิภาพ				
	1	2	3	4	5
2. ด้านการบันทึกและการแก้ไขข้อมูล					
2.1 แบบฟอร์มบันทึกและแก้ไขข้อมูลมีความเหมาะสม ใช้งานง่าย					
2.2 แบบฟอร์มสำหรับบันทึกข้อมูลมีความเหมาะสม ครบถ้วน					
2.3 การแก้ไขข้อมูล ทำได้สะดวก รวดเร็ว ใช้งานง่าย และถูกต้อง					
3. ด้านการประมวลผลและการแสดงผล					
3.1 หน้าจอการสืบค้นและรายงานมีความเหมาะสม					
3.2 สืบค้นข้อมูลได้สะดวก และใช้งานได้ง่าย					
3.3 การสืบค้นข้อมูลมีความถูกต้อง					
3.4 ตัวอักษร ขนาด สี ในการแสดงผลข้อมูล มีความเหมาะสม					
3.5 การรายงานสามารถทำได้ง่าย สะดวก และถูกต้อง					
4. ด้านการสืบค้นข้อมูล และการรายงาน					
4.1 การสืบค้น และการรายงานผล สะดวก ใช้งานง่าย					
4.2 การประมวลผลแต่ละขั้นตอนมีความรวดเร็ว					
4.3 ข้อมูลที่ได้ มีความแม่นยำ					
5. ด้านประสิทธิภาพการใช้งานของระบบ					
5.1 สามารถตอบสนองวามต้องการของผู้ใช้ได้รวดเร็ว					
5.2 สามารถช่วยลดระยะเวลาในการประมวลผล					
5.3 มีการตรวจสอบสิทธิ์การใช้งานในระดับต่างๆ					
5.4 มีการเชื่อมโยงข้อมูลในแต่ละส่วนมาแสดงผลได้อย่างรวดเร็ว					

ผู้วิจัย ขอขอบพระคุณเป็นอย่างสูงในความร่วมมือ ข้อมูลจากท่านมีคุณค่าอย่างยิ่งต่อการพัฒนางานวิจัยในครั้งนี้ หากท่านมีข้อสงสัยประการใด กรุณาติดต่อผู้วิจัยโดยตรงที่หมายเลขโทรศัพท์ 080-934-9887 หรือ e-mail : keaittisuk@gmail.com

ภาคผนวก ง
ผลงานตีพิมพ์

[1] เกียรติศักดิ์ ลุยทอง, เอกฉัตร บ่ายคล้อย และ ประสงค์ ปราณีตพลกรัง, “**การตรวจสอบความพร้อมและพัฒนาตัวแบบการประเมินความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ไซเบอร์กองทัพบก,”** การประชุมวิชาการระดับชาติมหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี ประจำปี 2561 เรื่อง ผลงานวิจัยและนวัตกรรมเพื่อส่งเสริมความก้าวหน้าอุตสาหกรรม 4.0, 12 กรกฎาคม 2561 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

บทคัดย่อ

งานวิจัยนี้ มีวัตถุประสงค์เพื่อศึกษาความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์สำหรับบุคลากรในศูนย์ไซเบอร์กองทัพบกและเพื่อพัฒนาตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในศูนย์ไซเบอร์กองทัพบก ลักษณะของการวิจัยเป็นการวิจัยเชิงปริมาณ โดยใช้แบบสอบถามกับกลุ่มตัวอย่างคือ บุคลากรภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน และสถิติที่ใช้ในการวิเคราะห์ข้อมูลคือ ร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน

ผลการวิจัยพบว่า ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในศูนย์ไซเบอร์กองทัพบกมีค่าอยู่ในระดับพร้อมมาก และตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในศูนย์ไซเบอร์กองทัพบก มีความเหมาะสมอยู่ในระดับมากที่สุด

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์, ความเสี่ยง

[2] เกียรติศักดิ์ ลุยทอง, เอกฉัตร บ่ายคล้อย และ ประสงค์ ปราณีตพลกรัง, “**การพัฒนาระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และ แจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก**,” วารสารมหาวิทยาลัยศิลปากร ฉบับวิทยาศาสตร์และเทคโนโลยี ปีที่ 11 ฉบับที่ 4 ก.ค.ถึง ส.ค. 61, Veridian E-Journal, Science and Technology Silpakorn University ISSN 2408 – 1248

บทคัดย่อ

การศึกษาวิจัยนี้ เพื่อเป็นการพัฒนาวิธีการเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ ของศูนย์ไซเบอร์กองทัพบก โดยใช้เครื่องมือในการพัฒนาระบบได้แก่ ภาษา PHP สำหรับการพัฒนาแอปพลิเคชัน และโปรแกรม MySQL สำหรับจัดการฐานข้อมูล กลุ่มตัวอย่างที่ใช้ ในการดำเนินการวิจัย มีจำนวน 2 กลุ่ม คือ กลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 ท่าน และกลุ่มผู้ใช้งานระบบ ซึ่งเป็นบุคลากรภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน สรุปผลการประเมินด้านเหมาะสมของระบบ โดยกลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์ อยู่ในระดับเหมาะสมมากที่สุด ($\overline{X}$=4.51, S.D.=0.54) และการประเมินด้านการประสิทธิภาพการใช้งานระบบ โดยกลุ่มผู้ใช้งาน ซึ่งอยู่ในระดับมีประสิทธิภาพมาก ($\overline{X}$=4.18, S.D.=0.78) แสดงให้เห็นว่าระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสม และสามารถตอบสนองการทำงานผู้ใช้งานได้ในทุกระดับการตรวจสอบและการรายงานผลสถิติภัยคุกคามทางไซเบอร์เป็นไปอย่างรวดเร็ว ลดขั้นตอนการตรวจสอบภัยคุกคามของเจ้าหน้าที่และลดปริมาณการใช้กระดาษ รวมถึงเป็นการรักษาความลับของทางราชการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้อย่างมีประสิทธิภาพ

คำสำคัญ : เฝ้าระวัง, การแจ้งเตือน, ความมั่นคงปลอดภัยไซเบอร์

ประวัติผู้วิจัย

ชื่อ-นามสกุล จ่าสิบเอก เกียรติศักดิ์ ลุยทอง

วัน เดือน ปี เกิด 28 ตุลาคม 2517

สถานที่เกิด จังหวัดชัยนาท

วุฒิการศึกษา พ.ศ. 2559 บริหารธุรกิจบัณฑิต สาขาวิชาคอมพิวเตอร์ธุรกิจ สถาบันรัชต์ภาคย์

สถานที่ทำงานในปัจจุบัน ศูนย์ไซเบอร์กองทัพบก

ประสบการณ์การทำงาน รับราชการ ณ ศูนย์การทหารม้า สระบุรี ตำแหน่ง ผู้ช่วยครู แผนกวิชาการขี่ม้า กองการศึกษา โรงเรียนทหารม้า ศูนย์การทหารม้า พ.ศ.2541 - 2549

รับราชการ ณ กรมจเรทหารบก ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล พ.ศ.2549 - 2560

รับราชการ ณ ศูนย์ไซเบอร์กองทัพบก ตำแหน่ง เจ้าหน้าที่วิเคราะห์ข้อมูล พ.ศ. 2560 - ปัจจุบัน

ผลงานทางวิชาการที่ได้รับการตีพิมพ์

[1] เกียรติศักดิ์ ลุยทอง, เอกฉัตร บ่ายคล้อย และ ประสงค์ ปราณีตพลกรัง, "**การตรวจสอบความพร้อมและพัฒนาตัวแบบการประเมินความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ ไซเบอร์กองทัพบก,"** การประชุมวิชาการระดับชาติมหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี ประจำปี 2561 เรื่อง ผลงานวิจัยและนวัตกรรมเพื่อส่งเสริมความก้าวหน้าอุตสาหกรรม 4.0, 12 กรกฎาคม 2561 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

[2] เกียรติศักดิ์ ลุยทอง, เอกฉัตร บ่ายคล้อย และ ประสงค์ ปราณีตพลกรัง, "**การพัฒนาระบบเฝ้าระวังภัยคุกคาม ตรวจหาการบุกรุก และ แจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก**," วารสารมหาวิทยาลัยศิลปากร ฉบับวิทยาศาสตร์และเทคโนโลยี ปีที่ 11 ฉบับที่ 4 ก.ค. ถึง ส.ค. 61, Veridian E-Journal, Science and Technology Silpakorn University ISSN 2408 - 1248